The Impact of Cybercrime on Security in Africa: A Case Study of Côte d'Ivoire

Belhaouari Zohra[1] *, Fasla Abdellatif [2]
[1] Oran 2 University, Algeria, belhaouari.zohra@univ-oran2.dz
https://orcid.org/0009-0001-0029-5772
[2] Oran 2 University, Algeria, fasladz@yahoo.fr
Ohttps://orcid.org/0009-00001-0032-2332

Received:30/07/2025 | *Accepted:12/10/2025* | *Published: 15/01/2026*

Abstract:
Cybercrime constitutes one of the most pressing legal and security threats undermining the foundations of legal certainty and institutional stability in African states, particularly in light of fragile digital infrastructure, insufficient legislative frameworks, and limited effectiveness of judicial and law enforcement institutions. This study seeks to analyze the legal and security ramifications of cybercrime through an applied case study of the Republic of Côte d'Ivoire, a country experiencing significant digital expansion coupled with a notable rise in cyber-related criminal activities.

The analysis reveals that several factors have contributed to the exacerbation of this phenomenon, including the rapid increase in internet accessibility, high youth unemployment rates, and low levels of awareness of digital legal culture. The primary offenses observed include cyber fraud, identity theft, and extortion via digital platforms, all of which pose a serious threat to public digital order and compromise national cybersecurity A major challenge identified is the inadequacy of domestic legislation in keeping pace with the evolving nature of cybercriminal methods, compounded by the shortage of specialized technical competencies within law enforcement bodies, thereby weakening the effectiveness of criminal investigation and prosecution mechanisms.

Keywords: cybercrime; security; combating; international cooperation.

*** Corresponding author**

1. INTRODUCTION

In the context of increasing globalization, the widespread adoption of internet technologies has reshaped social interaction patterns across the African continent. This shift is facilitated by the diversification of communication tools and the integration of technologies that play a central role in transforming modern societies[1]. The ease with which these technologies are accessed, particularly by young people, has unfortunately opened the door to various forms of criminal behavior motivated by the pursuit of quick financial gain through illicit means.

Although criminal law penalizes any act that causes harm to others, methods of committing crimes have evolved considerably. One major development is the emergence of cybercrime in the late 1990s, which has grown into a serious threat, especially in developing countries[2].

Its effects are most visible in cybersecurity systems, particularly in Southern African nations such as Côte d'Ivoire.

In the late 2000s, such offenses became increasingly prevalent in Côte d'Ivoire, damaging the country's international reputation and undermining the legitimate benefits of adopting modern digital technologi[3] This situation raises several critical questions:

How should cybercrime be defined legally in this context?

What are the root causes of this phenomenon?

What legal and institutional mechanisms has Côte d'Ivoire adopted to counter and reduce the spread of cybercrime?

2- The Conceptuel Framework of Cybercrime

Cybercrime is legally defined as any act or omission that is premeditated or planned and that involves the use of computer systems whether personal computers, network systems, the Internet, or social media platforms for the purpose of facilitating the commission of a crime or an act that contravenes the law. This also includes crimes that target computer networks themselves, such as unauthorized access, data breaches, or malicious interference aimed at altering, disabling, or damaging the content of data or software applications[4].

The cyberspace, in this context, is primarily understood as an information domain created through the global interconnection of digital systems. It is the space where data is generated, processed, and stored. Technically, cyberspace encompasses the physical infrastructure that underpins the digital environment, including cables, routers, satellites, and other fixed electronic devices located within defined geographical and political boundaries. In essence, it is an intangible environment through which data, information, and ideas are exchanged and circulated[5].

This dual nature combining physical infrastructure with intangible virtual exchange renders cyberspace a fertile ground for the proliferation of modern criminal conduct, necessitating the development of new legal interpretations and institutional responses.

2-1- The Legal Nature of Cybercrime

The legal characterization of cybercrime has sparked a significant doctrinal divide. One school of thought maintains that, under traditional legal principles[6], only tangible property can be subject to possession and misappropriation. According to this view, an object must be physically perceptible in order to be considered capable of theft, since unlawful possession or appropriation presumes material existence. Consequently, intangible assets

such as data or digital content do not qualify as stolen property unless embodied on physical media (e.g., a disk or tape). If such physical carriers are stolen, then the offense is easily classified as theft of tangible informational property. However, complications arise when the misappropriated object is immaterial digital content[7].

In contrast, a more modern approach argues that information itself constitutes a new category of asset: a set of values susceptible to appropriation, regardless of the medium through which they are accessed. This position emphasizes the economic value of digital data, which can be unlawfully seized independently of its physical form, thus warranting legal protection under property and criminal law frameworks.

Logically, a distinction should be made between purely physical IT assets (e.g., hardware components such as monitors) and magnetized digital assets those comprising both a material substrate and a moral or intellectual component that imparts economic value. An example is remote cyber espionage, where offenders operate discreetly behind screens, far from the physical crime scene. According to a 2020 report by Frank Kié, a cybersecurity advisor and founder of Cyber Africa Forum, financial losses in Africa from such crimes amounted to 1 billion USD, with Côte d'Ivoire alone accounting for over 6 billion USD in 2021, largely due to the activities of so-called "brouteurs"[8], These developments prompted several

European states to place Côte d'Ivoire on a red list of jurisdictions highly vulnerable to cybercrime[9].

Accordingly, cybercrime is primarily classified as economic crime, as its principal aim is to obtain financial gain, whether through tangible fraudulent means or intangible manipulation such as deception, breach of trust, or digital misappropriation. Notable methods include:

- Automated embezzlement programs, which are designed to conduct unauthorized fund transfers between bank accounts either within the same financial institution or across different ones. Some software executes operations at pre-set times, or rounds decimal interest values from deposit accounts, diverting minute amounts into the perpetrator’s account. The repetitive, large-scale nature of these operations often conceals the cumulative financial loss from detection by individual account holders[10]
- Credit card fraud, which may involve intercepting PIN codes from ATMs, phishing techniques, or the theft of card information from online marketplaces that store customer payment credentials.

Beyond property crimes, cyber offenses may also be categorized as crimes against persons, including extortion, defamation, threats, identity theft, and invasion of privacy, such as unauthorized access to personal email accounts. Data repositories often referred to as information banks serve users in scientific, cultural, or military sectors and now represent vulnerable digital assets. Criminals increasingly launch ransomware attacks, encrypting files and demanding payment in exchange for data restoration.

Lastly, cybercrimes may also constitute crimes against the state and public morals, such as espionage, incitement to unrest, forgery of official documents, and impersonation, all of which undermine national security and social cohesion.

2-2- Distinctive Features of Cybercrime

Given its inherent link to the internet and social media platforms, cybercrime exhibits a set of distinctive characteristics that differentiate it from conventional forms of criminal activity:

a. Transnational Nature

Cybercrime is inherently transboundary in nature. The global reach of the internet particularly in regions like Africa where legal and security frameworks are often underdeveloped has transformed the digital space into a fertile ground for the commission of crimes across jurisdictions.

Offenders and victims may be located in entirely different countries, thereby raising complex legal questions concerning jurisdiction, applicable law, and procedures for international cooperation

. The absence of territorial constraints has underscored the urgent need for harmonized legal instruments and enhanced judicial collaboration.

b. Difficulty of Detection and Evidence Collection

Unlike traditional crimes that typically leave physical traces, cybercrimes are ephemeral by nature. They often leave behind no tangible evidence, as they rely on transient digital signals that can vanish immediately after execution. In many cases, the perpetrator effectively destroys the evidence as part of committing the offense. This makes detection, attribution, and prosecution particularly challenging[11].

c. The Unique Profile of Cyber Offenders

Cybercriminals are typically individuals with advanced technical knowledge and computing skills. They may also possess a strong understanding of organizational and financial systems. Scholars often categorize cyber offenders into three main groups:

- **Hackers**

Technically skilled individuals who unlawfully gain access to others' systems out of curiosity or a desire to demonstrate their capabilities. Many are unemployed youth or adolescents seeking recognition.

- **Professionals**

The most dangerous group, these individuals are motivated by profit and specialize in illicit access to banking systems and financial institutions. They usually range in age from 25 to 40 years.

- **Vindictive Actors**

These offenders are primarily driven by personal grievances and aim to spread discord or inflict harm as a form of revenge[12]

d. High Appeal to Criminals

Due to its low risk of detection, the difficulty of tracing offenders, and the potential for substantial financial rewards, cybercrime presents an attractive opportunity for offenders. The perceived anonymity and technical complexity of the cyber environment embolden criminals, especially in contexts with weak enforcement capabilities[13].

e. Commission During Automated Data Processing

A distinctive feature of cybercrime is that it occurs during automated data processing. Such crimes may take place at any stage of the data processing cycle during input, processing, or output of digital information. The occurrence of a crime at one of these stages is a necessary condition for its legal qualification as a cybercrime. In the absence of this element, the act may fall outside the definitional scope of cybercrime.

f. Emerging and Evolving Nature[14]

Cybercrime is classified as an emerging criminal phenomenon. The exponential pace of technological advancement over recent decades has effectively outpaced the regulatory and enforcement capacities of many states, especially in the Global South. The unregulated expansion of digital technology has created vulnerabilities that compromise national and individual security alike.

3- Mechanisms of Cybercrime Execution

Electronic communication systems especially the internet play a dual role in the context of cybercrime. They may serve as the target, the instrument, or even the environment in which cybercrimes are conceived and executed. At the same time, these platforms may also facilitate the detection and investigation of such crimes. The mechanisms may be categorized as follows:

3-1 The Internet as a Target of Crime

In certain instances, the internet infrastructure itself is the direct object of criminal activity. This occurs, for example, when unauthorized access is gained to data systems hosted on specific websites, with the intent to destroy, alter, or exfiltrate stored or transmitted data. In some cases, offenders conceal their unlawful conduct by reproducing and redistributing the compromised data via the same network, especially to users engaged in online payment systems[15]

3-2 The Internet as a Tool for Crime

Cybercriminals often exploit the internet as a technical medium to facilitate offenses that would be difficult or impossible to commit in the physical world. This includes illegal money transfers, the use of digital tools for forgery or counterfeiting, and the theft and misuse of credit card information for unauthorized purchases and payments. Such techniques are frequently used to launder illicit proceeds by masking the origin of the funds through successive online transactions[16] .

3-3 The Internet as a Criminal Ecosystem

Beyond being a tool or target, the internet also constitutes a criminal environment, offering a virtual space where illegal networks flourish. This includes the negotiation and conclusion of drug trafficking agreements, the operation of pornographic or terrorist networks, and the organization of money laundering schemes. These activities often occur on encrypted platforms and the dark web, creating significant obstacles for law enforcement [17].

4- The Role of Technology in Crime Detection

While the internet facilitates cybercrime, it also plays a critical role in its detection. Law enforcement agencies must adopt sophisticated and continuously updated technologies capable of tracking and intercepting evolving criminal tactics. This includes the use of digital forensics, intrusion detection systems, and cross-border intelligence cooperation[18].

4-1- Common Methods of Cybercrime

Cyber offenses are typically committed using several well-documented methods:

4-2- Phishing attacks

where fake emails or messages impersonate legitimate institutions to trick individuals into revealing financial or personal data.

4-3- Sextortion

where explicit images or videos are used to blackmail victims.

4-4- Business Email Compromise (BEC)

where hackers infiltrate corporate communication systems to gain access to payment structures, then deceive employees into initiating unauthorized wire transfers to the criminals' accounts.

4-5- Ransomware attacks

particularly against hospitals and public institutions, in which computer systems are locked or disabled, followed by a demand for ransom in exchange for restored access.

These methods illustrate the technical sophistication and adaptive strategies of cybercriminals, requiring a coordinated, multi-level response from national and international actors alike[19].

5- The Causes of Cybercrime in the Republic of Côte d'Ivoire

The causes of cybercrime in Côte d'Ivoire are numerous and varied, depending on the intended target of the cyber-offender. These factors can be summarized as follows:

5-1- Unstable Socio-Economic Conditions

Unemployment is considered one of the main drivers behind the commission of cybercrimes, as many perpetrators seek to achieve personal gains. The prevalence of such offenses is particularly high among young people, especially university graduates, who often innovate new techniques to carry out cybercrimes. One notable example is the practice of "broutage", a form of internet fraud involving the seduction of individuals online with the intent of extorting money from them.

5-2- Lack of Parental Supervision

The absence of parental oversight leaves children vulnerable to engaging in cyber-delinquency. The family environment plays a crucial role in a child's social upbringing; without proper guidance, minors may freely engage in illicit online activities. Numerous cases have been reported involving perpetrators aged between 13 and 20. For instance, on September 5, 2022, the Criminal Police in Abidjan were notified of the kidnapping of a 17-year-old girl. The abductor demanded a ransom of 350,000 CFA francs from her parents, sending them photos of the girl bound in an abandoned, unfinished house. He had obtained the parents' contact information from the victim's phone. Investigations led the police in Yamoussoukro to identify the suspect, known as OYS, aged 19. The victim stated that she had met her abductor on Facebook seven months prior, continuing communication via WhatsApp without ever meeting. The suspect had sent her photos of an unknown attractive man, which led to her attraction. On September 2, 2022, he invited her to Yamoussoukro for the day, promising to return with her to Abidjan. At the last moment, he claimed to be unavailable and sent a "friend" to meet her. The abductor took her to an abandoned house, where he tied her up and assaulted her under threat.

5-3- Desire for Quick Profits[20]

The virtual world has opened the door to various cybercrimes motivated by the pursuit of rapid profits. Perpetrators often send fraudulent emails to bank accounts to extract confidential data or steal credit card information. A widespread technique is the "Nigerian scam," whereby fraudsters send emails imitating those of reputable institutions such as banks or insurance companies randomly targeting multiple users. These attacks allow criminals to collect banking information, which can then be used for direct withdrawals or blackmail.

5-4- Development of the Digital and Internet Ecosystem

The capital, Abidjan, has been flooded with internet cafés, granting widespread access to the web through simple means. Unfortunately, such access is often misused, making Côte d'Ivoire particularly vulnerable to cyber-attacks. The number of cyber-related offenses is significantly higher in this region compared to other parts of the country.

5-5- Weak Legal Framework for ICT Regulation

Traditional legal systems often struggle to prosecute cybercrime effectively, due to the complexity and elusiveness of these offenses[21]. Many crimes are committed through computers and executed rapidly, making evidence collection difficult. The absence of updated legal provisions aligned with technological developments exacerbates the problem. In this regard, Mr. Vladimir Aman has highlighted several contributing factors:

- The negative influence of more experienced cybercriminals who operate covertly, using third parties or false identities.
- The appeal of high profits with low risks; once the crime is committed and the profit is made, the perpetrator deletes all traces of incriminating evidence.
- The impact of urban and cultural models that encourage excessive online commerce involving both material and financial goods.
- The inadequacy of existing legal frameworks to meet the demands imposed by evolving information and communication technologies and cybercrime patterns.

In summary, cybercrime in Côte d'Ivoire poses several significant challenges. Firstly, it tarnishes the country's international image and the reputation of Ivorian nationals abroad. Secondly, it creates economic hardships, as Ivorian entrepreneurs and businesses become victims of these shameful acts, impeding their ability to benefit from digital opportunities in dealings with foreign partners. Thirdly, it presents a major educational issue, as most cyber offenders are alarmingly young

6- Mechanisms Adopted in Côte d'Ivoire to Combat Cybercrime

In general, the African continent lags behind in adopting the evolving legal frameworks necessary to effectively prosecute and combat cybercrime. In the specific case of Côte d'Ivoire, three main legal texts constitute the theoretical foundation for addressing such offenses:

6-1- Law No. 2013-450 of June 19, 2013

on electronic transactions, establishes a legal framework for protecting personal data and preventing cybercrime. It governs:

The applicable legal regime for personal data processing, particularly regarding declarations and authorizations (Articles 5–13).

The principles of lawfulness, transparency, and confidentiality in processing data.

Individual rights such as access, opposition, rectification, or deletion of personal data.

Criminal sanctions for controllers who violate the law (Articles 14–25) (Loi n°2013-450, 2013).

6-2- Law No. 2013-451

on combating cybercrime aims to protect information systems and automated data processing. It penalizes:

Unauthorized access or fraudulent intrusion into protected computer systems.

Disruption of the integrity of information systems.

Fraudulent input or alteration of digital data (Law n°2013-451, 2013).

6-3- Law No. 2013-546 of July 30, 2013

also on electronic transactions, includes:

Mandatory disclosure of identity by online vendors.

Regulation of online advertising and publication, with mandatory transparency of advertiser identity.

Requirement of prior consent for electronic actions such as SMS or direct outreach.

Penalties including one to five years of imprisonment and fines ranging from 1 to 10 million CFA francs.

Legal recognition of electronic signatures and secure electronic messaging.

Encryption of messages to preserve communication confidentiality (Loi n°2013-546, 2013).

Given the growing threat of cybercrime and limited state capacity, Ivorian authorities have reinforced punitive measures. On September 8, 2021, the Council of Ministers adopted a draft amendment to Articles 17, 33, 58, 60, 62, and 66 of Law No. 2013-451 to enhance deterrence. These articles address:

Article 17: child exploitation and trafficking.

Article 33: violations of intellectual property.

Article 58: dissemination of obscene content.

Article 60: insult and defamation via information systems.

Article 62: threats and invasion of privacy.

Article 66: attacks against personal property through digital means[22].

7- Institutional mechanisms have also been implemented

7-1 CI-CERT (Côte d'Ivoire Computer Emergency Response Team)

a national unit for incident prevention and response.

7-2- DITT (Direction de l'Informatique et des Traces Technologiques

a technical division of the National Police providing digital forensics support.

7-3- PLCC (Plateforme de Lutte Contre la Cybercriminalité)

a partnership between the National Police (DGPN) and ARTCI, composed of police officers and civilian experts. It processes around 4,500–5,000 complaints annually, with a 50% resolution rate. It also regulates telecom services and contributes to legal drafting on cybercrime and data protection. Since July 2021, multiple offenders have been prosecuted, particularly for:

- Violating human dignity.
- Online fraud and identity theft.
- Defamation and damage to reputation.
- Electronic scams .

More broadly, the African continent must develop a robust cybersecurity culture and coherent national strategies. Given the borderless nature of cybercrime, international cooperation is essential. For instance, a hacker in South Korea can target victims in Côte d'Ivoire, requiring multilateral responses[23]

To this end, Côte d'Ivoire ratified the Budapest Convention on Cybercrime in March 2019, aligning its national legal framework with international standards and enabling cross-border[24].

8. CONCLUSION

In conclusion, cybercrime constitutes a pressing and complex issue that requires in-depth and specialized legal and technical studies. Addressing such crimes necessitates both substantial resources and expertise in information systems and digital forensics. Consequently, it is imperative to examine the most recent legal and technical developments adopted by advanced countries in this domain[25]

The occurrence of cybercrimes is inherently linked to the rapid pace of technological innovation, particularly in the fields of information and communication technologies. As cybercriminals employ increasingly sophisticated techniques to conceal their actions and eliminate digital evidence, traditional evidentiary mechanisms such as confessions and witness testimonies often prove inadequate..

Therefore, it is essential to retrain judicial police officers and criminal investigators in methods compatible with emerging digital crime trends.

Based on these findings, the following recommendations are proposed:

- Establish a unified legal definition of cybercrime that encompasses all relevant criminal behaviors and digital misconduct[26]
- Adopt and adapt the best practices of technologically advanced nations to enhance domestic capabilities in combating cybercrime
- Create a specialized law enforcement unit dedicated to investigating cybercrimes, equipped with qualified technical experts and forensic analysts.
- Rethink traditional notions of territorial jurisdiction, without compromising national sovereignty, recognizing the transnational nature of many cyber-offenses.
- Harmonize international legal frameworks addressing cybercrime, given that certain acts may be criminalized in one country but not in another.
- Develop an international registry of cybercriminals to assist in cross-border investigations and prosecution efforts.
- Strengthen global cooperation by facilitating the exchange of information, evidence, and relevant documentation between countries and law enforcement agencies.
- Improve investigative techniques by locating offenders, conducting joint investigations, and utilizing advanced digital tools.
- Enhance foundational training in computing and Internet use for cybercrime investigators in coordination with specialized institutes.
- Improve the English language proficiency of investigators through targeted training programs, given the dominance of English in technical documentation and international cooperation.
- Formulate a national cybercrime strategy aimed at increasing public awareness and safeguarding the integrity of national IT infrastructure.

- Continue enacting substantive legislation that addresses emerging forms of cybercrime using technology-neutral language, ensuring compatibility with future developments in ICT.
- Ensure that new laws reflect technical realities, fulfill investigative needs, respect international sovereignty, and uphold human rights, privacy, and civil liberties.
- Foster effective collaboration among national security agencies and both public and private stakeholders involved in digital investigations.
- Develop a practical manual for handling cybercrime cases and processing digital forensic evidence.
- Introduce a structured career progression framework for cybercrime investigators, including performance-based incentives.

9. Endnotes

[1]-Yourmeche. Mourad, The legal Nature of cybercrime, publication date 2025, journal of legal Studies and Researches, vol n:10,June 2025, p 38.
[2]- Official Page of the Cybercrime Fighting Platform in Côte d'Ivoire (2022). Article published on 10/10/2022, accessed on 21/11/2024
[3]- Cybercrime as a New Form of Struggle in Côte d'Ivoire. Article published on Academia.edu. Accessed on November 24, 2024
[4]- Al-Zoubi, Jalal Mohammad & Al-Manassa, Osama Mohammad (2013). Jara'im Taqniyat Nuzum al-Malumat al-Iliktruniya [Crimes of Information Systems Technology], 1st ed., 4th issue, Dar Al-Thaqafa, Amman.. p322
[5]- Al-Husseini, Omar Al-Farouq (1995). Al-Mushkilat al-Hamma fi al-Jara'im al-Mutasila bi al-Hasib al-Ali [Important Issues in Computer-Related Crimes], Dar Al-Nahda Al-Arabia, Cairo.p 111.
[6] - Abd El Nour Baadji, Nassima Malek, "Cyberterrorism between the Globalization of Crime and the Necessity of Combatting It, publication date 2022, journal of legal Studies and Researches, vol n:07,June 2022, p 72.
[7]- Ibrahim Khaled Mamdouh (2009). Al-Jara'im al-Ma'lumatia [Information Crimes], 1st ed., Dar Al-Fikr Al-Jami'i, Alexandria. P 55.
[8] - Salama, Mohammed Abdullah (2007). Mawsu'at Jara'im al-Ma'lumat [Encyclopedia of Cybercrimes], Al-Maktab Al-Arabi Al-Hadith, Alexandria. P 130.
[9]-AQatawneh (2010). Al-Ijra'at al-Jina'iyya al-Khassa fi al-Jara'im al-Ma'lumatia [Special Criminal Procedures in Cybercrimes], Research for Jordanian Legal

Network bdullah Daghsh Al-Ajmi (2014). Al-Mushkilat al-Amaliyya wal Qanuniya lil-Jara'im al-Iliktruniya: Dirasah Muqarana [Practical and Legal Problems of Cybercrimes: Comparative Study], Master's Thesis, Public Law, Middle East University.p 118.

[10]- Bougi, J.-J. (n.d.). Cybercrime: A Threat to Development. Internet Scams in Côte d'Ivoire. ICT in Africa, p. 160. Accessed on November 26, 2024.

[11] -Roumi, Mohammed Amin (2003). Jara'im al-Kombiyouter wal Internet [Computer and Internet Crimes], Dar Al-Matbou'at Al-Jami'iyya, Alexandria. P 35

[12]-Al-Kandari, Abdullah (2013). Al-Jara'im al-Iliktruniya fi al-Tashri' al-Kuwaiti [Cybercrimes in Kuwaiti Legislation], Al-Anbaa Newspaper, 22 July 2013. Available at: www.alalnba.kw.

[13]- Boukarnaoui, H., & Attouche, H. (n.d.). Nation Branding: A Pathway to Improve the Reputation of Countries. International Researcher Journal, Vol. 2, No. 3, p. 1958. Accessed on marsh 22, 2025.p 223.

[14]- Qoura, Na'ila Adel (2012). Jara'im al-Hasib al-Ali al-Iqtisadiyya [Economic Computer Crimes], 1st ed., Halabi Legal Publications, Beirut. P115.

[15]-Al-Motardi, Miftah Bou Baker (2012). Al-Jarima al-Iliktruniya [Cybercrime], Paper presented at the 3rd Conference of Presidents of Supreme Courts in Arab Countries, Sudan, September 2012.p 135.

[16]-. Al-Junayhi, Mohammed Mounir (2005). Borotokulat wa Qawanin al-Internet [Internet Protocols and Laws], 1st ed., Dar Al-Fikr Al-Jami'i, Alexandria. P 120.

[17]- Mohammed Zayed (2016). Al-Jarima al-Iliktruniya [Cybercrime], Symposium of the Arab League Digital Center, Tunisia, 05 March 2016.

[18]- Koffi Hamanys Brous De Ismael. (2022). Strategy to Combat Cybercrime in Côte d'Ivoire. PhD in Communication Sciences, Peleforo Gon Coulibaly University, Korhogo. International Researcher Journal, Vol. 3, No. 2, May.

[19]- Kaid, Osama Abdullah (1999). Al-Himaya al-Jina'iyya lil-Hayat al-Khassa wa Bunuk al-Ma'lumat [Criminal Protection of Privacy and Databases], Dar Al-Nahda Al-Arabia, Cairo.p 30.

[20]-Abdullah Abdullah Abdul Karim (2011). Jara'im al-Ma'lumat wal Internet [Information and Internet Crimes], 1st ed., Halabi Legal Publications, Beirut

[21] - Law No. 2013-450 of June 19, 2013, on electronic transactions in Côte d'Ivoire.

[22]- Law No. 2013-451 of June 19, 2013, on combating cybercrime in Côte d'Ivoire.

[23]- Allechi, D. (2021). Opportunity to Revise Certain Articles of the Ivorian Law on Cybercrime. Retrieved from www.village-justice.com

[24]- Benabid, A. (2022). Cybercrime: What Are the Challenges and What Prospects? (Comparative Law: Morocco, France, and Canada). Undergraduate thesis in French Law.

[25]- Douzet, F. (2016). Cyberspace: A Major Geopolitical Issue. La Revue des Médias. Retrieved from https://larevuedesmédias.ina.fr/lecyberespace-un-enjeu-majeur-de-geopolitique. Accessed on November 20, 2022.

[26] - Affagnion, G. (2012/2022). Cybercrime in Benin: Threats, Legal Gaps, and Power Dynamics. Affagnon Review.