

The Legislation of the Notary System and Electronic Data Evidence in Different Countries*

Cao Zhaoxun^{1*}, Ramalinggam Rajamanickam², Nur Khalidah Dahlan³, Min Bingyuan⁴, Rajini Kumar Sreedharam⁵

¹ Vocational University of Art, China

² Universiti Kebangsaan Malaysia (UKM), Malaysia

³ Universiti Kebangsaan Malaysia (UKM), Malaysia

⁴ Jingdezhen Vocational University of Art, China

⁵ Universiti Tunku Abdul Rahman, Malaysia



[10.15408/jch.v13i3.46860](https://doi.org/10.15408/jch.v13i3.46860)

Abstract

As digital applications continue to expand across various fields, the importance of reliable electronic data evidence and an efficient notary system has become even more prominent. The improper handling of electronic data not only affects the fairness of judicial proceedings but also poses threats to the legitimate rights and interests of individuals and organizations. This paper analyzes the characteristics of notarial system in different countries through comparative research method, elaborates in detail the situation of EU and China in electronic data evidence legislation, and carries out a comparative analysis of the similarities and differences between the Chinese and European legislation. It is found that the notarization system of civil law countries is characterized by strong state intervention, high authority of notarial acts, and wide scope of application; while the notarization system of common law countries is relatively flexible, with simple procedures but limited authority. EU legislation on electronic data evidence is centered on the General Data Protection Regulation (GDPR), which is detailed and has strong extraterritorial effect in protecting personal data rights. China has actively constructed a legal framework for electronic data evidence, focusing on combining it with national development strategies and reflecting Chinese characteristics while safeguarding data security and privacy. Based on this, the article puts forward suggestions in terms of technological upgrading, legislative optimization, professional development of personnel and international cooperation, with the aim of promoting the development of the notary system in the era of electronic data, and facilitating the effective use and protection of electronic data evidence.

Keywords: Notarial System; Electronic Data Evidence; Legislative Comparison; Challenges; Digital Age.

* Received: June 18, 2025, revised: July 12, 2025, accepted: July 29, 2025, published: December 30, 2025.

¹ **Cao Zhaoxun.** Faculty of Economics and Law, Jingdezhen Vocational University of Art, China, Corresponding Author; Email: caozhaoxun@163.com, ORCID: <https://orcid.org/0009-0007-4665-5992>

² **Ramalinggam Rajamanickam.** Faculty of Law, Universiti Kebangsaan Malaysia (UKM), Malaysia, Email: rama@ukm.edu.my, ORCID: <https://orcid.org/0000-0003-4017-8826>

³ **Nur Khalidah Dahlan.** Faculty of Law, Universiti Kebangsaan Malaysia (UKM), Malaysia, Email: nurkhalidahdahlan@ukm.edu.my, ORCID: <https://orcid.org/0000-0001-5358-3797>

⁴ **Min Bingyuan.** Faculty of Economics and Law, Jingdezhen Vocational University of Art, China, Email: minbingyuan@163.com, ORCID: <https://orcid.org/0009-0002-2216-3145>

⁵ **Rajini Kumar Sreedharam.** Faculty of Creative Industries, Universiti Tunku Abdul Rahman, Malaysia Email: rajini@utar.edu.my, ORCID: <https://orcid.org/0000-0001-9347-4229>

**Corresponding Author: caozhaoxun@163.com

A. INTRODUCTION

In the contemporary digital landscape, the proliferation of electronic data has been nothing short of revolutionary (Dinter, B., & Krämer, J., 2018). The exponential growth of information technology has led to the generation of vast amounts of electronic data in every conceivable domain of social and economic life (Dakhaeva, F., & Datsaeva, R., 2021). From the minutiae of daily online transactions to the complex data flows within multinational corporations and the extensive information networks of governments, electronic data has become the lifeblood of modern society.

This digital transformation has had a profound impact on the legal and notarial arenas. The traditional notarial system, which has long served as a cornerstone for ensuring the legality and authenticity of transactions and documents, now finds itself at a critical juncture (BABKIN, I. S., 2024). In the past, notaries primarily dealt with paper-based documents, relying on established procedures and physical signatures to confer legal validity. However, the advent of electronic data has disrupted this paradigm. Moreover, the sheer volume and complexity of electronic data present formidable challenges to the notarial process (Cao Zhaoxun, Ramalinggam Rajamanickam, & Nur Khalidah Dahlan., 2024). The diversity of data formats, sources, and purposes makes it arduous for notaries to sift through, extract, analyze, and store the relevant information (Sitdikova, L. B., & Galkin, N. A., 2024). This has led to concerns regarding the efficiency and effectiveness of notarizing electronic data evidence, as well as doubts about its legal admissibility and probative value.

In the realm of business, the globalization of economic activities has further compounded these issues. Cross-border transactions and international cooperation have become the norm, but the differences in legal systems, business practices, and technological infrastructures across countries have created a complex web of challenges (Nainggolan, B., Susanto, H., Yuniartin, H., & Suwarno, S., 2023). Ensuring the legal recognition and enforceability of electronic data evidence in such a diverse and interconnected environment is of paramount importance (Amalia, A. N., & Anggayasti, U. H., 2024). It is essential for facilitating seamless international trade, protecting the rights and interests of parties involved in transnational investments, and resolving disputes that inevitably arise in the course of global business operations.

It needs to be clear that notarization service plays a key role in data protection. Notarization service can prove the authenticity and legality of electronic data. Through rigorous notarization procedures, it can ensure that data conforms to legal norms in all aspects such as generation, storage and

transmission, and prevent data from being tampered with or forged, thus ensuring the security and reliability of data and safeguarding the legitimate rights and interests of data subjects. When choosing countries/regions to study, this study chooses the European Union and China because the European Union is in the leading position in the legislation of electronic data evidence, and its related laws and regulations have had a far-reaching impact on global data governance. As an important force in the development of global digital economy, China has its own characteristics in the legislation of electronic data evidence, and is actively in line with international standards. A study and comparison of the two can provide valuable reference for notarization services and electronic data evidence legislation worldwide.

B. METHODS

Comparative research has been systematically carried out to comprehensively analyze the similarities and differences in the notary system and electronic data evidence legislation across different countries and regions. Beginning with the classification of legal systems, a detailed comparison has been made between civil law countries and common law countries. When it comes to the EU and China, further in-depth comparisons have been conducted. The EU has formulated a series of comprehensive and detailed regulations and policies related to electronic data evidence, with the GDPR being a prime example. In contrast, China's legislation takes into full account national development strategies and focuses on promoting the healthy development of the digital economy. This comparative research not only helps to clarify the unique features of different legal systems and regions but also provides valuable references for promoting the improvement and innovation of the notary system and electronic data evidence legislation.

Here, China belongs to the civil law countries. China's legal system is systematic and logical, and it is consistent with the characteristics of civil law system to regulate social behavior by formulating written codes. Comparing the EU and China in the study will help to analyze the differences and commonalities between notarization services and electronic data evidence legislation from the perspective of different legal systems, thus providing a richer dimension for the study.

C. RESULTS AND DISCUSSION

1. The Characteristics of the Notary System in Different Countries

In civil law countries, exemplified by France and Germany, the notary system is marked by strong state intervention. The appointment of notaries is a highly regulated process. Prospective notaries are required to undergo rigorous training in law, often obtaining relevant degrees and then passing a comprehensive notary qualification examination. This examination encompasses a wide range of legal knowledge, including legal theory, practical notarial procedures, and professional ethics. Through this state-controlled appointment mechanism, notaries are bestowed with the authority to act on behalf of the state in performing notarial functions. This elevates their status and credibility significantly (Ilyushina, M. N., 2024).

Notarial acts in civil law countries are highly legal and authoritative. The entire notarization process, from the acceptance of notarial matters to the issuance of notarial documents, is strictly regulated by law. Each step must comply with the established procedures and requirements. This legalistic approach ensures the uniformity and standardization of notarial acts, making the results highly predictable and reliable. The probative value of notarized documents is substantial. In many cases, they can be directly used as the basis for determining facts in legal proceedings, unless there is compelling contrary evidence (Mikhaylova, E. v., 2023).

The notarization system in civil law countries has a wide application range. It covers almost all significant aspects of social and economic life. In real estate, notaries are responsible for verifying the authenticity of property rights, the legality of transaction contracts, and the compliance of the transaction process. In inheritance matters, they play a crucial role in notarizing wills, inventorying and distributing inheritances, thus protecting the legitimate rights and interests of heirs and preventing inheritance disputes. In corporate affairs, notaries are involved in notarizing important matters such as the formulation of articles of association, company establishment, share transfers, mergers, and separations. This provides legal protection for the proper operation of companies and market transactions.

In contrast, the notary system in common law countries like the United Kingdom and the United States is characterized by relative flexibility. The main duty of notaries in these countries is to attest to the authenticity of the signing of documents. Their focus is primarily on verifying the identity of the signatories, ensuring the voluntariness of the signing act, and confirming that the signing

process complies with the legal form requirements (Junyu, M.-., 2020). In the notarization of a business contract or power of attorney, for example, the notary mainly checks the identity information of the signatory to ensure that they are signing of their own free will, are sober, and are not under any fraudulent or coercive influence. The notary then attests to the signing act with a seal or a statement, thereby proving the authenticity of the document. However, they generally do not conduct in-depth examinations of the content of the document or the underlying legal relationships, unless there are obvious doubts or specific legal requirements.

The notarization procedures in common law countries are relatively simple. The aim is to enhance the efficiency and accessibility of notarization services to meet the fast pace of social and economic activities. Compared to the more complex and strict procedures in civil law countries, the acceptance process of notarization applications in common law countries is quicker, and the requirements for notarization materials are less stringent. This enables notaries to complete the notarization act in a relatively short time. Such simplicity makes notarial services more convenient for the parties involved, especially in routine commercial and personal affairs such as document authentication and the notarization of simple contracts.

In common law countries, the authority of notaries is relatively restricted. Their power mainly lies in attesting to the authenticity of signed documents. When it comes to major legal issues such as decision-making powers regarding legal interpretations and substantive reviews of notarial matters, notaries generally do not have such authorities. In legal disputes or cases requiring in-depth legal analysis, notaries in common law countries do not play a leading role like their counterparts in civil law countries. Instead, they rely on the participation and judgment of other legal professionals such as lawyers and judges. This authority setting reflects the more auxiliary role of the notary system in the common law system, where it cooperates with other legal systems to maintain social legal order.

In judicial practice in common law countries, notarial instruments need to be comprehensively judged in conjunction with other evidence. Since the notarial act mainly focuses on the surface authenticity of the document signing, the notarized document does not have the same absolute and independent probative value as in civil law countries. In court proceedings, judges consider the notarial document along with other types of evidence such as witness testimony, documentary evidence, and physical evidence. They weigh the credibility, relevance, and legality of each piece of evidence according to specific criteria and

then form a judgment on the facts of the case. This approach reflects the judicial philosophy in common law countries that emphasizes the comprehensive consideration of evidence and the restoration of the complete facts of the case.

Table 1. Summary Comparison between Civil Law and Common Law Countries

Comparison Items	Notary System in Civil Law Countries	Notary System in Common Law Countries
Degree of State Intervention	High. The appointment of notaries is highly regulated. Prospective notaries must undergo rigorous legal training, obtain relevant degrees, and pass comprehensive qualification exams. They are empowered by the state to perform notarial functions.	Relatively low. The regulation of notaries' qualifications and other aspects is less strict compared to civil law countries.
Characteristics of Notarial Acts	Highly legal and authoritative. The entire notarization process is strictly regulated by law, ensuring the uniformity and standardization of notarial acts. Notarized documents have high probative value and can often be directly used as the basis for determining facts in legal proceedings.	Mainly focus on attesting to the authenticity of document signings. The examination of document content and underlying legal relationships is relatively shallow (except in special cases), and notarial acts are relatively flexible.
Notarization Procedures	Complex and strict. Each step from accepting notarial matters to issuing notarial documents has clear legal procedures and requirements.	Relatively simple. The acceptance process of notarization applications is faster, and the requirements for notarization materials are less stringent. Notarization can be completed in a relatively short time to adapt to the fast-paced social and economic activities.
Powers of Notaries	Extensive. Notaries can act on behalf of the state in performing notarial functions. They play important roles in many fields such as real estate, inheritance, and corporate affairs, involving property rights verification, contract legality review, and more.	Relatively restricted. Their main power is to attest to the authenticity of signed documents. They have limited powers in major legal decision-making, legal interpretation, and substantive reviews of notarial matters.
Probative Value of Notarized Documents	In legal procedures, notarized documents usually have high probative value. Unless there is strong contrary evidence, they can be directly used as the basis for determining facts.	The probative value of notarized documents is not absolutely independent. They need to be judged comprehensively together with other evidence. Judges will weigh the credibility, relevance, and legality of various types of evidence before making a judgment on the facts of the case.
Scope of Application	Wide, covering almost all important aspects of social and economic life, such as important links in real-estate transactions, inheritance matters, and corporate establishment and operation.	Conveniently applied in daily commercial and personal affairs such as document authentication and simple contract notarization, but the overall depth and breadth of application are not as extensive as in civil law countries.

2. The EU Legislation on Electronic Data Evidence

The EU has been at the forefront of electronic data evidence legislation, enacting a series of regulations and policies that have had a significant impact on data governance both within the EU and globally (Casolari, F., Buttaboni, C., & Floridi, L., 2023).

The GDPR is the cornerstone of the EU's data protection framework. It imposes extremely stringent and detailed requirements on personal data protection. For data subjects, it endows EU citizens with a comprehensive set of rights. The right to be informed ensures that individuals have the right to know the purpose, methods, and controllers of their data collection and processing. This empowers them to make informed decisions about their personal data (Ke, T. T., & Sudhir, K., 2023). The right of access allows data subjects to access their data at any time and understand how it is being used. In case of inaccuracies or incompleteness, the right of rectification enables them to request corrections. The right to erasure, also known as the right to be forgotten, gives them the power to have their data deleted under specific circumstances, such as when the data is no longer necessary or the legal basis for retention has expired. The right to restriction of processing allows data subjects to limit the processing of their data in certain situations. Additionally, the right to data portability enables them to obtain and transfer their data to another controller.

For data processors, the GDPR mandates a series of strict obligations. They are required to conduct a data protection impact assessment prior to any data processing activity. This assessment helps identify and mitigate potential risks to personal data. In the event of a data breach, data processors must notify the data subject and the supervisory authority promptly within a specified timeframe. This ensures that affected individuals can take appropriate measures to protect their rights and that the authorities can intervene quickly to investigate. Moreover, data processors are obligated to implement appropriate technical and organizational measures to safeguard data security. This includes measures to prevent illegal access, tampering, and leakage of data (Amaral, O., Abualhaija, S., Sabetzadeh, M., & Briand, L., 2021).

Regarding cross-border data transfers, the GDPR sets strict conditions and mechanisms. To ensure the protection of EU citizens' personal data during cross-border flows, such transfers must meet specific legal bases. These include explicit consent from the data subject, necessity for contract performance, or the public interest. For transfers to third countries, the EU requires that these countries have an equivalent level of data protection or that appropriate safeguards are in place.

Such safeguards can include the conclusion of standard contractual clauses or the application of binding corporate rules.

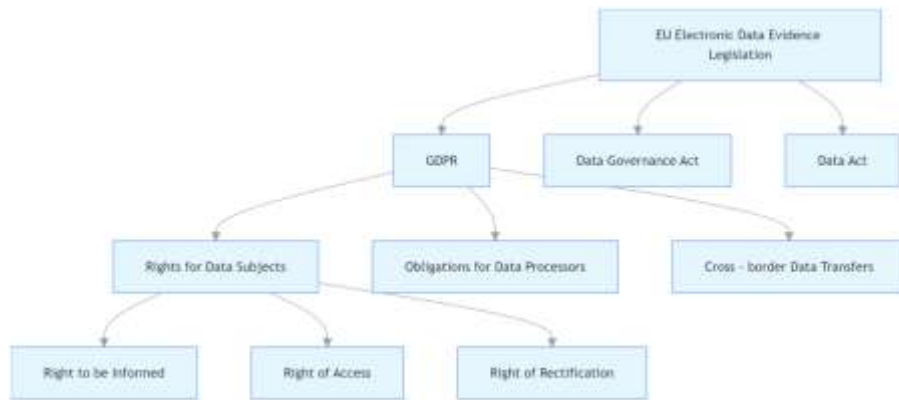
In addition to the GDPR, the EU's Data Governance Act and Data Act focus on different aspects of data management. The Data Governance Act aims to break down data silos within the EU. It promotes the circulation and sharing of data, especially the reuse of public sector data. By encouraging public bodies to open up their data in a lawful, fair, and transparent manner, it stimulates innovation in data utilization (Pathak, M., 2024). At the same time, it establishes a data governance mechanism to ensure the fairness, legality, and security of the data sharing process. The Data Act, on the other hand, concentrates on regulating the use and access to data, particularly non-personal data. It clarifies the rights and obligations of data holders and users, promoting the rational use of data and safeguarding the healthy development of the data economy. It also takes measures to prevent data monopolization and unfair competition and ensures the protection of data security and personal privacy during data utilization.

The EU's electronic data evidence legislation is characterized by its pursuit of a delicate balance between data protection and economic development. It places a high emphasis on the rights of personal data subjects, elevating data protection to the level of a fundamental human right. This reflects the EU's deep understanding of the value of personal data and the potential risks in the digital age. By granting citizens extensive control over their data, it enhances their autonomy and sense of security.

Through harmonized legislation, the EU has effectively integrated and regulated the data market within its member states. The elimination of differences in data protection and governance regulations has facilitated the free flow of data within the EU. This provides a uniform market environment for the development of the digital economy, attracting more enterprises to engage in data-related businesses in the EU. It also promotes innovation in the EU's digital industry and strengthens the EU's position in the global digital economy competition.

Globally, the EU's legislation has played a leading and exemplary role. Many countries have looked to the EU's experience when formulating their own data protection and governance regulations. It has spurred increased attention to data protection issues worldwide and has promoted international exchanges and cooperation in data governance. The EU's regulations have also influenced the development of international standards for data protection and cross-border data transfer, contributing to the construction of a more comprehensive and rational global data governance system (Ryngaert, C., & Taylor, M., 2020).

Figure 1. EU Legislation on Electronic Data Evidence



3. The Status of China's Electronic Data Evidence Legislation

China has been actively engaged in formulating and improving legislation related to electronic data evidence in line with the rapid development of the digital era. A series of important laws and regulations have been promulgated, which together have constructed a relatively comprehensive legal framework for the protection and utilization of electronic data.

The Cybersecurity Law of the People's Republic of China serves as a fundamental law in the field of cybersecurity. It places a strong emphasis on safeguarding cyberinformation security. The law clearly stipulates the security protection obligations of network operators during the collection, storage, transmission, and use of network information (Langford, L., 2020). Network operators are required to take necessary measures to ensure the integrity, confidentiality, and availability of network information. For example, they must establish and improve user information protection systems to strengthen the protection of users' personal information and prevent information leakage, tampering, and destruction. At the same time, the law defines various behaviors that endanger network security, such as cyberattacks and network intrusions, and prescribes corresponding legal responsibilities. This provides a solid legal basis for combating cybercrime and maintaining network order, thereby laying a foundation for the secure operation of electronic data in the network environment.

The E-Commerce Law of the People's Republic of China focuses on the e-commerce field and pays particular attention to the protection of consumer

information. In e-commerce transactions, a large amount of consumer personal information, including name, contact information, address, shopping preferences, etc., is collected and used. To address this, the law imposes strict requirements on e-commerce operators regarding the collection and use of consumer information. E-commerce operators must clearly state the purpose, manner, and scope of information collection and use and obtain the consent of consumers. They are prohibited from collecting or using consumer information in violation of the agreement or the law. In addition, the law also clarifies the responsibilities and obligations of e-commerce platform operators (Liu, F., 2024). They are required to supervise the information protection behaviors of operators within the platform and safeguard the legitimate rights and interests of consumers in e-commerce activities. This helps to ensure the legality and security of electronic data related to e-commerce transactions.

The Law of the People's Republic of China on Data Security and the Law of the People's Republic of China on the Protection of Personal Information further penetrate into the core aspects of data processing activities. The Data Security Law establishes a data classification and protection system. It classifies data into different levels based on their importance in economic and social development and the potential harm that tampering, destruction, or leakage of data may cause to national security, public interests, or the legitimate rights and interests of individuals and organizations. Corresponding protection measures and security management requirements are then stipulated for each level. In data processing activities, the law also emphasizes the data security protection obligations of data processors, including risk monitoring and disposal and data exit security management. Data processors are required to establish and improve a full-process data security management system, strengthen data security risk monitoring and assessment, and take necessary measures to safeguard data security.

The Law on the Protection of Personal Information provides detailed and comprehensive provisions for the protection of personal information. It clearly defines the scope and definition of personal information and endows data subjects with a wide range of rights, such as the right to know, the right to make decisions, the right to inquire, the right to make corrections, the right to erasure, the right to portability, etc. These rights enable individuals to have greater control over their personal information. At the same time, the law strictly regulates the obligations of personal information processors. They are required to handle personal information in accordance with the principles of lawfulness, legitimacy, necessity, and good faith (Zhu, M., 2024). Necessary measures must be taken to ensure the safety of personal information, and a personal information

protection impact assessment must be conducted before handling personal information. In addition, the law also regulates the rules for the cross-border provision of personal information, specifying the conditions and procedures for such provision and ensuring the safety of personal information during cross-border flow.

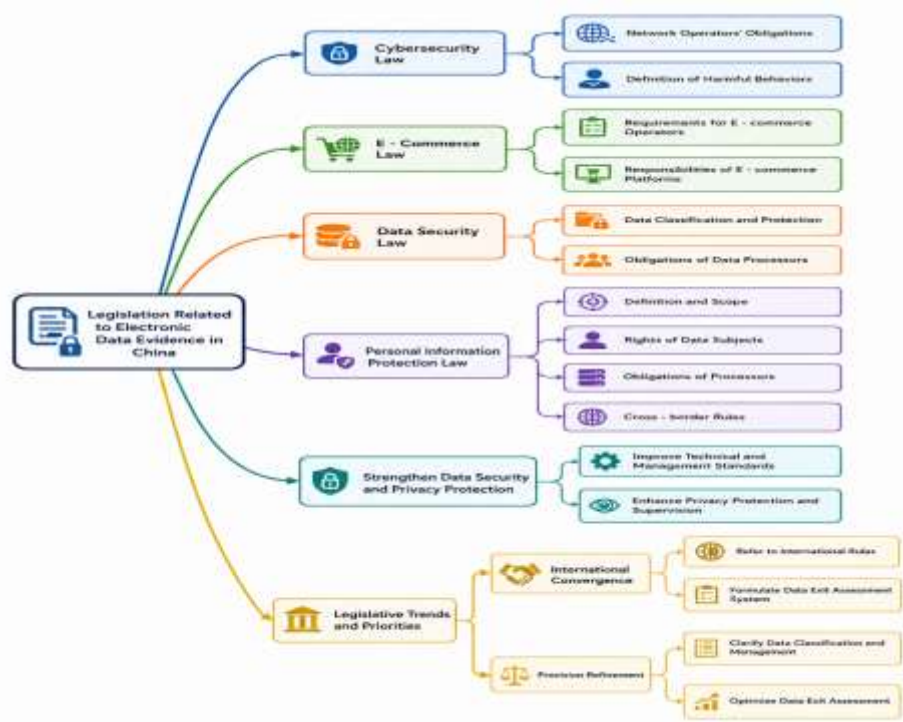
In the development process of China's electronic data evidence legislation, several trends and priorities have emerged. Firstly, in terms of strengthening data security and personal privacy protection, continuous efforts have been made. On the one hand, technical standards and management requirements for data security protection have been continuously improved. Enterprises are encouraged to adopt advanced encryption technologies, data backup and recovery technologies, etc., to enhance data security. On the other hand, the protection of personal privacy has been strengthened, and the crackdown on infringement of personal privacy has been intensified. By clarifying the scope and protection standards of personal privacy and strengthening the supervision of all aspects of personal information collection, use, storage, and transmission, the illegal infringement of personal privacy is effectively prevented. At the same time, publicity and education on the protection of personal information have been enhanced to improve citizens' awareness and ability to protect personal information.

Secondly, China's legislation focuses on international convergence. In the context of globalization and the increasing frequency of cross-border data flow, China has fully considered internationally accepted rules and standards in the legislative process. By drawing on advanced international experience, China's legislation on electronic data evidence can better adapt to the general trend of international data governance. For example, in the rules for cross-border data transmission, China has referred to the relevant provisions of the EU and other countries and regions and combined them with its own actual situation to formulate systems such as the security assessment of data exit. This ensures that the process of cross-border flow of data is safe and controllable. At the same time, China has actively expressed its stance on the international stage, striving to promote the establishment of a fair and rational international data governance system, safeguard national data sovereignty and security, and promote the healthy development of the global digital economy.

Finally, in accordance with national conditions and actual needs, China has gradually refined the relevant provisions on electronic data evidence. In the area of data classification and hierarchical management, specific classification standards and corresponding protection measures for different levels of data

have been further clarified. This guides enterprises and relevant organizations to carry out classification and management according to the importance and sensitivity of data, improving the pertinence and effectiveness of data management. In the area of data exit security assessment, the assessment process and standards have been continuously optimized, and the supervision of data exit activities has been strengthened to ensure that data exit meets the requirements of national security, public interests, and the legitimate rights and interests of individuals. In addition, China is also exploring the establishment of legislation on data trading rules and the regulation of the data element market to meet the demand for the market-oriented allocation of data elements brought about by the development of the digital economy, promote the reasonable circulation and effective utilization of data, and promote the innovative development of the digital economy (Creemers, R., 2021). Overall, China's legislation on electronic data evidence is constantly evolving and improving based on the actual situation of the country, providing a solid legal guarantee for the protection and utilization of data in the digital age.

Fig 2. Lists of Legislation in China on Electronic Data Evidence



4. The Comparative Analysis of Similarities and Differences between China and Europe

In the context of the digital era, both China and Europe have recognized the crucial significance of electronic data evidence in social and economic life. With the rapid development of information technology, electronic data has permeated various fields, becoming an essential element in promoting economic growth, social progress, and scientific and technological innovation. Whether in e-commerce transactions, e-government operations, or corporate data management, electronic data evidence plays an indispensable role.

Both regions emphasize data security and personal privacy protection in their legislation. In the EU, the GDPR is a prime example of strict data protection legislation. It endows data subjects with a comprehensive set of rights, such as the right to be informed, the right of access, the right of rectification, the right to erasure, the right to restriction of processing, and the right to data portability. This reflects the EU's high regard for individual privacy and the elevation of data protection to the level of a fundamental human right. In China, laws such as the Cybersecurity Law, the Law on the Protection of Personal Information, and the Law of the People's Republic of China on Data Security also place great emphasis on safeguarding data security and personal privacy. These laws stipulate the security protection obligations of network operators and data processors, and clarify the rights of data subjects. The common focus on data security and privacy protection in both China and Europe is aimed at maintaining social stability, promoting economic development, and safeguarding citizens' fundamental rights.

Both China and Europe are committed to regulating data processing activities through a series of comprehensive and detailed laws and regulations. These regulations cover all aspects of data collection, storage, transmission, use, sharing, and destruction. For instance, in the data collection process, both require data collectors to clearly inform data subjects of the purpose, manner, and scope of collection and obtain their explicit consent. During data storage and transmission, corresponding security measures such as data encryption and access control are mandated to ensure the confidentiality and integrity of data. By strictly regulating data processing activities, both regions strive to ensure the legality, fairness, and transparency of these processes (Weber, P. A., Zhang, N., & Wu, H., 2020).

The core objective of the legislation in both China and Europe is to effectively protect the legitimate rights and interests of data subjects and related parties. Data subjects, as the owners of data, are given a series of rights to enable

them to have a certain degree of control over their data. When their rights are infringed upon, they can defend themselves in accordance with the law. At the same time, data processors and other related parties are clearly defined with their obligations and responsibilities in data processing activities. This ensures that they operate within the legal framework and avoid causing damage to the rights and interests of data subjects and other related parties. Through such legislative efforts, both China and Europe aim to build a fair, orderly, and secure data ecosystem to meet the needs of the digital era and promote the healthy and sustainable development of the digital economy.

However, there are also notable differences between the two. The EU legislation on electronic data evidence, especially the GDPR, focuses intensively on the protection of personal data rights and places the control of data subjects at the core. It provides extremely detailed provisions for the rights of data subjects in the process of personal data processing. Data subjects have extensive powers, such as the ability to withdraw consent at any time and request data processors to delete or rectify data. This legislative tendency showcases the EU's strong emphasis on individual privacy and basic human rights in the digital age, aiming to ensure that individuals are always in a dominant position in data processing activities and can effectively protect their privacy and data rights.

The EU's regulatory system is relatively unified and has a strong extraterritorial effect. Through a series of coordinated regulations and policies such as the GDPR, the Data Governance Act, and the Data Act, the EU has established a relatively complete and coherent data protection framework. These regulations are uniformly applicable among member states, eliminating differences and conflicts in data protection within the EU. This promotes the integrated development of the data market within the EU. Moreover, the extraterritorial effect of the EU regulations means that they are binding on data processors outside the EU when processing the personal data of EU citizens. As long as there is a connection with the EU, these data processing activities must comply with EU data protection regulations. This reflects the EU's proactive stance in global data governance, attempting to extend its data protection standards globally and have a significant impact on international data flows and processing activities.

In contrast, China's legislation on electronic data evidence, while also emphasizing data security and privacy protection, pays more attention to close integration with national development strategies. China is an important force in the development of the global digital economy and actively encourages and supports digital technology innovation, digital industry development, and

digital infrastructure construction. In the legislative process, China fully considers the needs of the development of the digital economy and provides a favorable legal environment for its innovative development. For example, in the rational utilization of data and the cultivation of the data element market, a series of encouraging measures have been introduced to promote the circulation and value mining of data, promote the deep integration of the digital economy with the real economy, and achieve high-quality economic development.

China also takes into full account its own national conditions and actual situation in the design of specific systems, showing distinctive Chinese characteristics. In the protection of critical information infrastructures (CIIs), China's legislation clearly defines the scope and importance of CIIs and stipulates the special obligations and responsibilities of operators in terms of security protection. Given the crucial role of CIIs in national economic security, national defense security, and social stability, China has strengthened its protection efforts to ensure the safe and stable operation of these important systems and facilities (Liu, J., 2020). Additionally, China has implemented a certain degree of data localization requirement. For certain specific types of data, it must be stored on servers within the territory. This requirement is mainly based on considerations of national security, public interest, and law enforcement convenience. It helps to strengthen the regulation and control of data, guard against security risks arising from cross-border flow of data, and ensure that data security is coordinated with national sovereignty and social public interest.

Fig 3. Legislation in EU and china on Electronic Data Evidence



5. Technological Upgrade and Adaptation

Leverage Advanced Digital Technologies. The notarial system should fully embrace and integrate digital signature, blockchain, and encryption technologies. Digital signatures can authenticate the identity of signatories and

ensure the integrity of electronic documents. For example, in e-contract notarization, a digital signature can be used to verify that the parties involved have indeed signed the contract and that the content has remained unaltered. Blockchain technology, with its distributed ledger and immutability features, can be employed to record the entire process of electronic data generation, storage, and transfer. This provides an unforgeable chain of evidence, especially useful in cases where the origin and history of the data are crucial. Encryption techniques should be used to safeguard the confidentiality of electronic data during storage and transmission, protecting it from unauthorized access and tampering.

Build a Unified Electronic Notarization Ecosystem. There is a need to establish a comprehensive and unified electronic notarization ecosystem. This ecosystem should integrate various stakeholders, including notary institutions, data providers, and end-users. It should provide a one-stop-service platform that supports all aspects of the notarization process, from evidence collection, pre-review, to final notarization. The platform should be designed with high-level security features, such as multi-layer access control and real-time data monitoring, to ensure the security and reliability of the entire notarization process.

6. Legislation and Regulatory Optimization

Refine Electronic Data Evidence Legislation. Existing legislation on electronic data evidence should be further refined. It should clearly define the scope, characteristics, and legal status of different types of electronic data evidence. For example, it should specify the conditions under which electronic messages, cloud-based data, and IoT-generated data can be considered as valid evidence. In addition, the legislation should establish detailed rules for the admissibility of electronic data evidence in court, including requirements for its authenticity, integrity, and reliability. This will help judges make more accurate decisions when evaluating electronic data evidence.

Harmonize Notarial and Electronic Data Laws. There is a requirement to harmonize the notarial laws with the laws related to electronic data. This includes aligning the notarization procedures for electronic data with the data protection, privacy, and security regulations. For instance, notarial institutions should comply with data protection laws when collecting, storing, and using electronic data for notarization purposes. At the same time, the legal effect of notarized electronic data evidence should be clearly defined in the context of data-related laws, ensuring that there is no contradiction or ambiguity.

7. Professional Development of Notaries

Offer Targeted Training Courses. To enhance notaries' professional capabilities in handling electronic data evidence, develop targeted training courses. These courses should cover a wide range of topics, including digital technology basics, data security and privacy, and the legal implications of electronic data evidence. For example, notaries should be trained in understanding the technical principles of blockchain, how to identify potential security risks in electronic data, and how to apply relevant laws and regulations in the notarization process. Practical training sessions can also be organized, where notaries can simulate real-world scenarios of electronic data notarization.

Establish a Professional Certification System. A professional certification system for notaries handling electronic data evidence should be established. This system can assess the knowledge and skills of notaries in this area through a series of examinations and practical evaluations. Notaries who pass the certification can be recognized as having the professional competence to handle complex electronic data evidence notarization tasks. This will not only improve the overall quality of notaries but also enhance the credibility of the notarial system in the eyes of the public.

8. International Collaboration and Standardization

Participate in International Standard-setting. In an increasingly globalized world, China should actively participate in international standard-setting activities related to electronic data evidence notarization. By engaging with international organizations and other countries, China can contribute its own experiences and perspectives, and at the same time, learn from the advanced practices of other countries. This will help to establish a set of international standards that are widely recognized and adhered to, facilitating cross-border notarization and the mutual recognition of electronic data evidence.

Promote Cross-border Mutual Recognition. China should actively promote cross-border mutual recognition of notarized electronic data evidence. This can be achieved through bilateral or multilateral agreements with other countries. These agreements should clearly define the conditions and procedures for the mutual recognition of notarized electronic data evidence, reducing the legal barriers and uncertainties in cross-border transactions. In addition, international cooperation in the verification and authentication of electronic data evidence can also be strengthened to ensure its reliability and authenticity across different jurisdictions.

D. CONCLUSION

Under the sweeping wave of global digitization, the central position of electronic data in social and economic life has become increasingly prominent, and its connection with the notary system has also become closer. This study's in-depth exploration of notarization systems and electronic data evidence legislation in different countries reveals the uniqueness and commonality of each legal system, and provides a multi-dimensional direction of thinking to meet the current challenges.

The notary systems of different countries show significant differences under the influence of history, culture and legal traditions, and the notary systems of civil law and common law countries are unique in many aspects, and these differences reflect different legal concepts and social needs. Although both the EU and China are committed to safeguarding data security and personal privacy in terms of electronic data evidence legislation, they differ in terms of focus and implementation. EU legislation focuses on the protection of personal data rights and unified regulation, while Chinese legislation closely integrates with the national development strategy, taking into account the needs of the development of the digital economy and national security.

In the face of the future, the continuous progress of technology will continue to reshape the application scenarios of electronic data, which will put forward higher requirements for the notarization system and legislation on electronic data evidence. The initiatives of technological upgrading, legislative optimization, professional development and international cooperation mentioned in the proposal are the key paths to address these challenges and grasp the opportunities for development. By embracing advanced digital technologies, improving laws and regulations, upgrading the professionalism of notaries and strengthening international collaboration, the notary system can better adapt to the changes in the era of electronic data and provide solid legal protection for socio-economic activities.

The international community should join hands to promote the formulation and improvement of international standards related to electronic data evidence, and promote cross-border notarization and mutual recognition of electronic data evidence. This will not only help eliminate legal barriers in cross-border transactions and enhance the efficiency and security of global trade, but also build a fairer, more orderly and secure data ecosystem globally, promote the healthy and sustainable development of the digital economy, and allow the notarization system to play a greater role in the era of electronic data to better serve the stable development of the global society and economy.

REFERENCES

- Amalia, A. N., & Anggayasti, U. H. (2024). Strengthening Law Enforcement: The Urgency of Establishing Regulations on Electronic Evidence in Civil Evidence. *INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH AND ANALYSIS*, 07(05). <https://doi.org/10.47191/ijmra/v7-i05-56>
- Amaral, O., Abualhaija, S., Sabetzadeh, M., & Briand, L. (2021). A Model-based Conceptualization of Requirements for Compliance Checking of Data Processing against GDPR. *2021 IEEE 29th International Requirements Engineering Conference Workshops (REW)*, 16–20. <https://doi.org/10.1109/REW53955.2021.00009>
- BABKIN, I. S. (2024). DIGITAL TRANSFORMATION OF THE NOTARY AS A SOLUTION TO CURRENT PROBLEMS WHEN PERFORMING NOTARIAL ACTIONS. *Нотариальный Вестник*, 1. https://doi.org/10.53578/1819-6624_2024_1_36
- Cao Zhaoxun, Ramalinggam Rajamanickam, & Nur Khalidah Dahlan. (2024). Cyber Notary: The Transformation of Public Legal Services Based on “Internet + Notarization.” *Asian Journal of Law and Governance*. <https://doi.org/10.55057/ajlg.2024.6.2.1>
- Casolari, F., Buttaboni, C., & Floridi, L. (2023). The EU Data Act in Context: A Legal Assessment. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.4584781>
- Creemers, R. (2021). China’s Emerging Data Protection Framework. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3964684>
- Dakhaeva, F., & Datsaeva, R. (2021). The digital economy in the management of socio-economic relations in the global economy. *SHS Web of Conferences*, 106, 01004. <https://doi.org/10.1051/shsconf/202110601004>
- Dinter, B., & Krämer, J. (2018). Data-driven innovations in electronic markets. *Electronic Markets*, 28(4), 403–405. <https://doi.org/10.1007/s12525-018-0316-3>
- Ilyushina, M. N. (2024). Problems of Qualification and Application of Financial Liability of a Notary: The Search for a Legal Regulation Model. *Civil Law*, 2–7. <https://doi.org/10.18572/2070-2140-2024-5-2-7>
- Junyu, M.-. (2020). Notary According To Civil Law And Common Law That Related Strongly With International Civil Transactions. *Jurnal Akta*, 7(3), 285. <https://doi.org/10.30659/akta.v7i3.11279>

- Ke, T. T., & Sudhir, K. (2023). Privacy Rights and Data Security: GDPR and Personal Data Markets. *Management Science*, 69(8), 4389–4412. <https://doi.org/10.1287/mnsc.2022.4614>
- Langford, L. (2020). Developments in China's data protection and privacy regulatory regime. *Journal of Data Protection & Privacy*, 3(4), 437. <https://doi.org/10.69554/BOTP1199>
- Liu, F. (2024). The Legal Implications of Information Disclosure Obligations for E-Commerce Platforms: An Analysis Based on the Electronic Commerce Law of the People's Republic of China. *Law and Economy*, 3(5), 62–67. <https://doi.org/10.56397/LE.2024.05.07>
- Liu, J. (2020). China's data localization. *Chinese Journal of Communication*, 13(1), 84–103. <https://doi.org/10.1080/17544750.2019.1649289>
- Mikhaylova, E. v. (2023). Notarial Acts as a Means of Protection of Rights of the State. *Notary*, 2, 9–13. <https://doi.org/10.18572/1813-1204-2023-2-9-13>
- Nainggolan, B., Susanto, H., Yuniantin, H., & Suwarno, S. (2023). Guarantee of Legal Protection in Cross-Border Electronic Transactions. *Journal of Law and Sustainable Development*, 11(12), e2700. <https://doi.org/10.55908/sdgs.v11i12.2700>
- Pathak, M. (2024). Data Governance Redefined: The Evolution of EU Data Regulations from the GDPR to the DMA, DSA, DGA, Data Act and AI Act. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.4718891>
- Ryngaert, C., & Taylor, M. (2020). The GDPR as Global Data Protection Regulation? *AJIL Unbound*, 114, 5–9. <https://doi.org/10.1017/aju.2019.80>
- Sitdikova, L. B., & Galkin, N. A. (2024). Contemporary Tendencies of Carrying Out Notarial Actions in the Digital Format. *Notary*, 40–43. <https://doi.org/10.18572/1813-1204-2024-1-40-43>
- Weber, P. A., Zhang, N., & Wu, H. (2020). A comparative analysis of personal data protection regulations between the EU and China. *Electronic Commerce Research*, 20(3), 565–587. <https://doi.org/10.1007/s10660-020-09422-3>
- Zhu, M. (2024). Study on the Protection and Rational Utilization of Personal Information in the Digital Era. *International Journal of Education and Humanities*, 16(2), 398–404. <https://doi.org/10.54097/49d8vf27>