Al-Istinbath
Jurnal Hukum Islam

Vol. 11. No. 1, 2026, 158-192
P-ISSN: 2548-3374 (p), 25483382 (e)
http://journal.iaincurup.ac.id/index.php/alistinbath

Regulatory Gaps in Digital Witness Protection for Cybercrime: Integrating International Standards, Egyptian Law, and Islamic Jurisprudence

Tarek El Sayed Mahmod[1], Khalid Awad Hammadi Al-Alwani [2], Ismael Hellawss[3], Mahmood Shaker Abood Alaloosh[4], Salah Ragab Fathelbab[5]

College of Law, University of Al Maarif, Iraq[1,2,5]
College of Law, University of Fallujah, Iraq[3]
Faculty of Administration and Economics, University of Kirkuk, Iraq[4]

Corresponding author: Khalid.awad@uoa.edu.iq

DOI: 10.29240/jhi.v11i1.16326

Received: 30/09/2025	Revised: 08/02/2026	Accepted: 11/04/2026

Cite this article:	Tarek El Sayed Mahmod, Khalid Awad Hammadi Al-Alwani, Ismael Hellawss, Mahmood Shaker Abood Alaloosh, Salah Ragab Fathelbab (2026), Regulatory Gaps in Digital Witness Protection for Cybercrime: Integrating International Standards, Egyptian Law, and Islamic Jurisprudence, Approach. Al-Istinbath : Jurnal Hukum Islam, 11 (1), 2026, 158-192. DOI : 10.29240/jhi.v11i1.16326

Abstract

This study examines regulatory gaps in digital witness protection in cybercrime by analyzing the relationship between international standards, Egyptian law, and Islamic jurisprudence. The increasing use of digital testimony in cybercrime cases has not been matched by adequate legal protection, exposing witnesses to risks such as cyber intimidation, data leakage, and cross border retaliation. This study aims to identify these gaps and develop an integrated legal approach that strengthens witness protection while maintaining the integrity of criminal justice. The research applies a normative juridical approach supported by descriptive, analytical, and comparative methods. It analyzes the United Nations Convention on Cybercrime, Egyptian legislation on information technology crimes, and Islamic legal principles related to testimony and protection. The findings show that international standards provide relatively comprehensive protection through mechanisms such as anonymity, remote testimony, and relocation. In contrast, Egyptian law lacks specific provisions addressing digital risks, particularly in relation to technical safeguards, remote protection mechanisms, and international cooperation. From the perspective of Islamic jurisprudence, witness protection is closely linked to the objectives of Sharia, especially the protection of life, dignity, and

property, as well as the obligation to ensure truthful testimony without coercion. These principles provide a strong normative basis for adopting modern protection mechanisms, including digital anonymization and remote testimony. The study concludes that addressing regulatory gaps requires the integration of international standards with national legislation supported by Sharia based principles. It proposes a comprehensive model of digital witness protection that combines legal, technological, and ethical safeguards to enhance witness security, strengthen legal certainty, and improve the effectiveness of cybercrime enforcement in transnational contexts.

Keywords: Digital witness protection; Cybercrime; Regulatory gaps; International legal standards; Egyptian law; Islamic jurisprudence; Comparative law; Cybersecurity law

Introduction

The rapid expansion of digital technologies has fundamentally transformed the landscape of criminal activity, giving rise to increasingly complex forms of cybercrime that transcend national boundaries and conventional legal frameworks. This transformation has also reshaped the role of evidence in criminal proceedings, where digital testimony and electronically mediated information have become central to establishing criminal liability.[1] In this context, witnesses no longer operate solely within physical environments but are increasingly embedded within digital ecosystems that expose them to novel and sophisticated risks. These risks include cyber intimidation, data breaches, online defamation, and cross border retaliation, all of which significantly undermine the willingness of individuals to cooperate with law enforcement authorities. As a result, the effectiveness of criminal justice systems in addressing cybercrime is increasingly dependent on the availability of robust and adaptive witness protection mechanisms capable of responding to these emerging threats.

From a social perspective, the growing reliance on digital infrastructure has intensified vulnerabilities not only for victims but also for witnesses who play a critical role in uncovering cyber offenses. The integration of technologies such as artificial intelligence, cloud computing, and the Internet of Things has enabled perpetrators to exploit digital environments in ways that facilitate anonymity and complicate detection.[2] Consequently, witnesses who possess crucial information

[1] Immanuel Ustradi Osijo et al., "The Legal Politics of Halal Tourism in Thailand: The Impact of Digital Advertising Interventions on Consumer Intent, Recommendations, and Engagement in the Contemporary Era," *MILRev: Metro Islamic Law Review* 3, no. 2 (December 30, 2024): 320–42, https://doi.org/10.32332/MILREV.V3I2.9992.

[2] Ismawati Septiningsih, "Consumer Protection in the Digital Era," *Journal Of Law Studies* 2, no. NO.2 (2023): 1–8, https://doi.org/10.5281/zenodo.17376951.

are often exposed to technologically mediated forms of retaliation that extend beyond traditional physical threats. These developments highlight a significant gap between the evolution of cybercrime and the capacity of existing legal systems to provide adequate protection for those who contribute to the administration of justice. The urgency of addressing this gap is further reinforced by the transnational nature of cybercrime, which requires coordinated legal responses and harmonized standards across jurisdictions.

In terms of existing scholarship, a growing body of literature has examined witness protection in criminal law, as well as whistleblower protection in the context of cybercrime.[3] Previous studies have explored confidentiality measures, procedural safeguards, and the use of technology such as remote testimony to enhance witness safety. Comparative analyses between national legal systems and international frameworks have also provided valuable insights into the development of witness protection programs. However, these studies largely focus on traditional witnesses or whistleblowers and tend to overlook the specific vulnerabilities associated with digital witnesses operating within cyber environments. Moreover, there remains limited integration between international legal standards, domestic legislation, and Islamic jurisprudence in addressing witness protection. While some research acknowledges the importance of ethical and legal principles derived from Islamic law, few studies systematically incorporate these principles into contemporary legal frameworks for cybercrime.

This study identifies a critical gap in the literature concerning the absence of a comprehensive and integrated approach to digital witness protection that bridges international standards, national legal systems, and Islamic jurisprudential principles. In particular, there is insufficient attention to the regulatory deficiencies that arise when existing legal frameworks fail to address technologically driven threats such as cyber intimidation, digital identity exposure, and cross border risks. Additionally, current research does not adequately provide normative models that can guide the development of legal systems in jurisdictions where Islamic law constitutes an important source of legal reasoning. This gap underscores the need for a more holistic analysis that not only evaluates existing frameworks but also proposes a coherent model for reform.

Accordingly, this study aims to examine the regulatory gaps in digital witness protection within the context of cybercrime by conducting a comparative analysis of international legal standards, Egyptian law, and Islamic jurisprudence. It seeks to answer the following central question: to what extent do existing legal frameworks provide effective protection for digital witnesses in cybercrime cases, and how can these frameworks be improved through an integrated legal

[3] Sophia Anne Milleer, "Integrating Local Wisdom and Global Knowledge to Develop Culturally Responsive Education Models," *Nusantara Education* 5, no. 1 (n.d.): 25–33.

approach? Unlike previous studies, this research focuses specifically on the concept of the digital witness and the unique risks associated with digital environments, while also incorporating Islamic jurisprudential principles as a normative foundation for legal reform.

The main argument advanced in this study is that current legal frameworks remain fragmented and insufficient in addressing the complex realities of digital witness protection in cybercrime. While international standards offer relatively advanced mechanisms, their effectiveness is limited by weak implementation at the national level. At the same time, domestic legal systems such as Egyptian law exhibit significant regulatory gaps, particularly in relation to technological safeguards and cross border cooperation. This study further argues that Islamic jurisprudence provides a robust ethical and legal foundation that can support the development of modern witness protection mechanisms, particularly through its emphasis on the protection of life, dignity, and justice. Therefore, integrating international standards with national legislation and Sharia based principles is essential to developing a comprehensive and adaptive framework capable of addressing the challenges posed by cybercrime.

By December 2024, the United Nations succeeded in establishing a global convention aimed at combating cybercrime, placing particular emphasis on witness protection. Undoubtedly, this underscores the critical importance of testimony in cybercrime cases and ensures that witnesses are encouraged to provide their testimony without fear, thereby contributing to the mitigation of these crimes.

Considering the principles of international human rights law, witness protection is not merely a modern legal concept, but also has a solid foundation in Islamic jurisprudence, which constitutes an important part of the legal heritage in many Islamic countries. The objectives of Sharia emphasize the preservation of life, honor, and property as a fundamental value system aimed at protecting individuals and society from injustice and harm, making the protection of witnesses an integral part of ensuring justice and preventing intimidation and oppression.[4]

Moreover, giving testimony in Islam is considered a religious trust as well as an ethical and legal duty that must be fulfilled. Islamic texts explicitly prohibit the concealment of testimony and regard it as an essential aspect of justice necessary for achieving the objectives of Sharia and maintaining social security. This grounding demonstrates that the concept of witness protection particularly in serious crimes such as cybercrime aligns with the principles of justice and

[4] Miftah Aghnayah Mohammed Aghnayah, "Protecting the Right to Life: A Legal Study in Maqasid Thought," *Al-Haq Journal for Sharia and Legal Sciences* 2, no. 1 (2015): 186–220, https://doi.org/10.58916/alhaq.v2i1.213.

human dignity found in both classical and contemporary Islamic sources and is not limited to modern positive law alone.[5]

Given the novelty of the topic of witness protection in cybercrimes, this study can be considered the first to comprehensively address witness protection under the Global Convention on Cybercrime, in comparison with Egyptian national legislation and analyzed from an Islamic jurisprudential perspective. Nevertheless, there exists a body of previous studies that have examined either the protection of whistleblowers in cybercrimes or witness protection in traditional crimes, which can be summarized as follows.

One of the earliest of these studies is by *Ahmed M. Bamashmoos*, which focused on the rules governing witness protection in the Saudi legal system in comparison with U.S. law. The study examined confidentiality protocols, technical protection measures, and the possibility of remote testimony, and discussed ways to develop these laws to address emerging threats, particularly electronic intimidation.[6]

As for the study by *Al Shorbagi*, it focused on the criminal protection of witnesses and whistleblowers by examining the position of national legislation and international efforts, while also highlighting the protection afforded to witnesses under international criminal justice. Although the study did not address digital witnesses, it recommended the use of modern technologies to provide the highest possible level of protection for witnesses across all types of crimes without discrimination.[7]

The 2024 report by *the Office of Global Criminal Justice* provides an official analysis published as part of the U.S. Department of State's series on the protection of witnesses testifying against complex criminal networks, including cybercrimes. The report emphasizes the differences between traditional protection measures and the need for modern technological mechanisms to ensure the safety of witnesses.[8]

In another study, *Stefan Bettina (2022)* adopted a multidisciplinary approach to examine reporting of cybersecurity violations and mechanisms for

---

[5] Abdulrahman Abdulqader Abdulqader, "Himayat al-Shahada fi al-Shari'ah al-Islamiyah wa al-Nuzum al-Wad'iyah al-Mu'asirah," *Academic Journal of Research and Scientific Publishing* 7, no. 73 (2025), https://doi.org/10.52132/Ajrsp/v7.73.1.

[6] A. M. Bamashmoos, "Witness Protection Programs: A Comparative Analysis of Saudi Arabian and U.S. Legal Mechanisms," *Journal of Humanities and Administrative Sciences, Shaqra University* 12, no. 2 (2025): 372–380.

[7] Ahmed Abdel Fattah Al-Shorbagi, *Criminal Protection for Witnesses and Whistleblowers in National and International Law* (PhD diss., Faculty of Law, Ain Shams University, 2024).

[8] United Nations Office on Drugs and Crime (UNODC), *Good Practices for the Protection of Witnesses in Criminal Proceedings Involving Organized Crime* (Vienna & New York: United Nations, 2008), https://www.unodc.org/documents/organized-crime/Witness-protection-manual-Feb08.pdf.

protecting whistleblowers. The study focused on measures adopted within the European Union, outlined the ethical frameworks surrounding the concept of anonymity and its legitimate boundaries, and concluded that collaboration among legal, technological, and social science experts is essential to ensure whistleblower protection while simultaneously serving the public interest.[9]

Despite the significance of these studies, several major gaps remain. First, there is a lack of focus on digital witnesses, as most studies concentrated on whistleblowers or witnesses in traditional crimes without addressing the specific vulnerabilities of witnesses in digital environments and the evolving threats posed by cybercrime. Second, there is limited comparison between international legislation, national law, and Islamic jurisprudence regarding the concept of witness protection and its implications for the design of modern legislation in Islamic countries. Finally, practical solutions are largely absent, as previous studies did not provide legislative proposals or operational frameworks to align national laws with international standards for effectively protecting digital witnesses.

Building on these gaps, the present study aims to analyze the digital witness, identify the risks associated with testifying in cybercrime cases, compare international frameworks with Egyptian legislation, and develop legislative and technical proposals consistent with Islamic jurisprudential principles and international standards. To comprehensively address these issues, the study employs a combination of methodologies: a descriptive approach to outline the context, an analytical method to examine the provisions of the new convention and its witness protection measures, and a comparative approach to evaluate the international standards against the Egyptian legislative framework, identifying deficiencies and proposing a model that could be adopted in Egyptian law to harmonize with global norms.

The study aims to provide a holistic analysis of witness protection in cybercrime, integrating international standards, Egyptian legislation, and Islamic jurisprudential perspectives. It seeks to define the concept of the digital witness, assess the nature of the risks they face in transboundary electronic environments including digital intimidation, cyber retaliation, geographic tracking, and cyber-extortion and compare the international frameworks established by the Global Convention on Cybercrime with current Egyptian law, highlighting strengths and shortcomings in national legislation. The analysis also examines practical and technological measures for witness protection, such as remote testimony, digital anonymity, and relocation, ensuring a balance between the witness's right to protection and the accused's right to a fair trial.

---

[9] Bettina Berendt and Stefan Schiffner, "Whistleblower Protection in the Digital Age – Why 'Anonymous' Is Not Enough: From Technology to a Wider View of Governance," *The International Review of Information Ethics* 31, no. 1 (2022), https://doi.org/10.29173/irie479.

From an Islamic jurisprudential perspective, the study explores the legal and ethical foundations for witness protection, ensuring testimony is given truthfully and honestly while safeguarding individuals from coercion or intimidation, in line with the objectives of Sharia in preserving life, honor, and property and achieving justice. Ultimately, the study is expected to provide practical and legislative recommendations for aligning Egyptian law with international standards, developing comprehensive protection mechanisms for digital witnesses, enhancing confidence in the judicial system, encouraging witnesses to testify without fear, reducing cybercrime proliferation, and adhering to Islamic ethical and legal values as a foundational framework.

Discussion

Conceptual Framework

In the contemporary era, humans live within two parallel worlds: one is the physical, real-world environment, and the other exists in the digital or cyber space realm.existence of legal safeguards and practical Undoubtedly, the [10] measures aimed at protecting society from all forms of deviant behavior in both of these worlds constitutes the primary means through which the state can ensure the protection of its citizens.'[11]

Despite the benefits brought about by technological advancement, it has directly contributed to threatening societies and their stability, particularly with the rise of cybercrimes, which have emerged as a major challenge with complex humanitarian, social, and economic implications.The exploitation of [12] technological developments by terrorist groups for promoting extremist ideologies and recruitment, coupled with the notable increase in organized crime, and the inherently transboundary nature of cyber offenses, has amplified the risks to the point that they have become a global threat requiring effective frameworks to address them. There is broad consensus that successfully countering these transboundary crimes requires the development of multidisciplinary models alongside the provision of legal protection, the enhancement of national cybersecurity capabilities, advocacy for global cooperation, raising awareness of

[10] A. Okeal and Tarek Elsayed Mahmoud, "The Role of Interdisciplinary Studies in Establishing the Rules of Technical Criminal Law – An Analytical Study," *Researcher Journal for Legal Sciences* 5, no. 2 (2024): 95–113, https://uofjls.net/index.php/new/article/view/226.

[11] Zamroni Zamroni and Basri Basri, "Legal Protection for Victims of Cybercrime as a Form of Transnational Crime," *Jurnal Ius Constituendum* 9, no. 1 (2024): 130–49, https://doi.org/10.26623/jic.v9i1.8288.

[12] K. Achuthan, S. Khobragade, and R. Kowalski, "Cybercrime through the Public Lens: A Longitudinal Analysis," *Humanities and Social Sciences Communications* 12 (2025): 282, https://doi.org/10.1057/s41599-025-04459-x.

cybersecurity issues, and the implementation of preventive measures against cyber offenses.[13]

Given the nature and severity of cybercrimes, it is essential to establish legal frameworks that ensure the protection of witnesses, considering it as one of the key mechanisms for curbing crimes in general and transboundary offenses in particular.[14]

The primary objective of witness protection measures is to enable witnesses to provide testimony in courts or cooperate with law enforcement investigations without fear of intimidation or retaliation. Such protection is essential for upholding the rule of law.[15]

Challenges and Significance of Testimony in Cybercrimes

Testimony remains a fundamental form of evidence in criminal justice; however, in the context of cybercrime, its role has become increasingly complex due to the digital environment in which witnesses operate. Unlike traditional settings, digital witnesses are exposed to technologically mediated risks, including data breaches, cyber intimidation, and online retaliation, which challenge the effectiveness of existing legal protection mechanisms.[16]

Witness protection programs and policies in various countries aim to achieve justice in criminal cases by ensuring the safety of witnesses and securing their cooperation, thereby facilitating prosecution and strengthening the judicial system. [17] Additionally, different legislations recognize the challenges witnesses

---

[13] Mohammad Fadil Imran, "Cyber Criminology and Human Security: An Analysis of ASEAN Countries Police's Paradigm," *Journal of Human Security* 18, no. 1 (2022): 49–53, https://doi.org/10.12924/johs2022.18010034.

[14] Zamroni Zamroni, Basri Basri, Legal Protection for Victims of Cybercrime as a Form of Transnational Crime, Jurnal Ius Constituendum,vol.9, No.1, 2024, pp.133: 143, at: https://journals.usm.ac.id/index.php/jic/article/view/8288

[15] United Nations Office on Drugs and Crime (UNODC), *Witness Protection*, in *UNODC Teaching Module Series: Organized Crime*, accessed February 3, 2026, https://www.unodc.org/cld/en/education/tertiary/organized-crime/module-9/key-issues/witness-protection.html.

[16] Abu Bakr Al-Deeb, Dina Ibrahim, Reflections of Artificial Intelligence on the Rules of Evidence, Journal of Legal and Economic Research, Faculty of Law, Mansoura, Volume 14 Special Issue April 2024, pp. 1065-1066, https://doi.org/10.21608/mjle.2024.386604

[17] Abdul Rahman, Ahmed Talaat Abdul Hakim. (2025). Substantive and Procedural Criminal Protection of the Witness in Comparative Law. The Legal Journal, 24(4), 1607-1660, https://doi.org/10.21608/jlaw.2025.380168.1243

may face and provide certain accommodations within the legal framework, helping witnesses fulfill their obligation to testify without undue burden.[18]

Testimony in cybercrimes holds particular significance due to the unique characteristics of these offenses, which pose numerous challenges related to prosecuting perpetrators and establishing proof. Some argue that there are considerable obstacles in investigating and pursuing those responsible for such crimes, as offenders employ advanced techniques to evade forensic evidence, alongside legal and resource-based challenges that hinder prosecution.These [19] factors impede criminal investigations, making convictions difficult to obtain. Challenges in conducting investigations on online social networks highlight a gray area regarding crime prevention and citizen safety on the internet worldwide. Consequently, the importance of testimony becomes evident, and it is crucial to protect and assist witnesses in their interactions with the criminal justice system to ensure their effective cooperation with law enforcement agencies and the provision of the most reliable evidence in court.

For testimony to be accepted as valid evidence by a criminal court, it is essential to enable witnesses to provide information freely and without any pressure or coercion. Criminal justice requires balancing the witness's right to protection with the rights of the accused, thereby contributing to the establishment of justice. It is widely agreed that for witness protection measures to be effective in addressing cybercrimes, strong coordination between countries and international cooperation in implementing these measures are essential.[20]

The following section clarifies the concept of testimony in relation to crimes committed in the digital environment, distinguishing it from other forms of testimony, and then highlights the risks faced by witnesses in such crimes, which necessitate the establishment of clear frameworks that provide them with the highest level of protection.

The Nature of the Witness in Cybercrimes and Its Distinction

In criminal law, the concept of a witness refers to an individual who possesses information or facts relevant to a criminal case, with such information having evidentiary value. The witness is required to appear before the competent

---

[18] Abdulla Hamad O. J. Al-Ghayathin et al., "Protection of Witnesses in Criminal Lawsuits: An Analytical Study," *PETITA: Jurnal Kajian Ilmu Hukum dan Syariah* 10, no. 1 (2025): 419–434, https://doi.org/10.22373/petita.v10i1.710.

[19] Bandr Fakiha, "Digital Forensics: Crimes and Challenges in Online Social Networks Forensics," *Journal of the Arab American University* 6, no. 1 (2020): 19–28.

[20] Sunbal Islam Chaudhary and Naseem Razi, "Witness Protection in Global Perspective: An Analysis of International Laws," *Contemporary Journal of Social Science Review* 2, no. 4 (2024): 171–84.

authorities to provide the information they hold. Witnesses in criminal cases can be classified into the following categories:[21]

1. Victim witnesses: These are individuals who have suffered harm as a result of the crime and, without doubt, play a central role in the investigation and trial process.
2. Expert or cooperating witnesses: These include individuals who assist justice, such as technical or scientific experts. They usually provide information about the crime based on their professional knowledge and experience, without having a direct connection to the offense itself.
3. Informant witnesses: These are individuals who provide authorities with crucial information about crimes committed by others; in some cases, the informant may have been involved in the criminal activity themselves.

In all cases, the classification of witnesses should take into account the level of risks they may face and the impact of their testimony on the course of criminal proceedings, in order to design protection programs that are tailored to their specific circumstances.[22]

In addition to these categories, we propose the concept of the cyber witness, which refers to a technical device or smart sensor that monitors and records digital activities and data related to a specific incident within the digital environment. This cyber witness relies on automated, unbiased tracking of big data and event logs,thereby enhancing the investigative authorities' ability to [23] accurately reconstruct the digital crime scene and reducing the likelihood of

---

[21] United Nations Office on Drugs and Crime (UNODC), *Good Practices for the Protection of Witnesses in Criminal Proceedings Involving Organized Crime* (Vienna & New York: United Nations, 2008), 19, https://www.unodc.org/documents/middleeastandnorthafrica/organised-crime/Good_Practices_for_the_Protection_of_Witnesses_in_Criminal_Proceedings_Involving_Organized_Crime.pdf. United Nations Office on Drugs and Crime (UNODC), *Witness Protection*, in *UNODC Teaching Module Series: Organized Crime*, accessed February 3, 2026, https://www.unodc.org/cld/en/education/tertiary/organized-crime/module-9/key-issues/witness-protection.html.

[22] Karen Kramer, "Protection of Witnesses and Whistle-Blowers: How to Encourage People to Come Forward to Provide Testimony and Important Information," in *149th International Training Course Visiting Experts' Papers* (Tokyo: UNAFEI, 2025), 18–23, https://www.unafei.or.jp/publications/pdf/RS_No86/No86_07VE_Kramer.pdf.

[23] Calvin Wai-Loon Ho and Karel Caals, "A Call for an Ethics and Governance Action Plan to Harness the Power of Artificial Intelligence and Digitalization in Nephrology," *Seminars in Nephrology* 41, no. 3 (2021): 282–293, https://doi.org/10.1016/j.semnephrol.2021.05.009.

human manipulation of testimony. Some scholars also advocate for the use of intelligent technologies to verify the credibility of such evidence.[24]

Some tend to confuse the concept of the cyber witness with electronic evidence[25]. When intelligent technologies are regarded as witnesses, the protection mechanisms applicable to them differ from those concerning the human witnesses discussed in this study.

The concept of testimony differs from reporting, as the latter constitutes one of the key pillars of cybersecurity legislation. Through reporting, rapid responses to cyberattacks can be achieved and effectively managed[26]. On the other hand, the informant may also be the victim of the crime, turning to law enforcement agencies for assistance and support. Some researchers have highlighted that the extent of response from the relevant authorities varies depending on the type of crime and the level of risk involved[27]. In all cases, strategies for reporting cybercrimes must be well-coordinated to ensure effective prevention and mitigation of these offenses.[28]

In some countries, such as Scotland, the rate of reporting cybercrimes is low, partly due to the cybersecurity policies adopted by the United Kingdom. Victims often blame themselves, and the lack of adequately trained law enforcement personnel to handle such crimes discourages victims from reporting incidents, as the level of protection provided is insufficient. This situation has led some researchers to propose strategies aimed at enhancing the reporting of cybercrimes.[29]

---

[24] Sumaya Jiad Al-Hamdani, "Criminal Evidence in the Digital Age: Towards an Intelligent System for Verifying the Credibility of Electronic Evidence," Supreme Judicial Council (Iraq), accessed February 6, 2026, https://www.sjc.iq/view/77460/.

[25] Ayman Abdullah Fikri Hassan, "Electronic Witness in Criminal Evidence," *Journal of Sharia and Law in Cairo* 44, no. 44 (2024): 3543–3607, https://doi.org/10.21608/mawq.2025.335120.1107.

[26] Simone Busetti and Francesco Maria Scanni, "Evaluating Incident Reporting in Cybersecurity: From Threat Detection to Policy Learning," *Government Information Quarterly* 42, no. 1 (2025), https://doi.org/10.1016/j.giq.2024.102000.

[27] Rachel L. McNealey, Camille I. Figueroa, and Cooper A. Maher, "'Police Can't Help You': Exploring Influences on Perceptions of Policing Cybercrime," *Journal of Criminal Justice* 101 (2025), https://doi.org/10.1016/j.jcrimjus.2025.102542.

[28] James Popham, Mary McCluskey, Michael Ouellet, and Owen Gallupe, "Exploring Police-Reported Cybercrime in Canada," *Policing: An International Journal* 43, no. 1 (2020): 35–48, https://doi.org/10.1108/PIJPSM-08-2019-0128.

[29] Juraj Sikra, Karen V. Renaud, and Daniel R. Thomas, "Investigating What Promotes and Deters Scottish Cybercrime Reporting," *Journal of Economic Criminology* 6 (2024), https://doi.org/10.1016/j.jeconc.2024.100103.

Some legislations have developed police mechanisms for investigating organized crime and cybercrimes. Among these is Spanish law, which authorizes the use of undercover agents. Spanish legal scholars define an undercover agent as a specialized officer within the judicial police, appointed by the competent judicial authority to infiltrate criminal organizations, conceal their identity, or assume a temporary false identity, and to pose as part of the organization to identify perpetrators and participants. In this sense, the undercover agent serves as a tool for law enforcement infiltration. This concept differs from that of an informant, who is another traditional investigative resource, typically involved only in police investigations. Informants usually belong to criminal circles and provide information to the police, not necessarily out of altruism, but often in exchange for money or preferential treatment from law enforcement officers.[30]

Thus, an undercover agent is a law enforcement officer performing a specific function, whereas a witness is an individual who possesses information about a crime that helps identify and prosecute the perpetrator, without the role being part of their official duties. Despite this distinction, under Spanish law, an undercover agent is entitled to protection in the capacity of a witness.

Testimony and Witness Protection in Islamic Jurisprudence:

In Islamic jurisprudence, testimony is considered one of the fundamental forms of criminal evidence, upon which rights are established and truth is revealed. Sharia regards it as a means to achieve justice and safeguard the interests of society. Accordingly, Islamic texts emphasize providing testimony with sincerity and truthfulness, while prohibiting the concealment or collusion to hide it, which could lead to injustice and harm. Scholars define testimony as conveying the truth to others with the intention of establishing justice. Reporting what the witness has observed and presenting it before the court is regarded as a religious responsibility and a trust that must be fulfilled without distortion or falsification to ensure the administration of justice.

Islamic jurisprudence requires certain conditions and attributes for an individual to serve as a witness, ensuring their ability to give testimony in a manner acceptable to Sharia. The most important of these include justice, honesty, and the freedom to testify. Al-Zuhaili explains that Islam requires the witness to be sane, mature, and free for their testimony to be accepted. Jurists have emphasized that freedom and the absence of coercion are essential for giving evidentiary value

---

[30] A. Valiño Ces, "The Importance of the Computer Undercover Agent as an Investigative Measure Against Cybercrime: A Special Reference to Child Pornography Crimes," in *Legal Developments on Cybersecurity and Related Fields*, ed. F. A. Carneiro Pacheco de Andrade, P. M. Fernandes Freitas, and J. R. de Sousa Covelo de Abreu, *Law, Governance and Technology Series*, vol. 60 (Cham: Springer, 2024), 143–62, https://doi.org/10.1007/978-3-031-41820-4_9.

to testimony, as any external influence on the witness's will undermines the responsibility of the testimony and compromises justice.[31]

In Islamic law, witness protection is intrinsically linked to the performance of testimony and the achievement of justice objectives, including the protection of life, property, and dignity. Jurists have theorized that the Sharia judge or authority is obligated to provide guarantees that shield witnesses from all forms of intimidation or pressure that might hinder their testimony or prevent them from fulfilling their duty. Such safeguards are essential because any obstruction to the witness's ability to testify can impede the establishment of justice and weaken the evidentiary value of testimony in criminal proceedings.[32]

Risks and Threats Associated with Testimony

Witnesses in cybercrime cases face numerous risks as a result of providing testimony. Among the most significant of these risks are:

Digital Retaliation and Online Defamation: Witnesses in cybercrime cases are increasingly exposed to systematic digital harassment, where offenders exploit their technical skills to breach the witness's privacy and disseminate personal or family information on social media platformsa phenomenon known as *doxing*. This behavior aims to damage the witness's social and professional reputation as a form of psychological pressure to dissuade them from testifying or as retaliatory punishment. The danger of this threat is heightened by the difficulty of controlling digital content once it spreads, leaving the witness in a state of continuous exposure to cyberattacks, which may escalate to identity theft or financial extortion. This, in turn, weakens the flow of critical information to law enforcement agencie[33]

Geolocation Tracking via Technical Vulnerabilities: The ability of perpetrators to determine the witness's geographical location constitutes one of the most severe threats arising from cybercrime. Cyber criminals can exploit *digital traces* left by the witness in daily life to pinpoint their exact location. This can be achieved through tracking IP addresses, compromising smart devices linked to the witness, or analyzing meta data from images and files they share. Such risks

---

[31] Abdullah Ali Al-Shibili, Ahmad Zaki Saleh, and Mohamad Zaharuddin Zakaria, "Witness Testimony and its Impediments between Islamic Law and Contemporary Laws," *Malaysian Journal of Syariah and Law* 7, no. 1

[32] Abd al-Rahman Bin Rais, "Protection of the Witness in Criminal Law between Statutory Law and Islamic Jurisprudence," *Maroc Law*, 2024, accessed February 5, 2026, https://maroclaw.com/.

[33] Cyberbullying: The New Face of Digital Revenge: Young People's Personal Data at Risk!," *Indigo Dergisi*, February 2026, accessed February [day], 2026, https://indigodergisi.com/ar/2026/02/.

transform a virtual threat into a tangible danger, endangering the physical safety of the witness and their family. Traditional witness protection measures are insufficient unless complemented by advanced cybersecurity protocols that ensure the witness is digitally insulated. [34]

Cyber Intimidation: *Systematic cyber intimidation* represents a novel method of obstructing justice, replacing traditional physical coercion with highly effective psychological and digital pressure. This criminal innovation involves the use of hostile algorithms and artificial intelligence to launch automated intimidation campaigns targeting the witness in their personal digital space, such as flooding accounts with encrypted threat messages or employing *deepfake* technology to create fabricated visual content placing the witness in compromising or illegal scenarios for extortion purposes. The danger of this form of intimidation lies in its ability to breach state-imposed physical security barriers, leaving the witness under continuous virtual persecution with no geographical limits, leading to what is described as *digital moral assassination*, aiming to break the witness's free will and compel silence or retraction of statements. [35]

The Islamic Dimension in Analyzing Digital Risks

The cyber threats faced by witnesses in the digital environment cannot be addressed solely from a technical criminal perspective; they can also be analyzed within the framework of Islamic law, which places great emphasis on protecting life, honor, property, and the sanctity of private life. In Islamic jurisprudence, digital defamation and the dissemination of false information online are considered actions that harm the dignity and reputation of individuals. These acts can be approached as equivalent to slander, libel, and forbidden backbiting in Islam, as spreading falsehoods or defamatory content without evidence violates the objectives aimed at preserving honor and reputation. Recent studies have examined the regulation of such phenomena in the context of the ethical use of social media within the Islamic criminal framework.

Regarding the violation of digital privacy and breaches of personal data, Islamic jurisprudence emphasizes the prohibition of spying and encroachment on others' privacy. Infringing on personal data in the digital sphere is considered as

---

[34] Esaam Eldeen Abdel Al Al-Sayed, "Legislative Confrontation of Extortion and Cyber Threat Offences in UAE Law: Comparative Study of Egyptian Law," *Al Fikr Al Sharati* 33, no. 129 (2024): 63–118.

[35] Yaqoub Belbashir, "Cybercrime in the Age of Artificial Intelligence: A Look at the Challenges and Emerging Risks," *Journal of Human Rights and Public Freedoms* 10, no. 2 (Algeria, 2025): 249–27. Ali Abdul Hussein Alwan, "Cyberbullying and its Impact on Freedom of Expression on Social Media: A Field Study of Professors at the University of Diyala," *Journal of Media Studies and Research* 3, no. 10 (2025): 300–312, https://msar.edu.iq/index.php/msar/article/view/115/53.

harmful as a physical violation of a person's sanctity in the real world, and such harm must be prevented to protect individual dignity.[36] Electronic extortion and the exploitation of personal data for unlawful gain can be viewed within Sharia as illicit appropriation of others' wealth or exploitation of individuals, which is prohibited due to its unjust nature and the harm it inflicts on individuals and society. Modern fiqh studies have addressed such conduct as a violation of the Sharia objectives of protecting property and safeguarding society from injustice.[37]

Finally, cyber intimidation or digital psychological pressurewhere perpetrators employ advanced technologies to terrorize, extort, or defame witnesses constitutes a form of corruption and coercion that conflicts with Islamic legal principles prohibiting harm to others. These principles require the protection of individuals from psychological and social harm, highlighting the necessity of integrating both Islamic and positive law measures to safeguard society from such violations.[38]

Witness Protection Mechanisms in the Global Convention Compared to Egyptian Law

Witness protection in cybercrime cases constitutes one of the key mechanisms adopted by the United Nations Convention to combat cybercrime. The Convention encourages witnesses to provide testimony while establishing safeguards that ensure their legitimate right to protection from retaliation. At the national level, various countries have placed special emphasis on addressing cybercrime. Some nations have enacted specific legislation to combat technical crimes, while others, such as India, have opted to make comprehensive amendments to their criminal laws to more effectively address contemporary offenses.[39]

Regarding witness protection, some countries have recently introduced dedicated legislation on this matter, whereas others have relied solely on provisions within their traditional laws. In some cases, such as Tanzania, existing legislation was supplemented in 2023 by the National Prosecution Authority, which issued a set of guidelines aimed at streamlining witness protection

---

[36] Tholfikar Kadhim, "Applicable Law Governing Electronic Violation of Privacy Rights," *Al-Sharaa: Journal for Legal and Administrative Studies* 5, no. 1 (2025): 140–184.

[37] Tamara Ibrahim Mohsen Al-Battawi, "The Role of Collective Ijtihad in Cybersecurity Issues," *Journal of the College of Islamic Sciences*, no. 84 (2025), accessed [insert date of access], https://jcois.uobaghdad.edu.iq/index.php/2075_8626/article/view/2618.

[38] Jurisprudence and Positive Law." Al-Diraya 25 (26): 255–320. https://doi.org/10.21608/drya.2025.410433.

[39] Dr. Rahul Kailas Bharati, "The New Criminal Law Paradigm in India and Its Impact on Cybercrime Adjudication," July 24, 2025, https://doi.org/10.70593/978-93-7185-183-1, available at SSRN: https://ssrn.com/abstract=5378219.

procedures and providing guidance to investigators, prosecutors, and law enforcement personnel on implementing the law. This section is dedicated to presenting the primary witness protection mechanisms outlined in the United Nations Convention on Cybercrime, in comparison with the provisions currently applied under Egyptian law, while highlighting the deficiencies within the Egyptian legal framework.[40]

Witness Protection Frameworks under the International Convention on Cybercrime

Unlike the Budapest Convention, the United Nations Convention on Cybercrime emphasizes the importance of providing protection for witnesses in cybercrime cases, considering it an essential component of criminal justice. Article 1 of the Convention states that its purpose is to promote and enhance measures aimed at efficiently preventing and combating cybercrime, as well as to encourage international cooperation in this area. [41]

Pursuant to Article 33 of the Convention, State Parties are obliged to take measures under domestic law to provide effective protection from all forms of intimidation or retaliation that a witness may face when giving testimony, or any person who, in good faith, provides information about criminal acts covered by the Convention. The same protection extends to anyone who cooperates in any manner with the competent authorities in pursuing these offenses. According to the provisions, protection measures are not limited to the individual witness but, if necessary, extend to relatives and anyone closely associated with the witness.[42]

---

[40] National Prosecutions Service of Tanzania, *Witness Care and Protection Guidelines*, issued May 1, 2023, under the National Prosecutions Service Act, Cap. 430, accessed February 5, 2026, https://tanzlii.org/en/akn/tz/doc/guidelines/2023-05-01/witness-care-and-protection-guidelines/eng@2023-05-01

[41] United Nations Convention against Cybercrime, Article 1" The purposes of this Convention are to:

(a) Promote and strengthen measures to prevent and combat cybercrime more efficiently and effectively.

(b) Promote, facilitate and strengthen international cooperation in preventing and combating cybercrime; and

(c) Promote, facilitate and support technical assistance and capacity-building to prevent and combat cybercrime, in particular for the benefit of developing countrie" at: https://www.unodc.org/unodc/en/cybercrime/convention/text/convention-full-text.html

[42] Article 33/1 "Each State Party shall take appropriate measures, in accordance with its domestic law and within its means, to provide effective protection from potential retaliation or intimidation for witnesses who give testimony or, in good faith and on reasonable grounds, provide information concerning offences established in accordance with this Convention or otherwise cooperate with investigative or judicial authorities and, as appropriate, for their relatives and other persons close to them"

This provision can be interpreted as encouraging States to provide the highest possible level of protection for anyone at risk due to their contribution to an investigation or trial involving cybercrime. The Convention does not distinguish between witnesses, informants, or other individuals assisting in uncovering such crimes. This inclusive approach is likely to encourage the provision of information and cooperation, thereby enhancing efforts to counter serious cyber offenses.

Furthermore, the Convention emphasizes the need to balance the witness's right to protection with the accused's right to a fair trial. Reinforcing this principle aligns with the requirements of criminal justice, and most national legislations adopt a protection framework governed by safeguards that ensure witness protection does not compromise the rights of the accused.[43]

Regarding protective measures, paragraph 2 of Article 33 of the Convention provides examples of measures that can be employed to safeguard witnesses. The text refers to physical protection measures, such as relocating witnesses, withholding the identity of the witness, or imposing restrictions on the disclosure of personal information. The provision also allows the use of technology in testimony, such as video links, and highlights the possibility of cooperation among States Parties in relocating witnesses. Through this provision, the Convention adopts mechanisms similar to those implemented in many national legislations regarding witness protection.

According to these legislations, procedural protection measures are generally divided into three categories:[44]

1. Measures aimed at reducing fear by avoiding direct confrontation with the accused, such as using prior statements instead of in-court testimony (where permitted); removing the accused from the courtroom (while allowing them to observe the trial via video); or providing testimony through closed-circuit television or audiovisual communications, such as video conferencing.[45]

---

[43] Ramadan Asim Taher, *The Role of Criminal Witness Protection in Achieving Justice in Criminal Cases: A Comparative Study,* master's Thesis, Graduate School, Arab American University, 2022–2023, 22–23.

[44] D. K. A. A. Aziz, "International and Regional Legal Frameworks for Witness Protection: Promoting Peace and Justice Through Strong Legal Institutions," *Journal of Lifestyle and SDGs Review* 5, no. 1 (2025): e04676, https://doi.org/10.47172/2965-730X.SDGsReview.v5.n01.pe04676.

[45] D. K. A. A. Aziz, "International and Regional Legal Frameworks for Witness Protection: Promoting Peace and Justice Through Strong Legal Institutions," *Journal of Lifestyle and SDGs Review* 5, no. 1 (2025): e04676, https://doi.org/10.47172/2965-730X.SDGsReview.v5.n01.pe04676.

2. Measures that make it difficult or impossible for the accused or organized criminal groups to trace the witness's identity, including anonymous testimony, screens or curtains, one-way mirrors during testimony, as well as local or international relocation of witnesses.[46]
3. Measures to reduce exposure to public or psychological pressure, such as changing the trial venue, excluding the public from the courtroom, and providing a companion to support the witness.

Key protective measures recognized by various legislations include:

Use of Remote Communication Technology: This modern technique is employed in some cases to hear the testimony of witnesses and justice collaborators, particularly in complex or organized crimes, through real-time audiovisual communication between two or more parties. Many legislations permit[47] the use of this technology during investigations and trials to protect witnesses from danger when appearing in court, or to shield children from psychological pressure. Jurisprudence emphasizes [48]that using this technology requires serious reasons indicating the witness is at risk, and its application must be motivated by protective purposes. Under the 2000 Council of Europe Convention on Mutual Assistance, remote communication technology is limited to hearing witness testimony and expert evidence.[49]

Digital Anonymization and Data Encryption: Anonymization and encryption of witness data are among the most important proactive technical and legal measures to prevent cyber retaliation. These measures aim to separate the witness's real identity from their testimony stored in information systems, using pseudonyms or encrypted digital codes accessible only by designated judicial authorities. This reduces the risk of cyberattacks targeting court databases to

---

[46] I. A. Salem, "Witness Protection Measures in Contemporary International Criminal Systems: The Rome Statute as a Model," *Al-Mukhtar Journal of Social Sciences* 38, no. 1 (2024): 168–187, https://doi.org/10.54172/vejhsn31.

[47] In UAE, Federal Decree-Law No. (38) of 2022 promulgating the Criminal Procedure Law stipulates that the competent authorities have the right to use remote communication technologies in criminal proceedings with the accused, the victim, witnesses, lawyers, experts, translators, civil plaintiffs, and other parties responsible for civil rights ; Article 706-71, Code de procédure pénale.

[48] Alnawayseh and Alnaqbi, "Using Video Conference Technology in Witness Protection: An Analytical Study in the Context of the UAE Legislation," *University of Sharjah (UoS) Journal of Law Sciences* 19, no. 3 (2022): 409–38, https://doi.org/10.36394/jls.v19.i3.16.

[49] Article (11), Convention established by the Council in accordance with Article 34 of the Treaty on European Union, on Mutual Assistance in Criminal Matters between the Member States of the European Union, at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:42000A0712(01) accessed 5/2/2026

extract witness information, thereby enhancing individuals' confidence in reporting cybercrimes without fear of digital retaliation or personal threats.

Relocation is considered one of the most extreme and effective measures to protect witnesses whose lives are at serious risk due to their testimony in cybercrimes involving international criminal organizations. This measure goes beyond geographic relocation and may include providing a completely new living environment, changing the official identity of the witness and their family if necessary, and severing all digital and physical links to their previous location to prevent tracking via open-source intelligence. The state ensures financial and logistical support for the witness to guarantee their stability in a location unknown to offenders, thus neutralizing the ability of cybercriminals to exploit leaked information to locate and pressure the witness.[50]

The Convention not only Establishes general frameworks for witness protection and outlines protective measures, but also, under Article 40, emphasizes the obligation of States Parties to provide the greatest degree of mutual assistance in investigations and prosecutions. This includes obtaining testimony or evidence from individuals, providing information and documents, and offering expert assessments.[51]

However, the Convention does not explicitly address substantive protection by prohibiting all forms of witness intimidation. This omission underscores the necessity of adopting such measures in national legislations, considering that criminal sanctions are among the strongest deterrents against harming witnesses.

Protection Afforded to Witnesses under Egyptian Legislation:

The Egyptian legislator has adopted an approach aimed at addressing cybercrimes through the enactment of a specific law, namely Law No. 175 of 2018, known as the Anti-Cyber and Information Technology Crimes Law. [52] However, the law does not explicitly address witnesses, nor does it provide any mechanisms to ensure their protection in cybercrime cases, which constitutes a clear legislative shortcoming. In our view, one of the most significant [53]

---

[50] Iman Ali Salem, "Witness Protection Measures in Contemporary International Criminal Systems: 'The Rome Statute as a Model,'" *Al-Mukhtar Journal of Humanities*, no. 38 (2020): 176–79, https://doi.org/10.54172/mjssc.v38i1.640.

[51] Article 40/1(3, A, h)

[52] Egypt, *Law No. 175 of 2018 on Combating Information Technology Crimes,* Official Gazette, August 2018, accessed [insert access date], https://www.deepl.com/ar/translator.

[53] Abdul Aal Al-Derby and Muhammad Al-Sadiq Ismail, *Cybercrime: A Comparative Legal Study of Arab Legislation in the Field of Combating Cybercrime and Internet Crime* (Cairo: National Center for Legal Publications, 2018), 148–56.

shortcomings lies in the absence of explicit mechanisms and measures through which witnesses can be protected from digital intimidation. The Egyptian Anti-Cyber and Information Technology Crimes Law does not include clear procedures or dedicated witness protection programs, particularly given that the current legal framework does not fully guarantee the confidentiality of witnesses' data, thereby exposing them to potential risksespecially considering the ease of accessing information in the digital environment.

Regarding the general rules of Egyptian criminal law[54], despite the existence of a constitutional provision that affirms the protection of witnesses in general and places upon the State the obligation to ensure such protectionnamely Article 96 of the 2014 Egyptian Constitution the Egyptian legislative framework has continued to suffer from notable short comings in this respect.[55]

1. The law allows a witness, upon obtaining permission from the Public Prosecution or the investigating judge, to use the police station or their work place as an official address.[56]
2. Where a witness or a member of their family may be exposed to danger as a result of giving testimony, it is permissible upon the witness's request or at the request of a judicial officerto petition the competent Public Prosecutor, investigating judge, or trial court to hear the testimony without disclosing identifying information. Nevertheless, a separate confidential file must be created within the case records containing the witness's true identity and personal details.[57]

However, Article 525 of the same law permits the accused and their legal counsel to challenge an order issued to conceal a witness's identity whenever disclosure is deemed necessary for the exercise of defence rights. It appears that through this provision the legislator sought to strike a balance between the witness's right to protection and the accused's right to a fair defence. Article 526 further allows the accused to request the examination of an anonymous witness without revealing the witness's identifying information.

---

[54] Law No. 174 of 2025 promulgating the Code of Criminal Procedure, Official Gazette No. 45 bis (d) dated November 12, 2025. https://www.eastlaws.com/legislation-full-text/ar/egypt/law/12-11-2025/no-174?type=1&id=4825460

[55] Dr. Aya Wafi, "Criminal Protection Guarantees for Witnesses in Egyptian Legislation and Comparative Legislation," *Nile Journal of Business, Law, and Information Systems* 5, no. 7 (2025): 26–64, https://mnsli.journals.ekb.eg/article_425860.html.

[56] Code of Criminal Procedure, Article 523

[57] Code of Criminal Procedure, Article 524

The law also criminalizes the disclosure of information relating to a witness whose identity has been ordered confidential. Any person who reveals such information is subject to imprisonment and a fine of no less than fifty thousand Egyptian pounds, or to either of these penalties. The penalty is aggravated to rigorous imprisonment if the act is committed for a terrorist purpose, and where such disclosure results in the death of the witness, the prescribed punishment is the death penalty.[58]

Islamic Jurisprudential Perspective

In Islamic jurisprudence, giving testimony constitutes a religious duty and a social obligation intended to ensure the realization of justice and the disclosure of truth. Sharia obliges witnesses to provide testimony and prohibits its concealment, as withholding testimony leads to the loss of rights and the obscuring of facts. Islamic legal doctrine also affords witnesses a degree of protection through recognized grounds of permissibility, allowing acts that might ordinarily be considered unlawful such as disclosure of confidential information or statements that could other wise be deemed offensive when made within the context of testimony before a court. This reflects the commitment of Islamic law to supporting witnesses and enabling them to fulfill their duty without fear of legal or moral repercussions that might deter them from presenting relevant information.

Furthermore, both substantive and procedural protections for witnesses are embedded within the Islamic legal system, where witness safeguards form an integral part of the broader framework of justice. These protections include shielding witnesses from intimidation, coercion, or undue influence that could compromise their testimony, in accordance with ethical and legal standards designed to preserve the integrity of evidence. Comparative studies between Islamic jurisprudence and contemporary legal systems demonstrate that Islamic law contains both procedural and substantive guarantees for witnesses throughout the stages of criminal proceedings. Such guarantees provide a valuable jurisprudential foundation for developing modern witness protection mechanisms aligned with the objectives of Sharia, particularly the preservation of rights and the promotion of justice.[59]

Moreover, Islamic jurisprudence recognizes testimony as a central evidentiary tool in adjudication and emphasizes that it must be given freely,

[58] Code of Criminal Procedure. Article,527

[59] Zubair Tahraoui, *Protection of Witnesses in Islamic Jurisprudence and Positive Law* (PhD diss., Department of Islamic Sciences [Comparative Interpretation and Legislation], University of Eloued, Algeria, 2021), https://archives.univ-eloued.dz/handle/123456789/10554.

honestly, and without coercion, as concealing testimony constitutes a serious injustice that undermines the administration of justice. Accordingly, the Islamic legal tradition does not overlook the risks faced by witnesses; rather, it seeks to establish principles that address these risks in a manner consistent with the overarching objectives of Sharia, including the protection of life, dignity, and legal rights.[60]

Shortcomings in Egyptian Legislation:

There is near consensus that the pro liferation of crime within the digital environment has become an issue of grave concern[61], requiring legislators world wide to adopt comprehensive strategies that employ all available measures and mechanisms to confront this growing threat. Any effective legislative response must therefore be holistic, proactive, and responsive to the evolving nature of cyber crime. Undoubtedly, any strategy that over looks the rights and protection of witnesses and victims runs contrary to the fundamental requirements of criminal justice and undermines the integrity and effectiveness of the legal system. [62]

Witness protection occupies a position of paramount importance closely linked to the principles of international humanitarian law. This significance was emphasized in the international report issued by the United Nations in July 2010, which affirmed that effective witness protection within criminal proceedings concerning serious crimes requires the presence of specific essential elements. In this regard, establishing a normative framework grounded in existing legal obligations may prove beneficial. The report also highlighted the need to enhance the effectiveness of witness protection mechanisms by ensuring adequate financial, technical, and political support for national protection programmes.[63]. In the absence of appropriate provisions safeguarding witnesses and victims

---

[60] Khalid bin Zaid Al-Wuzayni, "Rights of the Witness in Islamic Jurisprudence," *Journal of the Saudi Fiqh Society* 10 (2011): 133–239, IslamicInfo / Imam Muhammad bin Saud Islamic University, Record No. 147440.

[61] M. Tampubolon and M. J. P. Tampubolon, "Cybercrime, Human Rights, and Digital Privacy: Navigating the Complex Landscape of Protection and Freedom," in *Integrating Artificial Intelligence, Security for Environmental and Business Sustainability*, ed. A. Hamdan, *Studies in Systems, Decision and Control*, vol. 608 (Cham: Springer, 2025), 89–110, https://doi.org/10.1007/978-3-031-96641-5_7.

[62] M. K. A. Lukings, A. Habibi Lashkari, and P. Hakimian, "Cybercrime Victim Services at an International Level," in *Understanding Cybercrime Victim Services*, *Progress in IS* (Cham: Springer, 2026), 89–108, https://doi.org/10.1007/978-3-032-13273-4_6.

[63] United Nations High Commissioner for Human Rights, *Report of the United Nations High Commissioner for Human Rights on the Right to the Truth,* Human Rights Council, Fifteenth session, A/HRC/15/33 (Geneva: United Nations, July 28, 2010), accessed February 6, 2026, https://docs.un.org/en/A/HRC/15/33.

including the protection of their physical and psychological integrity, privacy, and dignitytheir reputations and even their lives may be placed at risk due to their involvement in judicial or quasi-judicial proceedings. Ensuring the safety and reliability of witness and victim testimony is therefore indispensable to securing justice for victims, upholding the right to truth, holding perpetrators accountable, and deterring potential offenders.

Given the central role of testimony in criminal proof, legislators have criminalized both the refusal to testify and acts that mislead the course of justice, thereby under scoring the strong nexus between the duty to testify, the functioning of criminal justice, and the broader concept of legal security. Accordingly, the very notion of criminal justice necessitates the provision of adequate and effective protection for witnesses and victims of crime.[64]

According to a study addressing mechanisms for combating cybercrime and enhancing victim and witness protection programmes, a comprehensive package of cybercrime victim services was proposed. This model represents a standardized system designed to provide immediate, compassionate, and coordinated support to individuals affected by digital crimes. Its objectives include digital harm containment and mitigation, the provision of psychological and social first aid, legal counselling and guidance, financial protection and identity safeguarding measures, as well as long-term education and empowerment initiatives aimed at strengthening resilience and promoting sustained recovery.[65]

At a time when states are striving to confront the growing risks posed by cybercrime, some countries such as India have moved toward comprehensive reforms of their criminal legislation to address contemporary forms of crime more effectively and to enhance the responsiveness of their legal frameworks to emerging digital threats[66]. We find that, despite the Egyptian legislator having introduced a new Criminal Procedure Law that includes certain provisions aimed at protecting victims, there remain significant shortcomings in this regard. The main points of deficiency can be highlighted as follows:

---

[64] Brent E. Turvey, "Forensic Victimology on Trial," in *Forensic Victimology: Examining Violent Crime Victims in Investigative and Legal Contexts*, 3rd ed., ed. Brent E. Turvey (Academic Press, 2023), 481–519, https://doi.org/10.1016/B978-0-12-821768-9.00014-8.

[65] M. K. A. Lukings, A. Habibi Lashkari, and P. Hakimian, "Cybercrime Prevention Techniques & Comprehensive Cyber Crime Victim Service Package Proposal," in *Understanding Cybercrime Victim Services*, *Progress in IS* (Cham: Springer, 2026), 155–76, https://doi.org/10.1007/978-3-032-13273-4_7.

[66] Dr. Rahul Kailas Bharati, "The New Criminal Law Paradigm in India and Its Impact on Cybercrime Adjudication," July 24, 2025, https://doi.org/10.70593/978-93-7185-183-1, SSRN: https://ssrn.com/abstract=5378219.

Absence of Specific Legislation Ensuring Effective Protection for Witnesses

The Egyptian legislator lacks specific legislation that establishes clear rules and mechanisms to guarantee the protection of witnesses and victims in serious crimes. This gap may discourage witnesses and informants from fulfilling their duties toward justice, thereby hindering efforts to combat cyber crime. This deficiency is particularly notable given the trend in several Arab countries to enact dedicated legislation providing protection for witnesses and victims.[67]

or example, the Saudi regulatory framework issued in 2024 established a specialized administration responsible for implementing protection measures. The protection extended to relatives, spouses, and anyone at risk, in line with the provisions of the international convention. The system also established a protection program for whistleb lowers and witnesses under the supervision of the Public Prosecution. Notably, the Saudi system ensures both procedural and substantive protection for witnesses. Substantive protection includes penalties for those who harm a witness, punishable by imprisonment of up to three years or a fine of 500,000 riyals, and even criminalizes attempts to commit such offenses.

The Saudi approach aligns closely with Qatar's Law No. 5 of 2022 concerning the protection of witnesses, whistleblowers, and those in similar positions. [68] This Qatari law provides both substantive and procedural protection and clearly outlines the measures that can be implemented in witness protection programs, in a manner consistent with the provisions of the international convention.

Second Lack of a precise framework for "remote" witness protection programs:

The Egyptian legislation does not provide a clear and structured plan aimed at protecting witnesses or setting rules for giving testimony via electronic means in a way that ensures complete confidentiality.[69] Although digital evidence is recognized, the measures for witness protection still lack binding "technical protocols" that prevent the leakage of witness data during preliminary

---

[67] Saudi Arabia, *Royal Decree (M/148) Approving the Law on the Protection of Whistleblowers, Witnesses, Experts, and Victims*, issued 8 Shaʿbān 1445 AH (18 February 2024), published in *Umm Al-Qurā Official Gazette* 5022 (1 March 2024), accessed February 5, 2026, https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/6c421c5c-c137-442e-a854-b12200c46ffe/1.

[68] Qatar, *Law No. 5 of 2022 on the Protection of Victims, Witnesses, and Others in Similar Circumstances* (2022), accessed February 6, 2026, https://www.deepl.com/ar/translator.

[69] Tarek Ahmed Maher Zaghloul, "Procedural Protection for Victims, Witnesses, and Informants: A Comparative Analytical Study," *Journal of Legal and Economic Sciences*, Faculty of Law, Ain Shams University 5, no. 1 (2017): 149–444.

investigations or online trials. Furthermore, the law does not establish sufficient incentives or guarantees for technical whistleblowers who operate within digital institutions, leaving them without adequate legal protection against arbitrary dismissal or malicious legal action by their employers[70]. This gap hinders the detection and prosecution of organized and complex cybercrimes.Third Weak mechanisms for international and cross-border judicial cooperation in witness protection:

Cybercrimes are often committed from outside national territories, requiring a flexible legal framework to secure witnesses residing in other countries. Egyptian legislation lacks explicit provisions regulating "electronic judicial assistance" specifically for protection purposes. In other words, there are no internationally certified encrypted protocols that allow a witness to give testimony from abroad without revealing their geographic location or digital identity to the state where the perpetrator resides. This renders the current legal protection "confined within national borders" and ineffective against international cybercriminal networks.[71]

The Sharia-Based Foundation for Modern Witness Protection Measures

When analyzing newly developed technical measures for protecting witnesses in cyber crime cases, strong Sharia-based principles emerge that justify and support these mechanisms. Islamic law prioritizes the preservation of life and human dignity, adding both an ethical and legal dimension to these modern protection measures. Safeguarding individuals from harm is considered one of the higher objectives (*maqasid al-shariah*), with the protection of life being a core component. Jurisprudential studies indicate that Sharia places significant emphasis on protecting individuals and preserving their dignity from any form of aggression or harm, including safeguarding uninvolved parties, such as witnesses, from risks, excesses, and attacks.[72]

---

[70] R. M. Judge, "Criminal Protection for Persons Cooperating with Criminal Justice Authorities (Witnesses, Victims, and Expert Informants) in the Context of Organized Crime in International Conventions and Egyptian Law," *Al-Haq Magazine* 40, no. 3 (2016): 1–104, https://doi.org/10.34120/jol.v40i3.2217.

[71] Noureddine Ben Farhat, Abdelkader Amri, The Transient Nature of Electronic Evidence and Its Impact on Criminal Investigations, Legal and Political Research Journal, Volume 9, Issue 1, p660: 673, https://asjp.cerist.dz/en/article/251462 ; Ibrahim, Mona Ghazi Hassan. (2025). The effectiveness of criminal policy in combating cybercrime (a comparative study considering cybersecurity requirements). Sharia and Law Magazine, Cairo, Issue 45, pp. 2619–2709

[72] Ahmed Al Domah Rahma et al., "The Principle of Human Dignity in Islamic Jurisprudence and Its Impact on the Protection of Non-Combatants," *Journal of Economic, Administrative and Legal Sciences* 2, no. 6 (2018): 17–33, https://doi.org/10.26389/AJSRP.A140218.

In this context, the Sharia principle "La darar wa la dirar" (No harm and no reciprocating harm) serves as a foundational rule, obliging the prevention of harm to oneself and others not merely removing harm after it occurs, but also preventing its causes.[73] This principle aligns with modern technical requirements to protect witnesses from digital intimidation and defamation, as harm inflicted via cyber space constitutes an extension of material and moral harm that Islam forbids.[74]

According to jurisprudential sources, concealing the witness's identity and implementing data-obfuscation measures can be justified through the principle of preemptive harm prevention, which allows taking necessary steps to avert anticipated and potential risks before they materialize. This aligns directly with the legal objective of safeguarding witnesses in cyber environments exposed to digital threats.[75]

Allowing testimony via encrypted electronic means corresponds with the Sharia principle of al-mashaqqah tajliz al-taysir (ease in hardship), which permits facilitation when strict procedures impose excessive difficulty on the witness. [76] Ensuring their safety and achieving the Sharia objective of establishing justice (*iqamat al-haqq*) takes precedence over rigid adherence to traditional procedures. Regarding the protection of family members or relatives who may face harm due to a witness's testimony, Sharia's objectives in preserving lineage and human dignity justify extending protective measures to these affected parties. This underscores the importance of incorporating technical measures that safeguard anyone indirectly at risk due to the witness's cooperation with investigative procedures.[77]

Finally, the measure of relocating a witness to protect them from serious risks draws on the Sharia principle permitting migration or relocation to avert harm. This allows a person to move if remaining in their current location exposes

---

[73] Institut Agama, Islam Negeri Curup, and Deo Agung Pratama, "Interfaith Marriage in Indonesia: Judicial Interpretation of Surabaya District Court Decision No. 916/Pdt.P/2022/PN.Sby in the Perspective of Human Rights and Islamic Law Compilation," *Berasan: Journal of Islamic Civil Law* 4, no. 1 (June 11, 2025): 14–34, https://doi.org/10.29240/BERASAN.V4I1.8390.

[74] S. Wahid, A. Musyahid, and R. HL, "The Logic of Impairment in Islamic Law: Philosophical Perspective as a Foundation for Ethics Education," *Journal of Education Review Provision* 4, no. 3 (2024): 25–28, https://doi.org/10.55885/jerp.v4i3.462.

[75] Ibid

[76] Fatimah Karim, "Application of the Islamic Legal Maxim 'Hardship Begets Ease' to Mitigate Hardship in the Religious Practices of the Elderly Muslims," *International Journal of Fiqh and Usul al-Fiqh Studies* 9, no. 3 (2025): 146–158, https://doi.org/10.31436/ijfus.v9i3.413.

[77] Talib Hussain Abdul Qayyum and Ashfaq Ahmad, "An Applied Study of the Objectives of Islamic Law (Maqāṣid al-Sharīʿah) and Jurisprudential Maxims (Qawāʿid al-Fiqhiyyah) on the Protection of Human Dignity in the Digital Age," *ASSA Journal* 4, no. 2 (2025): 3384–3395, https://assajournal.com/index.php/36/article/view/1267.

them or their family to significant danger. This principle reflects the spirit of Sharia, which prioritizes human safety and well-being, even if it requires leaving one's original residence for an alternative location ensuring physical and psychological security. By connecting Sharia texts and objectives with modern technical measures for witness protection, it becomes evident that Islamic jurisprudence provides a robust theoretical foundation for adopting and developing witness protection mechanisms in cybercrime cases, in alignment with the goals of criminal justice and the preservation of life and dignity emphasized by Sharia.

Conclusion

This study demonstrates that digital witness protection has become a critical yet underdeveloped component of contemporary cybercrime regulation. The findings confirm the existence of significant regulatory gaps, particularly in national legal systems such as Egyptian law, which remain insufficient in addressing the complex and evolving risks faced by digital witnesses, including cyber intimidation, data exposure, and cross border threats. In contrast, international legal standards provide a more comprehensive framework by incorporating advanced protection mechanisms, such as anonymity, remote testimony, and relocation, alongside an emphasis on international cooperation. However, the absence of fully integrated and enforceable measures at the national level undermines the effectiveness of these standards in practice. From the perspective of Islamic jurisprudence, the study establishes that witness protection is firmly grounded in the objectives of Sharia, particularly in preserving life, dignity, and property, and ensuring justice through truthful and voluntary testimony. These principles not only support but also legitimize the adoption of modern legal and technological protection measures within contemporary legal systems.

The study argues that addressing regulatory gaps requires a systematic integration of international standards into domestic legal frameworks, supported by Sharia based normative foundations. It proposes a comprehensive model of digital witness protection that combines legal, technological, and ethical safeguards, including data anonymization, secure remote testimony systems, and cross border cooperation mechanisms. Ultimately, strengthening digital witness protection is essential to enhancing legal certainty, encouraging witness participation, and improving the effectiveness of cybercrime enforcement in an increasingly transnational digital environment. The study contributes to the development of a more adaptive and integrative legal framework capable of responding to the challenges posed by cybercrime while maintaining alignment with both international norms and Islamic legal principles.

References

Abdul Qayyum, Talib Hussain, and Ashfaq Ahmad. "An Applied Study of the Objectives of Islamic Law (Maqāṣid al-Sharīʿah) and Jurisprudential Maxims (Qawāʿid al-Fiqhiyyah) on the Protection of Human Dignity in the Digital Age." ASSA Journal 4, no. 2 (2025): 3384–3395. https://assajournal.com/index.php/36/article/view/1267.

Karim, Fatimah. "Application of the Islamic Legal Maxim 'Hardship Begets Ease' to Mitigate Hardship in the Religious Practices of the Elderly Muslims." *International Journal of Fiqh and Usul al-Fiqh Studies* 9, no. 3 (2025): 146–158. https://doi.org/10.31436/ijfus.v9i3.413.

Wahid, S., Musyahid, A., and R. HL. "The Logic of Impairment in Islamic Law: Philosophical Perspective as a Foundation for Ethics Education." *Journal of Education Review Provision* 4, no. 3 (2024): 25–28. https://doi.org/10.55885/jerp.v4i3.462.

Rahma, Ahmed Al Domah, Mohammed Hassan Jama'a, Abker Ali Abdul Majid, and Ahmed Hammad Abdullah Abdul Rahim. "The Principle of Human Dignity in Islamic Jurisprudence and Its Impact on the Protection of Non-Combatants." *Journal of Economic, Administrative and Legal Sciences* 2, no. 6 (2018): 17–33. https://doi.org/10.26389/AJSRP.A140218.

Ben Farhat, Noureddine, and Abdelkader Amri. "The Transient Nature of Electronic Evidence and Its Impact on Criminal Investigations." *Legal and Political Research Journal* 9, no. 1 (Year): 660–73. https://asjp.cerist.dz/en/article/251462.

Hassan, Mona Ghazi Ibrahim. "The Effectiveness of Criminal Policy in Combating Cybercrime (A Comparative Study in Light of Cybersecurity Requirements)." *Sharia and Law Magazine*, Cairo, no. 45 (2025): 2619–2709.

Judge, R. M. "Criminal Protection for Persons Cooperating with Criminal Justice Authorities (Witnesses, Victims, and Expert Informants) in the Context of Organized Crime in International Conventions and Egyptian Law." *Al-Haq Magazine* 40, no. 3 (2016): 1–104. https://doi.org/10.34120/jol.v40i3.2217.

Zaghloul, Tarek Ahmed Maher. "Procedural Protection for Victims, Witnesses, and Informants: A Comparative Analytical Study." *Journal of Legal and Economic Sciences*, Faculty of Law, Ain Shams University 5, no. 1 (2017): 149–444.

Qatar. *Law No. 5 of 2022 on the Protection of Victims, Witnesses, and Others in Similar Circumstances*. Promulgated 2022. Accessed February 6, 2026. https://www.deepl.com/ar/translator.

Saudi Arabia. *Royal Decree (M/148) Approving the Law on the Protection of Whistleblowers, Witnesses, Experts, and Victims*, issued 8 Shaʿbān 1445 AH (corresponding to 18 February 2024). Published in *Umm Al-Qurā Official Gazette*5022 on 1 March 2024. Accessed February 5, 2026. https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/6c421c5c-c137-442e-a854-b12200c46ffe/1.

Bharati, Dr. Rahul Kailas. "The New Criminal Law Paradigm in India and Its Impact on Cybercrime Adjudication." July 24, 2025. https://doi.org/10.70593/978-93-7185-183-1. SSRN: https://ssrn.com/abstract=5378219.

Lukings, M. K. A., A. Habibi Lashkari, and P. Hakimian. "Cybercrime Prevention Techniques & Comprehensive Cyber Crime Victim Service Package Proposal." In *Understanding Cybercrime Victim Services*, *Progress in IS*, 155–76. Cham: Springer, 2026. https://doi.org/10.1007/978-3-032-13273-4_7.

Turvey, Brent E. "Forensic Victimology on Trial." In *Forensic Victimology: Examining Violent Crime Victims in Investigative and Legal Contexts*. 3rd ed. Edited by Brent E. Turvey. Academic Press, 2023. https://doi.org/10.1016/B978-0-12-821768-9.00014-8.

United Nations High Commissioner for Human Rights. *Report of the United Nations High Commissioner for Human Rights on the Right to the Truth.* Human Rights Council, Fifteenth session, A/HRC/15/33. Geneva: United Nations, July 28, 2010. Accessed February 6, 2026. https://docs.un.org/en/A/HRC/15/33.

Lukings, M. K. A., A. Habibi Lashkari, and P. Hakimian. "Cybercrime Victim Services at an International Level." In *Understanding Cybercrime Victim Services*, *Progress in IS*, edited by [Editor's Name if available], 89–108. Cham: Springer, 2026. https://doi.org/10.1007/978-3-032-13273-4_6.

Tampubolon, M., and M. J. P. Tampubolon. "Cybercrime, Human Rights, and Digital Privacy: Navigating the Complex Landscape of Protection and Freedom." In *Integrating Artificial Intelligence, Security for Environmental and Business Sustainability*, edited by A. Hamdan, *Studies in Systems, Decision and Control*, vol. 608, 89–110. Cham: Springer, 2025. https://doi.org/10.1007/978-3-031-96641-5_7.

Al-Wuzayni, Khalid bin Zaid. "Rights of the Witness in Islamic Jurisprudence." *Journal of the Saudi Fiqh Society* 10 (2011): 133–239. IslamicInfo / Imam Muhammad bin Saud Islamic University. Record No. 147440.

Tahraoui, Zubair. *Protection of Witnesses in Islamic Jurisprudence and Positive Law*. PhD diss., Department of Islamic Sciences (Comparative Interpretation and Legislation), University of Eloued, Algeria, 2021. https://archives.univ-eloued.dz/handle/123456789/10554.

Wafi, Dr. Aya. "Criminal Protection Guarantees for Witnesses in Egyptian Legislation and Comparative Legislation." *Nile Journal of Business, Law, and Information Systems* 5, no. 7 (2025): 26–64. https://mnsli.journals.ekb.eg/article_425860.html.

Al-Derby, Abdul Aal, and Muhammad Al-Sadiq Ismail. *Cybercrime: A Comparative Legal Study of Arab Legislation in the Field of Combating Cybercrime and Internet Crime*. Cairo: National Center for Legal Publications, 2018, 148–56.

Egypt. *Law No. 175 of 2018 on Combating Information Technology Crimes*. Official Gazette, August 2018. Accessed [insert access date]. https://www.deepl.com/ar/translator.

Salem, Iman Ali. "Witness Protection Measures in Contemporary International Criminal Systems: 'The Rome Statute as a Model.'" *Al-Mukhtar Journal of Humanities*, no. 38 (2020): 176–79. https://doi.org/10.54172/mjssc.v38i1.640.

Alnawayseh, and Alnaqbi. "Using Video Conference Technology in Witness Protection: An Analytical Study in the Context of the UAE Legislation." *University of Sharjah (UoS) Journal of Law Sciences* 19, no. 3 (2022): 409–38. https://doi.org/10.36394/jls.v19.i3.16.

Salem, I. A. "Witness Protection Measures in Contemporary International Criminal Systems: The Rome Statute as a Model." *Al-Mukhtar Journal of Social Sciences* 38, no. 1 (2024): 168–187. https://doi.org/10.54172/vejhsn31.

Aziz, D. K. A. A. "International and Regional Legal Frameworks for Witness Protection: Promoting Peace and Justice Through Strong Legal Institutions." *Journal of Lifestyle and SDGs Review* 5, no. 1 (2025): e04676. https://doi.org/10.47172/2965-730X.SDGsReview.v5.n01.pe04676.

Ramadan Asim Taher, *The Role of Criminal Witness Protection in Achieving Justice in Criminal Cases: A Comparative Study,* master's Thesis, Graduate School, Arab American University, 2022–2023, 22–23.

United Nations. *United Nations Convention against Transnational Organized Crime (Palermo Convention),* adopted November 15, 2000, entered into force September 29, 2003, Article 33(1). Accessed February 6, 2026. https://treaties.un.org/pages/viewdetails.aspx?src=treaty&mtdsg_no=xviii-12&chapter=18&clang=_en.

National Prosecutions Service of Tanzania. *Witness Care and Protection Guidelines*. Issued May 1, 2023, under the National Prosecutions Service Act, Cap. 430. Accessed February 5, 2026. https://tanzlii.org/en/akn/tz/doc/guidelines/2023-05-01/witness-care-and-protection-guidelines/eng@2023-05-01.

Bharati, Dr. Rahul Kailas. "The New Criminal Law Paradigm in India and Its Impact on Cybercrime Adjudication." July 24, 2025. https://doi.org/10.70593/978-93-7185-183-1. Available at SSRN: https://ssrn.com/abstract=5378219.

Al-Battawi, Tamara Ibrahim Mohsen. "The Role of Collective Ijtihad in Cybersecurity Issues." *Journal of the College of Islamic Sciences*, no. 84 (2025). Accessed [insert date of access]. https://jcois.uobaghdad.edu.iq/index.php/2075_8626/article/view/2618.

Kadhim, Tholfikar. "Applicable Law Governing Electronic Violation of Privacy Rights." *Al-Sharaa: Journal for Legal and Administrative Studies* 5, no. 1 (2025): 140–184.

Belbashir, Yaqoub. "Cybercrime in the Age of Artificial Intelligence: A Look at the Challenges and Emerging Risks." *Journal of Human Rights and Public Freedoms* 10, no. 2 (Algeria, 2025): 249–27.

Alwan, Ali Abdul Hussein. "Cyberbullying and its Impact on Freedom of Expression on Social Media: A Field Study of Professors at the University of Diyala." *Journal of Media Studies and Research* 3, no. 10 (2025): 300–312. https://msar.edu.iq/index.php/msar/article/view/115/53.

Al-Sayed, Esaam Eldeen Abdel Al. "Legislative Confrontation of Extortion and Cyber Threat Offences in UAE Law: Comparative Study of Egyptian Law." *Al Fikr Al Sharati* 33, no. 129 (2024): 63–118.

"Cyberbullying: The New Face of Digital Revenge: Young People's Personal Data at Risk!" *Indigo Dergisi*, February 2026. Accessed February [day] 2026. https://indigodergisi.com/ar/2026/02/.

Bin Rais, 'Abd al-Rahman. "Protection of the Witness in Criminal Law between Statutory Law and Islamic Jurisprudence." *Maroc Law*, 2024. Accessed February 5, 2026. https://maroclaw.com/.

Al-Shibili, Abdullah Ali, Ahmad Zaki Saleh, and Mohamad Zaharuddin Zakaria. "Witness Testimony and its Impediments between Islamic Law and Contemporary Laws." *Malaysian Journal of Syariah and Law* 7, no. 1

Valiño Ces, A. "The Importance of the Computer Undercover Agent as an Investigative Measure Against Cybercrime: A Special Reference to Child

Pornography Crimes." In *Legal Developments on Cybersecurity and Related Fields*, edited by F. A. Carneiro Pacheco de Andrade, P. M. Fernandes Freitas, and J. R. de Sousa Covelo de Abreu, 143–62. *Law, Governance and Technology Series*, vol. 60. Cham: Springer, 2024. https://doi.org/10.1007/978-3-031-41820-4_9.

Sikra, Juraj, Karen V. Renaud, and Daniel R. Thomas. "Investigating What Promotes and Deters Scottish Cybercrime Reporting." *Journal of Economic Criminology* 6 (2024). https://doi.org/10.1016/j.jeconc.2024.100103.

Popham, James, Mary McCluskey, Michael Ouellet, and Owen Gallupe. "Exploring Police-Reported Cybercrime in Canada." *Policing: An International Journal* 43, no. 1 (2020): 35–48. https://doi.org/10.1108/PIJPSM-08-2019-0128.

McNealey, Rachel L., Camille I. Figueroa, and Cooper A. Maher. "'Police Can't Help You': Exploring Influences on Perceptions of Policing Cybercrime." *Journal of Criminal Justice* 101 (2025). https://doi.org/10.1016/j.jcrimjus.2025.102542.

Busetti, Simone, and Francesco Maria Scanni. "Evaluating Incident Reporting in Cybersecurity: From Threat Detection to Policy Learning." *Government Information Quarterly* 42, no. 1 (2025). https://doi.org/10.1016/j.giq.2024.102000.

Hassan, Ayman Abdullah Fikri. "Electronic Witness in Criminal Evidence." *Journal of Sharia and Law in Cairo* 44, no. 44 (2024): 3543–3607. https://doi.org/10.21608/mawq.2025.335120.1107.

Al-Hamdani, Sumaya Jiad. "Criminal Evidence in the Digital Age: Towards an Intelligent System for Verifying the Credibility of Electronic Evidence." Supreme Judicial Council (Iraq). Accessed February 6, 2026. https://www.sjc.iq/view/77460/.

Ho, Calvin Wai-Loon, and Karel Caals. "A Call for an Ethics and Governance Action Plan to Harness the Power of Artificial Intelligence and Digitalization in Nephrology." *Seminars in Nephrology* 41, no. 3 (2021): 282–293. https://doi.org/10.1016/j.semnephrol.2021.05.009.

Kramer, Karen. "Protection of Witnesses and Whistle-Blowers: How to Encourage People to Come Forward to Provide Testimony and Important Information." In *149th International Training Course Visiting Experts' Papers*, 18–23. Tokyo: United Nations Asia and Far East Institute for the Prevention of Crime and the Treatment of Offenders (UNAFEI),

2025. https://www.unafei.or.jp/publications/pdf/RS_No86/No86_07VE_Kramer.pdf.

United Nations Office on Drugs and Crime (UNODC). *Good Practices for the Protection of Witnesses in Criminal Proceedings Involving Organized Crime*. Vienna & New York: United Nations, 2008. https://www.unodc.org/documents/middleeastandnorthafrica/organised-crime/Good_Practices_for_the_Protection_of_Witnesses_in_Criminal_Proceedings_Involving_Organized_Crime.pdf.

Chaudhary, Sunbal Islam, and Naseem Razi. "Witness Protection in Global Perspective: An Analysis of International Laws." *Contemporary Journal of Social Science Review* 2, no. 4 (2024): 171–84.

Fakiha, Bandr. "Digital Forensics: Crimes and Challenges in Online Social Networks Forensics." *Journal of the Arab American University* 6, no. 1 (2020): 19–28.

Al-Deeb, Abu Bakr, and Dina Ibrahim. "Reflections of Artificial Intelligence on the Rules of Evidence." *Journal of Legal and Economic Research*, Faculty of Law, Mansoura 14, Special Issue (April 2024): 1065–66. https://doi.org/10.21608/mjle.2024.386604.

Al-Ghayathin, Abdulla Hamad O. J., Siti Aisyah Samudin, Mohd Norhusairi Mat Hussin, Mahamatayuding Samah, and Erik Sabti Rahmawati. "Protection of Witnesses in Criminal Lawsuits: An Analytical Study." *PETITA: Jurnal Kajian Ilmu Hukum dan Syariah* 10, no. 1 (2025): 419–434. https://doi.org/10.22373/petita.v10i1.710.

Prashant Rahamgdale, "Witness Protection: Comparative Analysis of Indian and Australian Legislation," *Journal of the Gujarat Research Society*, 2020, 141–151.

United Nations Office on Drugs and Crime (UNODC), *Witness Protection*, in *UNODC Teaching Module Series: Organized Crime*, accessed February 3, 2026, https://www.unodc.org/cld/en/education/tertiary/organized-crime/module-9/key-issues/witness-protection.html.

Imran, Mohammad Fadil. "Cyber Criminology and Human Security: An Analysis of ASEAN Countries Police's Paradigm." *Journal of Human Security* 18, no. 1 (2022): 49–53. https://doi.org/10.12924/johs2022.18010034.

Achuthan, K., S. Khobragade, and R. Kowalski. "Cybercrime through the Public Lens: A Longitudinal Analysis." *Humanities and Social Sciences Communications* 12 (2025): 282. https://doi.org/10.1057/s41599-025-04459-x.

Zamroni, Zamroni, and Basri. "Legal Protection for Victims of Cybercrime as a Form of Transnational Crime." *Jurnal Ius Constituendum* 9, no. 1 (2024): 130–49. https://doi.org/10.26623/jic.v9i1.8288.

A. Okeal, Tarek Elsayed Mahmoud. "The Role of Interdisciplinary Studies in Establishing the Rules of Technical Criminal Law – An Analytical Study." *Researcher Journal for Legal Sciences* 5, no. 2 (2024): 95–113. https://uofjls.net/index.php/new/article/view/226.

Berendt, Bettina, and Stefan Schiffner. "Whistleblower Protection in the Digital Age – Why 'Anonymous' Is Not Enough: From Technology to a Wider View of Governance." *The International Review of Information Ethics* 31, no. 1 (2022). https://doi.org/10.29173/irie479.

United Nations Office on Drugs and Crime (UNODC). *Good Practices for the Protection of Witnesses in Criminal Proceedings Involving Organized Crime*. Vienna & New York: United Nations, 2008. https://www.unodc.org/documents/organized-crime/Witness-protection-manual-Feb08.pdf.

Al-Shorbagi, Ahmed Abdel Fattah. *Criminal Protection for Witnesses and Whistleblowers in National and International Law*. PhD diss., Faculty of Law, Ain Shams University, 20

Bamashmoos, A. M. "Witness Protection Programs: A Comparative Analysis of Saudi Arabian and U.S. Legal Mechanisms." *Journal of Humanities and Administrative Sciences, Shaqra University* 12, no. 2 (2025): 372–380.

Abdulqader, Abdulrahman Abdulqader. "Himayat al-Shahada fi al-Shari'ah al-Islamiyah wa al-Nuzum al-Wad'iyah al-Mu'asirah." *Academic Journal of Research and Scientific Publishing* 7, no. 73 (2025). https://doi.org/10.52132/Ajrsp/v7.73.1.

Aghnayah, Miftah Aghnayah Mohammed. "Protecting the Right to Life: A Legal Study in Maqasid Thought." *Al-Haq Journal for Sharia and Legal Sciences* 2, no. 1 (2015): 186–220. https://doi.org/10.58916/alhaq.v2i1.213.

Council of Europe. *The Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Protocols*. Accessed February 6, 2026. https://www.coe.int/en/web/cybercrime/the-budapest-convention.

World Economic Forum. *Global Risks Report 2026*. January 14, 2026. https://www.weforum.org/publications/global-risks-report-2026/.

Rani, Sita, Aman Kataria, Vishal Sharma, Smarajit Ghosh, Vinod Karar, Kyungroul Lee, and Chang Choi. "Threats and Corrective Measures for

IoT Security with Observance of Cybercrime: A Survey." *Wireless Communications and Mobile Computing* (2021): Article 5579148, 30 pages. https://doi.org/10.1155/2021/5579148.

SEON, *Global Cybercrime Report: Which Countries Are Most at Risk in 2023*, accessed February 2, 2026, https://seon.io/resources/global-cybercrime-report/.

United Nations Convention against Transnational Organized Crime, art. 24(1),

Mahmoud, Tarek Elsayed. *The Pre-Trial Stage in the International Criminal Case.* PhD diss., Faculty of Law, Benha University, 2018.