Revista científica Portal de la Ciencia

ISSN: 2953-6502
Fecha de presentación: 20/06/2026
Fecha de aceptación: 20/07/2026
Fecha de publicación: 01/08/2026

Smail Brahimi
**E-mail:** s.brahimi@univ-blida2.dz - smailbrahimi405@gmail.com
**Orcid:** https://orcid.org/0009-0009-6906-4604
University of Blida 2 - Lounici Ali – Algeria

**Cita sugerida (APA, séptima edición)**

Brahimi, S. (2026). The impact of digital evidence on international criminal law. *Portal de la Ciencia*, 7(S1), 384-397, DOI: https://doi.org/10.51247/pdlc.v7iEspecial1.993

**==== o ====**

# The impact of digital evidence on international criminal law

**ABSTRACT**

The increasing incorporation of digital evidence into international criminal law has transformed evidentiary activity by providing objective, verifiable, and technically sound elements for clarifying facts of criminal relevance. This article aimed to analyze the advances, challenges, and perspectives of digital evidence in the context of international criminal law, considering its impact on judicial cooperation and the administration of justice. To this end, a qualitative review study was conducted, based on the critical and interpretive analysis of recent scientific literature, international normative instruments, and specialized studies related to the obtaining, preservation, authenticity, and evaluation of digital evidence. The results showed that digital evidence strengthens the effectiveness of criminal proceedings by increasing evidentiary objectivity, facilitating the reconstruction of events, and reducing the limitations associated with testimonial evidence. However, challenges were also identified related to regulatory heterogeneity across jurisdictions, rapid technological evolution, privacy protection, cybersecurity, preservation of the digital chain of custody, and difficulties in transnational judicial cooperation. It is concluded that the development of technologies such as artificial intelligence and machine learning will increase the capacity to identify and analyze digital evidence, although their incorporation will require dynamic legal frameworks, harmonized international standards, effective cooperation mechanisms, and ongoing specialized training programs to guarantee respect for due process and the protection of fundamental rights.

**Keywords**: digital evidence, international cooperation, technological advancements, cybersecurity, legal frameworks

**==== o ====**

# El impacto de la prueba digital en el derecho penal internacional

**RESUMEN**

La creciente incorporación de la prueba digital en el Derecho Penal Internacional ha transformado la actividad probatoria al proporcionar elementos objetivos, verificables y técnicamente sustentados para el esclarecimiento de hechos de relevancia penal. El presente artículo tuvo como objetivo analizar los avances, desafíos y perspectivas de la prueba digital en el contexto del Derecho Penal Internacional, considerando su impacto en la cooperación judicial y en la administración de justicia. Para ello, se desarrolló una investigación de revisión con enfoque cualitativo, basada en el análisis crítico e interpretativo de literatura científica

reciente, instrumentos normativos internacionales y estudios especializados relacionados con la obtención, preservación, autenticidad y valoración de la evidencia digital. Los resultados evidenciaron que la prueba digital fortalece la eficacia de los procesos penales al incrementar la objetividad probatoria, facilitar la reconstrucción de los hechos y reducir las limitaciones asociadas a la prueba testimonial. Sin embargo, también se identificaron desafíos vinculados con la heterogeneidad normativa entre jurisdicciones, la rápida evolución tecnológica, la protección de la privacidad, la ciberseguridad, la preservación de la cadena de custodia digital y las dificultades para la cooperación judicial transnacional. Se concluye que el desarrollo de tecnologías como la inteligencia artificial y el aprendizaje automático incrementará las capacidades de identificación y análisis de la evidencia digital, aunque su incorporación exigirá marcos jurídicos dinámicos, estándares internacionales armonizados, mecanismos efectivos de cooperación y programas permanentes de capacitación especializada para garantizar el respeto al debido proceso y la protección de los derechos fundamentales.

**Palabras clave**: prueba digital; cooperación internacional; avances tecnológicos; ciberseguridad; marcos jurídicos.

**==== o ====**

## O impacto da prova digital no direito penal internacional

**RESUMO**

A crescente incorporação da prova digital no direito penal internacional transformou a atividade probatória, fornecendo elementos objetivos, verificáveis e tecnicamente sólidos para esclarecer factos de relevância penal. Este artigo teve como objetivo analisar os avanços, os desafios e as perspetivas da prova digital no contexto do direito penal internacional, considerando o seu impacto na cooperação judiciária e na administração da justiça. Para tal, foi realizado um estudo de revisão qualitativa, baseado na análise crítica e interpretativa da literatura científica recente, de instrumentos normativos internacionais e de estudos especializados relacionados com a obtenção, preservação, autenticidade e avaliação de provas digitais. Os resultados mostraram que as provas digitais fortalecem a eficácia dos processos penais, aumentando a objetividade probatória, facilitando a reconstrução de eventos e reduzindo as limitações associadas à prova testemunhal. Contudo, também foram identificados desafios relacionados com a heterogeneidade regulatória entre jurisdições, a rápida evolução tecnológica, a proteção da privacidade, a cibersegurança, a preservação da cadeia de custódia digital e as dificuldades na cooperação judiciária transnacional. Conclui-se que o desenvolvimento de tecnologias como a inteligência artificial e a aprendizagem automática aumentará a capacidade de identificação e análise de provas digitais, embora a sua incorporação exija enquadramentos jurídicos dinâmicos, normas internacionais harmonizadas, mecanismos de cooperação eficazes e programas de formação especializada contínua para garantir o respeito pelo devido processo legal e a proteção dos direitos fundamentais.

**Palavras-chave:** evidência digital; cooperação internacional; avanços tecnológicos; cibersegurança; marcos legais.

**==== o ====**

### INTRODUCTION

As digital evidence becomes more important in various disputes, international criminal law is similarly affected. Frequently serving as a concrete means to validate various assertions and reinforce facts that were previously considered only in theory, the collection of digital evidence has gained significant legal attention in recent years. This can be attributed, in large measure, to the increasing significance of science and technology in the field of law overall. Today, for instance, courts take into account the usually distinct features of digital evidence, highlighting the inherent worth that such information frequently provides. From the viewpoint of judicial

decision-making, digital evidence can be very valuable, as it frequently holds significant probative value, helps minimize discrepancies among testimonies, can be presented demonstrably, and facilitates additional documentation through various digital software tools. Additionally, it can offer insights that are otherwise unattainable or unfeasible through alternative means of evidence generation.

The swift advancement of technology and the relatively unyielding characteristics of law have, nevertheless, rendered effective collaboration on the utilization of digital evidence more challenging. To enhance states' capacities to collaborate effectively on the use of digital evidence in prosecutions, it is essential to address some of the challenges related to the gathering and application of such data. Certainly, this type of evidence creates significant challenges for the successful prosecution of suspects across national borders, a topic that will be explored in depth. Naturally, not every country has the same level of digitalization, which means that the utility of digital evidence in legal cases will differ based on the jurisdictional country.

So, in what ways does the growing dependence on digital evidence pose challenges to established principles of admissibility and authenticity in international criminal law? In particular, what are the ramifications for maintaining the integrity and dependability of digital evidence in global courts, and how could this affect the prosecution of cybercrimes or evidence obtained from non-state entities? Moreover, how can global legal frameworks evolve to tackle the changing nature of digital evidence while ensuring due process and safeguarding individual rights?

**The Evolution of Digital Evidence in Legal Proceedings**

Digital evidence refers to electronic information that is saved on a computer or server and can be retrieved and examined. Documentation shows that the initial occurrence of digital evidence introduced in a legal court happened in 1978. Since that time, the fields of digital forensics, law enforcement, and international criminal law have advanced greatly. Four cases served as pivotal moments for the acceptance of digital evidence. A pivotal case was important not only in digital evidence law but also in the handling of electronic evidence overall. Initial views on the function of digital evidence in law suggested that accused individuals or offenders might utilize 'hacking' as a potential reason for the inadmissibility of digital evidence in prosecution.

As time passed, appeals in case law demonstrated that the judiciary began to transition from a complete rejection of digital evidence to permitting a conditional acceptance of such evidence. They accomplished this by incorporating stipulations into their decisions, including the need for a chain of custody, the credentials of the expert, the analytical methods utilized, the condition of the facility or site examined, and the dependability of the software application employed. As time passed, digital technology enhanced its role in society, broadening the various kinds of investigative or criminal intelligence resources that could be employed to reinforce an analysis focused on identifying criminal behavior. As law enforcement's operational roles continuously strive to enhance their capabilities through advanced technology, tools, and specialized skills, the judiciary's functions must similarly evolve.

The question that needs to be posed is straightforward: 'Is it more crucial to collect evidence sooner than usual, or is it more vital to guarantee that the evidence is collected without any corruption?' In a transformed world, how significant is the general evidence considered unprovable?

**Historical Background**

In earlier centuries, evidence was generated and utilized in tangible form, and similar to any physical item, it could be physically moved, changed, harmed, or obliterated. This transformation occurred by the late 20th century because of the emergence of digital technologies. The emergence of digital technologies in the late 20th century led to relevant

evidence transforming into digital formats, making it essential to create and support systems for its generation, handling, acceptance, and assessment. The earliest recorded instance of digital evidence in a court case is from 1978, when an inquiry into a murder in Munich utilized data discovered on a printing plate linked to a typewriter to pinpoint the killer. (Casino et al. 2022).

By the early 1980s, arrests and trials of hackers began, with digital evidence being used in these cases as well. These initial cases provided a basis for incorporating digital evidence into current legal frameworks, leading to alterations in the definitions of evidence in the law. For instance, in the USA, the Federal Rules of Evidence were revised in 1974 to include and consider electronic evidence within their definition of "writings." In Finland, the expanded definition of a "Document" was revised to encompass a "first print-out, which may be generated using a data processing system." (Delfino, 2022)

With advances in technology, digital tools became increasingly prevalent, yet the files and data that could serve as cyber evidence in legal proceedings became less visible, more challenging to erase, and simpler to alter. As a result, the legal framework needed to evolve: judges and expert witnesses were required to seek solutions regarding the collaboration between technical science and criminal law to tackle these issues (Custers2022).

The frequently referenced landmark case is "U.S. v. Riggs," where Jeffrey Riggs was found guilty of bank fraud tied to email. A judge stated, "...the dependability of computer-stored records greatly relies on the computer's proper functioning, the reliability and credibility of the software generated by the computer, and the accuracy of the foundational algorithms employed for calculations (Siman, 2022).

The decision in U.S. v. Schwartz highlighted the evidentiary guidelines that courts must adhere to regarding electronic evidence, allowing such evidence into trials, and, crucially, stressing the necessity for procedural rules that ensured greater information and a presumption of the evidence's integrity before the trial commenced, enabling the judge to understand the types of evidence that would be introduced. U.S. v. Ruster, recognized as France's initial computer forgery case, involved the court relying on an expert who would perform a comprehensive examination of the hard disk in the accused's computer for signs of alterations and hire an expert to confirm that a digital image captured from a computer operating a CD related to a celebration they organized for a birthday occasion. The court clarified in their ruling that they would acknowledge evidence only if the judicial system could depend on it (Purshouse & Campbell, 2022). The judge stated: "...and, in addition, attention must be paid to whether it is legal to utilize such transcripts in criminal cases." An increasing number of offenses involved computer systems, necessitating digital evidence on a global scale. Consequently, an extra protocol to the cybercrime convention featured regulations concerning the acceptance of electronic evidence, with Article 17 addressing its admission in legal proceedings. Certainly, although courts and legal experts were at first doubtful regarding the idea of digital signatures (Rojszczak, 2022).

**Technological Advancements**

A primary catalyst and transformation in criminal proceedings, particularly concerning witnesses and evidence, arises from advancements in multimedia and digital information technology. Numerous technological innovations have played a crucial role in creating devices that can record, store, retrieve, and transmit audio, images, or videos at progressively lower prices. Technologies for data storage and retrieval, essential for digital evidence development, rank low among the most utilized products or innovations globally. Among these, only a few can be mentioned. (Lavorgna & Ugwudike, 2021)

A primary beneficiary of these advancements has been law enforcement, transitioning from tape audio recordings to digital voice recorders and then to contemporary devices like smartphones and body-worn cameras. Moreover, digital evidence can serve as a collection

instrument for anyone. Typically, only a user's devices are capable of capturing evidence; however, services like cloud computing enable recordings to be transferred to servers, offering remote backups of these recordings. These tools are simplifying the process for individuals to bring their devices to court, thereby aiding in the presentation of digital witnesses and witness testimony. Legislation is intricately linked to these shifts, particularly concerning the presence of legal structures for utilizing electronic images and video recordings in court, as well as the authentication of digital evidence overall. (Moussa, 2021)

The rapid embrace of emerging information technology, including personal computing, databases, networking, and web technologies, is constantly transforming the environment. There is a notable rise in the count of victims of crimes and the volume of information that must be documented in various formats, consisting of extensive data. The rise in information complicates and makes challenging the recording, securing, managing, collecting, and presenting of evidence. (Abiodun et al. 2022) Methods for utilizing recent advancements and technological resources demonstrate significant promise. Methods like automatic speech, facial and object recognition, blurring faces to safeguard sensitive identities, extensive processing of binary data, simulating ballistic shots for reconstruction, along with machine learning and big data have been examined for their potential to enhance public safety and justice in the future (Shafiq & Gu, 2022).

The functions of these technological tools can aid in automating various evidence collection and processing tasks, which can save time and, in certain instances, offer greater insight into how evidence ought to be combined with the investigation and evidence presentation. However, they also introduce risks since AI systems may exhibit bias if trained on incorrect data and might be vulnerable to adversarial attacks. Prosecutorial attempts to enhance international criminal law and justice procedures encounter various opportunities and threats, which must be managed by the rule of law. Collectively, these factors illustrate an increasing interaction between international criminal law and electronic or intelligent robotic technology (Norori et al., 2021).

**Legal Frameworks and Principles Governing Digital Evidence**

Numerous global treaties and conventions offer broad principles regarding the acceptance and application of digital evidence in international criminal law. At the global stage, treaties along with their conventions or protocols on anti-corruption, anti-money laundering, data protection, transnational organized crime, and terrorism offer direction to deter, combat, and penalize offenses while facilitating cross-border cooperation. Overall, these agreements include nations aligning their regulations, even if the conventions do not specifically mention digital evidence. Nevertheless, variations exist in the creation and approval of instruments across different regions. When the ratification of treaties cannot occur or is inadequate for assessing the admissibility or utilization of digital evidence in criminal cases, its personal usage and oversight are directed by national law. (Le Nguyen & Golman, 2021)

Legislators globally have started to modify or create local laws and rules to cover different facets related to digital evidence, such as standards and procedures for admissibility or usage. Similar to international law, national laws and regulations specify particular principles that must be taken into account as a foundation for these guidelines. Generally speaking, most domestic laws specify that the acceptance or utilization of digital information must adhere to the regulations governing the admission or usage of evidence from any source, in accordance with procedural rules. The regulations typically pertain to cases where the evidence is obtained directly by authorities or via online platforms, whether it is willingly given or taken under a warrant (Antoliš, 2023).

Exceptions for research, intelligence, and security maintenance are typically outlined in the law enforcement or intelligence agencies. There is no unified method of legislative protection globally; user rights encompass access to information, privacy, risk mitigation, and consent, including data in foreign nations. Research data are typically omitted only when a criminal

search warrant is issued. The application, safeguarding, and elimination of coerced evidence also establish the guidelines. Moreover, legislation concerns individuals within a state party involved in criminal cases or other legal actions in national jurisdictions. Certain laws restrict the relocation of individuals from the home, while also prohibiting the confiscation of effects, money, assets, and remittances (Javed et al. 2022).

**International Treaties and Conventions**

The international community, in general, has acknowledged the uniqueness of digital evidence and has worked towards reaching an agreement on how to handle digital evidence, especially concerning its transfer between various states and jurisdictions to promote consistency among them. Nations have been assuming various roles and offering diverse contributions towards convergence, leading to a range in the adoption, implementation, and enforcement of these agreements from very high to low (Mihelj & Jiménez-Martínez, 2021). The Budapest Convention is acknowledged as the initial crucial international agreement to set forth the principles and procedures for gathering and utilizing electronic evidence in cross-border criminal prosecutions. Nevertheless, in addition to the international law clauses specified in the Budapest Convention, the emergence and growth of electronic evidence concerns have largely surpassed the technological advancements, making certain parts of the convention rather outdated (MArcén, 2023).

Regarding significant international treaties and conventions, special attention will be given to the Budapest Convention on Cybercrime, which was adopted in 2001, along with the global acceptance of the cooperation mechanisms under the United Nations Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children. Besides these treaties, there are two more treaties established by the Council of Europe that play an important role in promoting the evolution and categories of evidence being acknowledged (Buçaj & Idrizaj, 2025). In addition to the Budapest Convention, certain specific provisions concerning electronic evidence were also included in various other international instruments. For example, Article 3 of the United Nations Security Convention mandates essential collaboration among states to share information and evidence regarding serious offenses and stipulates that the systems must be established and maintained according to international standards (Dulskyi et al. 2023).

**Domestic Legislation**

Although many countries have yet to include international treaties related to digital evidence in their new domestic laws, domestic legislation varies greatly from one state to another. Most national laws have created a legal structure that allows electronic evidence to be assessed based on admissibility requirements, regardless of its source. In these areas, evidence is permitted as long as it adheres to the established guidelines regarding due process and fundamental rights. The legislation on data protection has greatly impacted the understanding of basic rights and the alignment of laws in this domain (Javed et al. 2022).

Concerning the details of the legislation that has been enacted, the majority of national laws include the creation and acceptability of current evidence that is already in digital format and the legal mechanisms to retrieve such evidence from electronic sources. However, some legal systems have created evidentiary processes exclusively for documents in electronic format that originate from official electronic databases. Legislation varies in creating specialized bodies tasked with overseeing such evidence, in how evidentiary tools are presented in court, and in the approach to establishing the admissibility of self-authenticating digital records. (OBAMANU, 2023).

Furthermore, legal norms vary in specifying the proper access point permissible and the particular techniques for obtaining digital evidence, particularly concerning the balance between the right to privacy and other human rights that may be violated by data access methods, up to its presentation in court and its protection from seizure, search, or other forms

of state access. Simultaneously, it seems probable that the swift advancement of digital technologies like electronic fingerprints or electronic sensors has surpassed the speed of legal and interpretative developments. (Wang et al., 2024) Telecommunications signals transmitted through satellites or drones, capable of intercepting different types of electronic evidence, are not explicitly recognized as permissible in domestic courts or internal legal procedures, nor are they clearly permitted by the jurisdiction of an international criminal tribunal. As a result, international standards are developing on a case-by-case, experimental approach concerning the matters I mentioned earlier, primarily focused on rulings made by national and regional courts (Labib et al., 2021).

**Challenges and Opportunities in Using Digital Evidence**

In creating an effective digital evidence framework, it is essential to confront the various challenges that arise from collecting and using digital data. Just acquiring digital evidence does not automatically ensure its admissibility; procedurally, some method of authentication is required to confirm the item's accuracy and integrity if it is to be submitted as evidence. For various reasons, this obligation creates a possible obstacle to the utilization of digital evidence. In terms of effort, digital files can easily be manipulated; the original viral edited video provided insight into how this could occur. Regarding evidence, it is extremely challenging to ensure the origin of each digital item and the methods by which it was collected, from the moment it is obtained right up to the presentation phase in court. The technical demands for digital evidence can also incur significant costs (Fallucchi et al., 2021).

A significant area of worry regarding digital evidence is human rights, especially a person's right to privacy. It is evident that enormous quantities of data about individuals are produced daily through choices to engage with a growing range of digital technologies. Moreover, analyzing that data can provide a vast amount of insight regarding any specific individual. Problems stem from the discretion involved in determining which collected data would be pertinent to the investigation. Definitions of what is considered "relevant" data can differ significantly (Almeida et al., 2022).

Ultimately, there are worries about the unforeseen effects of investing significant resources to obtain a comparatively minor result in terms of effective execution. The implementation of Project Whitcoulls may demonstrate the proactive nature within the field, yet it also poses the danger of resulting in overreaching (Branch & Minkova, 2023).

Speaking of The execution of Project Whitcoulls , it marks a crucial advancement in updating the gathering and unification of digital evidence in the realm of international criminal law. The project seeks to improve the acceptance and validity of digital evidence in court by encouraging increased cooperation among international legal organizations, law enforcement agencies, and digital forensics specialists. This initiative promotes the uniformity of processes for managing electronic evidence, thus enhancing its importance in prosecuting intricate, cross-border crimes like cyberattacks, terrorism, and war crimes, ultimately bolstering international justice systems.

**Authentication and Admissibility**

Authentication refers to the method by which the source and validity of a document, item, or other forms of evidence are established. Courts need to be assured that the submitted materials are authentic, without any tampering or modifications. In the digital realm, authentication is essential to confirm the source of images and other digital content used as evidence. In a global context, it is crucial for various nations to trust the electronic resources shared among them and comprehend their precise meaning, which is especially challenging when it comes to audiovisual evidence (Nigam et al. 2021). Various methodologies are employed to verify digital evidence. At the forefront are digital signatures, which safely sign and encrypt files, embedding data within them to guarantee authenticity and integrity. A sender must utilize their private key to encrypt a hash of the file, which is subsequently

decrypted upon reaching its destination to ensure its authenticity. Additional approaches to confirm a file's integrity also involve cryptographic hash functions, a checksum, or a comparison with a fingerprint. (Saepulrohman & Ismangil, 2021)

It is essential to highlight the dangers linked to the collection and analysis of digital evidence. The police and others engaged in identifying and gathering evidence frequently carry a degree of subjectivity and potential bias, which may ultimately affect the investigation, inquiry, or trial. For instance, a police department might utilize software that analyzes digital videos to recognize people; the software's creator and the specific officer operating the tool can possibly influence the system and its classification criteria to inconsistent benchmarks. The manual gathering of digital evidence might also be called into question in court, making it essential to understand how to verify a digital image. Improper management and/or storage of digital evidence during police investigations, along with the inaccessibility of digital data, would ultimately result in the exclusion of that digital data or evidence in legal proceedings (Crosby et al.2022).

The chain of custody outlines the continuous path of responsibility that guarantees the physical protection of digital evidence. This involves a procedure where it is officially documented how the evidence was obtained, including who collected it, the precise time and date of collection, and whether anyone was present to assist the person who gathered it. Additionally, this should encompass any actions taken by the individual during the retrieval process, such as documenting the crime scene prior to the retrieval of evidence, the removal of items, and procedures related to evidence handling, etc. (Ganguli, 2024). This aims to challenge the old notion that digital evidence is immune to manipulation. Individuals acting as expert witnesses providing evidence on digital issues in court must demonstrate their impartiality and restraint. Professionals should ensure their skills and knowledge do not seem to manipulate evidence and must depict an image of integrity and impartiality. Certainly, bias is ultimately inescapable on a purely subjective level; however, from an objective standpoint, it is still wise for legal professionals to prioritize their judgment to fulfill the goals of justice. Here is where the fundamental comprehension of digital evidence is essential—practitioners need to identify which items are classified as digital evidence, enabling them to avoid a narrow perspective of the gathered evidence and to maintain objectivity. There was a direct link between the lack of awareness of digital data related to criminal trials and the capacity of lawyers, forensic specialists, and law enforcement to effectively present their case. This indicated the necessity for educational and training advancement in the area of new technologies (Thunberg and Arnell 2022).

**Privacy Concerns**

Digital evidence depends significantly on gathering extensive data about people, with certain aspects of this evidence being generated automatically as we engage in daily activities. The gathering of this type of data consequently relates to numerous crucial issues concerning privacy and data protection law, in addition to broader human rights and civil liberties matters. All jurisdictions handle the use of digital evidence and personal data during investigations; however, there is a significant variation in the level of protection provided by certain countries compared to others. (Muir and Walcott, 2023)

Despite having its detractors, the right to privacy in the United States is reflected in the Fourth Amendment. The 'reasonable expectation doctrine' establishes constraints on law enforcement and investigators regarding electronic surveillance, specifying restrictions on the timings and methods of searches and the access to electronic data. Numerous European and international legal frameworks likewise include clauses that safeguard the right to privacy and personal information, especially concerning government surveillance and data protection (Cauffman & Goanta, 2021). A person's right to privacy is thus 'restricted' to safeguard not only that individual's privacy, but also various other societal interests, like personal liberty, the right to solitude, security, and freedom of association. While numerous provisions adopted

in the UK were seen by the legal community as establishing a greater level of privacy protection than mandated by international law, significant worries persist regarding the susceptibility of digital evidence to misuse by governments and law enforcement agencies. These issues can be categorized into two broad types (Karagiannis & Vergidis, 2021).

To start, there exists the potential for abuse or overextension by law enforcement while gathering, handling, and utilizing digital evidence. There is widespread worry that governmental bodies can access more private details about people's lives than in the past, with a sentiment that states might be inclined to gather such information for numerous motives that arguably extend beyond the fear and prosecution of adversaries and ordinary offenders. Moreover, legal monitors have raised worries that governments may unintentionally gather, handle, and utilize personal data about themselves and others without proper accountability. In other words, governments may participate in community policing efforts, typically focused on improving public safety, which often depend on gathering extensive data regarding a person's private life, or utilize specific law enforcement instruments that violate an individual's privacy and safety (Lloyd, 2023).

The reasons for these actions encompass concerns over 'unforeseen repercussions' and the widespread transition by numerous states from a previously legally and administratively grounded system of law and order to one that highlights enforcement, discretion, and adaptability. Consequently, most contemporary laws concerning electronic offenses and digital evidence typically include provisions that safeguard human rights against the exploitation and misapplication of electronic data. This encompasses protections and protocols that restrict unwarranted surveillance, along with enabling a person to contest the gathering and application of digital evidence in court through a defense grounded solely in the absence of proper legislative or judicial authorization. Nonetheless, numerous individuals contend that an appropriate equilibrium between security and privacy concerning digital evidence has yet to be achieved, indicating a need for reform in this domain. (Le Nguyen & Golman, 2021)

**Enhancing Investigative Techniques**

With the growth of digital communication and various computer activities, there has been a rise in the volume of data produced and offered in different formats that law enforcement and other investigators can access. The benefits that law enforcement organizations still struggle with regarding the gathering, storing, and examining of large quantities of data are clear. Different data analysis tools, investigative techniques, and algorithms can enhance the evaluation of digital evidence. Digital investigative instruments are available for deciphering encrypted messages, along with automated systems that convert spoken language into written or transcribed English for additional analysis when language barriers are present (Hantrais et al.2021).

The ability to compare facial images, voices, sounds such as gunfire, and visuals of objects and places, coupled with diverse supplementary facial recognition tools and databases for digital analyses, allows investigators to suggest possible suspects with increased precision. The examined outcomes in instances like the Migration Response pushback and the detention of several individuals across at least six states resulted in the circulation of video content on a social media platform that reportedly depicted the mistreatment of asylum seekers. While society is largely enthusiastic about the adoption of various new surveillance, investigative, and evidential methods, there are also apprehensions (Thielgen et al. 2021). An ongoing issue is the accountability of private providers in gathering digital evidence, particularly given recent disclosures about government interception of information, which some top data analysts often find more challenging to clarify. Recently, reports have shown a limited number of major social media and search engine firms that provide regular customer data streams—commonly in real-time—via encrypted portals. Personnel in law enforcement agencies need continual training and skill enhancement to remain effective, especially due to the rapid advancements in communication technologies and media. Simultaneously, there exists potential for hope

regarding how the vast amounts of data produced by digital devices and available to researchers may create a foundation for more detailed and insightful links between individuals in intricate criminal investigations than ever before (Hassan et al. 2024).

**Future Trends in Digital Evidence and International Criminal Law**

Digital technologies are continually progressing, and these swift developments will influence how digital evidence is gathered, processed, and utilized in international criminal law. Considering the perspective of future digital evidence, the advancements in computer technologies may progressively enable the collection of digital evidence that was previously too intricate to acquire. The growing effectiveness and distribution of surveillance technologies could enhance the quality of digital evidence accessible in international criminal cases. The growing application of machine learning and artificial intelligence technologies will aid in the rapid and automatic analysis of digital evidence, potentially resulting in novel types of evidence-based cases, like deepfake incidents (Timotheou et al. 2023). Significant resources and efforts will be invested by global organizations and governments in digital investigations to aid efforts in various non-conflict sectors, especially in the prosecution of cyber crimes. This could result in criminal cases concerning digital evidence, raising issues for new laws on digital evidence and associated challenges. It is crucial that the existing laws and procedures regarding digital evidence remain adaptable and supportive of justice, enabling them to effectively address and manage the growing threats posed by advanced and intrusive digital technologies. It is essential that training and education focused on digital evidence are expanded in line with the rise in the use of new digital investigative technologies; heightened digital investigation and analysis activities may lead to both unintentional and intentional failures in mastering technological challenges (Agestina).

Moreover, a singular global digital law solution cannot exist: various alternatives must be provided to meet the diverse national digital evidence regulations. It is improbable that the cybersecurity facet of digital investigation will enhance soon, considering the diverse risks and threats associated with numerous privacy measures and security protocols that obscure, complicate, and safeguard digital evidence. Agreements and bilateral treaties for state cooperation in the exchange of digital evidence will aid in guaranteeing that justice can still be sought. (Salih & Dabagh, 2023)

## CONCLUSION

The incorporation of digital evidence into international criminal law has significantly altered legal processes, changing the methods for investigating, prosecuting, and resolving cases. Once viewed as secondary, digital evidence has become an essential resource for substantiating assertions and determining facts with enhanced accuracy and dependability. Its transformation from a theoretical idea to a tangible asset in international law signifies wider technological progress, as digital evidence has become crucial for demonstrating criminal acts, ranging from cybercrime to war crimes. Consequently, global legal frameworks have progressively depended on digital evidence to enhance testimonies, minimize discrepancies, and offer strong documentation via digital methods.

The legal structures regulating digital evidence have developed alongside its increasing importance. Nonetheless, these frameworks continue to be fragmented across different jurisdictions, featuring varying standards and processes for the collection, preservation, and admissibility of digital evidence. Global treaties and agreements, crafted by entities like the United Nations and INTERPOL, aim to unify practices; however, obstacles remain in aligning regulations because of differing levels of technological advancement and legal frameworks across nations. Therefore, legal concepts like the right to privacy, due process, and the doctrines of proportionality and necessity need to remain balanced when incorporating digital evidence into international criminal law.

Even with its possibilities, the utilization of digital evidence poses considerable difficulties. Jurisdictional intricacies, cybersecurity issues, and the swift evolution of technology hinder cross-border collaboration and the efficient collection of digital information. Moreover, the dangers linked to data alteration, encryption, and privacy violations necessitate continuous legal and technological awareness. Nevertheless, these obstacles also offer chances for innovation, as global legal entities strive to enhance cooperation, create new instruments for digital forensic examination, and set up guidelines for safe evidence-sharing.

In the future, digital evidence is expected to assume an even more pivotal role in international criminal law. As technologies like artificial intelligence, machine learning, and sophisticated surveillance devices progress, they will provide novel approaches for gathering, analyzing, and presenting evidence. This evolution will likewise require continual adjustment of legal structures to tackle new issues like deepfakes, AI-based alteration of evidence, and the growing reach of cybercrime. In the end, the convergence of law and technology will necessitate a flexible and cooperative strategy to guarantee that international criminal justice can adequately address the intricacies of the digital age.

## REFERENCES

Abiodun, O. I., Alawida, M., Omolara, A. E., & Alabdulatif, A. (2022). Data provenance for cloud forensic investigations, security, challenges, solutions and future perspectives: A survey. Journal of King Saud University-Computer and Information Sciences, 34(10), pp.10217-10245, DOI: https://doi.org/10.1016/j.jksuci.2022.10.018

Agestina, E. (n.d.). The Effectiveness of Law Changes as Progressive Law Implementation on Law Enforcement by Prioritizing Islamic Law as a Benchmark. Ratio Legis Journal. 1(4), pp.464-479, file:///C:/Users/admin/Downloads/29201-71089-1-PB.pdf

Almeida, D., Shmarko, K., & Lomas, E. (2022). The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: A comparative analysis of US, EU, and UK regulatory frameworks. AI and Ethics. Pp.377-387, DOI: https://doi.org/10.1007/s43681-021-00077-w

Antoliš, K. (2023). The challenges of collecting digital evidence across borders. Policija i sigurnost. DOI: 10.59245/ps.32.3.2 https://hrcak.srce.hr/file/445780

Branch, A., & Minkova, L. (2023). Ecocide, the Anthropocene, and the International Criminal Court. Ethics & International Affairs,37(1), pp.51 – 79, DOI: https://doi.org/10.1017/S0892679423000059

Buçaj, E., & Idrizaj, K. (2025). The need for cybercrime regulation on a global scale by international law and cyber convention. Multidisciplinary Reviews.pp.1-10 file:///C:/Users/admin/Downloads/e2025024.pdf , DOI: https://doi.org/10.31893/multirev.2025024

Casino, F., Dasaklis, T. K., Spathoulas, G. P., Anagnostopoulos, M., Ghosal, A., Borocz, I., ... & Patsakis, C. (2022). Research trends, challenges, and emerging topics in digital forensics: A review of reviews. IEEE Access, 10, pp. 25464-25493, DOI: http://doi.org/10.1109/ACCESS.2022.3154059

Cauffman, C., & Goanta, C. (2021). A new order: The digital services act and consumer protection. European Journal of Risk Regulation. 12(4),pp.758- 774, DOI: https://doi.org/10.1017/err.2021.8

Crosby, A., Rea, A., Infantino, F., & Sredanovic, D. (2022). The irregularization of mobility: Performing border control at the airport. Migration Control in Practice: Before and Within the Borders of the State, pp. 99-135. https://inesthinktank.be/www/wp-content/uploads/2023/01/MigrationcontrolinpracticeCrosby_Rea.pdf

Custers, B.H.M. (2022) AI in Criminal Law: An Overview of AI Applications in Substantive and Procedural Criminal Law, in: B.H.M. Custers & E. Fosch Villaronga (eds.) Law and Artificial Intelligence, Heidelberg: Springer, pp. 205-223. https://ssrn.com/abstract=4032094 or DOI: http://dx.doi.org/10.2139/ssrn.4032094

Dulskyi, O., Leliuk, T., Luhovyi, V., Melnyk, V., & Morgun, I. (2023). International cooperation when collecting evidence in the investigation of transnational organized crime: Challenges and opportunities. Revista Amazonia Investiga, 12 (70), pp. 88-101. 88, DOI: https://doi.org/10.34069/AI/2023.70.10.8

Fallucchi, F., Gerardi, M., Petito, M., & De Luca, E. W. (2021). Blockchain framework in digital government for the certification of authenticity, timestamping and data property, Proceedings of the 54th Hawaii International Conference on System Sciences, Hawaii.edu. pp.2307-2316, https://scholarspace.manoa.hawaii.edu/server/api/core/bitstreams/b55e28e4-b5dd-4314-8dbc-ac1a9f2fdabf/content

Ganguli, P. (2024). Admissibility of digital evidence under Bharatiya Sakshya Sanhita: A comparative study with the Indian Evidence Act. pp.1-22, https://ssrn.com/abstract=4977238 or http://dx.doi.org/10.2139/ssrn.4977238

Hantrais, L., Allin, P., Kritikos, M., Sogomonjan, M., Anand, P. B., Livingstone, S., ... & Innes, M. (2021). Covid-19 and the digital revolution. Contemporary Social Science, 16 (2), pp.256-270. DOI: https://doi.org/10.1080/21582041.2020.1833234

Hassan, A. O., Ewuga, S. K., Abdul, A. A., Abrahams, T. O., Oladeinde, M., & Dawodu, S. O. (2024). Cybersecurity in banking: A global perspective with a focus on Nigerian practices. Computer Science & IT Research Journal, 5 (1), 41-59, file:///C:/Users/admin/Downloads/701-Article%20Text-2154-1-10-20240109.pdf or DOI: 10.51594/csitrj.v5i.701

Javed, A. R., Ahmed, W., Alazab, M., Jalil, Z., Kifayat, K., & Gadekallu, T. R. (2022). comprehensive survey on computer forensics: State-of-the-art, tools, techniques, challenges, and future directions. IEEE Access, 10, 11065-11089, https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9678340 or DOI:10.1109/ACCESS.2022.3142508

Karagiannis, C., & Vergidis, K. (2021). Digital evidence and cloud forensics: Contemporary legal challenges and the power of disposal. Information. 12(181), pp.1-16, https://doi.org/10.3390/info12050181

Labib, N. S., Brust, M. R., Danoy, G., & Bouvry, P. (2021). The rise of drones in the Internet of Things: A survey on the evolution, prospects, and challenges of unmanned aerial vehicles. IEEE Access ,9, pp. 115466-115487, https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9514555 or DOI: 10.1109/ACCESS.2021.3104963

Lavorgna, A., & Ugwudike, P. (2021). The datafication revolution in criminal justice: An empirical exploration of frames portraying data-driven technologies for crime prevention and control. Big Data & Society. pp.1-15, https://journals.sagepub.com/doi/pdf/10.1177/20539517211049670 or DOI: 10.1177/20539517211049670

Le Nguyen, C., & Golman, W. (2021). Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries: 'Law on the books' vs 'law in action'. Computer Law & Security Review, 40(105521), DOI: 10.1016/j.clsr.2020.105521

Lloyd, M. (2023). Skirting the Fourth Amendment: How law enforcement agencies abuse technology and constitutional exceptions to surveil the public. Washington and Lee Journal of Civil Rights & Social Justice, 30(2), pp.438-491.

MArcén, A. A. G. A. (2023). The push for the international regulation of cross-border access to electronic evidence and human rights. Cuadernos Derecho Transnacional. Pp.1-26, https://zaguan.unizar.es/record/125896/files/texto_completo.pdf

Mihelj, S., & Jiménez-Martínez, C. (2021). Digital nationalism: Understanding the role of digital media in the rise of 'new' nationalism. Nations and Nationalism, Wiley,27, pp.331–346. https://onlinelibrary.wiley.com/doi/pdfdirect/10.1111/nana.12685 or DOI: 10.1111/nana.12685

Moussa, A. F. (2021). Electronic evidence and its authenticity in forensic evidence. Egyptian Journal of Forensic Sciences, 11(20), pp.1-10, https://link.springer.com/content/pdf/10.1186/s41935-021-00234-6.pdf or https://doi.org/10.1186/s41935-021-00234-6

Muir, R. I. C. K., & Walcott, S. T. E. P. H. E. N. (2021). Unleashing the value of digital forensics. The Police Foundation, pp.1-18.

Nigam, A., Pasricha, R., Singh, T., & Churi, P. (2021). A systematic review on AI-based proctoring systems: Past, present and future. Education and Information Technologies, 26 (5), 6421-6445. https://link.springer.com/content/pdf/10.1007/s10639-021-10597-x.pdf or https://doi.org/10.1007/s10639-021-10597-x

Norori, N., Hu, Q., Aellen, F. M., Faraci, F. D., & Tzovara, A. (2021). Addressing bias in big data and AI for healthcare: A call for open science. Patterns. 2(10), pp.1-9, https://www.cell.com/action/showPdf?pii=S2666-3899%2821%2900202-6 or https://doi.org/10.1016/j.patter.2021.100347

OBAMANU, G. V. (2023). Legal issues and challenges in the admissibility of digital forensic evidence in courts in Nigeria. AJIEEL. 8, pp.96-109, file:///C:/Users/admin/Downloads/10+Vol.+8.pdf

Purshouse, J., & Campbell, L. (2022). Automated facial recognition and policing: A bridge too far? Legal Studies, 42 (2). pp. 209-22, https://eprints.whiterose.ac.uk/178322/3/accepted%20version.pdf or https://doi.org/10.1017/lst.2021.22

Rojszczak, M. (2022). E-Evidence cooperation in criminal matters from an EU perspective. Wiley. Pp.1-39, https://onlinelibrary.wiley.com/doi/am-pdf/10.1111/1468-2230.12749 or https://doi.org/10.1111/1468-2230.12749

Saepulrohman, A., & Ismangil, A. (2021). Data integrity and security of digital signatures on electronic systems using the digital signature algorithm (DSA). International Journal of Electronics and Communications Systems. 1(1), pp.11-15, https://repository.unpak.ac.id/tukangna/repo/file/files-20210715185920.pdf

Salih, K. M., & Dabagh, N. (2023). Digital forensic tools: A literature review. Journal of Education and Science. 32(1), pp.109-124, https://www.iraqoaj.net/iasj/download/92e10e337dd404d9 or DOI: 10.33899/edusj.2023.137420.1304

Shafiq, M., & Gu, Z. (2022). Deep residual learning for image recognition: A survey. Applied Sciences, 12 (1), 112, pp.1-43, file:///C:/Users/admin/Downloads/applsci-12-08972.pdf or https://doi.org/10.3390/app12188972

Siman, F. A. (2022). The wrong road taken: Social media content, self-authentication and misapplication of the business records rule. Universiti Teknologi MARA (UiTM) Journal, 1, pp.19-20, https://ir.uitm.edu.my/id/eprint/65184/1/65184.pdf

Thielgen, M. M., Schade, S., & Bosé, C. (2021). Face processing in police service: The relationship between laboratory-based assessment of face processing abilities and performance in a real-world identity matching task. Cognitive Research: Principles and Implications, 6 (1), 54, pp.1-18, https://link.springer.com/content/pdf/10.1186/s41235-021-00317-x.pdf or https://doi.org/10.1186/s41235-021-00317-x

Thunberg, S., & Arnell, L. (2022). Pioneering the use of technologies in qualitative research–A research review of the use of digital interviews. International Journal of Social Research Methodology, 25 (6), pp.757-768, https://www.tandfonline.com/doi/pdf/10.1080/13645579.2021.1935565 or https://doi.org/10.1080/13645579.2021.1935565

Timotheou, S., Miliou, O., Dimitriadis, Y., Sobrino, S. V., Giannoutsou, N., Cachia, R., ... & Ioannou, A. (2023). Impacts of digital technologies on education and factors influencing schools' digital capacity and transformation: A literature review. Education and Information Technologies, 28 (6), pp.6695-6726, https://link.springer.com/content/pdf/10.1007/s10639-022-11431-8.pdf or https://doi.org/10.1007/s10639-022-11431-8

Wang, S., Jiang, X., & Khaskheli, M. B. (2024). The role of technology in the digital economy's sustainable development of Hainan Free Trade Port and genetic testing: Cloud computing and digital law. Sustainability, 16 (6025), pp.1-20, file:///C:/Users/admin/Downloads/sustainability-16-06025-1.pdf or https://doi.org/10.3390/su16146025