DIGITAL EVIDENCE AS A MEANS OF PROOF IN CRIMINAL PROCEEDINGS

OSCO ESCOBEDO MIGUEL ANGEL¹, CHIPANA FERNÁNDEZ YOLANDA MARIBEL MERCEDES², QUIÑONES LI AURA ELISA³, DÍAZ-PÉREZ JOSÉ JOAQUIN⁴, CALVO DE OLIVEIRA DIAZ DENY GIOVANNA⁵, GARCIA QUI SPE GLADYS BEATRIZ⁶.

¹ ORCID: 0000-0003-1885-3549. César Vallejo University - Lima - Perú.
² ORCID: 0000-0002-8609-3409. César Vallejo University - Lima - Perú.
³ ORCID: 0000-0002-5105-1188. César Vallejo University - Lima - Perú.
⁴ ORCID: 0000-0003-1663-8626. César Vallejo University - Lima - Perú.
⁵ ORCID: 0000-0002-8907-676X. César Vallejo University - Lima - Perú.
⁶ ORCID: 0000-0002-3064-7919. César Vallejo University - Lima - Perú.

Email: moscoe@ucv.edu.pe¹, ychipana@ucv.edu.pe², aquinonesl@ucv.edu.pe³, jdiazpe@ucv.edu.pe⁴, denycalvo@gmail.com⁵, Ggarciaqu@ucvvirtual.edu.pe⁶

Abstract: Digital evidence is information stored on a technological device that is propagated through cyberspace. The computer record is accessible by people, electronics, or computers and is collected from a digital device. The purpose of this investigation is to specify the correct treatment of digital evidence to be admissible within the judicial process, respecting guarantees and fundamental rights of people. Also identify the procedure for obtaining, preserving, analyzing, and presenting digital evidence before the Judge. This theoretical review of sources was prepared under the systematic verification methodology, usable in the Scopus, Ebscohost, Scielo, Core, IG Global, Ciencia Latina, Latindex, Jurn, Openaire, and Redalyc databases of advantageous configuration and in Spanish for the last 5 years. The exploration and review of scientific production were used, selecting the expressions of: "criminal process", "digital evidence" and "evidence". Based on the results obtained, the importance of the treatment of digital evidence as an instrument of proof is inferred, for the evaluation of the judge as an element of conviction in a criminal process. It is concluded that digital evidence has particular characteristics that distinguish it from physical evidence and procedural rules do not regulate its proper treatment, and are currently considered documentary evidence.

Keywords: digital evidence; evidence and criminal proceedings

Table of Contents

1. INTRODUCTION
2. METHODOLOGY
3. DISCUSSION
4. FINAL CONSIDERATIONS

1. INTRODUCTION

Digital evidence is unknown in the judicial environment, especially by judges, prosecutors, and legal professionals. Human life is being influenced by the causal relationship between technological innovation and the usefulness of digital tools or devices for any activity, as Montecé et al. (2020) showed. The International Organisation for Computer Evidence states that digital evidence is information produced, transmitted, or stored by electronic media that is used in legal proceedings, internal cybersecurity investigations, malware analysis, etc. As an example, the procedures for obtaining an email transaction differ from those for obtaining audit process files or logs in a database (Ochoa, 2018). Digital evidence has certain characteristics that make it very particular, it is easy to duplicate and transmit, weak to be changed and erased, contaminated by other new data, and sensitive to time, it is also transnational and jurisdictional, as it breaks physical borders (Prayudi, 2020). Added to this is the technological progress generated by new ways of storing information, such as in the cloud, giving rise to the new possibility of accessing it and getting digital evidence (Palomo,
It is essential to alter the paradigms that enclose the means of proof and comprehend that digital evidence signals new processes distinct from physical evidence. From the above, it is important to specify that digital evidence needs experts with knowledge of special techniques. It is necessary to take into consideration the characteristics of volatility, the care of the collection of files that frequently are not possible to observe, as well as knowing what information is going to be stored, as it presents formats that are sometimes complicated to understand, and therefore requires technological translation to be qualified by the operators of the criminal system or the parties (Rodrigo, 2021).

Regarding, the procedure for the admissibility of digital evidence is the focus of the research. There are several processes that give rise to loopholes as a consequence of the application of written procedural rules for physical evidence, and not for digital evidence. In the international context, few countries have appropriate legislation on cybercrime and the preservation of evidence (Molina et al. 2019). This is compounded by digital illiteracy and the technological gap among legal professionals. The administration of justice requires trained computer professionals to examine and collate the evidence provided by the parties, within the computer environment, protecting it from the modifications to which it is exposed, giving it an environment of authenticity in the evidentiary phase, and assistance to justice operators, incorporating technical knowledge in the use of digital media; it is, therefore, advisable to educate the community about the interest of digital evidence, with emphasis on their rights (Alshaibani, 2021). In Peru there is no procedural norm that standardizes the collection, obtaining, conservation, and analysis of digital evidence, as well as the lack of technology of computer devices, applications, and licensing; and the delay in the work of experts on digital evidence; as well as the lack of training of justice operators and police forces, in techniques for the treatment of digital evidence, regarding the obtaining, collection, conservation, and analysis, that allow ensuring its originality, to which is added the doubt about the presentation of the evidential means in digital format. There are no specific rules, as the procedures are processed on paper, in traditional files, so the method applied in the presentation of digital evidence will be important when analyzing its probative value (Appendino et al. 2019).

Likewise, the importance of the research is to know the adequate treatment of the digital evidence in all its phases and the appropriate application of the procedural norms by the justice operators. Finally, the research seeks to establish the normative procedures for the correct treatment of digital evidence, as well as to determine the difference between physical evidence and digital evidence in the procedural norm and the procedures for obtaining, preserving, analyzing, and presenting digital evidence.

2. METHODOLOGY

The present study was carried out using a qualitative approach, through a systematic review of scientific production related to the research topic, by searching for information in journals indexed in Scopus, Ebscohost, Scielo, Core, IG Global, Ciencia Latina, Latinindex, Jurn, Openaire, and Redalyc, using the keywords Digital Evidence, Means of Evidence, and Criminal Procedure as the starting point for the search.

It carried a conceptual search out using mentions of preferential and complementary studies found in the digital search results. It carried the research out in Scopus, Ebscohost, Scielo, Core, IG Global, Latin Science, Latinindex, Jurn, Openaire, and Redalyc databases, with a search by title, synthesis, and the keywords Digital Evidence, Means of Evidence, and Criminal Procedure. It was developed within a structured verification of scientific articles, which contained: the identity of the author(s), year, title, origin, DOI, and citations. The scope of the data was carried out over a period of only 5 years.

The researcher carried the process of compiling the scientific research out. The studies were chosen in two periods. The first step was the re-examination of titles and synthesis of citations found with various information search operators and contrast by Boléan, AND, and OR logical operators, linking digital evidence to proof in criminal proceedings. A sample of 45 results was obtained from the
systematic search and combination. Scanning the full text of the selected research to ratify its eligibility, we gave 20 articles.

Theoretical literature reviews that did not form part of the research topic were excluded. A limited amount of research on digital evidence as proof in criminal proceedings was found, the aim of this review is to analyze the existing knowledge on the topic in question and to identify the study products, training designs, classes, variables, and weightings. The following were chosen as the primary products: empirical inquiries, study events, experiences, and the like.

**Results**

The following table describes each of the selected articles according to their relevance:

<table>
<thead>
<tr>
<th>Author(s)/Year/Title</th>
<th>Database</th>
<th>Type of Study</th>
<th>Methods</th>
<th>Results</th>
<th>Conclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abigaila (2021)</td>
<td>Scopus</td>
<td>Qualitative</td>
<td>Descriptive study</td>
<td>Digital evidence is a distinct type of evidence because of its scientific characteristics and standard specifications.</td>
<td></td>
</tr>
<tr>
<td>Apprendico et al. (2019)</td>
<td>Core</td>
<td>Qualitative</td>
<td>Theoretical study</td>
<td>Getting, preserving and presenting digital evidence in a court case is not so simple because of drawbacks from its definition, format, and treatment in the judicial process.</td>
<td></td>
</tr>
<tr>
<td>Aichert, Costelin &amp; T. Berti (2016)</td>
<td>Scielo</td>
<td>Qualitative</td>
<td>Descriptive study</td>
<td>It analyses contain of the Budapest Convention, identifying matters that national legislation should reform in order to adapt to the treaty.</td>
<td></td>
</tr>
<tr>
<td>Borel R. (2015)</td>
<td>Scielo</td>
<td>Descriptive study</td>
<td>Descriptive study</td>
<td>The challenge of criminal proceedings for the present century is to produce and present computer crime conduct using the means of evidence admitted in law.</td>
<td></td>
</tr>
<tr>
<td>Eren, M. &amp; Morina, M. &amp; Papiagoz, E. (2017)</td>
<td>Scopus</td>
<td>Qualitative</td>
<td>Descriptive study</td>
<td>Digital evidence is a means of proof that can ascertain the material truth of the event.</td>
<td></td>
</tr>
<tr>
<td>Estrada &amp; T. More K. &amp; Sanché (2018)</td>
<td>Scopus</td>
<td>Qualitative</td>
<td>Deductive study</td>
<td>The relationship between memory and the handling of digital evidence in a forensic investigation is based on the analysis of techniques, methodologies, and tools that facilitate the collection of forensic information.</td>
<td></td>
</tr>
<tr>
<td>Gómez-Aguirre &amp; D. (2020)</td>
<td>Redacx</td>
<td>Qualitative</td>
<td>Documentary study</td>
<td>It identifies the legislative and jurisprudential background of digital evidence in Colombia, in order to detail its treatment in the judicial process.</td>
<td></td>
</tr>
<tr>
<td>Gómez, D., Acero, J. &amp; Aquino (2021)</td>
<td>Scielo</td>
<td>Qualitative</td>
<td>Descriptive study</td>
<td>Digital evidence is easy to change, so it is necessary to verify authenticity. This has led to the need to guarantee the authenticity of digital evidence.</td>
<td></td>
</tr>
<tr>
<td>Illoia et al. (2019)</td>
<td>Latindex</td>
<td>Descriptive</td>
<td>Comparative study</td>
<td>Evidence must meet maximum standards of relevance and reliability to be admitted.</td>
<td></td>
</tr>
<tr>
<td>Isla de-Marcos &amp; A. &amp; Zuñiga (2020)</td>
<td>Openlay</td>
<td>Qualitative</td>
<td>Descriptive study</td>
<td>To support the effectiveness of a prosecution case, the correct application of the chain of custody within the procedural investigation is critical.</td>
<td></td>
</tr>
<tr>
<td>Nadia y Garcia (2018)</td>
<td>Redacx</td>
<td>Qualitative</td>
<td>Qualitative approach</td>
<td>The digital information attaches facts to the prosecutorial investigation, which is introduced into the process as evidence, complying with procedural rules.</td>
<td></td>
</tr>
<tr>
<td>Octavio P. (2018)</td>
<td>Redacx</td>
<td>Qualitative</td>
<td>Comparative study</td>
<td>The treatment of digital evidence is necessary in forensic investigation, through analysis and local practices.</td>
<td></td>
</tr>
<tr>
<td>Ochino, P. (2021)</td>
<td>Scielo</td>
<td>Qualitative</td>
<td>Descriptive study</td>
<td>Digital evidence allows to know the origin, time, and source of digital evidence in order to establish reliable evidence and to follow the judicial processes.</td>
<td></td>
</tr>
</tbody>
</table>
Table 1: Authors of texts and indexed scientific journals whose contents strengthen the topic of study.

Source: Own elaboration

The first article in table 1 by Alshaibani was written in Saudi Arabia. Alshaibani stated that collecting evidence with ICTs violates a person’s right to privacy, accessing sensitive personal data stored in their intimate environment and unrelated to the event. He concludes that electronic evidence can be subject to manipulation like any other conventional evidence, but nevertheless, technologically generated evidence shows accurate and complete information.

Antwi and Venter developed the second research. The admissibility of digital evidence is a key issue arising from the application of digital forensics in case law. They conclude that advances in ICTs have an impact on the technical and legal requirements that create the basis for the admissibility of digital evidence.

The third study was by Appendino, Parra del Gallo, and Aprile in Argentina. Qualitative approach and theoretical analysis. The article reflects the drawbacks from its definition, mention of current legislation, treatment in the judicial process, and its implication in the field of computer forensic digital evidence. They concluded that technology cannot be separated from the criminal act, with technological dependence becoming ever stronger.

The fourth article is a study developed in Chile by Becker and Viollier. Qualitative research and descriptive method. It aimed the ratification of the Budapest Convention at developing a common criminal policy against cybercrime, through the standardization of fundamental concepts and the treatment of criminal, substantive, and procedural legislation. They conclude that the implementation of the Convention will make it possible to identify the amendments incorporated into the draft law and recommendations that can be used to improve the proposed legislation.

The fifth article is a study carried out in Bolivia, by Borges. Qualitative study and descriptive method. In the jurisdictional sphere of punishment, the cases in which cybercrimes are judged present electronic evidence as the only element of proof. He concludes that further research on the subject must be carried out, making use of comparative law to tackle cybercrime, which will soon become a mandate for proceduralists.

The sixth study carried out by Bravo in Peru. Qualitative and descriptive approach. The freedom of evidence is manifested in the provision and admission of evidence, as well as in the evaluation of evidence. He concludes that the main constitutional legal conceptions of evidentiary freedom consider that the Peruvian procedural system is inclined towards the free rational assessment of evidence.

The seventh study by Bujosa, Bustamante and Toro, research carried out in Colombia. Qualitative analysis of descriptive method of texts. Digital evidence presents notions and characteristics, as well as problems in this type of evidence in criminal proceedings. They conclude that the elements that make up digital evidence are authenticity, integrity, inalterability, traceability, recoverability and conservation.
The eighth research, developed by Eren, Morina and Papajorgji; elaborated in Turkey. Digital evidence is abstract in essence in relation to other classical evidence and is only found in digital systems. They conclude that the most significant distinguishing feature of digital evidence is that it is manipulable, intangible, invisible and virtual.

The ninth article by Estupiñan, Mora and Santiago in Colombia. Qualitative deductive scope. They refer that computer forensics has as a fundamental competence to collect sufficient evidence to be used in a process and to serve as a reasoning against cybercriminals. They conclude that the information that passes through the network is volatile, which is why it is necessary to have the necessary tools to generate digital evidence that is admissible in court.

Gómez’s tenth article was performed in Colombia. It shows the reality of the problem of assessing technological evidence in cases of unlawfulness. He concludes that digital evidence cannot be denied effectiveness and evidential validity because it is in the form of bytes, and the authenticity of the content must be established.

The eleventh paper by Gómez, Acevedo, and Aguirre was a study developed in Chile. They indicate that to check the integrity as well as the authenticity of digital evidence, a tool called hash code should be used, which is ideal for securing digital evidence. They conclude that the hash code is a mathematical algorithm that ensures that digital evidence is not altered or modified.

The twelfth research concerns the article developed by Molina, Santillán, Luna, Lozada, and Guaiña; performed in Ecuador. It is a qualitative study and applies the descriptive and comparative methods. Currently, every institution generates digital information that, by legal mandate, must be preserved by means of techniques or methods that make it technically possible to make digital information available. They conclude that the PREDEC model is capable of aligning the preservation objectives of digital evidence with the aspects of admissibility and integrity of evidence.

The thirteenth article was developed in Ecuador by Montecé and Izquierdo. Qualitative inquiry and descriptive method. The aim is to determine the difficulties encountered in the procedure of chain of custody of digital evidence, which could lead to the contamination of evidence. They conclude that training on new digital evidence custody procedures is an urgent need.

The fourteenth section of Naula and Quevedo is in Ecuador. Qualitative, legal analytical methodology. They emphasize the due process that states have an obligation to apply in criminal matters by means of the procedural guarantees that the Public Prosecutor’s Office must comply with. They conclude that videos, data, and photographs are instruments that citizens can use, including the recording of events on a mobile phone, which constitutes a source of evidence.

Ochoa’s fifteenth research was a study carried out in Ecuador. Qualitative analysis of the comparative descriptive method. Digital evidence is volatile, referring to temporary information. Non-volatile remains in memory, even when the device is turned off. It concludes that a structured process of evidence handling is required to enable learning from and prosecution of security incidents, with international cooperation to enable the protection of records.

Bravo’s sixth study in Peru. Qualitative and descriptive approach. It manifested the freedom of evidence in the provision and admission of evidence, as well as in the evaluation of evidence. He concludes that the main constitutional legal conceptions of evidentiary freedom consider that it inclined the Peruvian procedural system towards the free rational assessment of the evidence.

The sixteenth study was carried out by Palomo and Guillet in Argentina. Qualitative approach and theoretical analysis. Procedural law must become more flexible and streamline its measures since with the advent of cloud computing, it will certainly often happen that it is not known in which country the server that holds the data required for the investigation is located. They conclude that it is necessary to make an effort to adapt to the legal situation of aspects such as security and privacy protection around these systems.

The seventeenth research was developed in Indonesia by Praduyi, Ashari, and Priyambodo. It explores qualitative exploration and applies the descriptive method. Digital evidence and electronic evidence are often confused and used, both in praxis and theory, with the increasing complexity and problem of cybercrime, which must begin to be differentiated. They conclude that physical and digital evidence is a unit of evidence in the process of investigating cybercrime cases.
The eighteenth scientific publication by the authors Puetate, Coka, and Méndez, a study developed in Ecuador. The methodological approach is qualitative and descriptive. The aim is to ensure that electronic information content has legal relevance, using effective and truthful evidentiary elements, to incorporate them into a given process. They conclude that one of the fundamental rights of human beings is the right to health and, in this case, the use of technology.

The nineteenth study developed in Brazil, authored by Rodrigo. Qualitative research, and legal analytical method. It refers to those who participate in the criminal process that can access and guide the procedure and the required understandings, true or possible, about the hypothesis to be investigated and known. He concludes that digital environments contain spaces of privacy for individuals and a judicial authority must find and order that state interference in the criminal process and with objective elements to support it.

Samonova’s twentieth article in Ukraine. Qualitative, comparative methodology. Courts consider the evidentiary value of metadata and the possibility of not using it. Metadata called data from data is very useful for proving its admissibility and reliability. It concludes that electronic evidence is used uncertainly and chaotically, without considering its performance and characteristics.

3. DISCUSSION

Before referring to digital evidence in our study, we must clearly specify what we mean by evidence in the context of criminal proceedings. To this effect, we must indicate that evidence requires the need to be examined and checked with every object that relates it to the fact, in order to know as closely as possible, the truth of the circumstances under investigation. Let us appreciate the concept from the angle of the process, where the parties access and conduct themselves knowing the procedures such as testimonies, expert opinions and others about the facts, subject of investigation within the criminal process, being of great utility for the judge by allowing him to have a better knowledge of the process. It is pertinent to specify that the means of evidence will be admitted if it complies with the precepts of respect for the fundamental rights and duties of individuals (Eren et al. 2021).

It is important to establish the difference between the source of evidence and the means of evidence; as far as the source of evidence is concerned, these are components that exist in reality and the object of evidence and what is to be proved is born, for example witnesses, documents, experts, etc. With regard to the means of proof, it is clear to state that it is any procedure that seeks to incorporate within the due process the objects of proof in relation to the facts that will guide the judge to a better conviction in the trial (Naula & Quevedo, 2022). It is relevant to indicate and emphasize due process, explaining that as a fundamental right of individuals, the state is required to apply it in a fair manner by the judge. The State must provide the minimum guarantees to ensure a fair trial and permanent and free access to the information and documents safeguarded by the judicial system.

Regarding to the means of proof in the admission of digital evidence, we must point out that in the absence of regulation in procedural legislation, there is a need to incorporate the principle of freedom of proof, with analogy as its basis. In this respect, I share this position, since due to the need and absence of the Criminal Procedural Codes of the treatment of digital evidence, these were created to admit physical evidence. This principle of evidential freedom establishes the power to use any means of evidence, with the viability of the law, as long as it does not transgress the guarantees and rights of the person, the faculties of the procedural subjects, to be able to incorporate it as an analogous means of evidence (Bravo, 2022).

On the other hand, it is important to specify the difference between digital evidence and electronic evidence. Digital evidence is evidence in the form of digital files generated by people’s own free will, such as photographs, Word documents, conversations, chats and various others, also generated without the user’s knowledge, such as metadata or log files. On the other hand, electronic evidence has the particularity that it is physical and visible. But what we must underline is that both types of evidence are significant for an investigation.

It is relevant to indicate that the procedural rules currently do not specify the concept of digital evidence and there is insufficient regulation generating legal uncertainty (Borges, 2018). In this
regard, different organizations have defined the concept, but the one that comes closest is that of the International Organization for Computer Evidence, which states that it is the information that is transmitted through digital devices after having been created and stored that could be used in a judicial process. I consider that the particular value of digital evidence would be that each country should regulate its procedural legislation to allow its use as evidence collected in the process. Digital evidence in terms of its content can be divided into records that are produced on the digital device, such as records of events, transactions or audits, records that are not generated but stored on the device and records that are generated by the user and stored on the device. It is also mentioned that the digital evidence collected within an investigation is not only that which is obtained as a result of a search and seizure, but also that which is obtained from the data generated when connecting to the network, such as tags, logs and metadata.

We should not leave aside the principles of relevance, reliability and sufficiency of digital evidence, in accordance with ISO/IEC 27037:2012, as these principles are essential and demanding for its admissibility in an investigation and judicial process. If the evidence does not meet these conditions, it will be considered irrelevant and will be excluded as probative elements, which is why it is important to validate its particularity for greater reliability, and it must be audited from the moment it is obtained and be verified and demonstrated, likewise in terms of its integrity, it must contain the appropriate elements that support and verify it through the participation of a computer expert (Samonova, 2022).

Regarding the volatility of digital evidence, we must specify that it is all information that remains temporarily on the device and non-volatile information that is permanently on the device, even when it is switched off. In addition to this, it is vital to specify the characteristics of digital evidence: firstly; they are not visible, both to non-technical users of technology and even to law enforcement officers and police officers. Likewise, digital evidence is fragile and volatile, because it is stored in digital devices and any action performed on it could alter its state, which is why it is necessary to establish special mechanisms to protect it during the procedure known as a chain of custody. They can be altered or destroyed, either by the action of the user of the digital device when copying or recording it or by the action of the operating system installed on the device being used. They are massive, making it difficult to locate the information required in the process. It can be copied without any limit. It performed technically this procedure and with the appropriate tools, it can clone the information while maintaining the originality of its characteristics. On the other hand, it is also necessary to indicate that with regard to the collection of digital evidence, it must be admissible in order to be used in the judicial process. It must be authentic and undoubtedly related to the fact. It must be complete and sufficient to enable us to have a full view of the fact. It must be reliable, so that its examination provides assurance of its authenticity and it must be credible, understandable and convincing for judges (Gómez, 2020).

In view of the above, digital evidence has undoubtedly generated as a consequence a problem in terms of the criminal process with regard to the new means of proof in relation to the traditional means of proof, this is due to the use of technologies. At present, the legal examination of digital evidence is complex and requires the safeguarding of constitutional guarantees that provide certainty as an element of proof. Also, these new evidences denote particularities regarding their manipulation as a consequence of the level of exhibition in the network and digital media operated by the users, that is why the digital evidence seeks to have the legal value of the information that it includes, so that it can be validated in a judicial process, being indispensable for its admission that the digital evidence is subject to processes that allow to evaluate its reliability, originality and contribution to the process.

Digital evidence is currently being treated procedurally as if it had developed the action in a physical space, generating consequently physical evidence, the iter crimines having been performed within cyberspace, this treatment has generated certain problems. Digital evidence raises complexities that must be taken into consideration, such as the fact of accessing personal information, violating the sensitive personal data of parties unrelated to the investigation, opening the way to future nullities for exceeding the limits of respect for their fundamental rights, thus exposing the evidence obtained.
The problems that digital evidence may face relate to aspects of its authenticity, admissibility and legality which, if not preserved, may lead to its irrelevance and lack of probative value because it does not prove credibility. It is therefore feasible to adequately analyze digital evidence within the forms of reasonableness, logic and veracity in the account, so that it is credible and convincing and does not have difficulties to be admitted within a judicial process. Thus, the Budapest Convention recommends guidelines on the considerations to be taken into account with means of evidence, such as the securing of data, production order of data, as well as the recording and seizure of data (Becker & Viollier, 2021).

It must be considered that digital evidence must be collected, transferred and guarded correctly to ensure its legitimacy, taking care that it is not altered and that it is secure in its validity and effectiveness in the process. A fundamental aspect is also that the digital evidence enters correctly into the process without being conditioned by any branch of law. Likewise, it is important to appreciate how the process is dealt with in the event that it challenged the digital evidence, and how the technical defense knows how to debate and argue so that the means of evidence is timely and valued by the judge. This is why it is necessary for the evidence to be provided by means of an expert witness, with the expert being competent to perform his analysis, review and the appropriateness of the evidence, providing the process with relevant information that will lead the judge to correct decisions in the conclusion of the process.

The process of collecting digital evidence presents us with two scenarios, the first when the evidence is within the territory, where the criminal law reaches it and investigations can be performed without inconvenience. The second is when the evidence is outside the jurisdiction. In this situation, the procedural arrangement is the letter rogatory, for which the judge in charge of the process must request the cooperation of the judge of the country where the evidence is located or the fact is being investigated. In this regard, this procedure is a formality, a situation which leads to long waiting times and often results in the collection of evidence being ineffective and therefore not being admitted. Likewise, with regard to the location of evidence, today there is a new problem called the cloud, which is defined as the place where information is stored in large volumes, from where information is accessed and housed in equipment called servers. This type of situation is not regulated in the Procedural Codes either, we must be clear that when accessing information in cyberspace through the Internet, this fact redirect us to a certain physical point where the information is located, which is delimited by a certain jurisdiction, where the server may be hosted. Therefore, when requesting information, we must promptly resort to international conventions and cooperation in order to obtain it, as doing otherwise could infringe the principle of territoriality of that country. The Budapest Convention is the international standard that offers the best alternatives when it comes to transborder data, and many countries have already acceded to it, including Peru.

We must bear in mind the need for digital evidence to be preserved, conserved and protected in the chain of custody through an expert procedure, for which it is very necessary that justice operators and police officers are trained to ensure that these procedures are properly executed in order to ensure the success of the admissibility of digital evidence (Bujosa et al., 2021). This expert procedure is performed through computer forensics, being that this science is responsible for executing a set of procedures and the application of techniques, to identify, collect, extract, preserve, document, presenting digital evidence in order to be accepted within a judicial process (Estupiñan, 2019). Computer forensics currently serves as a support and great help to judges in different judicial processes.

Another of the actions that would effectively serve to verify the integrity and authenticity of digital evidence is through the use of the tool called Hash, which is an algorithm that allows us to be sure that communications or files have not been altered, it is performed through an examination generating a record in the form of a string of characters before and after the communication of the data, if these are identical it is interpreted that they have not been altered. The Hash is the digital fingerprint of a file that allows us to verify its integrity and authenticity (Gómez et al, 2021). Also, when digital devices communicate with each other, they do so through an identification protocol called IP Internet Protocol, to connect the devices to each other, they are identified by IPs that
perform the function of redirecting data traffic; it is important to note that each device that connects to the Internet has an IP address. Additionally, it is important the copies that are made through computer forensic imaging, this procedure consists of making an exact copy that is made from a device where the information is stored, it performs a process called bit by bit copy that duplicates exactly to a storage medium other than the origin. Another purpose of computer forensic imaging is to search for and obtain relevant information that could have been deleted or hidden and that could be used successfully in a judicial process (Antwi & Venter, 2018). And finally, it is important in the processes to consider as a probative value of digital evidence the metadata which means data, very useful information, as it describes in detail the characteristics of any type of file such as when it was created, when it was modified, file type, geolocation data of images and numerous others that are very useful to demonstrate admissibility and reliability (Samonova, 2022).

4. FINAL CONSIDERATIONS

From the results of the systematic study of the present work entitled, digital evidence to proof in the Criminal Procedure, it is concluded that:

The evidence to be admitted requires to be examined and verified with the object in relation to the fact, as well as the procedure led and gives access to the parties, a matter of investigation, respecting their fundamental rights and the principle of due process. Procedural legislation has not regulated digital evidence, it has been incorporated by the principle of freedom of evidence, its basis being analogy, which allows the use of a legal means of proof, without transgressing the guarantees and rights of the persons and the faculties of the procedural subjects.

Digital evidence is a means of proof as a digital file, which is produced by the user or without his knowledge, as the operating system generates it; digital evidence distinguished from electronic evidence, as the former has the particularity that it is physical, visual and the latter as binary files, but both evidences are significant for the investigation. Digital evidence in terms of content is that which is produced on the digital device, such as events, transactions or audits, and user-generated records, both of which are stored on the device. They are also those got by connecting to the network, such as tags, logs and metadata.

The principles of relevance, reliability and sufficiency of digital evidence are essential for its admissibility in an investigation and prosecution, as displayed in ISO/IEC 27037:2012. Non-visible, fragile and volatile digital evidence characteristics distinguish, can destroy or alter, are massive and can be copied without limit. Regarding its collection, it must be admissible, it must be authentic, complete and sufficient, and it must be reliable. If the evidence does not meet these conditions, it will be irrelevant and will be excluded.

Digital evidence is treated as if the action had occurred in a physical space and not in cyberspace. From the analysis of comparative procedural legislation and digital evidence treatment in European and Latin America countries, it can be concluded that digital evidence is documentary evidence, and its probative force must be evaluated in order to be certain of its reliability and integrity and to be used in legal proceedings.

Digital evidence must be collected, transferred and guarded to ensure its legitimacy, which is why it needs to be got through computer forensic expertise, which requires that justice operators and police forces consider its importance and value, and that they be trained in these procedures to ensure their correct execution and the admissibility of digital evidence.

REFERENCES


