Use and Development of Information and Communication Technology In Criminal Procedure of China*

College for Criminal Law Science, Beijing Normal University*

With constant improvement of social informationalisation, information and communication technology (hereafter ICT) has been widely used in criminal proceedings in China. The ICT plays an increasingly important role in the investigation, evidence collection, preservation, presentation, verification, examination and trial at court. In criminal justice system, the ICT has both technical attributes and legal attributes: on the one hand, proper use of the ICT can assist in detection of crimes, timely and accurate collection of criminal evidence, etc. This makes successful charge and trial possible, especially for those crimes relying upon information network; on the other hand, abuse of the ICT may cause threats and infringements upon the privacy of citizens, business secret of corporate, information about national security, etc. Therefore, in criminal justice, the ICT shall be strictly restrained by procedure and rules.

Given the urgent needs about the ICT from legal practice, the provisions of the ICT in Criminal Procedure Law in China (hereafter CPL) is still relatively backward, so that the criminal justice agencies often encounter many difficulties in applying the laws in handling the relevant cases. On March 14, 2012, the new Criminal Procedure Law has been issued. In this law, electronic evidence becomes statutory evidence for the first time. Also, technical investigation measures which can be used to investigate cyber crimes are stipulated. Prior to this enactment, the Supreme Court, the Supreme Procuratorate and the Ministry of Public Security successively issued some interpretations and regulations regarding collection and examination of electronic evidence. Basically, these rules are not comprehensive and systematic enough. A number of important issues, such as search, inspection, identification, network monitoring, filtering, investigative trap by use of the ICT and exclusive rules against illegal evidence, etc, are not probably regulated by procedural rules. It is clear that legislations upon the ICT in criminal proceedings in China are still in its infancy.

1. Use of the ICT in Investigation

1.1 Audio-visual Record of Interrogation

1.1.1 Features and Functions

Audio-visual record of the process of interrogation is a use of the ICT in criminal proceedings. Compared with its use in other fields of criminal procedure, audio-visual record of the interrogation were used and developed earlier, in that audio-visual record has the following merits:

(1) Synchronicity. Audio-visual record is made for the events happening at exactly the same time. Although a written record is synchronous record of what is happening, its synchronicity is impacted by record speed and other factors;

(2) Objectivity. Differing from the prosecuting perspective of the investigators, audio-visual recording equipment, as a physical device, is objective and not influenced by any subjective elements. In other words, both information against the suspects and information for them are faithfully recorded;

(3) Reproducibility. Due to the replay device of audio-visual record, the whole interrogation process can be

* Important notice: this text is the last original version of the national report sent by the author. The Review has not assured any editorial revision of it.

* The authors include 5 researchers of College for Criminal Law Science of Beijing Normal University: Prof. Song Yinghui, Prof. Shi Limei, Associate Prof. Yang Xiong, Associate Prof. He Ting and Associate Prof. Yin Bo.

reproduced at any time;

(4) Comprehensiveness. On the one hand, audio-visual recording can be not only used to keep, without any omissions, all content of investigators' questions and the criminal suspects' answers, but also demonstrate much other information, such as the environment of interrogation location, investigators' manner and body movements, suspects' physical condition and mental state, etc.

In addition, audio-visual recording has the following functions:

(1) Fixing and preserving evidence, providing basis for cross-examination at trial. Due to synchronous, objective, reproductive and comprehensive features, entire audio-visual record can fix and preserve high quality confessions from criminal suspects, make entire interrogation process reappear before the court, assist in examining authenticity of different confessions and provide the accurate basis for cross-examination at trial;

(2) Supervising legitimacy of interrogation and protecting human rights. The record can demonstrate criminal suspect's physical and mental state at the time of being questioned and is thus useful for supervising investigator's interrogation activities. Once the investigator(s) use illegal means to extract confession, such as threat, enticement, and extortion of confession by torture, illegal conducts will be clearly and vividly displayed from audio-visual record. This is a potential piece of evidence which can be used to curb forced confession.

1.1.2 China's Endeavour in Legislation and Practice upon Audio-visual Record of Interrogation

By the end of last century, China began to legislate upon audio-visual record of interrogation process. In 1998, article 184 of Procedural Regulations of the Public Security Bureaus in Handling Criminal Cases prescribed that investigator(s) can keep video record at the same time of writing records if needed when interrogating criminal suspects. Article 218 prescribed that recordings, videotapes, electronic data storages, which are used as evidence, shall be recorded clearly in terms of the cause of action, object, content, admissibility, duplication time, location, magnitude, categories, applicable length, file format and length, etc., and be appropriately stored. In Shenzhen of Guangdong Province, a pilot of carrying out entire synchronous audio-visual recording in investigation since 1999 were effective to supervision upon investigation and deterrence to the defendant's withdrawal of confession at trial. But in general, as regards how to specifically carry out audio-visual recording when interrogating criminal suspects, how to use information from audio-visual record, how to punish violations of rules and other issues, there are not any standardized regulations. The synchronized audio-visual recording in investigating criminal suspects cannot be fully implemented. In 2005, the Procedure Law Research Center of the China University of Political Science and Law carried out a pilot of interrogation of a criminal suspect with attorney present and voice and video recording. This pilot focused upon the outstanding problems of failure in prohibiting tortures in judicial practice and high rate of confession withdrawal done by criminal suspects. They tried to establish a supervision and certificate mechanism in the interrogation process, so as to curb torture, ensure the quality of oral confession. The result of pilot showed that, on the one hand, the ratio of confession withdrawal effectively decreased through attorneys at present and recording system, torture hardly occur again; on the other hand, this system was supported by the public security agencies and investigators in pilot, and did not create any difficulties or negative impact upon case handling.

Since the end of 2005, the Supreme People's Procuratorate began to promote entire uninterrupted synchronous audio-visual recording system in interrogation on crimes by taking advantage of duty nationwide. On December 16, 2005, the Supreme Procuratorate issued Regulations of the Procuratorate in Investigating Crimes by Taking Advantage of Duty through Synchronous Recording and Video Recording, which requires that entire uninterrupted synchronous audio-visual recording system shall be gradually used in interrogation on crimes by taking advantage of duty since March 1, 2006, and completed promoted nationwide till October 1, 2007. In order to promote this

project smoothly, the Supreme Procuratorate guaranteed human resources, funds, system, etc. In December 2006, the General Office of the Supreme procuratorate issued two regulations. The first one regulated audio-visual recording from acceptance of case, recording, sealing, storage, etc. Moreover, the regulation clarified the application of synchronous recording criteria. The second one has prescribed the recording equipment standards, specifications and function requirements, which provided basis for all levels of the procuratorial agencies on synchronous recording system construction. In accordance with the provisions created by the Supreme Procuratorate, each place formulates specific rules combining with their own practice.

On the basis of early exploration, article 121 of the China stipulated that the investigators may, when interrogating a criminal suspect, record the sound or image of the interrogation; the sound or image of the interrogation shall be recorded for cases in which life imprisonment or death penalty may be sentenced or other major criminal cases. Recording the sound or image of the interrogation shall be conducted thoroughly and completely. According to the relevant judicial interpretations, 'other major crimes' refer to serious crimes endangering public security or infringing upon the personal rights of the citizens and causing serious injury or death, and organized syndicate crimes, serious drug crimes and other major intentional crimes. Where investigators record the sound or image of the interrogation process, the fact shall be indicated in the interrogation. Where the procuratorate or the court may draw on audio-visual record of the interrogation process, the relevant agencies shall provide it timely. Every interrogation should be recorded fully without any interruption to safeguard its integrity. Selective recording, editing or deletion shall not be allowed. In the court process, audio-visual record of the interrogation process may be reviewed when necessary.

The above regulations provide a legal basis for further promoting audio-visual record of the interrogation process system in China. It is demonstrated by the following facts: (1) It is the first time to regulate audio-visual record of the interrogation process through legislation, which makes the system guided by laws; (2) Applicable scope for audio-visual record of the interrogation process system has been regulated by law. Audio-visual record of the interrogation process shall be made in handling cases in which life imprisonment or death penalty may be sentenced or other major criminal cases; (3) audio-visual recording of the interrogation process shall be the whole process, and its integrity shall be maintained without any cutting or deletion; (4) The way of reviewing audio-visual record material was preliminarily regulated; (5) mature audio-visual record of crimes by taking advantage of duty in interrogation in practice is incorporated into the law.

1.1.3 Problems and Development in Future

(1) The probative capacity of synchronous audio-visual recordings is not clear. China's Criminal Procedure Law didn't provide evidence capability of synchronous audio-visual recordings. Synchronous audio-visual recordings are different from traditional evidence. For example, the storing method of audio-visual recording is different from the traditional approach. A written record cannot take all statements of suspect. If a written record deviates from or even conflicts with synchronous audio-visual recordings, how to decide the fact has no definite conclusion.

(2) Suspect's rights safeguards shall be further improved. Although taking synchronous audio-visual record shall inform the criminal suspect who is being questioned according to law, and shall reflect in audio-visual recordings and recorded in the transcript. To some extent, this ensures the criminal suspect's right to the information. Whether the suspect being questioned have the right to request or refuse synchronous audio-visual recording under certain circumstances have not been clearly regulated.

(3) Procedural sanctions for violation of audio-visual record's regulation have not been established. The amended criminal procedure law and relevant judicial explanation has established the exclusion rules of illegal evidence in

China, where exclusion conditions of illegal verbal or physical evidence, burden of proof and standard on evidence collection have been provided. However, exclusion of audio-visual recording material's evidence has not been clarified, and the legal consequence of violation of audio-visual recording has not regulated. Therefore if the relevant rules are broken, whether the corresponding procedural sanctions may follow has not been clarified.

(4) Further operating rules are needed. Current operation rules are not perfect, which in practice led to the following problems: (a) Recording. The investigative agency is de facto in a dominant position at trial. The record might be a rehearsal or 'record after interrogation'. Investigators may interrogate the suspect firstly to get key statements, and then take nominal "synchronization of audio-visual recording". This kind of audio-visual recording will crush its synchronous advantages. It cannot put extorting confessions by torture to end, but will make unjust case seriously. Some substandard operations result in recordings cannot reflect interrogation process exactly. Invisible expression and manner of the criminal suspect, lack of important details, no workplace scenarios and start-stop time are widely seen. Investigators apply audio-visual recording on interrogation selectively, rather than "full", "synchronous" or "not interrupt" audio-visual recording. In addition, how to ensure interrogation investigator distinguished with recorder and recorder's independence is a question need to further discussed. (b) Storage. Because content of audio-visual recording needs to be saved in audiotape or videotape, whether the audio-visual recording functions depends on audiotape or videotape's safekeeping. How long that audiotape or videotape shall be kept and what kind of medium it shall preserved on need support of relevant technology. (c) Unsealing and obtaining. How to regulate specific procedures of obtaining and unsealing, prevent investigation secrets leaked in process, content of audio-visual recording tampered with, etc., are all operational issues that need to be resolved.

1.2 Technical Investigation Measures

Technical investigation measures are special investigative measures for the public security bureaus and the procuratorates to investigate the crimes, including electronic monitoring, wiretapping, electronic surveillance, secret photographing or videoing, secret procurement of material evidence, postal inspection, network interception and other special technical means. Legislation upon technical investigation has undergone a process from inexistence to appearance, from simple to complex, from secret to public. Criminal Procedure Law in 2012 and its following judicial interpretations stipulates the applicable scope of technical investigation measures, conditions and procedures, etc. However, for the purposes of combining crime control and human rights protection, technical investigation shall be further legislated.

1.2.1 Legislative Evolution of Technical Investigations

Criminal Procedure Law in 1979 did not regulate technical investigation. Article 10 pf the National Security Law promulgated in 1993 provides that the national security bureaus, for the purpose of investigating offences against national security, may, in accordance with the relevant provisions, use technical investigation measures after being approved. Article 16 of the People's Police Law in 1995 stipulates the same provisions. In Part Eight, Chapter Two of the Criminal Procedure Law in 2012, technical investigation measures are specially provided for. This part include five articles, stipulating the scope of cases where technical investigation shall be used, decisive agencies, implementing agencies, procedure of examination and implementation, and use of evidential materials obtained, etc. Subsequently, Criminal Procedure Rules of the People's Procuratorate (Trial) issued by the Supreme Procuratorate and Procedural Regulations of the Public Security Bureaus in Handling Criminal Cases revised by the Ministry of Public Security in 2012 specifies the above-mentioned rules, ensuring technical investigation measures further regulated by the law.

1.2.2 Scope of Cases and Conditions for Applying Technical Investigation

As a kind of special investigative measures, technical investigation intervene the privacy of citizens. Therefore, most jurisdictions across the world only apply these measures in serious criminal cases. According to Criminal Procedure Law and its interpretations, technical investigation measures shall be applied in the following three conditions: First, under the jurisdictions of the public security bureaus, crimes endangering national security, terrorist crimes, organized syndicate crimes, major drug crimes, intentional homicide, intentional injury causing grievous harm or death, rape, robbery, kidnapping, arson, explosion, throwing dangerous substance, and other serious violent crimes, group, series, cross-regional major crimes, and serious crimes committed via telecommunications, networks, delivery channels, and serious crimes against computer network, other crimes seriously harming to the society which may be sentenced more than seven years. Second, under the jurisdiction of the People's procuratorate, serious crimes which involve an amount over 100,000 yuan, major corruption and bribery cases which are difficult to procure evidence by other means, or severely infringe upon personal rights via abuse of public powers. Third, the fugitive criminal suspects or defendants chased by the public security agencies or procuratorate or approved by the latter to be arrested. In addition, technical investigation can be only carried out after filing the cases. The applicable subjects of technical investigation are criminal suspects, defendants and personnel directly related to offences. After all, the above regulations demonstrate the principle of application in felony and the principle of last resort. These two principles can be used to prevent wide use of technical investigation. However, because the existing statutes and judicial interpretations have not stipulated evidential elements for initiating technical investigation, the principle of proportionality may be violated in the process of technical investigation. In the future, it shall be legislated that technical investigation can only be used when there are certain evidence prove the suspicion of criminal suspects in committing the above crimes.

1.2.3 Approval Procedure of Technical Investigation

In order to prevent the investigative agencies from arbitrary use of technical investigation measures with the motives of prosecuting crimes, laws in most jurisdictions across the world stipulate that technical investigation must be used after authorization from a neutral court or judge. Article 11 of the Decision concerning the Human Rights Issues in Criminal Procedure Law passed by the 15th Session of the World Penal law Association provides that the evidential means severely infringing upon fundamental rights of privacy, such as wiretapping, unless authorized by the judge and explicitly provided by the law, cannot be admitted as evidence. According to Criminal Procedure Law in China and its judicial interpretations, technical investigations, no matter whether they are done by the public security bureaus or by the procuratorate, only need to be internally reported to and approved by the higher authorities, without necessity of prior authorization from the court or the judge. This administrative, written approval mechanism is lack of effective external supervision, and may result in breakthrough of the applicable scope of technical investigations against the existing legal rules and challenge against the citizenry privacy. Based upon China's present judicial system, we recommend that approval power of the public security agency in technical investigation shall be transferred to the procuratorate, the latter's approval power shall be transferred to the court in the future legislation. By means of this judicial review system with Chinese characteristics, abuse of technical investigation measures can be effectively prevented.

1.2.4. Implementation Procedure of Technical Investigation

As regards implementation procedure of technical investigation, the Criminal Procedure Law provides categories, objects and time limit. Specifically, the decision to approve shall be based upon the need to investigate crime and confirm the categories and applicable objects of technical investigations. Approval decision has been effective within three months after its being issued. For those cases that technical investigation measures are not necessary, these

measures shall be timely dismissed. For those complicated and hard cases, if it is still necessary to take technical measures after its expiration, the period can be extended after being approved. Each extension shall not exceed three months. Technical investigation measures shall be implemented in accordance with the lawful categories, applicable objects and time limits. The above mentioned expressions are too vague and principled, which may leave too much discretionary room for implementation and approval of technical investigation and result in wide use of these measures. In addition, different technical investigation measures may intervene the communication, objects, locations of the individuals in different degrees. Only if different approval processes and applicable time limit are used, the principle of proportionality can be met.

Pursuant to article 150(4) of the Criminal Procedure Law, the public security agencies shall take lawful technical investigation measures whilst the related units and individuals shall cooperate with the public security agencies and ensure the relevant case confidential. According to article 227 of the Procedural Regulations of the Public Security Bureaus in Handling Criminal Cases and article 238 of People's Procuratorates' Criminal Procedure Rules (Trial) stipulate that seizure of criminal suspects' mails, e-mails, telegraph notices shall be approved by the head of the public security agency above county level or the Chief of the procuratorate. The relevant notice to seize these documents shall be made and sent to the post office or network service for examination and seizure. According to the provisions from the Security Administration Punishment Law and Criminal Law, if the related unit and individuals have not fulfilled the duty of cooperation and confidentiality, they may be dealt with by administrative liability. If the circumstances are serious, they may be criminally liable.

1.2.5 Procurement of Evidence by Means of Technical Investigation

In judicial practice before the amendment of the Criminal Procedure Law in 2012, technical investigation was aimed at finding the clues of a crime. In other words, the evidential materials obtained through technical investigation can be neither directly used as evidence nor presented before the court. They are only used as the clues. In other words, only if the clues are transferred into statutory evidential forms, can they be used as evidence. This means cause that some major cases cannot be decided as a result of the lack of key evidence, weakening the attack to the crimes. The Criminal Procedure Law in 2012 and its interpretations made the following modifications for resolving this problem: first, it is stipulated that materials collected by means of technical investigation measures can be used as evidence in criminal proceedings; second, special methods for verifications in the technical investigation. In other words, if the evidence obtained by means of this technical investigation may endanger the personal safety of the relevant persons, or may cause other serious consequences, the protective measures such as concealing the identities of the relevant persons. If necessary, the evidence shall be examined and verified by the judges out of the court; third, pursuant to article 54 of the Criminal Procedure Law, where material evidence or documentary evidence by means of technical investigation is obtained against the legally prescribed procedure, which may severely impair the judicial impartiality, supplements and corrections, or reasonable explanations shall be made; if the above mentioned measures cannot be taken, the said evidence shall be excluded.

In our opinions, given the special attributes of technical investigation, the principle of 'ultima ratio' shall be applied for use of technical investigation to procure evidence. Meanwhile, even if special measures of cross-examination and verification are used for the purposes of protecting the operators of technical investigation, the right of procedural participants, especially the defendants, to be cross examined and verified shall be ensured. Moreover, in order to motivate the agencies seised of technical investigation collect evidence in a lawful manner, the law shall explicitly stipulates that evidential effect of the recording, video-tapes, and other materials obtained against lawful technical investigation shall be clearly stipulated.

2. Electronic Evidence

As the cyber crime is a relatively new category of crime emerging with the use of information and communication technology in last two decades, electronic evidence and the rules thereof are newly created in most jurisdictions. P. R. China is not an exceptional in this trend. It is known that audio-visual technology has been developed before computer and internet systems and laid a solid foundation for the latter. Evidence rules regarding electronic data are naturally an extension of rules regarding audio-visual evidence. Being similar to audio-visual evidence, electronic evidence is characterized as an enormous amount of visibility, information, accuracy as well as being susceptible to falsification or tampering. According to Article 48 of the Criminal Procedure Law in China, electronic data and audio-visual materials are grouped into one of the eight categories of evidence.

China, in this electronic revolution, does not take the lead but is the most important consumer. The innovation and regulations of ICT lags far behind the need for consuming the relevant materials in China. It indicates that its rules regarding electronic evidence are not complete and systematic at present. Meanwhile, there are many cyber crimes committed in this materialized soil, such as the smuggling crimes and online gambling crimes. Especially, in dealing with the online gambling cases, most evidence emerges as electronic evidence. The Supreme Court, the Supreme Procuratorate and the General Administration of Customs demonstrate active roles in response to these cyber crimes and have jointly created certain evidence rules governing electronic data. In order to effectively punish smuggling and gambling offenders, the Supreme Court, the Supreme Procuratorate and the General Administration of Customs jointly issued 'Opinions on Particular Issues concerning Handling the Smuggling Cases' and 'Opinions on Particular Issues concerning Handling the Online Gambling Cases' in 2010 respectively.

It is stated that electronic evidence shall be collected, duplicated and fixed as criminal evidence. The electronic evidence mentioned here include the web page, surfing record, electronic mail, electronic contract, electronic transaction record, electronic account book, and other digital data stored in electronic equipments. The investigators shall make literal statement; record the brief, object, content of the case relevant to the process of collecting, duplicating and fixing electronic data. The maker(s) and/or holder(s) of electronic data shall sign or seal on these documents. Where the electronic data are stored in abroad computers or the criminal suspect does not attend at the time of collecting electronic data, or the holder(s) of the electronic data are not able to sign or refuse to sign, the witness who can testify the process of collecting, duplicating or fixing evidence shall sign or seal upon it. If necessary, the process shall be photographed or videotaped. The use of witness is to ensure the objectivity of source of evidence.

On June 25, 2010, China's Supreme People's Court, Supreme People's Procuratorate, Ministry of Public Security, Ministry of State Security, and Ministry of Justice formally published rules regarding the use of evidence in capital cases, i.e. 'Rules Concerning Questions About Examining and Judging Evidence in Death Penalty Cases' (hereafter Death Penalty Evidence Rules). The Death Penalty Evidence Rules may be used as a reference for implementation in handling other criminal cases and specify the collection, storage, retention, production, presentation and evaluation of evidence. Article 29 of the Death Penalty Evidence Rules specifies the issues of electronic evidence, such as electronic mail, electronic data exchange, online chat transcripts, blogs, mobile telephone text messages, or electronic signatures or domain names. It also provides the aspects that shall be considered in examining electronic evidence, the approach to evaluating (probative value) ICT-related evidence, etc.

According to this article 29, electronic evidence include electronic mail, electronic data exchange, online chat transcripts, blogs, mobile telephone text messages, or electronic signatures, domain names, etc. In examining electronic evidence, the following aspects must be emphasised: (1) whether electronic evidence stored on a storage medium such as a computer disk or CD has been submitted together with the printed version; (2) whether the time,

place, target, producer, production process, and equipment for the electronic evidence is clearly stated; (3) whether production, storage, transfer, access, collection, and presentation [of the electronic evidence] were carried out legally and whether individuals obtaining, producing, possessing, and witnessing the evidence affixed their signature or chop; (4) whether the content is authentic or whether it has undergone cutting, combination, tampering, or augmentation or other fabrication or alteration; (5) whether the electronic evidence is relevant to the facts of the case. The authenticity and relevance of electronic evidence should be examined in consideration of other case evidence. If there are questions about electronic evidence, an expert evaluation should be conducted.

On March 14, 2012, the new Criminal Procedure Law has been issued. In this law, electronic evidence becomes statutory evidence for the first time. Evidence rules on electronic data have been scarcely referred to in this law. It is only stipulated that according to article 52 (2) of the CPL, audio-visual materials and electronic data collected by the administrative organ in the process of law enforcement and investigating and handling cases may be used as evidence in criminal proceedings.

Article 93 and 94 of the Explanations of the Supreme Court as to Implementing Criminal Procedure Law (hereafter the Explanations) passed on November 5, 2012 further specify the rules concerning electronic evidence. The contents that shall be emphasized in the examination are provided in detail: (1) whether duplicated electronic evidence has been submitted together with the original storage medium; whether procurement and duplication of electronic data shall be conducted by more than two personnel, whether the integrity of electronic data can be ensured, whether there are annotations of process for procurement and duplication of evidence and the location of the original storage medium and the signatures thereupon; (2) whether the procedure and means of procurement conforms with the law and the related technical regulations, whether the record and inventory are attached and signed by the investigators, electronic data holders and observers; where it has been not signed by the holders, whether the reasons are indicated; where the electronic data are transferred from abroad or other region(s), whether the relevant circumstances are indicated; whether the norms, categories and formats of electronic data are clearly stated; (3) whether the content is authentic or whether it has undergone cutting, alteration or augmentation; (4) whether the electronic evidence is relevant to the facts of the case; (5) whether the electronic data relevant to the fact of the case are entirely collected. The circumstances where electronic data are inadmissible are also stated. Where electronic data are doubtful, they shall be tested or verified. Electronic data cannot serve as the grounds for conviction if one of the following circumstances occurs: (1) the authenticity cannot be ascertained after examination; (2) time, place, means, etc. of evidence production or procurement are questionable whilst necessary proof or reasonable explanation cannot be provided.

These laws and judicial interpretations are specific for electronic evidence. In a sense, the chain of stages, i.e. collecting/storing/retaining/producing/presenting/evaluating electronic evidence is more or less provided. There are some rules on admissibility of evidence that are specific for ICT-related information. It can be anticipated that evidence rules on electronic data will be dramatically developed soon. However, the evidence rules regarding electronic evidence is still at the initial stage. It is clear that the exclusion of illegally obtained electronic evidence is not specially provided by the rules.

3. ICT in the Trial Stage

3.1 Presentation, Cross-examination and Verification of Electronic Evidence

Only if the evidence is examined to be factual, can it be used as the basis for conviction. In the new Criminal Procedure Law in 2012, electronic evidence is ruled as a new type of statutory evidence. Thus, prior to being the basis for conviction, electronic evidence must undergo the above mentioned examination procedure of the court.

Electronic evidence has special attributes compared with traditional evidence, in that the information used to prove the case are stored in computer, movable disk, U disk, mobile, digital camera and other medium, and the content of information include characters, signals, pictures, videos, etc. Therefore, the procedure and manners for presentation, identification, cross-examination, verification shall be different from the traditional oral and physical evidence. The Criminal Procedure Law has not stipulated this aspect whilst articles 93 and 94 of the Explanations of the Supreme Court as to Implementing Criminal Procedure Law further supplement this to an extent:

(1) Manner of presenting electronic evidence; According to article 93(1) (2) of the Explanations, the submission of electronic evidence shall follow the principle of attaching the original storage medium, written record and inventory. Only if the original storage medium cannot be maintained, moved or otherwise shall be protected, handled, returned by the relevant departments, other storage medium, such as movable disk, U disk, can be used to collect and duplicate electronic evidence. Collection and duplication shall follow the statutory procedure. For example, the number of investigators must be not less than two. The written record and inventory shall be attached and must be signed by the investigators, electronic data holders and observers. Where the electronic data are transferred in a long-distance from abroad or other regions, the relevant conditions shall be denoted. And the magnitudes, formats and categories of electronic evidence shall be clearly noticed.

(2) Examination of electronic evidence; According to article 93(3)(4)(5) of the Explanations, in the process of examining evidence, the principle of authentication, the principle of relevance and the principle of expert verfication are used. The first principle requires that the court shall examine whether the content of evidence is authentic or whether it has undergone cutting, alteration or augmentation. The principle of relevance requires that the court shall examine whether the electronic evidence is relevant to the facts of the case. The principle of expert verification requires that where electronic data are doubtful, they shall be tested or verified by the expert agencies.

These provisions provide the guidelines for the court to examine and judge electronic evidence in legal practice. However, the existing provision is still inadequate, particularly demonstrated by lack of cross-examination rules regarding electronic evidence. Although adversarial mode cannot be entirely applied in criminal trials in China, the Criminal Procedure Law entrust the right to cross-examination to the prosecution and the accused. This right is mainly exercised in the stage of court examination. Because electronic data can be easily deleted, forged or tampered, it is difficult for the court to conduct a thorough investigation of the authenticity ex officio. Adequate cross-examination between the prosecution and the accused is the prerequisite for the judge to decide whether electronic data are authentic. According the provisions of the Criminal Procedure Law, if the court is doubtful to the authenticity of the evidence resulting from the cross-examination of two parties, expert verification shall be used to investigate out of the court. The Explanations do not specify the rules of cross-examination of electronic data. From the perspective of legal practice, the cross-examination may revolve around the formation, transmission, storage and collection of electronic evidence, the relevance of its content and the function of the technical device. This cross-examination shall confirm with the following rules:

(1) Presentation at court; the presenter shall display the content of original version of electronic data. When it cannot be identified or is difficult to identify, the extended evidence or other evidence can be used to collaborate. The expert opinion shall be presented together with electronic evidence.

(2) Explanation of the presenter; Where the presenter displays electronic evidence at court, he shall specify some basic information including time, location, manner of collection of electronic evidence and its content. When he cannot entirely and precisely clarify these information or make clear explanations, he shall apply for the assistance from the relevant expert from the court;

(3) Rules of allowing search. Where the presenter submit a number of computer materials whilst the contested party has dispute about whether the computer data transmitted fully and precisely reflect the information stored in the computer, the contested party shall be allowed to use directly search for information in the computer;

(4) Rules of appearance of the subjects who collect, procure, store and verify evidence. Where the prosecution and the accused questions the legitimacy and scientific nature of collection, procurement, storage and verification of electronic evidence, the relevant persons in charge of these activities shall present and undergo cross-examination.

(5) Rules of expert assistance; Based upon the technical attributes of electronic evidence, the prosecution and the accused shall be allowed to invite the experts to appear and be cross-examined with regard to technical issues or to enquiry with the expert witnesses.

3.2 Distant Interrogations by Satellite Connections

One application of ICT in criminal procedure is distant interrogations by satellite connections. Interrogation of the defendant is a compulsory process of the trial at first instance, the appeal trial and the procedure for review of death sentences in China. In practice, there are two ways to interrogate the defendant: one is the face to face interrogation which means that the defendant appears in court to answer the questions or the judges come to the detention center to interrogate the defendant. The other is the distant interrogations by satellite connections. Based on the Criminal Procedure Law, all first trial cases and some appeal cases should be trialed in open court and the defendant should appear in court. But some appeal trials and the procedure for review of death sentences can be conducted in closed court, where the distant interrogation may be applied. Based on the Article 544 of The Supreme People's Court Rules, the courts may interrogate the defendants by satellite connections. It is the first time in China to legalize the distant interrogation, although many district courts have practiced it for years. The distant interrogation can reduce the work and risk of escorting the defendants, save tremendous judicial expenditure and improve the efficiency of trial, especially in the procedure for review of death sentences. In China, only the Supreme Court has the power to approve the death penalty and the defendants are always detained in which the first trial court stands. It is unrealistic to escort the defendants to Beijing. The distant interrogation is necessary to solve this dilemma. However, the rules of distant interrogations are not enough to protect the defendants answering the judges from the upper courts or the Supreme Court with free will. For example, the defendants should have the right to silence or the right to counsel when being interrogated. Such rules are so important to protect the defendants' rights and safety that they should be incorporated into the Law in future.

3.3 Witnesses Testifying via Video Links

Another application of ICT in criminal procedure is that the witnesses present their testimony via video links. Based on the Criminal Procedure Law (2012) of China, the key witnesses should be testified in court so that the defense lawyer can confront them. If the witness refuses to appear, the court can take compulsory measures or punish him by 10 days detention. However, the witnesses cannot testify in court because of many excuses, such as long distance or worrying about the revenge of the parties. Using video links to allow witnesses to testify from afar can not only solve the difficulty of distance, but also guaranty the confrontation of the witnesses. Even more, using video testifying can protect the witnesses by covering their images or changing their voices. Nowadays, there is no law or judicial rules to regulate it in China, but many local courts have explored it in practice. With the spread of IT and ICT in China and the court system walking into the electronic age, witnesses testifying via video links will be legalized and used in wide range.

3.4 Informatization of the Courts

Informatization of the courts is an important goal of the courts construction in recent years. The Supreme Court

published construction norm in 2008 to require the informatization of all levels courts. According to the norm, the informatization of courts include arrangement of wire, demonstration of evidence, trial recording, management of audio and video equipments, center control of the trial, simultaneous interpretation, and so on. The courts which fit the norm will not only achieve the demonstration of multi-types of evidences, such as electronic evidence, real evidence, documentary evidence, audio and video evidence, but also realize the distance testifying, trial retransmit, cases management and digitalizing the trial proceedings. Some local courts have constructed such tribunals and use them in practice. The informatization can improve the work efficiency of courts and facilitate the litigants and counsel in knowing the proceedings, case paper and evidence in time. It will be the development direction of China's future courts.