Use of Digital Evidence in Trademark Cases

Yan Jing and Zhao Zhao

Introduction

With the rapid development of network information technologies, e-commerce has flourished, online trading has constantly expanded, and trademark infringement has no longer been subjected to traditional geographical and spatial restrictions, the scale of which has expanded substantially, and the Internet, e-commerce and the like are increasingly becoming fields with a high incidence of trademark infringement. At the same time, digital evidence has emerged in large numbers in trademark cases, thereby becoming a critical type of evidence for crucial aspects such as the use of trademark, commodity trading, brand promotion, and corporate culture communication. Digital evidence plays a key role in the accurate factual findings in trademark cases. The characteristics of digital evidence such as highly technology-reliant, easy to tamper, and prone to loss, together with their corresponding particularities in the collection, fixation, preservation, examination and authentication of digital evidence, pose many challenges to both parties concerned and courts. As a matter of fact, these challenges also exist for courts and judges in various countries around the world. To this end, the World Intellectual Property Organization (WIPO) organized a webinar for judges themed "Digital Evidence in Trademark Cases" in early 2025, providing an opportunity for judges from the courts of WIPO member states to conduct discussion on this common issue and share their respective judicial experiences in this field. [1] This article will, with reference to the discussed topics in the webinar, mainly sort out the current use, examination and authentication of digital evidence in trademark cases in China, while introducing relevant overseas development and analyzing the difficulties and challenges in the use of digital evidence.

I. Regulations on digital evidence in China's legal system

In China's laws, judicial interpretations and normative documents, digital evidence is described as "electronic data" or "data messages". At present, the system of regulations on digital evidence has been preliminarily established in China, which provides a fundamental basis for the use of digital evidence in trademark cases. The relevant regulations are mainly in the following five aspects:

1. Articles 2 and 8 of the Electronic Signature Law of the People's Republic of China (hereinafter referred to as the Electronic Signature Law) promulgated in 2005 stipulate for the first time that "electronic signatures" and "data messages" can be used as evidence, with detailed rules for admissibility and authentication thereof. [2]

2. The Civil Procedure Law of the People's Republic of China (hereinafter referred to as the Civil Procedure Law) revised in 2012 clearly includes "electronic data" as one of the statutory types of evidence, and recognizes the legal status of such evidence in civil proceedings. [3] The Interpretation of the Supreme People's Court on the Application of the Civil Procedure Law of the People's Republic of China (hereinafter referred to as the Judicial Interpretation of the Civil Procedure Law) further defines the concept of electronic data, which makes the scope of digital evidence clearer. [4]

3. Two judicial interpretations, i.e., Several Provisions of the Supreme People's Court on Evidence in Civil Proceedings [5] (hereinafter referred to as the Provisions on Evidence in Civil Proceedings) and Several Provisions of the Supreme People's Court on Evidence in Civil Litigation Involving Intellectual Property Rights [6], have set forth detailed provisions on the forms, types, investigation and collection, preservation, as well as examination and authentication principles, of digital evidence.

4. The Provisions on Several Issues Concerning the Trial of Cases by Internet Courts [7] issued by the Supreme People's Court in 2018 confirm the legal validity of evidence-fixing and evidence-preserving methods such as electronic signatures, trusted timestamps, hash value verification, and blockchain for the first time in the form of judicial interpretation, and stipulate implementable rules for verifying the authenticity of digital evidence. The provisions cover the verification of the authenticity of e-evidence in the stages of generation, collection, storage, transmission, etc., emphasize the examination of electronic data generation platforms, storage media, preservation methods, extraction subjects, transmission processes, verification forms, etc., encourage and guide the parties concerned to fix, retain, collect, and extract evidence with technical means such as electronic signatures, trusted timestamps, hash value verification, and blockchain, as well as through evidence collection and preservation platforms, so as to make up for the shortcomings of authentication of digital evidence by notarization only and enhance the admissibility of digital evidence.

5. The Opinions on Strengthening the Judicial Application of Blockchain issued by the Supreme People's Court in 2022 specifically provide guidance on the functions and practices of using blockchain technology to ensure the reliability of digital evidence, in a bid to construct a full-process closed loop of "on-chain evidence storage—intelligent verification—judicial admission", and realize the transformation from technical reliability to judicial reliability.

The relevant provisions of the aforesaid laws, judicial interpretations and judicial documents provide sufficient legal support for the use of digital evidence in the factual-finding process and lay a solid foundation for the full-chain protection of trademark rights and interests in the context of digital network technologies.

II. Types of digital evidence and major application scenarios thereof in trademark cases

1. Typological spectrum of digital evidence

The types of digital evidence are mainly stipulated in the provisions of the Judicial Interpretation of the Civil Procedure Law and the Provisions on Evidence in Civil Proceedings:

Pursuant to Article 116 of the Judicial Interpretation of the Civil Procedure Law, electronic data refer to the information formed or stored with electronic media by means of email, electronic data exchange, online chat records, blog, microblog, text message, electronic signature and domain name. The regulations on electronic data are applicable to the recorded materials and image materials stored with the electronic media. This provision defines electronic data and lists the main types and forms of digital evidence.

Article 14 of the Provisions on Evidence in Civil Proceedings further broadens the types and forms of digital evidence and organizes them systematically. It stipulates that electronic data include the following information and electronic documents: (i) information published on such online platforms as webpages, blogs and microblogs; (ii) messages transmitted through network communication applications such as mobile phone text messages, emails, instant messages, group chat messages, etc.; (iii) user registration information, identity authentication information, electronic transaction records, communication records, login logs, etc.; (iv) electronic documents such as text files, pictures, audio and video records, digital certificates, computer programs, etc.; and (v) other information stored, processed or transmitted in a digital form which can prove the facts of cases.

The above provision substantially encompasses the types and forms of digital evidence emerging and used in judicial practice. In view of the ever-changing development and fast iteration of information network technologies, the judicial interpretation also leaves some room for digital evidence by the expression "other information" so as to adapt to future development. Emerging evidence forms such as blockchain and cyber notary cloud are such examples.

2. Full-cycle usage scenarios of digital evidence in trademark cases

In comparison with conventional physical evidence, digital evidence can be acquired in a faster, more efficient and cheaper manner, and is characterized by objectivity and traceability, which enables digital evidence to be widely used in trademark cases. Judging from trademark cases in judicial practice, there are mainly six major scenarios in which digital evidence is used, which can be divided into three phases, that is, before trademark registration, during trademark registration and after trademark registration.

(1) Before trademark registration

Scenario 1: Trademark owners use digital evidence to prove the prior use of unregistered trademarks. The acts of

unregistered trademark owners, or acts of registered trademark owners before the registration are usually subjected to Articles 13.2, 32 and 59.3 of the Trademark Law of the People's Republic of China (hereinafter referred to as the Trademark Law). Trademark owners use digital evidence such as emails, sales records, promotional webpages, which indicate the time and status of the use of their trademarks, to prove the prior use of unregistered trademarks or that the unregistered trademarks are well-known or have certain influence, so as to further seek legal protection for unregistered well-known trademarks or trademarks with certain influence, or support their non-infringement arguments.

(2) During trademark registration

Scenario 2: Trademark applicants use digital evidence to prove priority. According to Articles 25 and 26 of the Trademark Law respectively, trademark applicants usually use digital evidence to prove that they have applied for registration of the same trademark in a foreign country, which has mutual recognition of the right of priority with China, within six months, or has used the trademark for the first time on the goods displayed at an international exhibition sponsored by China within six months , thereby proving that they enjoy the priority for the trademark application.

(3) After trademark registration

Scenario 3: Trademark owners use digital evidence to prove the genuine, legitimate and public commercial use of registered trademarks. In administrative trademark cancellation cases or in civil trademark infringement lawsuits, the owners of registered trademarks are required to prove their genuine, legitimate and public use of the registered trademarks within a specified period, or otherwise have to bear the adverse consequences of the cancellation of registered trademarks or denial of damages award according to Article 49.2 or 64.1 of the Trademark Law respectively. Digital evidence exerts a vital role in such a scenario. For instance, screenshots of sales records on e-commerce platforms, online advertising data, details of online trading orders, etc. all have probative value in proving the use of registered trademarks by their owners.

Scenario 4: Trademark owners use digital evidence to prove infringing acts and details of the accused infringement. This is the scenario in which digital evidence is used most widely. Whether the right holder's claim can be granted by the court and to what extent it can be granted depend on whether the right holder can prove the infringing acts and details of the accused infringement by evidence. Digital evidence such as sales records on e-commerce platforms, online advertising content and caches of the online trading of infringing goods can directly show the infringer's use of trademark without permission, sale of infringing goods or provision of infringing services; and digital evidence such as online search records and discussions at social media can be used to determine the time, scope and impact of infringement. For instance, in a case involving infringement of the trademark of a milk tea shop [8], the plaintiff Lai made live video recordings of the infringement scene through Notary Cloud, which is an electronic data evidence preservation platform. The record of the entire infringing process made the infringement obvious and served as a solid basis for the establishment of infringement.

In the cyberspace, newly emerged trademark infringement acts are highly concealed. Under such circumstances, conventional physical evidence usually may not be sufficient, while digital evidence can exert its unique advantages. In the "Hailiang" trademark infringement and unfair competition case,[9] the defendant purchased keywords including the plaintiff's registered trademark "Hailiang" on a network platform, and used it in its own websites and promotional web pages, such that network users whoever search with that keyword will be led to the defendant's website, for the purpose of increasing website traffic and grabbing profits. In this case, since infringement occurred during the operation of the network platform, finding of facts such as the identity of the defendant and the number of keywords used by the defendant relied on digital evidence, including, among other things, registration records of related websites, email users' information, and WeChat chat history. In particular, the keyword setting and modified data submitted to the court by the nonparty who operates the network platform play a key role in the identification of infringer and finding of infringement.

Blockchain is an important type of digital evidence used for proving infringement as well. In the Xiaomi trademark infringement case [10], the plaintiff's trademarks like Xiaomi on home appliances have enjoyed a high reputation, while the defendant used commercial signs identical or similar to the plaintiff's trademarks on the same goods by selling them on online platforms. After evidence preservation through a judicial alliance chain (legalXchain), the blockchain data were submitted by the plaintiff and admitted by the court, and the plaintiff's claims were eventually granted.

In the great majority of trademark cases, the parties

concerned use conventional evidence and digital evidence together to prove the facts of cases. For instance, in the BURBERRY trademark infringement case [11], the plaintiff is the owner of some well-known trademarks including BURBERRY, while the defendant used the accused logo similar to the plaintiff's registered trademark and tags and packaging bags highly similar to those of the plaintiff on the accused products manufactured and sold thereby. In view that the infringing facts include not only offline production and sale, but also online sale, the plaintiff submitted to the court digital evidence collected by means of offline notarization in combination with timestamping authentication, in such a way to prove that the online channels and physical shops sold the accused products, and finally obtained a favorable judgement.

Scenario 5: Trademark owners use digital evidence to prove the degree of knowledge of their registered trademarks. The protection strength of a trademark is positively correlated with the distinctiveness and degree of knowledge thereof. To what extent the right holder can be protected in an infringement lawsuit largely depends on the degree of knowledge of the registered trademark. The recognition of a trademark is usually enhanced through media reports, online dissemination, publicity, etc. which are usually in the form of electronic data and highly time-sensitive. If electronic data are not converted into digital evidence by traceable evidence collection, storage and fixation methods, it is very unlikely to fulfill the burden of proof. In the great majority of cases involving well-known trademarks, digital evidence is used to prove the degree of knowledge or recognition of a trademark.

Scenario 6: Trademark owners use digital evidence to establish the factual basis of their damage claims. The determination of damages in trademark cases is a hard nut to crack and usually lacks direct evidence support, especially when the defendant does not cooperate in submitting evidence, such as financial books, in relation to its profits made from infringement. The court needs to determine the number of damages with the help of supplementary information such as online sale information or promotional media reports in relation to the accused infringement. In the Siemens trademark infringement and unfair competition case [12], the court ordered the defendant to submit evidence in relation to infringement, such as financial books, production plans and manufacturing records, to find the basis for damages, but the defendant refused to do so. Since the defendant's refusal to submit evidence constituted spoliation of evidence, the court determined factors for calculating damages, including the defendant's total annual sales and the proportion of sales of the accused products, with reference to online media reports on the defendant's sales data provided by the plaintiff, together with other evidence on file and the profit margin of the industry, finding that the defendant's profits gained from infringement had far exceeded the plaintiff's claimed damages, and eventually fully granted the plaintiff's claim, holding that the defendant is liable for the damages of 100 million RMB and the plaintiff's reasonable expenses for enforcing rights.

III. Key points for examination of digital evidence and rules for the authentication thereof

Like other conventional types of evidence, digital evidence generally should be examined from the aspects of authenticity, legality and relevance. Data with trusted timestamps are the most widely used and most typical type of digital evidence in trademark cases. We are going to expound the key points for examination of digital evidence and rules for the authentication thereof in judicial practice by the evidence-collecting steps and evidence-fixing principle of trusted timestamps.

1. Authenticity examination

In the process of examining the "authenticity, legality and relevance" of evidence, the authenticity of digital evidence is the core of examination. Article 93 of the Provisions on Evidence in Civil Proceedings specifically enumerates and stipulates the factors to be considered when examining the authenticity of digital evidence, wherein the integrity and reliability of data are the most important factors, for which consideration shall be given to the aspects including, but not limited to, whether the software and hardware environment in which the digital evidence was formed is clean, whether the system operates normally, whether the means to prevent and detect errors and omissions are effective, whether data are complete and whether the subject is qualified. Article 94 of the Provisions on Evidence in Civil Proceedings further stipulates that under the following circumstances, courts may presume the authenticity of digital evidence unless there is sufficient evidence to the contrary: where the digital evidence is submitted or confirmed by an

independent third party platform that records or retains the data; where the digital evidence is stored as archives; where the contents of the electronic evidence have been notarized by a notary public, etc. Trusted timestamps fall within the first circumstance.

A trusted timestamp is a trusted timestamp certificate issued by the United Trusted Timestamp Service Center (hereinafter referred to as the Timestamp Service Center) [13] to the electronic data file submitted by a party by means of the legal time source and cryptographic technology, which can be used to prove the time of formation of the electronic data file and the integrity of its content and its unchanged state. The trusted timestamping process is similar to the electronic notarization of electronic data files.

The Timestamp Service Center released the Operation Guidelines to regulate the steps for collecting, storing and fixing evidence by means of timestamping. The basic steps generally include: (1) to start screen recording; (2) to check computer security and cleanliness; (3) to check the authenticity of internet connection; (4) to collect and fix evidence; and (5) to apply for authentication of the fixed evidence and screen recordings by the timestamping system and download the certificate. The principle of authentication by the trusted timestamp electronic certificate is that a unique digital fingerprint (hash value) and a corresponding electronic certificate given by a Time-Stamp Authority (TSA) are automatically created for each file when applying for a timestamp; when verifying the timestamp, the file to be verified is compared with the electronic certificate of the TSA generated at the time of applying for the timestamp; if the content of the verified file is kept intact and has never been changed since the application for the timestamp, the file is verified by the timestamp, or otherwise the file fails the verification.

Based on the steps and principle of evidence collection, storage and fixation as mentioned above, the key of examination of the authenticity of the digital evidence verified by the trusted timestamp is to examine whether the collection, storage and fixation of the digital evidence follow the corresponding steps in the Operation Guidelines. Since forged and tampered evidence can be greatly filtered out if evidence collection is conducted under the Operation Guidelines, the authenticity of evidence verified by the trusted timestamp is usually recognized in the absence of evidence to the contrary.

In judicial practice, it is highly likely that evidence with trusted timestamp certificates is admitted by the courts in trademark cases. Of course, there have also been cases in practice where a party did not fix evidence in strict adherence to the Operation Guidelines, thereby leading to the failure of evidence preservation or that the authenticity of evidence is challenged. For instance, in the "Re Xue Jiang Hu Zhuan" trademark infringement case [14], the plaintiff Longtu did not fix the evidence with the timestamp evidence collection system in the process of evidence collection, but uploaded a recorded video to a timestamping website for authentication. Although Longtu also checked the version of the operating system of the mobile phone, network and apps in the mobile phone before evidence collection, it cannot be ruled out that the mobile phone was linked to a virtual website or virtual proxy website because the standard operation procedures for collecting evidence by timestamp authentication were not followed. Especially since the real route that the network server takes to reach a target webpage cannot be checked on the mobile phone, it is impossible to determine the authenticity of the linked website. Therefore, the evidence with the trusted timestamp, as provided by Longtu, had great defects and was eventually not admitted by the court.

It should be noted that the most important function of the trusted timestamp is to retroactively prove the authenticity and reliability of evidence collection and fixation. The authenticity of the content of the collected evidence sometimes has to be comprehensively judged in combination with other related evidence.

2. Legality examination

The legality of evidence mainly means the form and source of evidence are in line with legal provisions. For digital evidence, what extremely matters is whether the channel and method for acquiring evidence are legal. If the right holder acquires digital evidence from the opposite party by illegally invading the opposite party's computer system or by network hacking means, such evidence collection method obviously stands in violation of the legal provisions on computer information security and citizens' right to privacy. Even if the evidence collected contributes to proving infringement, it should not be admitted as it is illegally obtained. In addition, whether those who authenticate the digital evidence are qualified is another vital aspect to be examined. At present, the Electronic Signature Law definitely stipulates that those who engage in electronic authentication services should obtain permission from the information industry department under the State Council and an electron-

ic authentication license issued by the latter. There have been no clear provisions on the qualification of entities that provide other electronic evidence collection and storage services yet.

3. Relevance examination

Relevance examination encompasses two aspects: one is the relevance between the digital evidence and the *factum probandum* in a case, i.e., if the evidence is irrelevant to the *factum probandum*, it cannot be used as a basis for factual finding even if the evidence *per se* is authentic and legal; and the other is the relevance between the digital evidence and other evidence on file, i.e., whether the digital evidence and others form a chain of evidence, and whether there are contradictions and conflicts therebetween.

All of the above aspects should be considered comprehensively by judges when reviewing and examining evidence.

IV. Overseas dynamics

About 400 judges, judicial officials, and examiners from administrative authorities of countries all over the world attended the WIPO's webinar for judges, at which representatives from China, India, and the European Union introduced and shared the practices of digital evidence in their own countries, and intellectual property judges from the United Kingdom, Germany and South Korea engaged in interactive discussions around the theme of the webinar.

Justice Prateek Jalan (Delhi High Court, India) introduced that Section 65-B of the Indian Evidence Act is a "compulsory threshold" of the legality of digital evidence, requiring the provider of digital evidence to provide an evidentiary document executed by the device operator to clearly indicate the generation method, device details and legality of digital evidence in a bid to ensure the authenticity and reliability of evidence; or otherwise, the digital evidence will not be admitted.

Based on the judgment of a trademark infringement case, *Lacoste & Anr. v. Crocodile International Pte Ltd. & Anr.*, Justice Prateek Jalan introduced the crucial role and examination principle of digital evidence in trademark disputes in Indian judicial practice. In this case, digital evidence was not admitted because the required certificate under Section 65-B of the Indian Evidence Act was not provided. The judgment of this case clarified the rule that if digital evidence does not meet the requirement on certificate under Section 65-B, the court will not admit it, and meanwhile overturned the lenient stance of allowing afterward supplements in *Tomaso Bruno v. U.P. State*, and *Shafhi Mohammad v. H.P. State*.

Justice Prateek Jalan said that this judgment aims to curb the risk of electronic evidence abuse in the digital era and maintain the rigor of judicial procedures. In addition, Justice Prateek Jalan emphasized that the digitization of the business ecosystem has a profound impact on the recognition of trademark and goodwill. The development of modern social media and globalization has thoroughly altered the construction mode of trademark and goodwill. They are no longer constrained by geographical boundaries, but quickly spread across markets of various countries through digital marketing and global trade. He also called for such legislation and judicial practice that advance with the times and are adapted to digitalized business ecosystem.

Based on *Oriflame Cosmetics AG v. EUIPO / Caramé Holding AG*, Judge Louise Spangsberg Grønfeldt (General Court of the European Union, Luxembourg) introduced the criteria for examining evidence of use of trademark at the General Court of the European Union and the application thereof in the digital era. The key issue of this case is whether the digital evidence proves the genuine use of the trademark in accordance with the requirements of Article 10(3) of Delegated Regulation 2018/625. In this case, Oriflame submitted several types of digital evidence, among which are extracts from social media, in a bid to support its claims. However, the General Court of the European Union deemed that the evidence has two major defects: (1) the evidence does not suffice to prove the genuine use of the trademark, and it is not adequately relevant: the evidence submitted, such as the invoices and product packages, does not clearly demonstrate the time, place and scope of use of the trademark on designated goods or services, thereby failing to prove the genuine use of the trademark; (2) although Oriflame provided screenshots which showed the use of the trademark on social media, they did not indicate any business association between the products and the enterprise due to, e.g., lack of data on user interaction or proof for actual sale, and therefore the genuine use of the trademark by Oriflame cannot be established. Judge Louise Spangsberg Grønfeldt stated that this case highlighted the strict standards of the court for examining the evidence in relation to trademark use. Especially in the digital context, the demonstration of a brand on social media alone is not sufficient to

prove the use of the trademark. What must be proved is that consumers directly associate the digital content with the goods or services protected by the trademark; or otherwise, the use of the trademark may be regarded as a symbolic use rather than a genuine commercial activity. The General Court finally ruled to cancel the registered trademark in dispute on the grounds of lack of sufficient evidence.

Comparatively speaking, India's laws and judicial practice tend to be conservative and more prudent in admitting digital evidence in trademark cases, followed by the European Union, and China is more open and inclusive. Judges from many countries all over the world paid great attention to the use of digital evidence in China. The majority of judges participating in the webinar said that they were unfamiliar with the principles of technologies such as timestamps and blockchain, and confused about how to examine the authenticity of digital evidence. German judges stated that although trusted timestamps had been proposed in the European Union laws and German laws, they had never encountered cases involving digital evidence authenticated by timestamps in their decades-long career. This differs significantly from the widespread use of trusted timestamped digital evidence in China.[15] Lord Justice Colin Birss of the United Kingdom thought that the Wayback Machine in Europe may be similar to the trusted timestamps used in China in terms of the principle. Korean judges were interested in how the courts in China ensure that the parties can fully exercise their right to challenge and defend the authenticity of electronic evidence in specific cases.

V. Difficulties and challenges in the use of digital evidence

As known from the webinar, digital evidence in trademark cases is characterized by great variety, huge quantity, technological sophistication, etc., all of which enhance the difficulty in examining and judging digital evidence on the part of judges. The judiciary at home and abroad is facing the same difficulties and challenges.

First of all, technology updates increase the difficulty in understanding and examination. It is hard for judicial officers to understand and master constantly iterated new technological principles and corresponding examination points within a short period of time due to their learning and professional experience. For instance, quantum encryption technology involves complex principles of quantum mechanics and high-end encryption algorithms. Judicial officers can hardly master technical details, thereby being faced with the risks of inaccuracy when examining digital evidence preserved by such technology, and further affecting the admissibility of evidence.

Second, loopholes may still exist in anti-tampering technical means. Although such anti-tampering technical means for digital evidence as trusted timestamps and blockchain have been substantively mature, digital evidence may still be tampered due to potential technical loopholes, and the traces of tampering may be extremely concealed and unperceivable. For instance, an electronic file with its underlying codes slightly modified may seem to be normal, but the content of the file has been altered, which may not be detected by common technical means. This poses a severe challenge to the court's accurate judgment of the authenticity of digital evidence, thereby affecting the outcome of the case.

Third, cross-regional and cross-platform data collaboration and integration is still a problem. Digital evidence in trademark cases is often scattered on servers in different regions or on different network platforms. To integrate cross-regional and cross-platform electronic data into valid evidence, there are difficulties such as differences in laws between countries and regions and inconsistent data accessibility and formats on various platforms, which greatly hinder the parties' adduction of evidence and courts' examination of evidence.

All the above problems are after all challenges to courts and judges posed by the development of new technologies. To cope with these challenges, on the one hand, judicial officers need to improve their judicial capabilities constantly, in a bid to ensure that digital evidence is accurately and effectively admitted in case trials for the sake of judicial justice; and on the other hand, judicial authorities should keep exploring and improving relevant systems and rules in practice so as to guarantee the uniform, determinative and authoritative examination of digital evidence. Furthermore, an effective way to deal with the above challenges is for judicial officers to learn from and communicate with each other.

Conclusion

With the continued rapid development of China's economy and comprehensive advancement of the construction

of digital economy, the number and complexity of digital evidence in various intellectual property cases like trademark cases have sharply risen. When dealing with these complex issues, Chinese courts have accumulated abundant experience and formed mature solutions. This valuable experience has brought remarkable achievements in China's judicial practice and is also of great value to be promoted internationally. We should take advantage of the good opportunities for international exchanges, and learn beneficial experience from international fellows, share Chinese solutions in international exchanges, and tell China's good judicial stories to the world. ■

The authors: Yan Jing, Presiding Judge of the Third Civil Division of the Supreme People's Court; and Zhao Zhao, Assistant Judge of the Supreme People's Court

[1] The first author participated as a distinguished guest in the webinar and delivered a keynote speech.

[2] Articles 2 and 8 of the Electronic Signature Law of the People's Republic of China (revised in 2019).

[3] Article 63 of the Civil Procedure Law (2012).

[4] Article 116 of the Judicial Interpretation of the Civil Procedure Law.

[5] Articles 14 and 15 of the Provisions on Evidence in Civil Proceedings summarize electronic data into five forms: information published on network platforms, communication information of network application services, record type information, electronic files and other digital information, and clarify the principle that the original of electronic data, if used as evidence, should be provided and what can be regarded as the original of electronic data. Articles 93 and 94 of the Provisions on Evidence in Civil Proceedings enumerate the major factors to be considered in the examination of the authenticity of electronic device, especially the circumstances under which the authenticity of electronic evidence can be presumed.

[6] Article 19 of the Several Provisions of the Supreme People's Court on Evidence in Civil Litigation Involving Intellectual Property Rights stipulates that the court may entrust an appraisal of the authenticity and integrity of electronic data as a specialized issue.

[7] Article 11 of the Provisions of the Supreme People's Court on Several Issues Concerning the Trial of Cases by Internet Courts.

[8] The Civil Judgment No. Zhe0784minchu 7608/2018.

[9] The Civil Judgment No. Zuigaofaminzai 131/2022.

[10] The Civil Judgment No. Wanminzhong 178/2024.

[11] The Civil Judgment No. Suminzhong 432/2022.

[12] The Civil Judgment No. Zuigaofaminzhong 312/2022.

[13] The Timestamp Service Center is jointly established by Beijing United Trust Technology Services Co., Ltd. and National Time Service Center of the Chinese Academy of Sciences.

[14] The Civil Judgment No. Jing73minzhong 478/2021.

[15] In the keynote speech entitled "The Role of Trusted Timestamps in Trademark Protection" at "Seminar on the Application of Electronic Evidence in the Field of Trademark Protection" of 2024, Zhang Changli, Chairman of the United Trusted Timestamp Service Center, introduced that trusted timestamps had been used in China since 2005, and there had been more than 180,000 effective judgments admitting trusted timestamps in the last two decades.

China boosts judicial shield for innovators

Innovators from China's private sector will benefit from stronger judicial protection, especially those working in new technologies and emerging businesses, under a guideline issued on 8 August 2025 by the country's top court.

Reiterating the private sector's important role in the Chinese socialist market economy, the Supreme People's Court released a 25-article guideline requiring courts all over the country to focus more on intellectual property cases involving high-tech fields and to strengthen legal protection for key areas and core technological innovations.

The guideline also encourages judges to use punitive damages in IP cases to effectively combat violators and provide incentives for innovators.

Additionally, it allows courts across China to foster the healthy development of the artificial intelligence industry, and conduct more research on safeguarding data rights while facilitating efficient data circulation.

Source: China Daily