DISCUSSION

GUARANTEES TO THE USE OF TELECOMMUNICATION TECHNOLOGY IN CRIMINAL PROCEEDINGS IN THE UNITED ARAB EMIRATES LEGISLATION

Mohammad Alkrisheh*

Abstract: The UAE legislature regulates the use of telecommunication technology in criminal proceedings pursuant to Decree Law No. (05) of year 2017 on the Use of Telecommunication Technology in Criminal Proceedings and Ministerial Decree No. (259) of year 2019 on the Procedural Manual for the Regulation of Litigation Using Electronic Means and Telecommunication in Criminal Proceedings. Despite the simple, fast and cost-effective justice this system achieves, it aims at achieving balance and equality between adversaries and supports the UAE trends in terms of using modern technology in transactions. Yet, it has emerged jurisprudential debate regarding the guarantees that can be provided to the accused when using the telecommunication technique. So, do such technologies provide the same guarantees provided by the conventional litigation proceedings?

Keywords: Telecommunication Technology, Teleprocedures, Remote Trial, Defendant's guarantees, UAE

1. INTRODUCTION

Technological development has brought about radical changes in all fields of life, resulting in the need to review the long-established legal principles and the introduction of new legal rules that keep pace with the issues that arise. As modern criminal policy, through its various mechanisms, tend to adopt several measures that aim at simplifying and expediting criminal trial proceedings in a manner that ensures the effectiveness of the Criminal Procedural Law; being the practical mechanism for the application of the Penal Law, without prejudice to the basic principles governing the criminal field.

The use of telecommunication technology in criminal proceedings is one of the most prominent modern methods designed to invest modern technology in the development of the justice system and increase the effectiveness of its work. For example, according to Braun et al (2016), 90% of all courts in the UK are quipped of videoconferences to facilitate and speed up trials. In light of the positive outcomes of using telecommunication technology, several legislations have adopted it in the field of criminal proceed-

^{*} Associate Professor, Dr. Mohammad Alkrisheh, of Criminal Law Public Law Department, College of Law Al Ain University, United Arab Emirates

¹ BRAUN, S., DAVITTI, E., DICERTO, S. The use of videoconferencing in proceedings conducted with the assistance of an interpreter. In: *Academia*. [online]. 2016 [2020-10-05]. Available at: .

ings.² In fact, several countries have adopted videoconference inside the courtroom, such as the USA, Canada, Australia.³ The UAE legislator has followed the same trend in the field of litigation proceedings when issuing Decree Law No. (05) of year 2017 on the use of telecommunication technology in criminal proceedings and Ministerial Decree No. (259) of year 2019 on the Procedural Manual for the Regulation of Litigation Using Electronic Means and Telecommunication in Criminal Proceedings.

The importance of this topic stems from its modern application in the UAE and the issues raise therefrom; how to establish balance between the effectiveness that ensures simplification of the proceedings sought by society to prosecute and punish criminals, on the one hand, and guaranteeing fair trials, on the other hand. This raises several questions: the scope of application of telecommunication technology, what guarantees can be provided to the parties of the criminal cases and does telecommunication technology provide the same guarantees as conventional litigation proceedings? Therefore, this research aims to answer these questions by explaining the use of telecommunication technology, the rationale for using it and the guarantees of using telecommunication technology.

2. WHAT IS THE USE TELECOMMUNICATION TECHNOLOGY?

2.1. Definition of the use of telecommunication technology

Generally speaking, video conferencing is defined as^{4,5}. video conference is a live, visual connection between two or more people residing in separate locations for the purpose of communication. At its simplest, video conferencing provides transmission of static images and text between two locations. At its most sophisticated, it provides transmission of full-motion video images and high-quality audio between multiple locations. (TecTaregt, 2017)

As far as the UAE law is concerned, the UAE legislator defines telecommunication technology in Article (1) of Federal Law No. (05) of year 2017 on the use of telecommunication technology in criminal proceedings as an "Audio-visual conversation between two parties or more through direct communication with each other via modern communication means to achieve remote attendance".

² Telecommunication technology was first used in Italy in the field of criminal investigation under Decree-Law No. (306) of year 1992. It is also widely used in the United States of America in domestic investigation and criminal prosecution and in international judicial assistance. Its use is also established by the European Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union for the year 2000, YAHYA, A. Remote Criminal Investigation and Trial. *Dar Al-Nahda Al-Arabiya*. 2016, p. 17.

³ DUMOULIN, L., LICOPPE, C. Trial at a Distance: Videoconference Technology as a Policy Tool? *International Conference in Public Policy*, 2015, Vol. 1, No. 5, pp. 211–231.

⁴ TechTarget [online]. 2017 [2020-10-05]. Available at: https://searchunifiedcommunications.techtarget.com/def-inition/video-conference.

⁵ FORELL, S., LAUFER, M., DIGIUSTO, E. Legal assistance by video conferencing: what is known? *Justice issues*. 2011, p. 3.

It is noted that the legislator confines the idea to conversation and required such conversation to be audio-visual simultaneously, through direct communication and not through an intermediary, where the work involved is limited to achieving remote attendance only.

2.2. Definition of Remote Trial

Remote trial is defined as "conducting a criminal trial through electronic connection of Visual Communication Technology (VCT) that allows the court to communicate with the litigating parties as if the trial is held within the judiciary domicile".⁶

The use of telecommunication technology in criminal proceedings requires the need to prepare and equip the places where the parties involved in the criminal case exist, by providing such places with the necessary means, in addition to the provision of a good communication network, ensuring a clear and continuous image and sound.⁷

The UAE legislator defines remote trial as "criminal proceedings undertaken by tele-communication technology to achieve attendance, publicity, confidentiality of investigations, pleadings, submission of documents, memos and verdicts issuance, whether in crimes investigation and collection of evidence or during investigation or trial".⁸

It is noted from the definition of the UAE legislator for remote trial that the use of telecommunication technology in criminal proceedings has not been limited to a certain stage of the criminal case, where this technology may be used at all stages in accordance with Article (4) of Law No. (05) of year 2017 on the use of telecommunication technology in criminal proceedings and Article (2) of Ministerial Decree No. (259) of year 2019 on the Procedural Manual for the Regulation of Litigation Using Electronic Means and Telecommunication in Criminal Proceedings, where the provisions of this Decree should apply to remote trials at any stage of the proceedings and in any of the proceedings stipulated in the Law to achieve attendance, publicity and confidentiality of the investigation.

The UAE legislator also granted discretionary powers to the judicial police, the public prosecution and the court to summon the parties litigating via telecommunication technology. The accused, as provided for in Article (6) of the aforementioned Federal Law, in the first hearing of the trial through telecommunication technology and in any degree, may request to appear in person before the court. In turn, the court should decide regarding that request by acceptance or refusal. Hence, the accused, his representative or the lawsuit-relevant parties should not refuse or accept to appear before the court in accordance with the system of communication technology; the entire matter is left to the discretion of the court. The legislator has not restricted that use by any conditions, nor to the cases consistent with the nature of this technology. Also, the legislator has not granted the

⁶ Al-DISMANI A. R. Remote Penal Trial in the Saudi System. *Nayef University for Security Sciences, MA Thesis, College of Criminal Justice, Department of Sharia and Law.* Riyadh, 2016, p. 3

⁷ *Justice, HM Courts & Tribunals Service* [online]. 2019 [2020-10-05]. Available at: https://www.justice.gov.uk/newsite/courts/video-conferences.

⁸ Article (1) of Law No. (05) of year 2017 on the Use of Telecommunication Technology in Criminal Proceedings and Article (1) of Ministerial Decree No. (259) of year 2019 on the Procedural Manual for Regulating Litigation Using Electronic Devices and Telecommunication in Procedures Penalty.

litigating parties the possibility of acceptance and rejection, which leads to the possibility of breaching fair trial guarantees.

Therefore, it is hoped that the legislator would limit the application of this technique to certain criminal trial proceedings, which nature is consistent with the technique, subject to the consent of the parties to the criminal case. The unlimited application of this technique in all stages of the criminal proceedings, without adherence to specific conditions in the scope of application, may lead to unsatisfactory results in some cases, especially when taking into consideration that the legislator is actually aiming from such mechanism to establish a serious balance between the public interest and the individual interest, given in guaranteeing the investigation and fair trials.

3. RATIONALE FOR THE USE OF TELECOMMUNICATION TECHNOLOGY

The use of telecommunication technology brings many advantages, including but not limited to the following:9

- 1. The use of telecommunication technology in remote trials depends on the used electronic correspondence system,¹⁰ which contributes to reducing the storage of documents in the traditional manner, thus reducing the likelihood of loss and accessibility of such documents through the electronic system.
- 2. The use of telecommunication technology shall result in the litigating parties obtaining prompt justice, as the use of such technologies should yield in decreasing the time wasted in summoning, as well as in the personal presence of the litigants or their representatives to the court in order to conduct the proceedings, which leads to promptly ending the dispute and stabilizing the legal situation of the litigants. However, the traditional procedure for summoning for or adjudicating a dispute in accordance with court proceedings in which the litigants or their attorneys appear before the court in person consume longer times due to the lengthy and complex proceedings.¹¹ This results in leaving the dispute before the judiciary for prolonged periods of time, causing instability and legal upheaval until the dispute is adjudicated.
- 3. The use of telecommunication technology in criminal proceedings should result in reducing the financial expenses incurred by the State in the transfer of accused persons from places of detention to the places where investigation and criminal hearings are held. The practical difficulties that may accompany the transfer of accused per-

⁹ BULRISS, M. E., FRANZ, J. F. U.S. Patent No. 7,061,521. Washington, DC: U.S. Patent and Trademark Office and Dumoulin, L., & Licoppe, C. 2006 (Ibid, 6-7).

¹⁰ Article (19) of Ministerial Decree No. (259) of year 2019 on the procedural manual for organizing litigation using electronic means and telecommunication in criminal proceedings provides for: (1) The records of remote litigation shall be recorded and kept electronically, whether they are wholly or partially conducted in accordance with the procedures set forth in this Decree. (2) Records of remote litigation shall be confidential and may not be accessed, copied or deleted from the electronic system unless authorized by the Public Prosecution or the Court, as the case may be. (3) The competent authority may report the litigation proceedings remotely in approved minutes, hard or soft copies, without the need for signature by the concerned parties.

¹¹ MANDIL, A. Remote Litigation (Legal Study). Kufa Journal for Legal and Political Sciences. 2014, Vol. 1, No. 21, p.108.

sons in custody for the case, especially those with serious criminal record, from their places of detention to the courtrooms and vice versa requires financial costs spent by the state. ¹² Such costs may include: transportation expenses and the required tight security, in addition to the fact that such process poses a serious risk to the safety and security of society by organized crime gangs, in an attempt to smuggle the accused in case opportunities emerge. ¹³

- 4. The use of telecommunication technology reduces the burden on judges and their assistants, as well as those dealing with the courts; this indirectly contributes to alleviating the judicial procedures carried out by judges and their assistants in a traditional way. Therefore, settling disputes in the shortest possible time saves the effort exerted by them, as well as the efforts of court officials and those dealing with the court, which represents an optimal use of human and technical resources.
- 5. The use of telecommunication technology protects the victims, witnesses and other collaborators with justice. The UAE legislature authorized the victims, witnesses, reporters and their attorneys, in accordance with the first paragraph of Article (04) of Ministerial Decree No. (259) of year 2019 on the Procedural Manual for the Regulation of Litigation Using Electronic Means and Telecommunication in Criminal Proceedings, to apply to the competent authority to undertake one or more of the trial proceedings via telecommunication technology, subject to the law, if serious reasons thereto exist, that would jeopardize their lives or basic interests if they testified.
- 6. The use of telecommunication technology strengthens the means of mutual judicial assistance between states in the judicial field. Telecommunication technology may be used as an additional means of international judicial assistance in criminal matters, in particular in the area of witness testimony, expert testimony, interrogation of the accused and confrontation between the litigating parties in criminal cases, where some of them are in another state other than the state undertaking the investigation or trial. This yields in avoiding the lengthy international judicial delegation proceedings and reducing the financial expenses required for the implementation of such delegation.

The UAE legislator has authorized the use of telecommunication technology to carry out the judicial delegations and assistance with foreign countries, in accordance with the provisions of Law No. (39) of year 2006 on international judicial cooperation in criminal matters.¹⁴

4. GUARANTEES OF THE USE OF TELECOMMUNICATION TECHNOLOGY

These guarantees can be described in several matters; such as ensuring the right of defence, the principle of publicity of hearings, recording and filing of remote trials records,

¹² BABCOCK, E., JOHANSEN, K. Remote Justice? Expanding The Use of interactive Video Teleconference in Minnesota Criminal Proceedings, William Mitchell Law Review. 2011, Vol. 37, No. 2, p 655.

¹³ YAHYA, A.ibid, p. 53.

¹⁴ AUTHORITY REQUESTS FOR ACCESS TO ELECTRONIC COMMUNICATION – legal overview. on use of telecommunication technology in criminal proceedings. *telenor group*. 2017, No. 5

the application of information security policies and the possibility of unloading remote proceedings, as well as the recognition of the authenticity of electronic signatures and documents, as follows:

4.1. Guaranteeing the Right of Defence

The right of defence is defined as the "right of an accused person to defend himself/herself and to refute the evidence submitted against him/her, and that the authority competent for the trial should not issue any decision against him/her before hearing and confronting him/her with the charges attributed to him". The right of defence is an essential element of the fair trial required by the UAE Constitution, Article (28)¹⁶.

Therefore, the UAE legislator granted the accused in a remote trial the right to defend himself/ herself, whether s/he exercised this right by himself/herself or through his defender. The Article (7) of Federal Law No. (05) of year 2017 on the use of telecommunication technology stipulates that "Taking into consideration the Criminal Procedure Law, the defendant's lawyer may meet his/her client or attend the investigation or trial proceedings with him/her through telecommunication, in coordination with the Competent Authority".

Paragraph (3) item (D) of Ministerial Decree No. (259) of year 2019 on Procedural Manual for the Regulation of Litigation Using Electronic Means and Telecommunication in Criminal Proceedings states that "After coordination with the competent authority, the accused's lawyer may meet with his/her client or appear with him/her during his/her remote trial. In that latter case, the lawyer should be technically ready as necessary and familiar with the use of the devices that enable him/her to communicate with the competent court, as per the circumstances, so that the sound and the image should be fully clear, provided that this shall take place in a place befitting the prestige of the court.

The lawyer should provide a summary of his defences, requests and proceedings orally in the remote trial as stipulated in item (E) of the third paragraph of Article (7) of Ministerial Decree No. (259) of year 2019 on the Procedural Manual for the Regulation of Litigation Using Electronic Means and Telecommunication in Criminal Proceedings and on the mechanism of submitting defence memoranda and lawsuit documents. Accordingly, the legislator authorized the lawyer, in accordance with Article (8) of the above-mentioned Ministerial Decree, to submit his/her memos and electronic documents to the court via e-mail and may communicate with the court secretary through this mail to confirm the receipt of those documents.

METWALLI, H. Guarantees of Justice in the Islamic Judiciary (1st ed.). Beirut: International Books House, 2003, p. 45.

¹⁶ Article 28 of the UAE Constitution stipulates: "Penalty is personal. An accused should be presumed innocent until proved guilty in a legal and fair trial. The accused shall have the right to appoint the person who is capable to conduct his defence during the trial. The law shall prescribe the cases in which the presence of a counsel for defence shall be assigned. Physical and moral abuse of an accused person is prohibited".

4.2. The principle of publicity

(public hearings – oral proceedings – confidentiality of investigations):

Publicity means that trial proceedings should be conducted in the presence of the public, who should be empowered, without discrimination, to have access to and be informed of the trial proceedings and to follow up on all debates, pleadings and decisions and judgments taken therein.¹⁷

In this regard, the provisions relating to publicity and confidentiality in remote trials should be applied in the same manner as in the Criminal Procedural Law ¹⁸ in accordance with the provisions of Article (3), which stipulates that "the provisions of attendance and publicity and the confidentiality of investigations provided for Federal Law No. (35/1992), should be fulfilled, as well as Decree Federal Law No. (12) of year 2009, referred to, if made through telecommunication technology in accordance with the provisions of this Law".

Trial publicity extends to include all procedures taken in all hearings. Therefore, publicity deals with all remote trial proceedings, including summoning of witnesses, charging the accused person and undertaking the investigations, as well as the statements of the complainant, the requests of the Public Prosecution and the defence of the accused. In case of multiple court hearings, they should all be conducted in public.

Article (7) of the abovementioned Ministerial Decree has confirmed that if telecommunication techniques are used to prove attendance and pleading, the following should be observed:

- 1. The accused, witnesses and experts should be summoned to appear before the criminal court remotely, in accordance with the provisions of the law. They may be notified electronically with the hearing, in accordance with the methods set forth in Article (9) of this Decree.
- 2. The technical officer should well-prepare the equipment used in the remote trial before commencing the hearing session and should deal promptly in cases of interruption or technical malfunction of any of them during the course of the hearing.
- 3. The lawyer should undertake the necessary technical preparation and use the devices that enable him to communicate with the respective judge or the competent court, as the case may be, so that the sound and image should be in full clarity, provided that it should be held in a place befitting the prestige of court.
- 4. During the hearing, the lawyer should provide an oral summary of his memos, requests and pleadings.
- 5. The proceedings of the hearing should be recorded electronically.
- 6. The Secretary should record what the judge or the litigating parties dictate during the hearing.

If the original for the remote trial is to be made public in accordance with Article (7) of the Ministerial Decree referred to, the question arises in this regard as to the penalty

¹⁷ NIMOUR, M. *Explanation of the Criminal Procedural Law (1st ed.)*. Amman: Dar Al Thaqafa for Publishing and Distribution, 2005, p. 640.

Article 161 of the Criminal Procedural Law states, "The hearing should be public but the court may for reasons relating to public policy or morals order that the action, in whole or in part be examined in closed session or prevent some class of people to attend."

of neglecting such publicity condition, since the UAE legislator has not referred to the invalidity of the proceedings that overlook the public procedure; therefore, it is believed that there is a need to develop a provision in this Decree that stipulates the invalidity of proceedings that lack the publicity condition and should be deemed as public order.

4.3. Remote Registration and Confidentiality of Records of Litigation:

In order to provide the litigants with a guarantee in terms of the use of telecommunication technology, it is essential for the records of the remote trial proceedings to be kept on the one hand, and preserve its confidentiality on the other hand, since without such guarantees, the litigants should not be encouraged to use such techniques.¹⁹

Records of remote litigation should be recorded and stored electronically, either done in whole or in part in accordance with the prescribed procedures. Such records should be confidential and may not be circulated, accessed, copied or even deleted from the electronic information system unless so is authorized by the Public Prosecution or the competent court, as the case may be.²⁰

Article (8) of Law No. (05) of year 2017 on the use of telecommunication technology in criminal proceedings stipulates that "proceedings should be recorded and kept remotely electronically and should be deemed confidential; should not be circulated, accessed or copied from the electronic information system, except as authorized by the Public Prosecution or the competent court, as the case may be.

It is therefore noted that:

 All remote proceedings (Teleprocedures) should be recorded and stored electronically, in addition to the possibility of printing them out and archiving them in hardcopies.

¹⁹ Article (5) of Law No. (01) of year 2006 on Electronic Transactions and Commerce regulates the preservation of electronic records, stipulating that: (1) If the law entails keeping any documents, records or information, for any reason, such condition should be deemed achieved if such documents, records or information are kept in the form of an electronic record, subject to the following:

⁽A) The electronic record should be kept in the form in which it was created, sent or received, or in a form that makes it possible to prove that it represents the information originally created, transmitted or received though it accurately;

⁽B) Maintaining the information kept in such a way that permits its use and later referring thereto;

⁽C) Keeping the information, if any, that enables specifying the origin and destination of the e-mail and the date and time of its transmission and receipt.

^{2.} The obligation to keep the documents, records or information in accordance with item (C) of paragraph (1) of this Article should not extend to any information that is necessarily and automatically created only to enable the transmission or receipt of the record.

^{3.} Any person may satisfy the requirements set forth in paragraph (1) of this Article with the assistance of the services of any other person, as long as that persons complies with the conditions set forth in that paragraph.

4. Nothing in this Article should prevent the following:

⁽A) The existence of a provision in another law that requires keeping the documents, records or information in the form of electronic records in accordance with a particular electronic information system, adopting certain procedures, or archiving or correspondence through a specific electronic medium.

⁽B) The right of government agencies to specify additional requirements for the maintenance of electronic records subject to their jurisdiction.

Article (8) of Law No. (05) of year 2017 on the use of telecommunication technology in criminal procedures, and Article (19) of the Ministerial Decree No. (259) of year 2019 on the Procedural Manual for Regulating Litigation Using Electronic Means and Telecommunication in criminal proceedings.

Such records should be confidential; they may not be circulated, copied or deleted from the electronic information system, unless so is authorized by the competent court.

4.4. Application of Information Security Policies.

The UAE legislator emphasizes the implementation of the information security policy in Article (9) of Law No. (05) of year 2017 on the use of telecommunication technology in criminal proceedings by stating that telecommunication technology is subject to the information security regulations and policies adopted in the UAE.²¹

In this regard, the UAE Telecommunication Regulatory Authority (TRA) has developed a "Cybersecurity Strategy – National Cybersecurity Strategy (NCSS)"²². Abu Dhabi Systems and Information Center (ADSIC) has also developed the Information Security Policy – Abu Dhabi Government²³.

The provision of information is intended to provide protection to the content of the data and information of remote trial proceedings against any attempts to change, amend or falsify during the stages of electronic exchange of the judicial papers and documents, which prevents others from accessing the said information, availing that only to persons authorized to access the electronic information system, e.g. judges and their assistants, lawyers and the litigating parties in the lawsuit, through providing them with an encrypted PIN number, so that they can view the most accurate details in their lawsuit. Thus, this ensures that unauthorized persons are prevented from hacking the electronic information system and accessing the lawsuit documents and papers.²⁴

²¹ This was confirmed by the Minister of Justice in Article (20) of the previous Decree, that "the techniques of telecommunication technology and the means provided for in this Decree are subject to the regulations and information security policies approved by the State."

²² According to the official portal of the UAE government, "The National Cybersecurity Strategy aims to secure information and communication in the UAE, in addition to building a secure and more informed society, aware of cybersecurity risks. This strategy focuses on five main themes:

Readiness and Prevention: This theme aims to raise the minimum level of protection of the electronic assets, achieving compliance with national standards of cybersecurity.

Detection, Response and Recovery: It aims to develop and consolidate the capabilities of electronic incident response management, response capabilities and the elimination of electronic threats.

Building national capacities: Raising awareness and educating citizens and national cadres, enhancing research and innovation capabilities in the field of cybersecurity.

Enhancing cooperation: Creating a collaborative national e-society, capitalizing on and contributing to international efforts.

Providing National Leadership: Developing a National Cybersecurity Strategy and Developing Coordination and Guidance Initiatives for the Implementation Process. UAE Government Portal and the Telecommunication Regulatory Authority. [online]. [2020-10-05]. Available at: .

²³ The first version of these policies was developed on 18. 11. 2008 and the second version was developed on 13. 1. 2013. [online]. 18. 11. 2008, 13. 1. 2013 [2020-10-05]. Available at: https://www.ecouncil.ae/Publications/information-security-policy-v2,en.pdf.

²⁴ El-TERSAWY, M. Lawsuit Proceeding Before Electronic Courts. Dar Al-Nahda Al-Arabeya. 2013, p. 109.

4.5. Reporting proceedings of remote litigation in minutes or hard/soft copies.

It may be required to report remote litigation proceedings in paper form, such as in the case of preparing a paper file for judicial application or at the concerned parties' request to have a copy of the case file, for example. It may also be required to report them in an electronic form (on electronic medium), as in the case of creating electronic files for judicial applications.

Thus, Article (10) of Law No. (05) of year 2017 on the use of telecommunication technology in criminal proceedings stipulates that "the competent authority may report Teleprocedures in in minutes, paper or Electronic Documents approved by it, without the need for the signature of the concerned parties".²⁵

Consequently, remote litigation proceedings may be reported, by the competent court or public prosecution, in paper or electronic minutes or documents, which should be approved by the competent authority without the need for the signatures of the concerned parties.

4.6. Recognition of Authenticity of Electronic Signatures and Documents

The legislator acknowledges the authenticity of electronic signatures and documents under Article No. (13) of Law No. (05) of year 2017 on the use of telecommunication technology in criminal proceedings, stating that "Electronic signature should have the same authenticity of the signatures referred to in the Federal Criminal Proceedings Law, if the provisions stipulated in the Law of Electronic Transactions and Commerce are observed. Electronic documents should be as authentic as the official and informative paper editions under the Federal Law of Criminal Proceedings once they meet the conditions and provisions stipulated in the Law of Electronic Transactions and Commerce.²⁶

²⁵ Article (19) item (3) of the Ministerial Decree No. (259) of year 2019 on the procedural guide to regulating litigation using electronic means and telecommunication technology in criminal proceedings.

²⁶ Article (12) of Ministerial Decree No. (259) of year 2019 on the procedural manual for organizing litigation using electronic means and telecommunication technology in criminal proceedings. The legislator confirmed the same in Article (17) item (3) bis of Law of Evidence in Civil and Commercial Matters, stipulating that "Electronic signature should have the same authenticity as the signatures referred to in this law if subject to the provisions stipulated in the Electronic Transactions and Commerce Law". This is in addition to Article (4) of the same article, which stipulates that: "Electronic writing, electronic editions and electronic records and documents should have the same authenticity granted to the written, official and customary edition included in the provisions of this Law, subject to the conditions and provisions stipulated in the Electronic Transactions and Commerce Law". On this topic, see:

YASEEN, A. R. Explanation of the Objective Rules for Proving (Traditional and Electronic) Civil and Commercial Transactions (3rd edition). *Dubai Police Academy*. 2008, pp. 92 et seq.

Electronic signature authenticity requirements for proving are as follows: (1) Electronic signature should be linked to a person to the extent that it can be distinguished from other persons. (2) Electronic signature should be sufficient to identify its owner. (3) Sole control of the owner of the signature on the electronic medium. (4) Electronic signature is closely related to the written signature. (5) Certified authentication; where the validity and integrity of the electronic signature are verified.

HIJAZI, A. The Legal System for Electronic Signature, "A Comparative Originating Study". *Dar Al-Qutub Al-Qanoneya*. 2007, pp. 443 et seq.

Al-ZUHAIRI, A. H. Provisions of Proof. *Bright Prospects for Publishing and Distribution*, pp. 135 et seq. According to Article (4) of Law No. (01) of year 2006, "Emails keep their legal effect or enforceability solely be-

In accordance with Article (14) of the above-mentioned Law, coordination should be held between the Ministry of Interior, Ministry of Justice, the judicial authorities and the relevant authorities with a view to provide electronic signature devices, prepare halls and provide modern means of communication to carry out Teleprocedures in the competent authorities, penal institutions and in other relevant authorities, in addition to provide the necessary technical and procedural assistance in accordance with the decisions issued by the Council of Ministers in this regard.²⁷

5. CONCLUSION

5.1. Results

- 1. The UAE legislator authorized the use of telecommunication technology in criminal proceedings at all stages of criminal cases (reasoning and investigation stage, preliminary investigation stage and the trial stage).
- 2. The legislator authorized the use of telecommunication technology in remote litigation proceedings; the legislator validated the authenticity of these proceedings if they are partially or fully undertaken by the use of telecommunication technology. S/he also gave the discretion in taking such actions remotely to the competent authority, as well as the possibility of requesting a transition from remote trial to trial in person.
- 3. The legislator authorized Teleprocedures outside the jurisdiction of the courts of any Emirate, using Teleprocedures for the execution of rogatory and judicial assistance with foreign countries, in accordance with the provisions included in Law No. (39) of year 2006 on international judicial cooperation in criminal matters.
- 4. The legislator developed several guarantees in the use of telecommunication technology: the right of defence, publicity of hearings, recording and filing of litigation records, application of information security policies, the possibility of reporting re-

cause they are in electronic form" and "information contained in emails keep their legal authenticity and validity even if included in brief, as long as the details of such information are available in the electronic system of the person who created the email, along with a reference in the email as to how to view such details. Article (10) of the same Law regulates the acceptance and authenticity of the electronic evidence by stating that: "(1) Email or electronic signature should not be rejected as an evidence because: (a) the letter or the signature should be in electronic form; (b) The letter or the signature is not original or in its original form, when such electronic letter or signature is the best evidence reasonably expected to be obtained by the person citing it. (2) In assessing the authenticity of electronic information in evidence, the following elements should be taken into account: (a) The extent to which the method of entering, creating, processing, storing, assessing or sending information can be relied on. (b) The extent to which the method used in maintaining the integrity of information can be relied on, (c) The extent to which the source of information, if known, can be relied on, (d) The extent to which the method used in ascertaining the identity of the creator can be relied on (e) Any other element related to the subject. (3) Unless proven otherwise, it is assumed that a protected electronic signature: (a) should be relied upon; (b) is the signature of the person to whom it relates; (c) electronic signature has been affixed by that person with the intent of signing or authenticating the email attributed to him/her. (4) Unless proven otherwise, it is assumed that the protected electronic record: (a) has not been changed since it was created; (b) acknowledged.

²⁷ Cf. KRAWITZ, M., HOWARD, J. Should Australian courts give more witnesses the right to Skype? *Journal of Judicial Administration*. 2015, Vol. 25, pp. 44–63.

- mote proceedings (Teleprocedures) and the recognition of the authenticity of electronic signatures and documents.
- 5. The use of telecommunication technology in the trial shall in no way prejudice the oral and confrontational rules, as it allows the accused to see, hear and discuss the investigating authority or the tribunal and other litigants in the proceedings.

5.2. Recommendations

- 1. We hope that the legislator would limit the use of telecommunication technology to certain criminal trial proceedings that are consistent with the nature of this technique, subject to the consent of the parties to the criminal case.
- We hope the legislator would provide for the invalidity of the proceedings using telecommunication technology without publicity and considering that of public order.
- 3. We suggest the use of 3D imaging technique to personify the accused, in lieu of VCT, so that the opinion of the judge should be better formed.