P-ISSN: 2790-6795	Annals of Human and Social Sciences	July-September 2025,Vol. 6, No. 3
O-ISSN:2790-6809	http://doi.org/10.35484/ahss.2025(6-III)39	[467-478]

Annals of Human and Social Sciences
www.ahss.org.pk

RESEARCH PAPER

Balancing Forensic Technology and Human Rights in the International Legal Framework and Financial Crime Context: A Legal Analysis

[1]Ghulam Mujtaba Malik, [2]Hyder Ali Memon and [3]Taniya Ahmed

1. PhD Scholar, Faculty of Law and Political Science, University of Szeged, Hungary.
2. Assistant Professor, Department of Criminology, University of Sindh, Jamshoro, Sindh, Pakistan
3. PhD Scholar, Department of Criminology, University of Sindh, Jamshoro, Sindh, Pakistan

Corresponding Author gh.mujtaba@hotmail.com

ABSTRACT

This study examines the impact of forensic technologies on human rights within the context of international law, focusing specifically on financial crime investigations involving digital evidence. It is delimited to legal and ethical implications under major international instruments.Forensic tools such as digital evidence extraction, network forensics, and big data analytics have enhanced the detection of complex financial crimes. However, their increasing use raises critical concerns over privacy, data protection, and due process. International frameworks, including the GDPR, UNCAC, and the Budapest Convention, seek to balance investigative powers with fundamental rights. A doctrinal research approach combined with qualitative analysis was applied to review legal texts, scholarly literature, and case studies. Findings reveal gaps in global regulatory consistency, inadequate ethical oversight, and risks of rights violations in cross-border digital investigations. Stronger scientific validation and ethical frameworks are urgently needed.The study advocates harmonised international standards, proactive regulation of AI-based forensic tools, and integration of ethical oversight to ensure rights-compliant financial crime investigations.

Keywords: Forensic Technology, Human Rights, International Law, Digital Evidence, Network Forensics, Big Data Analytics

Introduction

Digital forensics defined as the application of scientifically grounded methods to preserve, collect, analyze, and present digital evidence—has become an indispensable component of modern criminal investigations (Casey, 2011). Its relevance is particularly pronounced in the context of financial crimes such as money laundering, fraud, and embezzlement, which continue to threaten economic stability at both national and global levels (Levi & Reuter, 2006). The capacity of digital forensics to uncover complex, cross-border financial schemes has significantly enhanced the effectiveness of law enforcement and prosecutorial processes, particularly where traditional investigative tools fall short (Brenner, 2010). Besides, identity verification technologies are powerful in filtering the legitimacy of users and in stopping financial fraud through identity verification (Zhou et al., 2019). Despite this, there are immense problems regarding human rights in the growing use of digital forensics in financial crimes. In the absence of regulation, these tools can interfere with the right to privacy, threaten fairness in justice operations, and be used for unlawful spying (Koops, 2012). The threat is especially critical when data gathering and analysis systems can run unchecked by proper legal systems of control or accounting. Therefore, the rigorous legal and procedural protection is yet to be provided to guarantee that the use of these technologies will be proportionate, necessary, and not violate the rights (UNODC, 2021). The EU has been at the forefront in protecting the confidentiality of data using regulatory frameworks like the General Data Protection Regulation (GDPR) that requires the lawful, fair, and transparent processing of data (European Union, 2016). The Law Enforcement Directive (LED) complements the GDPR by detailing the data processing that

may be performed with the goal of criminal justice, and it serves to enhance the necessity to weigh investigatory interests with the core rights protection (European Union, 2016b). At an international level, mechanisms discussing international collaboration, in addition to setting the moral and legal standards that would be used to guide digital evidence management, include, but are not limited to, the United Nations Convention against Corruption (UNCAC) and the Budapest Convention on Cybercrime (United Nations, 2003; Council of Europe, 2001).

In the development of these standards, a significant role has also been played by case law. In Carpenter v., the United States (, the U.S. Supreme Court ruled that courts' access to cell-site location data without warrants as violated the privacy rights under U.S. law, thereby emphasizing the need for supervision in digital investigations. In the same note, in United States v. In her presentation, Scheinberg (2011) highlighted the evidential and jurisdictional complexities of crimes in the digital financial field, particularly in the cross-border aspect. The above developments make the necessity of harmonized international standards and an ethical framework that can determine the responsible use of digital forensic technologies evident. It is important to comply with the principles of necessity, proportionality, and transparency not only to increase the effectiveness of the investigation of financial crimes but also to ensure that the rights of people are not violated (Bigo et al., 2019). This study, written in 2022, explores two interrelated research questions: (1) What human rights challenges arise from the use of forensic technologies in financial crime investigations—particularly concerning privacy, fair trial rights, and protection from unlawful surveillance? (2) How do national and international legal frameworks seek to reconcile the use of these technologies with the imperative to protect individual rights?.

The paper focuses on the application and implications of big data analytics, network forensics, and digital identity verification in the context of financial crime. The structure of the paper begins with a comprehensive literature review tracing the evolution and scope of digital forensics in financial investigations. Subsequent sections delve into specific forensic technologies, followed by a critical analysis of associated legal and ethical issues. The discussion draws upon relevant international instruments, comparative legal frameworks, and illustrative case law. The paper concludes with key findings, emphasizing the necessity of cohesive global standards and ethical guidelines that uphold the integrity of human rights while enabling effective enforcement of financial crime laws.

Literature Review

Digital forensics refers to the collection and analysis of digital evidence from electronic devices to aid in the investigation and prosecution of crimes. This includes data such as browser histories, financial records, emails, metadata, and communications stored or transmitted electronically (Casey, 2011). Figure 1 illustrates the digital evidence process, from identification to presentation in legal proceedings.

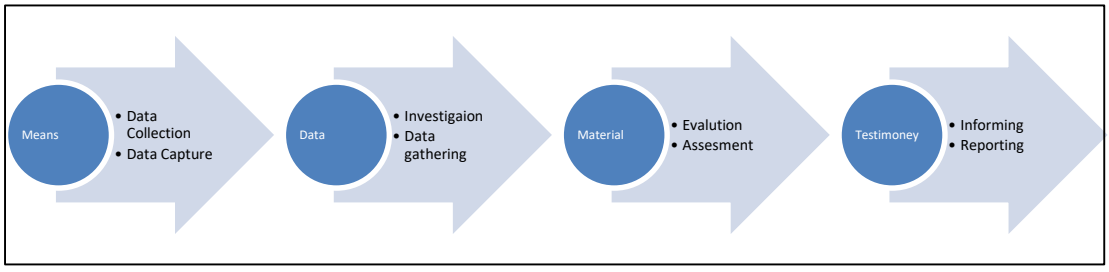

Figure 1 Digital Evidence Process

The field of digital forensics has evolved alongside technological advancement, beginning with manual audits and physical surveillance in the 1970s, progressing to

complex forensic tools like EnCase and The Sleuth Kit by the late 1990s. These tools enabled the systematic recovery of electronic data, improving evidence reliability and judicial outcomes (Carrier, 2003). The history of digital forensics is one characterized by the further development of computing technology into a field that is dynamic and adaptive. It started emerging in the 1970s with the rise of personal computers. During the 1980s and 1990s, computer forensic procedures were developed along with the creation of forensic tools like the Sleuth Kit and EnCase, which facilitated the extraction of digital evidence (Marcella, Albert J., ed., 2021). The evolution of forensic technology, from basic techniques in the 1970s to sophisticated tools like The Sleuth Kit and EnCase, underscores its growing importance in modern judicial processes (Jones, G. Reflecting; S. Godfrey Winster, 2022). Table No.1, given below, summarizes the most relevant and important developments in the evolution of forensic technology for financial crime investigation:

Table 1
Important Developments & The Evolution

Decade	Technologies & Techniques	Key Tools And Developments
1970s	Basic Techniques	• Manual audits and paper trails. • Examination of bank records • Witness interviews- Physical surveillance
1980s	Introduction of Computer Technology	• Computerized accounting systems • Early Database Systems - Emergence of Forensic Accounting.
1990s	Digitalization and Software Tools	• Advanced DBMS • Forensic accounting software (e.g., ACL, IDEA - Electronic records and email as evidence • EnCase (introduced in 1997) • The Sleuth Kit (introduced in the late 1990s • Electronic fund transfer analysis
2000s	Rise of the Internet and Cyber Forensics	• Internet banking and online transactions • Cyber forensics • AML software • Data mining and analytics
2010s	Big Data and Machine Learning	• Big data analytics • Machine learning algorithms • Blockchain and cryptocurrency forensics • AI-powered systems
2020s	AI, blockchain analytics, RPA, RegTech	• Blockchain analytics tools • Integrated forensic platforms • Regulatory technology (RegTech)

This table, No. 1, highlights the key technologies and techniques defined in each decade, providing a clear overview of how forensic technology in financial crime investigation has evolved. This progression has enabled authorities to investigate complex digital trails. For example, in the Silk Road case, law enforcement utilized forensic analysis of blockchain transactions to identify anonymous users behind illegal marketplaces (Greenberg, 2014). The rise of mobile devices, cloud storage, and encrypted platforms introduced new challenges in accessing digital evidence, prompting the development of mobile forensic tools to extract data from smartphones and cloud environments (Quick & Choo, 2014). Today, digital forensics must grapple with exponentially increasing data volumes, the sophistication of financial crime schemes, and regulatory compliance demands—making it central to combating fraud in the digital age (Shah & Issac, 2021).

Integration into Financial Crime Investigation

The application of digital forensic technologies in financial crime investigations has significantly strengthened the detection, investigation, and prosecution of complex financial

offenses. These technologies span across digital evidence collection, network and mobile forensics, big data analytics, identity verification systems, and intrusion detection tools. Together, they provide law enforcement with the capacity to analyze large volumes of data, trace hidden financial transactions, and build robust digital trails. As Coronel, Morris, and Rob (2018) argue, the increasing reliance on technological solutions corresponds to the rise of more sophisticated and transnational financial crime networks. Modern forensic investigations can retrieve and analyze massive datasets from digital devices such as computers, smartphones, and external drives, enabling investigators to recover deleted files, trace illicit transfers, and reconstruct criminal activities (Casey, 2011). Network forensics, a core area within this field, involves monitoring and analyzing data traffic to uncover unauthorized access, intrusions, or suspicious behavior across networks. However, such surveillance tools raise questions about privacy and proportionality. Shebaro and Crandall (2011) caution that without proper oversight, network surveillance can infringe on civil liberties and fundamental rights. Big data analytics has also become indispensable in financial crime investigations.

Legal and Regulatory Frameworks

To complement the GDPR, there is the Law Enforcement Directive (Directive EU 2016/680), which sets forth the circumstances in which law enforcement authorities can process personal data and underlines the value of accountability, control and proportionality. On the international level, the United Nations Convention Against Corruption (UNCAC, 2003) helps countries to cooperate in their efforts to combat financial crime, with an insistence that particular consideration should be given to upholding human rights. At the same time, Budapest Convention on Cybercrime (Council of Europe, 2001) offers a legal framework, to harmonise the laws on the topic of cybercrime and facilitate exchange of digital evidence, where the importance of privacy should be stressed. On the strength of these frameworks, the increased awareness of the two-sided issue of the improvements of forensic technologies as a means of creating a sense of security and safeguarding rights is observed. The contents of the provisions offer principles, which can be used by any countries wishing to strengthen their capacity to anticipate and initiate Laws and enforcement in contemporary manner without interfering with individual freedom.

Forensic Technologies in Financial Crimes

Forensic technologies, including computer forensics, forensic auditing, and digitalisation-data frameworks, are no longer optional methods for solving financial crimes and satisfying anti-money laundering (AML) requirements. In such a case, when properly integrated, these technologies can increase the efficiency of investigative work, perform follow-up investigations promptly in cases of fraudulent operations, and make the process of collecting and analyzing evidence more accurate (Casey, 2011; Coronel et al., 2018). Tene and Polonetsky (2012) address the ethical issues of big data in forensic science, especially transparency and privacy in forensic analysis. Intrusion Detection Systems (IDS) are security mechanisms that monitor system activity, such as on a network, to identify and react to unauthorized or malicious attacks. This would be beneficial in preventing cyber intruders, which may be used to facilitate financial crimes. The significance of their role was affirmed in the case United States v. Jones (2012), which involved the issue of warrantless searches. Although the case primarily focused on surveillance, it highlighted the broader issue of striking a balance between the technological tools for surveillance, such as IDS, and the constitutional right to privacy. Ethically deployed IDS offers a vital solution to limit the intrusion on the digital domain with the added characteristics of accountability and transparency. Probably the main characteristics of forensic technologies are summarized in Table 2, given below:

Table 2
Overview Of Forensic Technologies In Financial Crime Investigations

Overview Of Forensic Technologies	Description	Legal Instruments (Provisions)	Case Law
Digital Evidence Collection	Systematic gathering and analysis of electronic data to uncover illicit activities.	USA PATRIOT Act (Section 215 - Bulk Data Collection), RIPA (Part II - Surveillance Powers), GDPR (Article 5 - Data Protection Principles)	United States v. Scheinberg et al. (2011), Carpenter v. United States (2018)
Network Forensics	Monitoring and analyzing network traffic to detect and investigate cybercrimes.	CFAA (Section 1030 - Fraud and Related Activity in Connection with Computers), ECPA (Title I - Wiretap Act), FATF Recommendations (Recommendation 29 - Detecting and Deterring Money Laundering and Terrorist Financing)	United States v. Mitra (2005)
Mobile Device Forensics	Extracting and analyzing data from smartphones and tablets to uncover evidence.	SCA (Section 2703 - Required Disclosure of Customer Communications or Records), GDPR (Article 32 - Security of Processing), Budapest Convention (Article 19 - Search and Seizure of Stored Computer Data)	Riley v. California (2014)
Big Data Analytics	Examining large datasets to uncover patterns and connections in financial activities.	GDPR (Article 22 - Automated Individual Decision-Making, Including Profiling), CCPA (Section 1798.105 - Consumer Rights to Delete Personal Information), OECD Guidelines (Principle 3 - Collection Limitation Principle)	Google Spain SL v. Agencia Española de Protección de Datos (2014)
Digital Identity Verification	Ensuring the authenticity of digital identities to prevent fraud.	eIDAS Regulation (Article 8 - Conditions for Legal Effect of Electronic Identification), GDPR (Article 9 - Processing of Special Categories of Personal Data), UNCAC (Article 13 - Participation of Society)	Matsushita Electric Industrial Co. v. Zenith Radio Corp. (1986), United States v. Nolan (2011)
Intrusion Detection Systems (IDS)	Preventing unauthorized access to networks and detecting suspicious activities.	CFAA (Section 1030 - Unauthorized Access to Protected Computers), ECPA (Title II - Stored Communications Act), Budapest Convention (Article 20 - Real-Time Collection of Traffic Data)	United States v. Jones (2012)

Table No. 2 provides an overview of key technologies, including interpretations of relevant legal instruments and specific provisions. Additionally, it includes a list of landmark cases. Despite the invasive nature of forensic technologies for financial crimes, they should be put into operation in a regulated manner that also safeguards against abuse for criminal purposes. Therefore, the present review seeks to contribute to the ongoing discourse on ensuring that the use of forensic technologies in financial crime investigations is both practical and respectful of fundamental human rights.

Fundamental Human Rights Impacted by Forensic Technology

Analyzing the current state of the available literature and case Law, it is necessary to come to a conclusion that the increasing popularity of forensic technologies in identifying financial frauds is not much to be approached when it comes to the core rights of people. These concerns being inherent are founded on the right to privacy, fair trial and against right of illegal surveillance. Despite many positive points related to forensic technologies and their strengthening of the investigation process, the use of the technologies in popular practice may threaten the personal freedoms of people, unless there are legal regulations to counter their utilization. That way, it is crucial to balance out such application of technologies and the strong legal and regulating frameworks. Current legal norms such as the General Data Protection Regulation (GDPR, 2018), the United Nations Convention Against Corruption (UNCAC, 2003) and the Budapest Convention on Cybercrime (2001) can be used quite effectively to form a legal framework that would be able to moderate the powers of forensics with respect to human rights.

One of the fundamental rights of a man that may be threatened by implementing forensic technologies is privacy. The digital forensic hardware can be used to intercept, analyze and store significant portions of personal data, which in many circumstances could not be made in the absence of the knowledge and consent of the subject. This is harmful overreaching, and particularly in the case when the surveillance mechanisms lack legal and governance safeguards. On the one hand, Nieto et al. (2019) highlight the pitfalls that reside in upholding the privacy of individuals in the sphere of forensics where people and their agencies need a high level of control and safeguards linked to the responsibility and reduction of misreporting. Another very relevant right that is undermined by the usage of digital forensic tools is the right to a fair trial. Digital evidence must be stored, gathered and introduced in Court in a way that due process has been followed to be admissible in Court. Improper handling of the evidence or improperly gathered digital information may prejudice the process and cause the whole judicial process to lose its integrity.

Table 3
Key Forensic Technologies And Human Rights Concerns

Forensic Technology	Human Rights Impacted	Legal Instrument & Provisions
Digital Evidence Collection	Privacy, Fair Trial	International: UNCAC (2003) - Articles 31, 32, Regional: GDPR (2018) - Articles 5, 6, 9, Domestic: USA PATRIOT Act (2001), RIPA (2000)
Network Forensics	Privacy, Protection from Unlawful Surveillance	International: Budapest Convention (2001) - Articles 16, 17, Regional: FATF Recommendations (2012), Domestic: CFAA (1986), ECPA (1986)
Mobile Device Forensics	Privacy, Fair Trial	International: Budapest Convention (2001) - Articles 18, 19, Regional: GDPR (2018) - Articles 7, 8, Domestic: SCA (1986)
Big Data Analytics	Privacy, Ethical Use of Data	International: OECD Guidelines (1980) - Chapter 4, Regional: GDPR (2018) - Articles 13, 14, Domestic: CCPA (2018)
Digital Identity Verification	Privacy, Non-Discrimination	International: UNCAC (2003) - Articles 28, 29, Regional: eIDAS Regulation (2014), GDPR (2018) - Articles 11, 12
Intrusion Detection Systems (IDS)	Privacy, Protection from Unlawful Surveillance	International: Budapest Convention (2001) - Articles 20, 21 Domestic: CFAA (1986), ECPA (1986)

Table No. 3 demonstrates that while various legal instruments provide a framework for the use of these technologies, significant challenges remain in ensuring that privacy, fair trial rights, and protection from illegal and unlawful surveillance are not compromised. GDPR underlines the significance of data safety and privacy, but encounters functioning challenges and issues across different jurisdictions. Also, the Budapest Convention and UNCAC provide international standards and guidelines that underscore the need for

cooperation and consistency in applying these technologies while safeguarding human rights.

Overview of Existing International Legal Frameworks

A transition of law enforcement to a digital scale has made the practices of conducting criminal investigations, its scale, and the aim essentially different. Complex analysis and computing technology is now commonly used to handle the increasing amounts and structures of computerized information, which allows more active investigations, algorithmically oriented, and data-centered. This transformation is a significant change regarding the classic concept of criminal justice, hitherto reactive, individualistic, and trial-focused. The increasing use of the automated tools and digital forensics not only increases capabilities but also the risks, especially those pertaining to the privacy, fairness and due process. Such changes require the extensive modernization of legal frameworks so that the introduction of forensic technologies would not harm the basic human rights. The international and regional legal instruments and national ones, including the GDPR, the Budapest Convention, and constitutional safeguards over privacy provide the most necessary direction to provide the efficiency of the digital forensic activities on par with civil liberty (Mayer-Schonenberger & Cukier, 2013).

In this segment, the explanation is provided on how the human rights issues related to the application of forensic technologies in financial crimes investigation are dealt with by different legal tools at international, regional and domestic levels. Such legal systems aim at achieving balance between the use of investigative skills and the protection of basic human rights. Indicatively, universal declaration of human rights (UDHR) and the international convention of civil and political rights (ICCPR) set up milestones on privacy rights. The act of arbitrary interference with privacy, family, home, and correspondences is therefore prohibited under Art. 12 of the UDHR as well as under Art. 17 of the ICCPR and the right to legal protection against the same is asserted (United Nations, 1948; United Nations, 1966). The European Convention on Human Rights (ECHR) endorsed these principles, by Art. 8, which ensures the right to respect for private and family life. The Human Rights Committee's General Comment No. 16 on Art. 17 of the ICCPR emphasizes and stresses that any interference with privacy must be lawful, necessary, and proportionate, requiring legal frameworks to be clear and precise (UNHRC, 1988). In the European Union, the General Data Protection Regulation (GDPR) sets stringent standards for data protection and privacy. It delegates transparency, responsibility, and the protection of personal data, significantly impacting how digital evidence is handled within the EU (European Union, 2016).

Material and Methods

This legal analysis and review employ a qualitative methodology using doctrinal analysis to examine forensic technologies in financial crime investigations. Primary data sources include academic articles, legal journals, case law databases, and government reports. These sources provide a comprehensive foundation for exploring the evolution of forensic techniques and legislative developments (Hutchinson & Duncan, 2012). Data collection involves a critical analysis of scholarly materials and legal precedents. Peer-reviewed papers offer insights into digital evidence collection, network forensics, mobile device forensics, big data analytics, and IDS. Case law, such as *Carpenter v. United States* (2018) and *Riley v. California* (2014), illustrates statutory interpretations. Government reports provide context on regulatory frameworks like the USA PATRIOT Act (2001), RIPA (2000), and GDPR (2018) (European Union, 2016). Data organization and analysis involve textual data to identify recurring themes and challenges, ensuring a comprehensive understanding of forensic technologies and human rights in financial crime investigations.

Results and Discussion

Academic Debates and Significant Criticisms: Academic controversies and serious objections by legal experts underscore the urgency of developments in digital forensics, big data analysis, and digital identity verification technologies. Such developments, which aim to strengthen the detection of intricate financial crimes, raise new privacy protection issues and jurisprudential surveillance concerns. Tene and Polonetsky (2013) explore the potential of big data analytics to significantly enhance the detection of complex financial fraud schemes by analysing large datasets, identifying anomalous patterns and correlations, and thereby indicating the possible occurrence of fraudulent practices. Nonetheless, in the absence of tight data protection and privacy laws, such technologies are a real threat to personal privacy. McDonald et al. (2022) maintain that the growing use of big data options raises considerable implications of privacy risks and associated risks of abuse, which is why the existing approaches to their regulation must be centralized or have a powerful impact on the rights of individuals, resulting in the preservation of the sanctity of the investigative work. Hussain et al. (2020) emphasize the quality of data in big data analytics. They specify that related noise, imprecision, and uncertain data may contribute to inaccurate analyses and alerts, which is especially dangerous in cases of financial crimes when precision is of primary importance.

Ferrara (2020) highlights the importance of ethical reasoning as the cornerstone of forensic science, as well as the fact that the inefficiency in that field may cause the occurrence of serious acts of injustice. The importance of Ferrara's work lies in its high moral and ethical rigour in digital forensics, which helps avoid miscarriages of justice. Network forensics is important in identifying and stopping cyber threats. However, the invasive nature of the said method may also contribute to the use of surveillance information in a way that may constitute a violation of the right to privacy. Mobile device forensics has proven helpful in supplying essential evidence, especially in high-profile cases such as the Enron scandal (Healy & Palepu, 2003). Nevertheless, there are legal and ethical issues outstanding, especially regarding the privacy matters of accessing personal data without any valid warrants. The Riley case was filed by a married couple who had initiated a patent application in 1993 due to their liabilities in making an initial investment. International cooperation in the fight against cybercrime should be simplified through the **Budapest Convention on Cybercrime**; however, it has yet to be applied evenly (Council of Europe, 2001). In cases like Riley v., the issue of legal dilemmas related to the ways of accessing and using data on mobile devices and issuing the rights to privacy are depicted. California, 2014 and Carpenter v. United States (2018). The cases illustrate the importance of balanced legal systems that will conduct successful investigations without intrusion into the privacy rights of individuals. The existence of such variation in legal systems in various jurisdictions poses a significant challenge, too. The European Union's stringent data protection rules, which require a need and proportionality in data processing (European Union, 2016), are outlined in the GDPR. On the other hand, the US CLOUD Act allows American officials to demand data stored abroad, and in EU privacy law, it often conflicts (Swire & Hemmings, 2019). Such inconsistency makes international cooperation more difficult, as seen in the EU-US e-evidence agreement negotiations, which illustrate the challenge of striking the right balance between privacy safeguarding and data access.

The Juxtaposition of Forensic Technology and Human Rights: Achieving the right balance between the use of the forensic technology and human rights involves many changes in respect to the law because there has to be no encroachment of the individual rights within the set-up of technological advancements. The current laws are often not able to maintain the pace of evolution of the forensic technology leading to their potential misuse and intrusion of privacy. To eliminate these problems, there are a number of legal amendments to be proposed:

- Better Privacy Defences: Laws like the USA PATRIOT Act (2001) and RIPA (2000) must be updated, to include more stringent privacy safeguards. The amendments ought to entail more stringent restrictions on the gathering of data and monitoring so that the information obtained should be befitting and justified to the necessity control of the investigations. As an example, the integration of GDPR-like measures including the stresses on data minimization and purpose limitation can help decrease privacy violations considerably. Such amendments may also follow the main concepts of data processing in the GDPR in paragraph 5 that involves lawfulness, fairness, and transparency, among others (European Union, 2016).
- Standardization and Validation of Forensic Tools: It is of immense concern to have a protocol of standardized steps as well as validation of the tools in order to make them accurate and reliable. It must be required by legal amendments that all forensic instruments must go through intensive scientific verification to be legitimized in investigations. This is capable of avoiding problems as noted by Casey (2011) whereby a high proportion of the digital forensics tools is not fully validated, thus rising concerns about their credibility and legality in Court proceedings.
- Algorithmic Process Transparency in the Legal framework should demand that forensic technologies reveal the algorithmic processes they utilize. Such openness would enable independent review and evaluation of such tools, and will be verified of any inclinations and fallacies. This would be especially significant when it comes to instances of AI and machine learning, where algorithmic understanding is crucial to address any discriminatory policies and to guarantee reasonable results, as noted by Binns and Veale (2018).

Conclusion

The paper has been able to scrutinize the interface of forensics technologies and crime finance investigation, especially the possible effects of these on human rights. The analysis showed that although digital evidence collection, network and mobile forensics, big data analytics, digital identity verification and intrusion detection systems (IDS) have significant advantages in terms of enhancing the capabilities of an investigation, they also present massive ethical and legal concerns (Tene & Polonetsky, 2013; Casey, 2011). In particular, it is important to note that AI-related forensic tools are fraught with incorrect convictions and discrimination-related malpractices, which is why it is necessary to integrate ethical protection measures into the implementation of technology (Ferrara, 2020). The results also show the continuing research, control and standardisation shortcomings which impede responsible control of forensic technologies. Differences in international standards still hinder the efforts of working across borders, and the lack of privacy protection causes questions about the proportionality and necessity of investigative actions (Swire & Hemmings, 2019; European Union, 2016; UN, 1966). In the absence of strict scientific proofs, the forensics tools will compromise the trustworthiness of evidence during legal proceedings (NIST, 2020). The consequent requirement is that ethical guidelines need to be supplemented by sound oversights to provide transparency, accountability and fairness as it is practiced. Essentially, the future of forensic technology in the area of financial crimes investigation lies in finding a delicate balance between finding the opportunities to use the potential that it offers in the fight against complicated criminal networks on the one hand and ensuring the maintenance of the basic human rights on the other. Societies can only be guaranteed that technological innovation is in the furtherance of justice, and not a subversion of justice, through the harmonious governance structures that are not only informed by ethical, scientific, and legal standards.

Recommendations

- Create consistency between legal and procedural requirements across jurisdictions to allow ease in conducting cross-border digital investigations.

- Instill principles of necessity and proportionality as introduced on the GDPR and ICCPR to every level of forensic investigation in protecting the right of individuals.
- Enact stringent standards on scientific validation and accreditation whereby forensic evidence would be admissible and dependable in courtroom.
- Implement mechanisms of continuous monitoring and auditing in order to maintain accountability, fairness, and transparency in the use of forensic technologies.
- Design legal frameworks to anticipate such issues as algorithmic fairness, due process, non-discrimination where the computer makes the decision to help fewer risks than applying it to forensic investigations.

References

Bigo, D., Carrera, S., Hayes, B., Hernanz, N., & Jeandesboz, J. (2019). *Mass surveillance of personal data by EU member states and its compatibility with EU law*. Centre for European Policy Studies.

Binns, R., & Veale, M. (2018). Is that your final decision? Multi-stage profiling, selective effects, and article 22 of the GDPR. *International Data Privacy Law, 8*(2), 73–87. https://doi.org/10.1093/idpl/ipy004

Brenner, S. W. (2010). Cybercrime: Criminal threats from cyberspace. ABC-CLIO.

Carrier, B. (2003). *Defining digital forensic examination and analysis tools*. International Journal of Digital Evidence, 1(4), 1–6.

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers and the internet* (3rd ed.). Academic Press.

Council of Europe. (2001). *Convention on Cybercrime (Budapest Convention)*. https://www.coe.int/en/web/conventions/full-list

Craig, P., & de Búrca, G. (2015). *EU law: Text, cases, and materials* (6th ed.). Oxford University Press.

European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation)*. *Official Journal of the European Union*, L119, 1–88.

Ferrara, S. D. (2020). Forensic science and miscarriages of justice. *Forensic Science International: Synergy, 2*, 276–285. https://doi.org/10.1016/j.fsisyn.2020.09.003

Greenberg, A. (2014). *This machine kills secrets: How WikiLeakers, cypherpunks, and hacktivists aim to free the world's information*. Penguin.

Healy, P. M., & Palepu, K. G. (2003). The fall of Enron. *Journal of Economic Perspectives, 17*(2), 3–26.

Hussain, A., Nazir, M., & Hashmi, A. H. (2020). Big data analytics for detecting financial crimes. *Journal of Financial Crime, 27*(4), 1103–1115. https://doi.org/10.1108/JFC-04-2020-0053

Hutchinson, T., & Duncan, N. (2012). Defining and describing what we do: Doctrinal legal research. *Deakin Law Review, 17*(1), 83–119. https://doi.org/10.21153/dlr2012vol17no1art70

Koops, B. J. (2012). Ten dimensions of technology regulation: Finding your bearings in the research space of an emerging discipline. In R. Brownsword, E. Scotford, & K. Yeung (Eds.), *The Oxford handbook of law, regulation and technology* (pp. 3–38). Oxford University Press.

Kuner, C. (2017). Data protection, privacy, and security in international law. In C. Kuner, F. Cate, & C. Millard (Eds.), *Transborder data flows and data privacy law* (pp. 15–44). Oxford University Press.

Levi, M., & Reuter, P. (2006). Money laundering. *Crime and Justice, 34*(1), 289–375. https://doi.org/10.1086/501508

Marcella, A. J. (2021). *Cyber forensics: From data to digital evidence*. John Wiley & Sons.

Mayer-Schönberger, V., & Cukier, K. (2013). *Big data: A revolution that will transform how we live, work, and think*. Eamon Dolan/Houghton Mifflin Harcourt.

McDonald, S., Cross, M., & Sheikh, S. (2022). Regulating big data in financial services. *Journal of Banking Regulation, 23*(3), 210–225. https://doi.org/10.1057/s41261-021-00188-9

National Institute of Standards and Technology. (2020). *Digital forensics tool testing program*. NIST. https://www.nist.gov/

Nieto, A., Robalinho, A., & Rodero-Merino, L. (2019). Privacy in digital forensics: Trends and future challenges. *Computer Standards & Interfaces, 66*, 103353. https://doi.org/10.1016/j.csi.2019.103353

Quick, D., & Choo, K.-K. R. (2014). Impacts of increasing volume of digital forensic data: A survey and future research challenges. *Digital Investigation, 11*(4), 273–294. https://doi.org/10.1016/j.diin.2014.09.002

Shah, M., & Issac, B. (2021). Digital forensics in the era of big data: Challenges and future trends. *Future Generation Computer Systems, 118*, 122–135. https://doi.org/10.1016/j.future.2020.12.007

Shebaro, B., & Crandall, J. R. (2011). Privacy-preserving network forensics. *Proceedings of the 2011 ACM Symposium on Applied Computing*, 192–198. https://doi.org/10.1145/1982185.1982221

Swire, P., & Hemmings, A. (2019). Mutual legal assistance in an era of globalized communications: The analytic framework, the significant trends, and the major challenges. *New York University Annual Survey of American Law, 75*, 509–562.

Tene, O., & Polonetsky, J. (2012). Privacy in the age of big data: A time for big decisions. *Stanford Law Review Online, 64*, 63–69.

Tene, O., & Polonetsky, J. (2013). Big data for all: Privacy and user control in the age of analytics. *Northwestern Journal of Technology and Intellectual Property, 11*(5), 239–273.

United Nations. (1948). *Universal Declaration of Human Rights*. UN General Assembly.

United Nations. (1966). *International Covenant on Civil and Political Rights*. UN General Assembly.

United Nations. (2003). *United Nations Convention Against Corruption*. UN Office on Drugs and Crime.