A review of cross-border cooperation regulation for digital forensics in LATAM from the soft systems methodology

Lelia Cristina Díaz-Pérez
Instituto Politécnico Nacional, UPIICSA, Mexico City, Mexico
Ana Laura Quintanar-Reséndiz
Instituto Politécnico Nacional, CICATA Querétaro, Queretaro City, Mexico
Graciela Vázquez-Álvarez
Instituto Politécnico Nacional, ESIME Zacatenco, Mexico City, Mexico, and
Rubén Vázquez-Medina
Instituto Politécnico Nacional, CICATA Querétaro, Queretaro City, Mexico

Received 17 January 2022
Revised 17 April 2022
18 July 2022
5 August 2022
Accepted 7 August 2022

Abstract

Purpose – Based on this holistic model, the authors propose and analyze seven key issues related to the admissibility of digital media in cross-border trials considering four Latin American countries.

Design/methodology/approach – The authors apply the modeling process of the soft systems methodology by Checkland in order to develop a holistic model focused on human situation problems involving digital media and information technology devices or systems.

Findings – The authors discuss the status of the identified key issues in each country and offer a perspective on the integration of cross-border work analyzing the contribution of these key issues to the collaboration between countries criminal cases or the use of foreign digital artifacts in domestic trials.

Research limitations/implications – In this study, the authors assumed that the problems of official interaction between agencies of different countries are considered solved. However, for future studies or research, the authors recommend that these issues can be considered as relevant, since they are related to cross-border cooperation topics that will necessarily require unavoidable official arrangements, agreements and formalities.

Practical implications – This work is aimed at defining and analyzing the key issues that can contribute to the application of current techniques and methodologies in digital forensics as a tool to support the legal framework of each country, considering cross-border trials. Finally, the authors highlight the implications of this study lie in the identification and analysis of the key issues that must be considered for digital forensics as a support tool for the admissibility of digital evidence in cross-border trials.

Social implications – The authors consider that digital forensic will have high demand in cross-border trials, and it will depend on the people mobility between the countries considered in this study.

Originality/value – This paper shows that the soft systems methodology allows elaborating a holistic model focused on social problems involving digital media and informatics devices.

Keywords Digital forensic in cross-border trials, International regulations on digital forensics, Soft systems methodology, Cross-border admissibility of digital evidence

Paper type Research paper

The authors acknowledge to King Saud University to support the open access publication of this work. The authors thank to Instituto Politécnico Nacional [GRANT SIP 20220531] for financial support of this research.

Applied Computing and Informatics
Emerald Publishing Limited
e-ISSN: 2210-8327
p-ISSN: 2634-1964
DOI 10.1108/ACI-01-2022-0010

1. Introduction

Mobile devices and computers are used in academia, leisure, work, communications and entertainment. They can be used to communicate data messages, as well as capture, publish, and communicate photos, videos and audios. This extensive social penetration of technology enhances the economic, social and cultural cross-country interactions, but it also enables and facilitates domestic and cross-border criminal activities. Therefore, we must be aware of the growing need to address issues related to cross-border digital forensics, as well as to analyze the country's legal and technological framework. In this sense, several works have been published about the global interoperability of information systems, international standards on digital forensics, the cross-border nature of crimes requiring procedural rules for digital evidence handling, and digital evidence collection across multiple jurisdictions [1, 2]. Furthermore, the requirements to accept digital evidence in multiple jurisdictions and the cross-country recognition of the qualifications of digital forensic examiners were analyzed in an international scenario for the United States of America (USA), South Africa and Namibia [3]. It was also proven in the European Union that the exchange of cross-jurisdictional data in criminal justice proceedings has been a serious problem; and consequently, there has been a call for developing strategies to facilitate the inter-country to promote judicial cooperation by applying two procedures [4]: Mutual Legal Assistance [5, 6] and European Investigation Order [7]. Furthermore, international forums have also been held to discuss the importance of establishing cross-border cooperation on issues related to digital forensics and digital evidence management. In 2020, networking efforts to collect and manage digital evidence of cartels were concerted during Latin American and Caribbean Competition Forum [8]. In addition, United Nations Office on Drugs and Crime outlined a vision for 2022–2025 in Latin America and the Caribbean that addressed the international cooperation networks and the exchange of best practices for crime prevention [9]. In 2021, the International Association of Women Judges and the Council of Europe addressed issues related to inter-country cooperation on cyberviolence and electronic evidence for Latin America and Caribbean supported by the Budapest Convention on Cybercrime [10], the Lanzarote Convention on Protection of Children against Sexual Exploitation and Sexual Abuse [11], and the Istanbul Convention on Violence against Women [12].

Hence, we analyze the legal scenario of four Latin American countries, Mexico, Chile, Colombia and Argentina, in order to explore issues related to cross-country cooperation in criminal cases or the use of foreign digital artifacts in domestic trials. We have selected these countries because, according to the Global Cybersecurity Index 2017, they have a legal framework that identifies and addresses cybercrime and cybersecurity concerns [13]. In this context, criminalistics, informatics, and digital forensics become relevant [14, 15]. When these three areas converge, the following concepts must be considered: cyberspace, computer crime, computer data, digital traces and digital evidence. Thus, according to the ISO/IECE/JTC1/SC27 group, cyberspace is the non-physical environment based on computers, devices and networks where illicit acts and crimes could be committed [16]. In this regard, from the Budapest Convention on Cybercrime, computer crimes are classified into four categories: criminal acts that use technology as the target, criminal acts that use technology as a tool, content-related criminal acts and criminal acts concerning intellectual property [10]. Likewise, from the Budapest Convention, computer data represent facts, information, concepts, program codes and records susceptible to computer processing [17]. At last, according to Guidelines for the Management of IT Evidence: Handbook, digital evidence is any information susceptible to human or other similar intervention, extracted from computers or digital media [18] but, from NIST SP 800-86, the evidence technically refers only to those items that are admitted into a trial by a judge [19].

So, keeping these notions in mind, when a crime is committed, the facts and acts should be technically and scientifically analyzed by specialized laboratories to determine the traces that

satisfy the requirements for a judge can qualify them as evidence. In this way, the work of the specialized laboratories must be based on digital forensic science to scientifically use derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources to facilitate or further the reconstruction of events found to be criminal or help to anticipate unauthorized actions shown to be disruptive to planned operation [20]. Thereby, a specialized laboratory must help to technically support an investigation by demonstrating that traces and digital artifacts satisfy the requirements of integrity, authenticity and chain of custody [21].

Ergo, this work is organized as follows. In Section 2, we provide basic concepts and guides related to digital forensic. In Section 3, we present an overview of the legal framework in the countries under consideration. In Section 4, we explain how traces or digital artifacts should be used, processed and qualified to be considered as evidence in a trial. In like manner, using the soft systems methodology, we proposed a holistic model to identify the key issues for the admissibility of digital evidence in cross-border trials. In Section 5, we describe in detail these seven key issues presenting a summary of their status in the countries under consideration. In Section 6, we discuss the practical implications and the future research of this work and present the objectives to be considered in addressing the key issues identified by applying the soft system methodology. Lastly, we present the conclusions.

2. Digital forensics considerations

Forensic science provides everyone involved in criminal investigations with the tools to achieve fairer trials, effective crimes investigation and evidence to prosecute or exonerate suspects [22]. In like manner, for the USA Department of Justice, forensic science is fundamental core of criminal justice system, assuming that the forensic scientists identify and analyze factual findings that may assist in the investigation and prosecution of criminal perpetrators or in the exoneration of innocent suspects [23]. Following NIST SP 800-86 USA, forensic process aims to achieve a better understanding of an incident by finding and analyzing facts related to it [19]. For this purpose, this guide proposes a forensic process model that includes the following phases: collection, examinations, analysis and reporting, which must be supported by specialists with skills and knowledge to apply specialized procedures, methodologies and technologies. When a forensic process is based on computer-related knowledge, expertise and procedures, we speak of digital forensics, which uses scientific investigation techniques to identify and store traces and digital artifacts involved in law violations [24]. Then, digital forensics defines methodologies that can be used to investigate crimes and internal policy violations, reconstruct computer-related security incidents, troubleshoot operational problems, recover systems after accidental damages or prevent a crime. Furthermore, digital forensics may help to face new ways of committing crimes, assuming that it does not support the truth, but it may help to establish the probative value of digital traces in a trial.

According to NIST SP 800-61 Rev. 2 USA, many law violations cannot be prosecuted because an appropriate process is not followed [25]. Thus, the incident response team should know how to address complaint procedures, and its specialists must be trained and certified in forensic investigation. In addition, the specialists should identify that the digital artifacts or traces can be qualified as one of the following four types of evidence in trials: documentary (satisfying with authenticity and integrity requirements), real (relevant authenticated material), testimonial (by witnesses who first swear or affirm that they will tell the truth) and demonstrative (digital objects useful for demonstrating law violations or for reconstructing events).

In this context, the statement on the requirements that digital traces must satisfy for a judge to qualify them as admissible in a trial depends on the legal framework of the country in

question [26–29]. However, after an exhaustive review, we can say that digital traces may be admissible at a trial only if they satisfy the requirements of relevancy, materiality (also called probative value) and jurisdiction (competency) [30]. Evidence relevancy means that the evidence can clarify or prove the facts under investigation. It is worth noting that evidence relevance depends on logical considerations, but evidence admissibility depends on the law. Therefore, evidence may be admissible at trials, but it must first be shown to be relevant. Conversely, evidence is inadmissible if it is not relevant. Also, the relevant evidence may be excluded from becoming admissible based on the rules of evidence for country in question [31]. Evidence materiality means that the digital artifacts are offered to prove a fact, and they also exist for further analysis in the case. Evidence jurisdiction or competency refers to whether digital artifacts satisfy the legal requirements of reliability to prove a fact, considering the legal framework in a specific region or country.

3. National cybersecurity policies and legal framework

Countries under consideration have made efforts to standardize aspects related to computer crimes recognition, evidential methods, acceptance of experts, accreditation of specialized laboratories, data preservation and chain of custody, digital forensics methodologies and membership in the Budapest Convention on Cybercrime. The homologation of these aspects represents an effort in each country to increase the effectiveness of crime investigation, prevention, prosecution and punishment. Thus, to analyze the possibility that the countries under consideration use digital forensics as a support in legal proceedings, similar to Wu [32], we have reviewed the efforts that each country has conducted to have a national cybersecurity strategy.

3.1 Efforts by the Mexican government

In 2017, the "National Cybersecurity Strategy" (ENC 2017[1]) was developed in congruence to the "National Development Plan" (PND 2013–2018[2]). This plan was updated in 2018 to PND 2018–2024[3], but this new version did not include a national cybersecurity strategy. That situation left the continuity and development of the ENC 2017 uncertain. So, in this work, we consider the ENC 2017 valid, since we are not aware that it has been repealed. Therefore, from ENC 2017, we can highlight that Mexico apply cybersecurity actions to the social, economic and political fields through five strategic objectives: 1. economy and innovation, 2. public institutions, 3. national security, 4. public security, and 5. society and human rights. Consequently, the ENC 2017 defines eight transversal themes, but given the topic that concerns us, we only deal with two of them: "Capability Development" and "Legal Framework and Self-Regulation", as they are the most influential in cross-border work for forensic process and digital evidence management. The first theme was defined to develop public policies, strategies, programs, projects, actions and initiatives that encourage human capital development considering the following areas: cybersecurity, cybersecurity strategies and policies, cybersecurity industry and commerce, investigation and prosecution of crimes committed by using IT systems, criminal pursuit and justice delivery. The second theme defines the actions to improve the legal framework and develop mechanisms for the country's digitalization, assuming that for the risks and threats prevention, the investigation and punishment of offenders are critical elements [33].

3.2 Efforts by the Colombian government

In 2016, the "National Digital Security Policy" (PNSD[4]) was released [34]. It enhances the capabilities of those who may be affected by identifying and managing risk to reduce the possibility of potential threats materializing. From review of this document, we can highlight

that in Colombia the national digital security policy includes five working areas with a risk management approach: (1) it establishes a digital security framework, (2) it creates the conditions for multiple stakeholders to manage digital security risk in their socio-economic activities to establish confidence in the users, (3) it strengthens the national and transnational security of individuals and State in digital environments, (4) it strengthens the national defense and sovereignty in digital environments, and (5) it generates mechanisms to promote national and international cooperation and assistance in digital security. Considering these five working areas, the PNSD includes three objectives: (1) implementing action, coordination and regulatory bodies to prevent, manage, control, and regulate cybersecurity incidents or emergencies in order to address the threats and risks that could compromise national cybersecurity and cyber defense; (2) providing information security training and expand research in cyberdefense and cybersecurity; and (3) strengthening the legal framework related to cybersecurity, cyberdefense, international cooperation and international organizations membership [34]. Hence, the PNSD articulates the efforts to implement digital security in Colombia, giving the country the opportunity and capacity to establish agreements for cross-border work in digital forensic and management of digital evidence.

3.3 Efforts by the Argentinian government

In 2019, the Resolution No. 829/2019 was issued in order to establish the "Cybersecurity National Strategy" (ENC[5]), and thence the "Cybersecurity Committee Executive Unit" (UECCS[6]) was created [35]. The ENC have two Annexes. Annex-I defines the purpose of ENC as providing a secure environment for individuals and organizations. Annex-II defines the functions of the UECCS. In addition, the Resolution No. 829/2019 considers individual rights, socio-economic development, federal leadership, international integration, culture and responsibility. The actions to implement this resolution are the awareness-raising, training and education, industry promotion, regulatory framework, prevention, detection, public security and international cooperation. As we can notice, ENC offers the coverage so that Argentina, as in Colombia and Mexico, has the capacity and opportunity to establish agreements for cross-border work in digital forensic and management of digital evidence.

3.4 Efforts by the Chilean government

In 2017, the "National Cybersecurity Policy" (PNCS 2017–2022[7]) was established, and it includes a national strategy aimed at ensuring that the country achieves a free, open, secure and resilient cyberspace [36]. The PNCS 2017–2022 outlines the following five actions: (1) define a robust and resilient information infrastructure prepared to withstand and recover from cybersecurity incidents, under a risk management perspective; (2) ensure human rights in cyberspace; (3) provide cybersecurity culture and responsibility in the management of digital technologies; (4) establish and maintain cooperation with other actors and participate in international forums and discussions; and (5) develop a cybersecurity industry. We have found that Chile considers the following priorities: the renewal of computer emergency response teams, the optimization of self-monitoring systems, the agreements signing on critical infrastructure (with other countries and academia-industry), as well as the legislative processing of projects related to personal data handling, the computer crimes classification, critical infrastructure and cybersecurity conceptualization. Lastly, the PNCS 2017–2022 identifies the following challenges: attribution of responsibilities in cyberspace, strong relationship with the national intelligence system, risks and threats analysis, and cybersecurity training.

From the brief overview of national cybersecurity strategies, we have found that the countries under consideration have the legal framework focused on cross-border cooperation in digital forensic and digital evidence management. Note that each country aims to provide

legal certainty to institutions so that they can develop domestic or cross-border cooperation in cybersecurity issues. In addition, this brief overview reveals that the country regulations have not fully matched technological changes and current practices for obtaining material with potential use as digital evidence. However, this analysis highlights that the legal framework of each country remains the main governance system for the subject at hand. Lastly, this analysis shows that the national context may influence the feasibility of cross-border handling of digital evidence.

4. Digital forensics as a support in legal proceedings

First, we should consider that to ensure digital evidence admissibility in trials, some legal and technical requirements must be satisfied [37]. To fulfill legal requirements, it should be examined that the records and seizures of informatic devices and computers were legally acquired considering their authenticity, integrity, reliability and case relevance. To fulfill technical requirements, the forensic procedures and tools used for the extraction, preservation and analysis of digital evidential material must be critically and professionally applied. In this way, the digital forensic laboratories must satisfy the following conditions: (1) They must be operated by skilled and trained personnel with the qualifications that endorse their technical and academic quality, (2) they must manage the evidentiary material using a chain of custody, (3) they must issue technical reports with the legal significance for trials, and (4) they must define and apply procedures ensuring results repeatability and reproducibility.

Assuming the above as a premise and from the analysis conducted in Section 3, we have applied the soft systems methodology (SSM) proposed in 1981 by Checkland to holistically review the problem situation of digital media admissibility in cross-border trials in the four countries. SSM is defined as a seven-stage model: 1. recognition of the unstructured problem situation; 2. description of the problem situation; 3. formulating basic definitions of relevant systems; 4. composing conceptual models; 5. comparing conceptual models and reality; 6. defining changes and 7. acting. SSM was developed to address the limitations of the systems engineering approach, which is considered ineffective in addressing the social complexity associated with human situations [38]. Specifically, we have applied SSM stages 1–3 to analyze the mentioned problem situation, and we have applied SSM stage 4 to create the HOLOS shown in Figure 1.

Thus, based on the defined HOLOS, we identify and explore, at different levels of coverage, the involved actors: accrediting authorities, criminalistics experts, computer experts, academic institutions, technology providers and accredited laboratories, assuming that each one of them has objectives, interests and influence area on the applicability of digital forensics. In the HOLOS, we also included cyberspace, cybercrimes, international agreements, digital forensic methodologies, and regulations for handling and preserving data. With this holistic analysis approach, we have been able to rescue collective ideas based on normative and the technical documents [39, 40]. From this analysis, we showed in Section 5, for the countries under consideration, the relevant regulatory issues that relate to achieving digital media admissibility in cross-border trials.

5. Key issues for the admissibility of digital media in cross-border trials

Based on the developed HOLOS, we defined and analyzed the following seven key issues that could help to adopt digital media admissibility in cross-border trials: (1) crimes typification, (2) digital media as evidentiary material, (3) acceptance of digital forensic experts, (4) laboratory accreditation, (5) evidentiary material preservation and chain of custody, (6) digital forensics methodologies and (7) membership in the Budapest Convention on

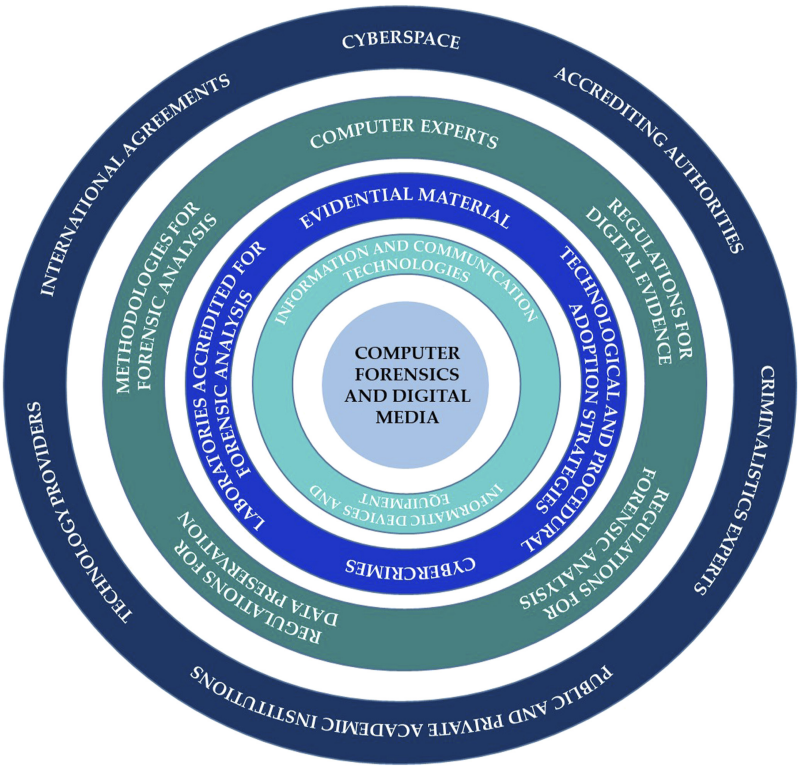

Figure 1.
HOLOS for the identified problem situation considering actors and components

Cybercrime. In this case, we emphasize our assumption that each country's legal framework is respected when a security incident or crime transcends borders and cross-country cooperation is required.

5.1 Crimes typification

We identified that the countries under consideration have established strategies and procedures to judge and punish crimes involving digital media, mobile devices or computers. In Mexico, the "Federal Penal Code in Law" (CPF[8]) comprises several offenses, such as pornography on minors or persons unable to defend themselves, disclosure of secrets and illicit access to computer systems. Although other computer-related offenses are not established, Mexican legislation has typified offenses that are already judged and punished in the current laws. For example, in Articles 127–129 of the CPF, the espionage by computer virus, social engineering or communications interception may be treated as cybercrime. Similarly, the unauthorized reproduction of computer programs is considered a crime under the "Federal Law on Copyright" (LFDA[9]).

In 2019, the "Penal Code in Law" (CP[10]) in Colombia was amended by Law 1273, creating a legal right related to information and data protection. This law recognizes as crimes violations of confidentiality, integrity, and availability of data and computer systems as well as computer attacks. Additionally, Colombia established Law 1581 on data protection, secret disclosure and security infringement reporting. Also, Colombia issued six decree documents: (1) External directive 052 (2007) on security and quality standards for information handling

through financial information channels; (2) Resolutions 3066 and 3067 of 2011, which refer to the protection of users' rights and quality indicators for telecommunications services; (3) Decree 1704 (2012) on legal interception of communications; (4) Decree 019 (2012) on digital certification entities; (5) Resolution 76434 (2012), which refers to the personal data protection and (6) Decree 2573 (2014) on e-government. Finally, we identified that Colombia has agreements with INTERPOL and EUROPOL.

In Argentina, the "Computer Crimes Law-388" (LDI[11]) in the "Penal Code in Law" (CPNA[12]) considers that technology may be used for committing crimes. This law includes as crimes the distribution and possession of digital media with child pornography, e-mails violation, illegitimate access to computer systems, computer damage, malicious code distribution and denial of service [41]. Argentina also has the Grooming Law (Law 26.904, 2013) applicable to anyone who contacts minors by any electronic means to commit any crime against their sexual integrity [42].

The "Computer Crimes Law-19.223" (LDICh[13]) in Chile considers as a legal asset the information contained in any information processing digital system. This law also protects the following aspects: patrimony (in the case of computer fraud), privacy (intimacy and confidentiality of data), security, and reliability of legal and evidentiary data (falsification of evidentiary data).

5.2 Digital media as evidentiary material

In Chile and Mexico, witnesses, presumptions, confessions, deferred oaths, personal inspection by the court, expert reports and digital media may be qualified by a judge as evidence. On the other hand, the data messages may be recognized as evidence in Colombia, Mexico and Chile, when they satisfy the following requirements: (1) accessibility for future consulting, (2) integrity and reliability, and (3) relevance, sufficiency and legality. In all cases, the legality of the digital artifacts and traces refers to their acquisition without incurring in other crimes. Lastly, in Argentina, digital media admissibility is considered in trials when official guidelines and procedures for investigation and evidence collection processes are applied [43].

5.3 Acceptance of digital forensic experts

The countries legislation under consideration recognizes the expert testimony in oral trials. In Mexico, the computer expert testimony is recognized in Article 220–239 of the "Federal Code in Law of Criminal Procedures" (CFPP[14]). In Chile, the computer expert testimony is recognized in Articles 412–414 of the "Federal Code in Law of Civil Procedures" (CPCCh[15]). In Argentina, the accreditation of computer experts can be obtained by complying with Articles 216–278 of the "Code in Law of Criminal Procedures" (CPP[16]). Finally, in Colombia, the report of computer experts can be established as evidential material based on Article 175, 233–243 of the "Code in Law of Civil Procedures" (CPCC[17]). In all cases, experts must demonstrate their technical competence in the country.

5.4 Laboratory accreditation

Digital forensics laboratories must comply with regulations accrediting their operation within the country in question. In Mexico, NMX-EC-17025-IMNC/ISO/IEC 17025 contains the requirements for the competence of testing and calibration laboratories, and it is the adoption of the ISO/IEC 17025. In Colombia, ISO/IEC 17025 is also adopted in NTC-ISO/IEC 17025. In Argentina, the "Comprehensive Guide to the Use of Computer Forensics in the Criminal Process" (GIEIFPP[18]) presents the essential aspects for the search, collection, preservation, expert examination, and presentation of digital traces guaranteeing their integrity and

evidentiary effectiveness for criminal procedure [43]. Finally, Chile does not have information published about this topic.

5.5 Evidentiary material preservation and chain of custody

These activities are not in force or implemented in all countries. In Mexico, four legal instruments address this issue: (1) "National Code in Law of Criminal Procedures" (CNPP[19]) describes the investigation stage, and from Article 227 to Article 252 it includes the investigation techniques used to define and establish the chain of custody of data, objects or properties, and the responsible parties [44]; (2) NOM-151- SCFI-2016, updated in 2017, refers to the conservation of data messages, and the digitizing files supported on physical media [45]; (3) Agreement A/009/15 establishes the guidelines for the chain of custody of data and finally (4) NMX-I-27037-NYCE-2015 establishes the guidelines for identification, collection, acquisition and preservation of digital media that may be relevant in a trial. On the other hand, the legal framework of Colombia includes two instruments related to the preservation and chain of custody for data messages: The "Chain of Custody Procedures Manual"[20] [46], and the "Unified Manual of Judicial Police"[21] [47]. For Argentina, the legal framework only includes the GIEIFPP, which is related to the preservation and chain of custody for data messages [43]. Finally, Chile has not established any specific legal regulations that address the chain of custody and data preservation.

5.6 Digital forensics methodologies

In this topic, Mexico and Argentina have regulations with an optional implementation approach. In Mexico, NMX-I-289-NYCE-2016 recommends a methodology for the execution and evaluation of computer forensic activities, but not limited to equipment that processes, stores and/or transmits information. Meanwhile, in Argentina, the GIEIFPP considers all the steps of a forensic analysis methodology.

5.7 Membership in the Budapest Convention on Cybercrime

The Budapest Convention on Cybercrime was established to address computer and Internet crime by harmonizing national laws, improving investigative techniques and increasing inter-country cooperation [10]. It was held in Strasbourg, France, with the participation of Canada, Japan, the Philippines, South Africa and the United States of America. It aims to closely integrate the member countries interested in cooperation to implement a joint criminal policy that protects society against cybercrime [48]. Mexico has not adhered to the Budapest Convention; it has participated as an invited country. Chile and Argentina joined in 2017, and Colombia in 2018.

In summary, Table 1 presents the status of these seven key issues that could help to achieve the admissibility of digital artifacts or traces as evidentiary material in cross-border trials for Mexico (MX), Chile (CH), Colombia (CO) and Argentina (AR).

Table 1. Seven key issues that could help to achieve the admissibility of digital artifacts or traces as evidentiary material in cross-border trials considering four Latin American countries

Category	Latin american countries			
	MX	CH	CO	AR
Crimes typification	✓	✓	✓	✓
Digital media as evidentiary material	✓	✓	✓	✓
Acceptance of digital forensic experts	✓	✓	✓	✓
Laboratory accreditation	✓	×	✓	✓
Evidentiary material preservation and chain of custody	✓	×	✓	✓
Digital forensics methodologies	✓	×	×	✓
Membership in the Budapest Convention on Cybercrime	×	✓	✓	✓

6. Discussion

In the countries under consideration there are advances in cybersecurity. In each country, improvement opportunities can be identified based on the country's lack of attention to one or more of the key seven issues. In this context, the following findings were identified. Argentina leads in the application of these seven key issues. Next, addressing six key issues are Mexico (1 to 6) and Colombia (except 6). Lastly, Chile addresses four key issues (except 4, 5, and 6). From these differences, we can understand that Chile will have more difficulties admitting digital media as probable evidence in a cross-border trial when they have already been admitted in other countries. Thus, we believe that it is important for each country to conduct research aimed at defining and implementing international strategies that contribute to recognizing, accepting, and managing digital media and artifacts.

Hence, we recommend that the countries interested in achieving admissibility of evidentiary material address the objectives summarized in Table 2, which are related to the seven key issues presented in this work. We also recommend that specialized forums and surveys can be organized including, for each country, the specialized personnel in cross-border trials. The key issues and their objectives may be validated, enriched or specified in detail in each country in order to achieve effective applicability and congruence with its current legal framework. For example, the cyber resilience policies and measures taken by the countries under consideration are issues that could be investigated in future works. For a new issue, the proposed HOLOS must be reassembled, considering that an in-depth study and a documental analysis must be conducted. Finally, it should be noted that in this study, we assumed that the problem of inter-country official interaction is solved. However, for future studies, we recommend that these issues can be deemed relevant since they are related to cross-border cooperation topics that will inevitably require official arrangements, agreements and formalities.

In addition, considering that there may be cross-border trials, we emphasize that our work is aimed at defining and analyzing the key issues that can contribute to the application of digital forensics techniques and methodologies as a support in domestic and cross-border legal proceedings. In this work, we have considered countries that, according to the Global Cybersecurity Index 2017, have a legal framework related to cybercrime and cybersecurity [13]. We also assume that the forensic process will have high demand in cross-border trials. Finally, we highlight the implications of our study lie in the identification and analysis of the

Table 2.
Objectives for the analyzed key issues

Subject	Objective
Crimes typification	Prosecuting and punishing crimes committed involving digital media, mobile communication devices or computers
Digital media as evidentiary material	Recognition of legal acts through electronic devices and systems and evidentiary material contained in digital media. It is required that the information be complete, attributable to the regulated persons or entities, and accessible for subsequent inquiries
Acceptance of digital forensic experts	Recognition of the participation of digital forensic experts in trials
Laboratory accreditation	Establishing the fundamental technical aspects that must be considered in the search, collection, preservation, expert examination, and presentation of digital media to guarantee their validity and evidentiary effectiveness
Evidentiary material preservation and custody chain	Establishing investigation techniques to guarantee the chain of custody and responsible parties
Digital forensics methodology	Performing and evaluating digital forensic activities. Homogenization of criteria and activities related to the forensic process
Membership in the Budapest Convention on Cybercrime	Establishing a policy to protect society against cybercrime

key issues that must be considered for digital forensics as a support for the admissibility of digital evidence in domestic and cross-border trials.

7. Conclusion

We have identified the strengths and capacities of each country under consideration for the admissibility of digital indicia as evidentiary material in cross-border trails. For this purpose, we have reviewed the legal framework, we have identified some improvement opportunities, and we have shown the efforts of each country. The considered countries should continue working to achieve a coupling not only in the legislative approach but also in the academic, technological, social, private and governmental approaches. We emphasize that the analyzed countries have a national cybersecurity strategy, which could allow them developing programs to homologate forensic work in domestic and cross-border trials. In closing, we emphasize in the defined HOLOS as a valuable tool to obtain information about the competing goals and perspectives of the actors involved in a specific context, which is not easily extractable through conventional qualitative research methods.

Notes

1. ENC 2017: Estrategia Nacional de Ciberseguridad.
2. PND: Plan Nacional de Desarrollo 2013-2018.
3. PND: Plan Nacional de Desarrollo 2018-2024.
4. PNSD: Política Nacional de Seguridad Digital.
5. ENC: Estrategia Nacional de Ciberseguridad.
6. UECCS: Unidad Ejecutiva del Comité de Ciberseguridad.
7. PNCS 2017-2022: Política Nacional de Ciberseguridad para el periodo 2017 a 2022.
8. CPF: Código Penal Federal.
9. LFDA: Ley Federal del Derecho de Autor.
10. CP: Código Penal.
11. LDI: Ley de Delitos Informáticos-388.
12. CPNA: Código Penal de la Nación Argentina.
13. LDICh: Ley de Delitos Informáticos 19.223.
14. CFPP: Código Federal de Procedimientos Penales.
15. CPCCh: Código de Procedimiento Civil.
16. CPP: Código Procesal Penal.
17. CPCC: Código de Procedimiento Civil.
18. GIEIFPP: Guía Integral de Empleo de la Informática Forense en el Proceso Penal.
19. CNPP: Código Nacional de Procedimientos Penales.
20. Manual de Procedimientos para Cadena de Custodia.
21. Manual Único de Policía Judicial.

References

1. Grobler M. Digital forensic standards: international progress. Proceedings of South African Information Security Multi-Conference (SAISMC 2010); 2010 May 17-18. 261-71.

2. Olber PD. The survey on cross-border collection of digital evidence by representatives from Polish prosecutors' offices and judicial authorities. J Digit Forensics Secur Law. 2021; 16(3).
3. Phillips A. An investigation of digital forensic concepts in an international environment: the U.S., South Africa, and Namibia. Theses (Computer Science), College of Engineering and Mines. University of Alaska Fairbanks; 2013.
4. Biasiottie MA. A proposed electronic evidence exchange across the European Union. in Digital evidence and electronic signature law review (DEESLR). 2017; 14: 1-12.
5. Council of Europe European Convention on Mutual Assistance in Criminal Matters (ETS No. 030), 30. Strasbourg: Council of Europe; 1959.
6. Council of Europe Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (ETS No. 182). Strasbourg Cedex: Council of Europe; 2001.
7. EUR-Lex Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters. Council of the European Union; 2014. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0041 (accessed 6 April 2022).
8. Ramos A, Borda W. Digital evidence gathering in cartel investigations. in: Latin American and Caribbean competition forum - session I: digital evidence, OECD-DAF/COMP/LACF(2020)11 ed. Virtual Meeting, Organisation for Economic Co-operation and Development; 2020. 1-8.
9. Zarovki P, Perez J, Calma D. UNODC strategic vision for Latin America and the Caribbean (2021-2025). Vienna: United Nations Office on Drugs and Crime; 2022.
10. Council of Europe The Budapest Convention (ETS No. 185) and its protocols. Strasbourg Cedex: Council of Europe; 2001.
11. Council of Europe Lanzarote convention; 2007. Available from: https://www.coe.int/en/web/children/lanzarote-convention (accessed 6 April 2022).
12. Council of Europe. Regional conference on cyberviolence and electronic evidence: Latin America and the Caribbean. Online Conference on 26-27 November 2021, Jointly organised by the International Association of Women Judges (IAWJ) and the Council of Europe (CoE); 2021.
13. International Telecommunication Union Global Cybersecurity Index 2017, Press Release. Geneva: International Telecommunication Union; 2017.
14. Benson V, Mcalaney J. Emerging cyber threats and Cognitive vulnerabilities. 1st ed. Academic Press; 2019. p. 1-6.
15. Pollitt M, Caloyannides M, Novothy J, Shenoi S. Digital forensics: operational, legal and research issues. In: Sabrina De Capitani du Vimercati IRaIR (Ed.). Data and applications security XVII: status and prospects. IFIP International Federation for Information Processing book series (IFIPAICT), Boston, MA: Springer Science + BUsiness Media; 2004; 142, 393-403.
16. ISO/IEC JTC1, ISO/IEC 27001 - Information security management The British Standards Institution; 2012.
17. Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (ETS No. 141). Strasbourg Cedex: Council of Europe; 1990.
18. Ghosh A. Guidelines for the management of IT evidence HB:171 2003. Standards Australia, Sydney: Standards Australia International; 2003.
19. Kent K, Chevalier S, Grance T, Dang H. SP 800-86, guide to integrating forensic techniques into incident response. Gaithersburg, MD: National Institute of Standards and Technology, U.S. Department of Commerce; 2006.
20. Palmer G. A road map for digital forensic research, technical report (DTR-T001-01). In: The Digital Forensic Research Conference, DFRWS 2001, New York. Utica; 2001.
21. Satpathy S, Mohanty SN. Big data analytics and computing for digital forensic investigations. CRC Press; 2020. 5.

22. Castillo-Peinado LS., Luque de Castro MD. An overview on forensic analysis devoted to analytical chemists. Talanta. 2017; 167: 181-92.

23. Department of Justice of the United States of America Forensic science; 2021. Available from: https://www.justice.gov/olp/forensic-science (accessed 7 July 2022).

24. Abdul Rehman J, Wagas A, Mamoun A, Zunera J, Kashif K, Thipa Reddy G. A comprehensive survey on computer forensics: state-of-the-art, tools, techniques, challenges, and future directions. IEEE Access. 2022; 10: 11065-89.

25. Cichonski P, Millar T, Grance T, Scarfone K. NIST SP 800-61 Rev.2 computer security incident handling guide. Revision 2nd ed. Gaithersburg, MD: National Institute of Standards and Technology, U. S. Department of Commerce; 2012. 1-79.

26. Centro de Estudios Constitucionales SCJN Evidencia Científica. Cuadernos de Jurisprudencia num. 2, A. M. I. Olguín, ed. Ciudad de México: Suprema Corte de Justicia de la Nación; 2020.

27. Acevedo-Vargas CM. Reglas de Evidencia: De Norteamérica a Colombia. Medellín: Universidad de Medellín; 2011.

28. Sergi N. Análisis Jurídico de la situación de la evidencia digital en el proceso penal en Argentina. Buenos Aires: Asociación por los Derechos Civiles; 2018.

29. Duce JM. The preparation of trials stage and its role in the admissibility of evidence in Chile. Quaestio facti. Int J Evidential Leg Reason. 2020: 103-32.

30. Cornell Law School, Legal Information Institute Admissible evidence; 2021. Available from: https://www.law.cornell.edu/wex/admissible_evidence (accessed 8 April 2022).

31. Michigan Legal Publishing Ltd Federal rules of evidence. 2021st ed. ISBN-13: 978-1-64002-090-0. With Internal Cross-References; 2021.

32. Wu Y. Protecting personal data in e-government: a cross-country study. Gov Inf Q. 2014; 31(1): 150-9.

33. Gobierno de México Estrategia Nacional de Ciberseguridad. Ciudad de México: Gobierno de la República; 2017.

34. Departamento Nacional de Planeación Política Nacional de Confianza y Seguridad Digital, Documento CONPES 3995, Departamento Administrativo de la Presidencia de la República. Consejo Nacional de Política Económica y Social, CONPES; 2020.

35. Jefatura de Gabinete de Ministros Resolución 829/2019, Estrategia Nacional de Ciberseguridad. Buenos Aires: Secretaría de Gobierno de Modernización; 2019.

36. Comité Interministerial sobre Ciberseguridad, Política Nacional de Ciberseguridad, Santiago de Chile: Ministerio del Interior y Seguridad Pública; 2017.

37. Antwi-Boasiako A, Venter H. A model for digital evidence admissibility assessment. In: Peterson G, Shenoi S (Eds). Advances in digital forensics XIII, IFIP International Federation for Information Processing, AICT 511-WG 11.9. Orlando, Florida: Springer International Publishing AG; 2017. 23-38.

38. Checkland P. Systems thinking and soft systems methodology. In: Currie RDGaWL (Ed.). The Oxford handbook of management information systems: critical perspectives and new directions. Oxford University Press; 2011.

39. Omer G, Hong A. A holistic analysis approach to social, technical, and socio-technical aspect of e-government development. Sustainability. 2017; 9(12): 2181.

40. Tokarz B, Kohlbeck E, Beuren FH., Fagundes AB., Pereira D. Methods and tools for the development of a Product-Service System: proposal of a conceptual model. Braz J Oper Prod Manag. 2021; 19(3): 1-19.

41. Honorable Congreso de la Nación Argentina In: Argentina Gd. (Ed.). Código penal de la Nación Argentina, Ley 26.388. Buenos Aires. Ministerio de Justicia y Derechos Humanos; 2008.

42. Honorable Congreso de la Nación Argentina, Código Penal, Ley 26.904, Buenos Aires: Senado y Cámara de Diputados de la Nación Argentina, 2013.

43. Di Iorio AH. Guía Integral de Empleo de la Informática Forense en el Proceso Penal. 2nd ed. Mar del Plata: Ministerio Público Fiscal Provincia de Buenos Aires y Universidad FASTA, Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense; 2016.

44. Secretaría de Gobernación Código Federal de Procedimientos Civiles. México: Presidencia de la República; 2014.

45. Secretaría de Economía Norma Oficial Mexicana NOM-151-SCFI-2016. Ciudad de México; 2017.

46. Fiscalía General de la Nación Manual de Procedimientos para Cadena de Custodia, 4. Bogotá; 2018.

47. Consejo Nacional de Policía Judicial Manual Único de Policía Judicial. Ver 2. Bogotá; 2005.

48. Council of Europe Chart of signatures and ratifications of Treaty 185, Convention on Cybercrime (ETS No. 185). 12/07/2022 ed. Council of Europe; 2001.

Corresponding author
Rubén Vázquez-Medina can be contacted at: ruvazquez@ipn.mx