ITJ | The International Tax Journal

Legal frameworks for combating information technology crimes: A study in light of Islamic Sharia and modern laws

Noumeir Tekkouk [1]

[1] Doctor, University of Abou Bekr Belkaïd Tlemcen, Faculty of Law and Political Sciences, (Algeria).
Email: teknoumeir@gmail.com

Abstract---This study examines the legal frameworks for combating information technology crimes, focusing on Islamic Sharia and modern laws. It highlights the challenges faced by traditional criminal law in addressing novel criminal patterns that exploit technological advancements. Information technology crimes are rapidly increasing due to technological evolution, placing significant strain on existing legal frameworks. This study demonstrates that Islamic Sharia, with its flexibility and comprehensiveness, offers both preventive and curative approaches to combat crimes, including emerging patterns like credit card theft, through traditional theft provisions or via discretionary (Ta'zir) punishments that grant judges broad latitude. In contrast, contemporary laws face challenges in keeping pace with these crimes, despite legislative efforts in countries such as the United States (CFAA), Algeria, Egypt, and Bahrain. The study underscores the critical importance of international cooperation, information exchange, and sharing expertise, citing the role of the Financial Action Task Force (FATF) in combating money laundering and terrorism financing linked to cybercrimes. The study concludes by emphasizing the historical precedence of Islamic Sharia in addressing these issues, recommending the development of Sharia-inspired legislation, protection of cultural identity, criminalization of intellectual property infringement, and the establishment of specialized courts for digital crimes.

Keywords---Information Technology Crimes, Islamic Sharia, Criminal Law, Cybersecurity, Ta'zir Punishments, International Cooperation, Money Laundering.

Introduction

In line with the accelerating technological development witnessed by our contemporary world, and the radical transformations it has brought about in various aspects of life, new criminal challenges have

How to Cite:
Tekkouk, N. (2025). Legal frameworks for combating information technology crimes: A study in light of Islamic Sharia and modern laws. *The International Tax Journal*, *52*(4), 1296–1308. Retrieved from https://internationaltaxjournal.online/index.php/itj/article/view/147

The International tax journal ISSN: 0097-7314 E-ISSN: 3066-2370 © 2025

Submitted: 05 March 2025 | Revised: 26 May 2025 | Accepted: 22 July 2025

emerged that exploit this progress for illicit activities. This has not been limited to the exploitation of modern technological tools in committing traditional crimes, but has extended to include the emergence of new criminal patterns that target these technologies themselves or benefit from their virtual nature.

This new type of crime, and the enormous losses and increasing threats associated with it, puts traditional criminal law to a real test in its ability to provide effective legal protection. This is partly due to the limited existing legislative texts and their failure to keep pace with the nature of the acts constituting the material element of these crimes, especially in light of the firmly established and comprehensive principles of Islamic Sharia.

Information technology holds a central position in this evolving landscape, as its use has extended to vital aspects of modern societies. With the massive expansion in the use of these technologies, new security and legal challenges have emerged in parallel, embodied in the emergence of various forms of related crimes.

Based on the recognition that technical systems, regardless of their level of development, remain vulnerable to exploitation and aggression, the importance of studying the legal frameworks capable of confronting these challenges emerges. In this context, this article seeks to clarify and analyze the available legal frameworks for combating information technology crimes. It specifically aims to review and evaluate these frameworks from the perspective of Islamic Sharia, and compare them with modern trends in contemporary laws. In pursuit of this goal, the study will address a set of fundamental axes that shed light on aspects of this problem.

First Axis: Ways to Combat Cybercrimes in Islamic Sharia

Islamic Sharia, as a universal law for all times and places, stems from the reality of human variation in self-control, which necessitates the existence of a deterrent penal system to ensure the safety of society from apparent and hidden manifestations of corruption.

Islamic Sharia has paid great attention to combating crime in all its forms, based on the principle that a person must strive to live by legitimate means and earn their livelihood through their work and effort. Islamic Sharia does not criminalize any act unless it involves actual harm to an individual or a group. This harm is manifested in affecting the six necessities (Maqasid al-Sharia), which are considered fundamental objectives of Sharia: religion, honor, life, progeny, wealth, and intellect."**1**

Islamic Sharia has been distinguished by a unique approach in confronting and eradicating crime through two integrated and balanced paths:

Firstly - The Preventive Aspect:

Among its most important features is the reform of the offender, opening wide the doors of repentance for them, not despairing them of God's mercy, urging them to cease and regret, and not persisting in falsehood. Sharia detests crime, threatens punishment for it in this world and the hereafter, and warns people who commit it secretly and then appear to people as pure and honorable**1**. Allah Almighty said:

"And do not argue on behalf of those who deceive themselves. Indeed, Allah does not like whoever is a betrayer, an arch-sinner. They conceal themselves from people, but they cannot conceal themselves from Allah; and He is with them when they plot by night that which is not pleasing to Him. And Allah is encompassing of [all] that they do."**2** [An-Nisa: 107-108].

Accordingly, the preventive role of Sharia is not limited to mere deterrent punishment, but includes taking all measures and procedures that prevent the occurrence of crime from the outset, through

continuous Islamic education with wisdom and good counsel, and raising awareness of the dangers of crime from various aspects of life, in addition to blocking the avenues that may lead to its commission. As Ibn al-Qayyim (may Allah have mercy on him) explained: "The soundness of the heart is by purifying it from corrupt desires and false doubts, and adorning it with beneficial knowledge and righteous intentions, which are the life, light, strength, nourishment, and medicine of the heart. Its corruption is by the opposite. The closer the heart is to safety and health, the further it is from the motives of evil and trials, and the quicker it is to good and obedience. Proper upbringing of souls is the foundation in protecting them from deviations and crime, as it works to strengthen religious and moral deterrents, develop the fear of Allah, and the awareness of His watchfulness, which prevents a person from falling into prohibitions."**3**

Secondly - The Curative Aspect:
The curative aspect comes second after the preventive aspect in confronting crime in general and cybercrime in particular.

Since crime is an abnormal behavior that threatens the security of individuals and the stability of societies and undermines the pillars of the state and country, the rulings of the glorious Islamic Sharia, with its upright justice and comprehensive principles, revolve around preserving the essential necessities that a person cannot do without and live without. Therefore, it has established deterrent and painful legal punishments for anyone who transgresses these essential necessities and violates their sanctity. It has set appropriate punishments for each crime to limit its commission. All these steps lead to combating crime and protecting society from its dangers. Thus, Islamic criminal legislations have taken upon themselves the burden of combating crime and confronting it; to protect society from falling prey to it in its various forms. There are two distinct rights that Islamic Sharia cares for:
The right of the wrongdoer to a chance to repent and start a cleaner reign.
The right of society to preserve its entity from the whims of disobedience and its turmoil that affects the innocent and the heedless.

Islam protects both rights. As for the right of the wrongdoer to repent, there is no religion on earth that facilitates repentance for sinners and pushes them towards it as Islam does. But what to do if a person turns into a rabid dog, so leaving him free only increases his ferocity, and only increases society's misery with him? The punishment of such a person is inevitable.**4**

There is no doubt that Islamic Sharia has assigned a suitable punishment to each crime, and has stipulated the controls, conditions, and rulings related to each crime and its punishment within the framework of traditional crimes and punishments, such as murder (qisas or blood money), adultery (stoning or lashing), theft (amputation), and drinking intoxicants (lashing). Thus, every crime for which a punishment is stipulated is a *hadd* punishment, and every crime for which a punishment is not stipulated is a *ta'zir* punishment. These are all traditional old crimes known to Islamic jurisprudence, for which estimated legal punishments) *hudud* (and non-estimated punishments) *ta'zirat* (have been established. With the emergence of new crimes related to technological advancement in the field of computers and the internet, Muslim jurists had to study these crimes and determine appropriate punishments for them.

It should be noted that the use of a computer as a means to commit a crime does not change its original description. The crime of fraud remains fraud whether committed by traditional means or via the internet, as do theft, slander, and others. To clarify how Islamic Sharia confronts cybercrime, it is useful to study some traditional crimes and apply their elements and conditions to crimes committed via computers. For example, the crime of theft, which is considered one of the most dangerous computer and internet crimes in the current era, its elements and conditions as mentioned by jurists in the era of codification can be applied to it. The theft of credit cards over the internet fulfills the definition of

theft, its conditions, and its estimated punishments in Islamic jurisprudence, which means that the prescribed legal punishment for it is the same as that prescribed for traditional theft.
The Hanafis defined theft as the taking by a sane, adult person of a protected *nisab*) minimum amount) or its value, belonging to another, without any doubt as to ownership, in a clandestine manner.**5**
The Malikis defined it as taking another's property secretly without being entrusted with it.**6**
The Shafi'is defined it as taking property clandestinely and unjustly from a protected place, with conditions.**7**

The Hanbalis defined it as taking property in a clandestine and concealed manner, including eavesdropping and furtive glances if done secretly.**8**
Based on these definitions, for theft to necessitate amputation, several conditions must be met, including:

- The thief must be a *mukallaf*) accountable person); if they are a child or insane, there is no *hadd* punishment for them.
- The theft must be committed voluntarily, not under duress.**9**
- The thief must not be compelled by hunger, having found no lawful food to eat.
- The stolen item must reach the *nisab* .The *nisab* for which the thief's hand is amputated is a quarter of a gold dinar, or three silver dirhams according to the majority of scholars, differing from the

Hanafis who believe the *nisab* is a dinar or ten dirhams or their value.**10** The source of the disagreement is in estimating the price of the shield for which the Prophet (peace be upon him) amputated the thief's hand. The Hanafis say its price was a dinar, while the majority say it was a quarter of a dinar. Authentic hadiths support the view of the majority, including what was narrated from him (peace be upon him): that he amputated the hand of a thief for a shield worth three dirhams.**11**

- The thief must not have any doubt of ownership over the stolen property; if they do, they are not considered a thief.
- The stolen property must have been taken from its protected place) *hirz* .(This condition is agreed upon by all jurists whose fatwas are followed.**12**

Practical Manifestations of Combating Electronic Theft in Islamic Sharia
By applying these conditions to online theft using stolen credit cards, it becomes clear that these conditions are met, as these cards are considered valuable property.

Perhaps this example shows that internet crimes can be adapted according to their description recorded in books of jurisprudence, after the judge seeks assistance from specialists to explain what they may wish to inquire about or clarify regarding the method and manner in which the crime occurred via the internet; so that they are fully aware of all the details through which they can issue their judgment on the accused.

This is if it is easy for specialists in Sharia sciences to attach the description of the electronic crime to the description of the traditional crime, then this case takes the ruling of that. However, if the mufti and the judge are unable to attach the description of the electronic crime to the description of the traditional crime, for example, due to a missing condition, then the field of discretionary punishment) *ta'zir* (is a wide field for confronting this crime. The judge chooses what is appropriate and suitable for the offender's situation, the severity of their harm, their motive, and the time and place .*Ta'zir* punishments are: unestimated punishments that are due to the right of Allah or the right of a human being for every transgression for which there is no *hadd* or *kaffara*) expiation).**13** They are like *hudud* in deterring and disciplining the Ummah. If the *ta'zir* punishment is unestimated, the ruler or judge may impose the punishment they deem appropriate, which may be a reprimand, beating, imprisonment, or confiscation, provided it does not reach the level of a *hadd* according to the majority of jurists.**14**

This differs from the Hanafis and Malikis, who expand the scope of *ta'zir* punishment, believing that *ta'zir* punishment may sometimes reach capital punishment.**15** This view has particular merit in the field of cybercrimes, as some of them may be more dangerous than murder, especially since they often transcend international borders.

Sheikh al-Islam Ibn Taymiyyah clarified the importance of *ta'zir* in achieving justice and preventing injustice, stating that: "When the Lawgiver establishes punishments for crimes, the purpose is to deter the offender, warn others, protect society from corruption and crime, and achieve justice among people .*Ta'zir* is among these punishments that are legislated where there is no estimated *hadd* in order to achieve justice and repel injustice."**16**

In summary of this axis, Islamic jurisprudence enjoys wide flexibility in dealing with new crimes via the internet and elsewhere, thanks to the *ijtihad*) independent reasoning) of jurists and the use of *qiyas*)analogical deduction) and the application of governing jurisprudential rules, such as the rule "Harm is to be removed"**17**, "Blocking the means"**18**, and "Averting harm takes precedence over bringing benefit"**19**.

Second Axis: Ways to Combat Cybercrimes in Contemporary Laws and International Systems
The confrontation of cybercrimes has received increasing global attention, manifested in the holding of conferences and seminars and the enactment of laws and legislations that criminalize these acts.

Firstly - Addressing Cybercrime from the Perspective of Laws in Some Countries:
Sweden is considered a pioneer in enacting special legislation for computer and internet crimes, with the Swedish Data Act issued in 1973, which addressed computer fraud in addition to crimes of unauthorized access, data forgery, alteration, or unlawful acquisition. The United States followed with the enactment of a special law for the protection of computer systems between 1976 and 1985, and in 1985, the National Institute of Justice identified five main types of information crimes.**20**

In 1986, the Computer Fraud and Abuse Act (CFAA) was enacted in the United States, and it has been amended several times since then. This federal law is a cornerstone in combating cybercrimes in the United States. The law primarily aims to protect federal computer systems, financial institutions, and systems used in interstate commerce, in addition to protecting internet-connected computers.

Key Aspects of the CFAA:

- **Criminalizing Unauthorized Access :**The law prohibits accessing a computer without authorization or exceeding the scope of granted authorization. This includes hacking systems, bypassing passwords, and using stolen credentials.
- **Criminalizing Unlawful Information Acquisition :**It prohibits obtaining information from a computer without authorization or by exceeding authorization ,even if no data is destroyed or altered.
- **Criminalizing Data Destruction or Alteration :**The law punishes intentionally destroying, altering, or transmitting information on a computer without authorization.
- **Criminalizing Computer-Related Fraud :**The law criminalizes the use of computers to commit fraud, such as identity theft or online financial fraud.
- **Criminalizing Causing Damage to Computer Systems :**The law punishes intentionally causing damage to computer systems, such as spreading viruses or launching Denial-of-Service (DoS) attacks.
- **Broad Scope of Application :**Over time, the scope of the CFAA has been expanded to include a wide range of activities related to computers and the internet, making it a powerful tool in prosecuting a variety of cybercrimes.

Impact of the CFAA in Combating Cybercrimes:
The CFAA has had a significant impact on combating cybercrimes in the United States by:

- **Providing a Legal Basis for Prosecution :**The law provides a clear legal framework for criminalizing a wide range of harmful computer-related activities, allowing federal authorities to criminally and civilly prosecute cybercriminals.
- **General Deterrence :**By criminalizing harmful behaviors and imposing penalties on violators, the law contributes to deterring individuals and organizations from engaging in cybercriminal activities.
- **Enabling Cooperation Among Law Enforcement Agencies :**The law facilitates cooperation among various federal and local law enforcement agencies in investigating cybercrimes and prosecuting their perpetrators.
- **Evolving with New Threats :**Despite some criticisms and challenges related to its interpretation and application, the CFAA has been amended over time to keep pace with developments in cybercrime and new threats.**21**

In 2000, the U.S. Department of Justice authorized five agencies, including the Federal Bureau of Investigation (FBI), to deal with computer and internet crimes.

Following the United States in its attention to combating cybercrimes is Britain, which ranks third after Sweden and America. It enacted the Forgery and Counterfeiting Act in 1971, which included in its definitions of forgery tools various computer storage media or any other tool on which data is recorded, whether by traditional or electronic means or by any other method.

Canada is also classified among these countries that have paid great attention to combating cybercrimes. In 1985, it amended its Criminal Code to include special laws for computer and internet crimes. The new law also included updated penalties for computer offenses and crimes of destruction or unauthorized access to computer systems. It also clarified the powers of investigative authorities as stated in the Competition Act, which authorizes judicial police officers, upon obtaining a court order, the right to inspect, deal with, and seize computer systems.**22**

Denmark has also enacted its first laws related to computer and internet crimes, which included in their paragraphs specific penalties for computer crimes such as unauthorized access to computers, forgery, or any illicit gain, whether for the perpetrator or a third party, and illicit manipulation of computer data such as destroying, altering, or exploiting it.**23**

Similarly, France has focused on developing its criminal laws to align with new criminal developments. In 1988, it issued a law that added computer crimes and their prescribed penalties to the Criminal Penal Code. Its Penal Code was also amended in 1994 to include a new set of legal rules related to information crimes and entrusted the Public Prosecution with the authority to investigate them, including requesting investigations and hearing statements.**24**

In the Netherlands, Japan, Hungary, and Poland, there are also special laws regarding computer and internet crimes that clarify how to deal with these crimes and their accused. These laws grant the accused the right not to print computer records, or disclose passwords or program codes. They also grant witnesses the right to refuse to print information retrieved from a computer if it would incriminate them or one of their relatives. Furthermore, the criminal laws in force in Poland go even further by stipulating that no coercive measure or interpretation detrimental to the accused should be applied.**25**

As for Arab countries, we find that Algerian legislation has introduced a section in the Penal Code, in Section Seven bis of Chapter Three, concerning felonies and misdemeanors against property, under the title "Infringement of Automated Data Processing Systems." Article 394 bis states: "Anyone who fraudulently accesses or remains, in whole or in part, within an automated data processing system or attempts to do so shall be punished by imprisonment from three months to one year and a fine of fifty thousand to one hundred thousand dinars. The penalty shall be doubled if this results in the deletion or alteration of the system's data. If the aforementioned acts result in the destruction of the system's operation, the penalty shall be imprisonment from 06 months to two years and a fine of fifty thousand to one hundred and fifty thousand dinars".

Article 394 bis 1: "Anyone who fraudulently introduces data into a system or fraudulently removes or alters data contained therein shall be punished by imprisonment from 06 months to 03 years and a fine of 500,000 DZD to 2,000,000 DZD".

Article 394 bis 2: "Anyone who intentionally and fraudulently performs the following shall be punished by imprisonment from two months to 03 years and a fine of 1,000,000 DZD to 5,000,000 DZD: 01- Designing, researching, assembling, providing, publishing, or trading in data stored, processed, or transmitted through an information system by which the crimes stipulated in this section can be committed. 02- Possessing, disclosing, publishing, or using for any purpose whatsoever data obtained from one of the crimes stipulated in this section".

Article 394 bis 3: "The penalty stipulated in this section shall be doubled if the crime targets national defense or public law bodies and institutions, without prejudice to the application of more severe penalties".

Article 394 bis 4: "A legal person who commits one of the crimes stipulated in this section shall be punished by a fine equivalent to five times the maximum prescribed for a natural person".

Article 394 bis 5: "Anyone who participates in a group or agreement formed for the purpose of preparing for one or more of the crimes stipulated in this section, and this preparation is embodied in one or more material acts, shall be punished with the penalties prescribed for the crime itself".

Article 394 bis 6: "Without prejudice to the rights of bona fide third parties, the equipment, software, and means used shall be confiscated, and sites that are the subject of a crime punishable under this section shall be closed, as shall the premises or place of exploitation if the crime was committed with the knowledge of its owner".

Article 394 bis 7: "Attempting to commit the misdemeanor stipulated in this section shall be punished with the penalties prescribed for the misdemeanor itself."**26**

Through the aforementioned articles, we find that crimes against automated processing systems primarily consist of the crimes of unauthorized entry and remaining within an automated data processing system.

1. Act of Entry:

Entry here refers to electronic entry through available technical methods and means, such as accessing the information system's core and viewing information. The Algerian legislator did not specify the method of entry, and therefore the crime is committed by any means. One of the most commonly used techniques to gain entry to the system is the use of programs specifically designed to breach security systems.

Article 394 bis of the Penal Code stipulates that anyone who fraudulently enters or remains, in whole or in part, within an automated data processing system or attempts to do so shall be punished by imprisonment from three months to one year and a fine of 50,000 DZD to 100,000 DZD.
This penalty shall be doubled if this results in the deletion or alteration of the system's data. If the aforementioned acts result in the destruction of the system's operation, the penalty shall be imprisonment from six months to two years and a fine of 50,000 DZD to 150,000 DZD.

2. Act of Remaining:
This refers to being present within the information system against the knowledge and will of the person who has the right to control this system. The crime of remaining can occur independently without the crime of entry, in cases where entry to the processing system is by virtue of status or error, or in cases where entry to the system is legitimate but remaining in it for a limited period of time requires immediate exit upon its expiration, yet the perpetrator remains within the system. The material conjunction between the crimes of entry and remaining occurs when the entry is unlawful and the perpetrator remains in it for a period of time.

A jurisprudential dispute has arisen regarding the determination of the period after which the crime of entry ends and the crime of unlawful remaining begins. One opinion held that as soon as the crime of entry is committed, a short period of remaining in the system is required for the crime of remaining to begin. However, this opinion is criticized for not precisely defining the starting point of the crime of remaining. Therefore, proponents of the second opinion defined the moment the crime of remaining begins as when the person becomes aware that their presence within the system is unlawful. This opinion is also criticized for the difficulty of proving the element of knowledge, which led to the emergence of a fixed opinion that the crime of remaining begins from the moment the person who entered the processing system is warned that their presence is unlawful. However, this opinion was criticized because it presupposes the existence of a warning system that performs this task.

Finally, there is a fourth opinion that believes the crime of remaining begins from the moment the perpetrator starts browsing within the system, or continues to browse within it after the specified time.
As for Egyptian law, it strives to apply the rules of traditional criminal law to information crimes, which impose a kind of criminal protection against acts similar to the acts constituting the elements of traditional crime. For example, the patent law applies to the material aspect of the automated information processing system, and the provisions of the private life protection law and the law criminalizing the disclosure of secrets have been adapted so that they can be applied to some information crimes. Criminal courts have been entrusted with examining cases committed against or by information systems.

The same applies to the Kingdom of Bahrain, where there are no specific laws for internet crimes. Even if there is a provision close to the committed act, the prescribed penalty does not match the extent of the damage resulting from the internet crime.**27**

Secondly - The International Dimension of Cybercrime
The international dimension of information crime has compelled the international community to seek more appropriate means for its nature, and to narrow the legal loopholes that its perpetrators have excelled in exploiting to evade punishment and spread their activity in different parts of the world. Since the optimal criminal policy will not achieve its desired purpose unless all its criminal, punitive, preventive, and executive elements are harmonized with each other; a number of technical and administrative mechanisms have been approved to combat organized crime, in order to benefit from technological progress – the source of information crime – in combating it. We will review two models of technical cooperation as follows:

1. Information Exchange:
The current era has witnessed a revolution in the field of information, which has made it imperative for the international community to give utmost importance to information exchange as a means of combating crime in general, and information crime in particular, due to the support that correct and reliable information provides to law enforcement agencies in all fields, including monitoring the activities of criminal organizations and sources of funds in all fields. Therefore, the Sixth United Nations Congress on the Prevention of Crime and the Treatment of Offenders recommended developing systematic information exchange as a key element of the international action plan for crime prevention and control, and recommended that the United Nations establish an information database to inform States Parties about global trends in crime.

Thus, cooperation on issues related to information crime should be supported by the deployment of information exchange systems among member states, and the provision of bilateral and multilateral technical assistance to member states, using training on law enforcement and treaties related to criminal justice, at the international level.**28**

The centralization of information should not prevent its dissemination and exchange among states, after its arrangement, study, and processing, in a way that allows it to be used in the investigation and trial stages, and to monitor suspicious persons, whether individuals or entities, while ensuring personal freedoms. This also includes matters related to the movements of organized criminals in a criminal group across borders and matters related to forged and stolen documents that they may resort to using, and all information related to the criminal activities they commit, such as alien smuggling, to coordinate among agencies combating organized human smuggling across national borders.

This applies to the various forms of information crime, which was confirmed by the Schengen Agreement of the European Union, through its formulation of an integrated information exchange system.**29**

Therefore, prevention – through information – is considered an essential element and a fundamental basis for the fight against information crime, and ensuring the creation of an effective confrontation system. On this basis, the draft convention on combating organized crime establishes information exchange as a preventive mechanism for combating this crime. Article 12, paragraph 2, of the draft framework convention states that States Parties shall facilitate the exchange of information related to all aspects of the criminal activity of persons involved in organized crime.

2. Exchange of Expertise and Technical Assistance:
To achieve integration with the general trend of computerizing criminal justice operations, and developing and analyzing information in a way that serves the objectives of modern criminal policy to combat crime in general... administrative elements and technical technologies should be exchanged, and the capacities of justice agencies should be enhanced, and available data and information on crime and innovative ways and mechanisms to combat traditional and non-traditional crimes should be analyzed and disseminated. Emphasis should be placed on new methods such as supporting technical cooperation, and providing extensive consulting services to cover all areas, such as those related to concealing the trace of money, to combat money laundering crime with the aim of depriving criminal organizations of the proceeds of crimes, because preventive policy will remain deficient unless all elements of the assumed criminal behavior are controlled.

The Financial Action Task Force (FATF) plays a vital role in setting international standards for combating money laundering and terrorist financing, and this increasingly includes addressing the links between these crimes and cybercrimes. FATF's efforts in this context can be summarized as follows:

- **Inclusion of Cybercrimes as a Source of Money Laundering :**FATF considers the proceeds of cybercrimes as illicit gains subject to money laundering operations. FATF recommendations oblige countries to criminalize money laundering and apply customer due diligence measures and report suspicious transactions to detect money laundering resulting from cybercrimes.
- **Identification of Cybercrime-Related Risks in National Risk Assessments :**FATF encourages countries to include money laundering and terrorist financing risks associated with cybercrimes in their national risk assessments. This helps in understanding threats and effectively directing combating efforts.
- Issuance of Guidance and Reports on the Links Between Cybercrimes and Money Laundering: FATF has published several reports and guidelines analyzing the methods used by criminals to launder money obtained from cybercrimes, such as online fraud, identity theft, extortion, and malware (Ransomware). These reports provide recommendations for countries and financial institutions to detect and prevent these activities.

  For example, FATF issued a report titled "Illicit Financial Flows from Cyber-Enabled Fraud" in November 2023, which analyzes the evolving landscape of cyber-enabled fraud and its links to other crimes and how criminals launder the proceeds. The report provides recommendations to enhance detection, prevention, and public-private sector cooperation at the domestic and international levels.

  FATF also issued a report on "Countering Ransomware Financing" in March 2023, which provides guidance to countries to prevent and detect the laundering of proceeds from ransomware attacks.
- **Focus on Virtual Assets :**Given the increasing use of virtual assets (such as cryptocurrencies) in cybercrimes and money laundering, FATF has updated its recommendations to include Virtual Asset Service Providers (VASPs) and oblige them to apply AML/CFT measures, including the Travel Rule.
- **Enhancing International Cooperation :**FATF emphasizes the importance of international cooperation in information exchange and mutual legal assistance to combat cybercrimes, money laundering, and related terrorist financing.**30**

Bilateral and multilateral technical assistance can be provided to member states, using training and international exchange programs and training on law enforcement and treaties related to criminal justice at the international level.

However, in this case, the legislative authorities of any country must make an amendment to the criminal procedure law to legitimize these procedures in a manner consistent with the nature of the crime and its new, different dimensions, which necessitate specific legal legislation to cover all legal aspects – substantive and procedural – without being restricted by general rules that may – sometimes – prevent criminal justice from achieving its purposes.

Article 14 of the Protocol against the Smuggling of Migrants by Land, Air and Sea stipulates that States Parties shall make every effort to provide materials such as vehicles, computer systems and document examination devices, and shall provide their assistance as countries of origin or transit for migrant smuggling, in addition to detecting the exploitation by these smugglers of the human vulnerability of their victims to achieve their purposes, by offering bribes and extortion.**31**

Conclusion

The greatness of Islamic Sharia is evident in its precedence over international legal systems in establishing principles and means to confront newly emerging criminal acts in the digital space. This is underscored by the comprehensiveness of Sharia rulings across all aspects of life, and its self-sufficiency in providing the necessary legal frameworks without the need to import external systems. The international legal system must internalize the essence of these principles and act accordingly. Islamic

Sharia has established the principle of expanding criminalization for emerging acts within specific jurisprudential rules and principles. If societies adopted a comprehensive and just view of Islam, they would find in it solutions to all legal dilemmas, and justice and prosperity would be achieved under its guidance. The fundamental disparity between Islamic Sharia and other positive legal systems, which reveal their shortcomings and deficiencies, becomes clear, necessitating Muslims' awareness of the value of their legal system and acting in accordance with it.

Recommendations

- **Call for Concerted International Efforts to Codify Legislation Derived from Islamic Sharia :** Emphasize the necessity for the international community to enact international laws and legislations based on the principles of Islamic Sharia and its jurisprudential rules in the field of combating cybercrimes, and to oblige member states to apply these legislations to reduce these crimes in the digital space.
- **Establish Legal Frameworks for Protecting Cultural Identity and Societal Values :**Enact legislations aimed at establishing legal controls to confront negative cultural influences, including deviant ideas and pornographic content that target youth and undermine societal values and beliefs.
- **Consider Infringement of Intellectual Property Rights a Punishable Crime :**Explicitly stipulate in laws the criminalization of digital software piracy and consider it among financial rights infringement crimes, similar to traditional theft crimes.
- **Establish Specialized Courts for Digital Crimes :**Establish judicial bodies with jurisdiction to hear cases related to crimes committed in the digital environment and the internet, ensuring the speed and effectiveness of judicial procedures.
- **Establish Specialized Law Enforcement Units in the Digital Space :**Create an agency or specialized units within security forces responsible for combating cybercrimes, and legally empower them to conduct investigations and apprehend perpetrators of these crimes directly and immediately through the use of technical means to track devices and communication lines used in committing the crime.

References

[1] Muhammad Al-Ghazali ,*Hadha Dinuna*) This is Our Religion), 3rd ed. (Cairo, 1975), p. 229.

[2] Surah An-Nisa, Verses 107-108 of the Holy Quran.

[3] Ibn Qayyim Al-Jawziyya, Muhammad ibn Abi Bakr .*Madarij Al-Salikin Bayna Manazil Iyyaka Na'budu wa Iyyaka Nasta'in*) The Stages of the Seekers Between the Stations of "You Alone We Worship and You Alone We Ask for Help"). Edited by Muhammad Hamid Al-Fiqi. Vol. 1. Beirut: Dar Al-Kutub Al-Ilmiyya, no date of publication.

[4] Muhammad Al-Ghazali ,*Hadha Dinuna* ,*op. cit* ,.p. 154.

[5] Kamal al-Din ibn al-Humam al-Hanafi ,*Sharh Fath al-Qadeer*) Commentary on Fath al-Qadeer), Dar Ihya al-Turath al-Arabi, p. 120.

[6] Abu Al-Walid Muhammad ibn Ahmad ibn Rushd Al-Qurtubi ,*Bidayat al-Mujtahid wa Nihayat al-Muqtasid*) The Distinguished Jurist's Primer), edited by Abu Abd al-Rahman Abd al-Hakim ibn Muhammad, Al-Maktaba Al-Tawfiqiyya (Cairo), p. 262.

[7] Qalyubi, Shihab al-Din Ahmad ibn Ahmad ibn Salama, and Umayra ,*Kanz al-Raghibin fi Sharh Minhaj al-Talibin li al-Imam al-Nawawi*) The Treasure of Desirous Ones in the Commentary on Minhaj al-Talibin by Imam al-Nawawi) (Cairo: Matba'at al-Ma'ahid al-Azhariyya), p. 186.

[8] Al-Bahuti, Mansour ibn Yusuf ,*Al-Rawd al-Murbi*) The Quadrilateral Garden) (Beirut: Dar Al-Fikr), p. 439.

[9] Qalyubi, Shihab al-Din Ahmad ibn Ahmad ibn Salama, and Umayra ,*Kanz al-Raghibin fi Sharh Minhaj al-Talibin li al-Imam al-Nawawi* ,*op. cit* ,.p. 196.

[10] Abu Al-Walid Muhammad ibn Ahmad ibn Rushd Al-Qurtubi ,*Bidayat al-Mujtahid wa Nihayat al-Muqtasid* ,*op. cit* ,.p. 663.

[11] Narrated by Muslim in his Sahih, Book of Hudud, Chapter on the Hadd of Theft and its Nisab.
[12] Abu Al-Walid Muhammad ibn Ahmad ibn Rushd Al-Qurtubi ,*Bidayat al-Mujtahid wa Nihayat al-Muqtasid* ,*op. cit* ,.p. 666.
[13] Wahbah Al-Zuhayli ,*Al-Fiqh Al-Islami wa Adillatuhu*) Islamic Jurisprudence and its Proofs) (Dar Al-Fikr, 1976.(
[14] Ibn Taymiyyah, Ahmad ,*Al-Siyasah Al-Shar'iyyah fi Islah Al-Ra'i wa Al-Ra'iyyah*) The Islamic Policy in Reforming the Ruler and the Ruled), Dar Ilm Al-Fawa'id lil Nashr wal Tawzi' (Jeddah, Saudi Arabia), p. 146.
[15] Abd Al-Aziz Amer ,*Al-Ta'zir fi Al-Shari'ah Al-Islamiyyah*) Discretionary Punishment in Islamic Law) (Dar Al-Fikr Al-Arabi), p. 322.
[16] Ibn Taymiyyah, Ahmad ,*Al-Siyasah Al-Shar'iyyah fi Islah Al-Ra'i wa Al-Ra'iyyah* ,edited by Muhyi Al-Din Abd Al-Hamid (Riyadh: Dar Alam Al-Kutub), p. 26.
[17] Jalal al-Din al-Suyuti ,*Al-Ashbah wal Naza'ir*) Similarities and Analogies), Dar Al-Kutub Al-Ilmiyya (Beirut), p. 83.
[18] Abu Ishaq Ibrahim ibn Musa Al-Shatibi ,*Al-Muwafaqat fi Usul Al-Shari'ah*) The Agreements in the Principles of Islamic Law) (Beirut: Dar Al-Ma'rifa, 1975), Vol. 4, p. 163.
[19] Jalal al-Din al-Suyuti ,*Al-Ashbah wal Naza'ir* ,*op. cit* ,.p. 87.
[20] Abd Al-Rahman Abd Al-Aziz Al-Shiniqi ,*Amn Al-Ma'lumat wa Jara'im Al-Hasub Al-Ali*)Information Security and Computer Crimes) (Kingdom of Saudi Arabia), p. 108.
[21] Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (1986.(
[22] Abd Al-Rahman Abd Al-Aziz Al-Shiniqi ,*Amn Al-Ma'lumat wa Jara'im Al-Hasub Al-Ali* ,*op. cit* ,.p. 108.
[23] Abd Al-Rahman Abd Al-Aziz Al-Shiniqi ,*Amn Al-Ma'lumat wa Jara'im Al-Hasub Al-Ali* ,*op. cit* ,.p. 110.
[24] Ahmad Hussam Taha Tamam ,*Al-Jara'im Al-Nashi'ah 'an Istikhdam Al-Hasub Al-Ali*) Crimes Arising from the Use of Computers), Dar Al-Nahda Al-Arabiyya (Cairo), p. 200.
[25] Ahmad Hussam Taha Tamam ,*Al-Jara'im Al-Nashi'ah 'an Istikhdam Al-Hasub Al-Ali* ,*op. cit* ,.p. 222.
[26] Articles 394 bis 1 to 394 bis 7 of Law No. 66-155 dated June 8, 1966, comprising the Algerian Penal Code, as amended and supplemented.
[27] Abd Al-Rahman Muhammad Najd ,*Obstacles to Investigating Cybercrimes: A Survey Study on Police Officers in the State of Bahrain*) Published Master's Thesis, Naif Arab University for Security Sciences, Riyadh, Saudi Arabia, 1440 AH.(
[28] Aliwali, "Echoes of the Sixth United Nations Congress on the Prevention of Crime and the Treatment of Offenders ",*Justice Journal* ,p. 146.
[29] MICHEL Quille ,*Stratégies en France par la police contre la criminalité organisée* ,(1996) p. 199.
[30] See the official website of the Financial Action Task Force (FATF ,(https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html) accessed: May 19, 2025.(
[31] Imad Atahina ,*Interpol in Conflict with Crime*1 ,st ed. (Dar Ma'ad lil Nashr, 1991)

Primary Sources:

- **The Holy Quran.**
- **Sahih Muslim .**By Imam Muslim ibn al-Hajjaj. Beirut: Dar Ihya' al-Turath al-Arabi.

Books:

- Ibn Taymiyyah, Ahmad .*Al-Siyasah al-Shar'iyyah fi Islah al-Ra'i wa al-Ra'iyyah*) Islamic Governance in Reforming the Shepherd and the Flock). Edited by Muhyi al-Din Abd al-Hamid. Riyadh: Dar Alam al-Kutub.

- Ibn Taymiyyah, Ahmad .*Al-Siyasah al-Shar'iyyah fi Islah al-Ra'i wa al-Ra'iyyah*) Islamic Governance in Reforming the Shepherd and the Flock). Jeddah, Kingdom of Saudi Arabia: Dar Alam al-Fawa'id lil-Nashr wa al-Tawzi.'
- Ibn Rushd, Abu al-Walid Muhammad ibn Ahmad .*Bidayat al-Mujtahid wa Nihayat al-Muqtasid*) The Distinguished Jurist's Primer). Edited by Abu Abd al-Rahman Abd al-Hakim ibn Muhammad. Cairo: Al-Maktabah al-Tawfiqiyyah.
- Ibn al-Humam al-Hanafi, Kamal .*Sharh Fath al-Qadir*) Commentary on Fath al-Qadir). Beirut: Dar Ihya' al-Turath al-Arabi.
- At-Tahina, Imad. (1991 .(*Al-Interpol fi Sira' ma' al-Jarimah*) Interpol in Conflict with Crime). 1st ed. Dar Ma'ad lil-Nashr.
- Al-Buhuti, Mansour ibn Yusuf .*Al-Rawd al-Murabbi*) 'The Square Garden). Beirut: Dar al-Fikr.
- Tamam, Ahmed Hussam .*Al-Jara'im al-Nashi'ah 'an Istikhdam al-Hasub al-Ali*) Crimes Arising from the Use of Computers). Cairo: Dar al-Nahdah al-Arabiyyah.
- Amer, Abd al-Aziz .*Al-Ta'zir fi al-Shari'ah al-Islamiyyah*) Discretionary Punishment in Islamic Sharia). Dar al-Fikr al-Arabi.
- Al-Ghazali, Muhammad. (1975 .(*Hadha Dinuna*) This is Our Religion). 3rd ed. Cairo: Hassan.
- Qalyubi, Shihab al-Din Ahmad ibn Ahmad ibn Salamah, and Umayrah .*Kanz al-Raghibin fi Sharh Minhaj al-Talibin li al-Imam al-Nawawi*) Treasure of the Desirous in Explaining Minhaj al-Talibin by Imam al-Nawawi). Cairo: Matba'at al-Ma'ahid al-Azhariyyah.
- Al-Zuhayli, Wahbah. (1976 .(*Al-Fiqh al-Islami wa Adillatuh*) Islamic Jurisprudence and its Evidences). Dar al-Fikr.
- Al-Suyuti, Jalal al-Din .*Al-Ashbah wa al-Naza'ir*) Similarities and Analogies). Beirut: Dar al-Kutub al-Ilmiyyah.
- Al-Shatibi, Abu Ishaq Ibrahim ibn Musa. (1975 .(*Al-Muwafaqat fi Usul al-Shari'ah*) The Concordances in the Principles of Islamic Law). Vol. 4. Beirut: Dar al-Ma'rifah.
- Al-Shiniqi, Abd al-Rahman Abd al-Aziz .*Amn al-Ma'lumat wa Jara'im al-Hasub al-Ali*) Information Security and Computer Crimes). Kingdom of Saudi Arabia.

Academic Theses/Dissertations:

- Najd, Abd al-Rahman Muhammad. (1440 AH .(*Mu'awwiqat al-Tahqiq fi Jara'im al-Internet Dirasah Mas'hiyyah 'ala Dubbat al-Shurtah fi Dawlat al-Bahrain*) Obstacles to Investigating Internet Crimes: A Survey Study on Police Officers in the State of Bahrain). Published Master's Thesis, Naif Arab University for Security Sciences, Riyadh, Saudi Arabia.

Articles and Periodicals:

- Aliwali. (1981). Echoes of the Sixth United Nations Congress on the Prevention of Crime and the Treatment of Offenders .*Journal of Justice* ,p. 146.

Laws and Legislations:

- Law No. 15-04 of November 10, 2004, Amending and Supplementing Order No. 66-156, Containing the Algerian Penal Code.
- Computer Fraud and Abuse Act, 18 U.S.C. p 1030 (1986.(

Websites:

- The Official Website of the Financial Action Task Force (FATF). (Accessed: 19/05/2025). Available at :https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html

Foreign References:

- Quille, Michel. (1996 .(*Stratégies en France par la police contre la criminalité organisée*) Strategies in France by the Police Against Organized Crime.(