The Sankalpa: International Journal of Management Decisions
ISSN: 2454-7425
Volume 12, Issue 1 (January - June 2026)

Transformations in the Structure of Criminal Behaviour (Cybercrimes and the Impact of Artificial Intelligence): A Descriptive and Analytical Study

Sid Ali Moussa
University of Blida 2 – Lounici Ali
Laboratory of Crime and Deviance between Culture and Social Representations
Email : Es.moussa@univ-blida2.dz

Received: 20/01/2026 Accepted: 27/02/2026 Published: 04/05/2026

Abstract :
This research paper presents a descriptive and analytical examination of the phenomenon of cybercrimes as an emerging social issue in the context of the use of artificial intelligence. The study is based on the descriptive and analytical approach applied to various reports and relevant sociological literature. The findings confirm that artificial intelligence contributes to changing the identity and structure of criminal behaviour and multiplies its social risks for individuals and institutions. This calls for the use of preventive methods based on more advanced technical or legal approaches to combat these risks .
Keywords: Cybercrimes, Artificial Intelligence, Criminal Behaviour, Social Risks, Prevention.

Introduction:

In today's contemporary world, digital transformation has become an inevitable necessity brought about by accumulated and rapid social changes. There is no longer any area of human society free from the use of technology to save time, reduce effort or cost – whether in daily life, work, study, and so on. Nor is this recourse to technology reserved solely for individuals or personal use; even major institutions, regardless of their activity or field, whether governmental or private, have also come to employ these technical tools to benefit from their many advantages. These include, for example, the digitisation of services to reduce burdens, effort, and save time, etc.

Despite the positive effects technology has had on human life in terms of information exchange and speed of communication, this digital environment has also seen the emergence of hidden, cross-border digital social afflictions. Cybercrimes, for instance, are today at the forefront of every country's concerns and fears. These crimes, which rely primarily on electronic platforms or websites for their execution, have posed an extremely high-level challenge: the need to adapt and develop legislative, legal, and security methods to confront this type of crime. These methods must keep pace with digital transformation, which, as much as it is a means of development, is also a danger that opens a digital gateway to organised cybercrime.

Algeria, like other countries, is not exempt from the danger of cybercrime. Almost daily, we read news about money being embezzled from individuals' financial accounts who have been deceived by criminals (identity theft) using electronic devices and websites. These devices and

websites have become highly sophisticated with the artificial intelligence revolution. This has led official state institutions to issue warnings and alerts on many occasions about the danger of falling victim to this type of electronic crime, as well as other crimes such as electronic blackmail, defamation, and online harassment.

Among the issues and problems raised by digital change and the artificial intelligence revolution in our current societies is the change in patterns of criminal behaviour, which has come to rely on electronic technical means that are difficult to trace and hold to account. Hence, this research paper serves as a descriptive and analytical study, seeking to answer the question:

To what extent has artificial intelligence contributed to the development of cybercrime as a social phenomenon, and how has this affected mechanisms of social control in contemporary societies?

The following sub-questions fall under this main question:

- What exactly are these crimes supported by artificial intelligence techniques?
- How have artificial intelligence techniques changed the structure of criminal behaviour?
- What are the counter-mechanisms that can combat cybercrime?

2. Conceptual and Theoretical Framework:

2.1 Key Concepts:

- **Cybercrime:**

This term is non-Arabic in origin, derived from the foreign phrase 'cybercrime'. In procedural terms, it refers to everything related to technology, informatics, and the world of communications. The term is linked to electronic security and has also become associated with academic scientific specialisations and branches now taught in some universities worldwide.

Cybercrime is defined as those crimes that use technology as a means or tool, such as a computer, for information fraud. They are crimes committed technically with a high level of precision and camouflage. In general, there is no unified definition of this type of crime given the dynamic development of information crime. However, there is agreement that these crimes use technology, especially artificial intelligence tools. This is a new pattern of crime that threatens information security in all countries, whether for individuals or institutions.

In another definition, electronic crime is defined as 'any negative or positive behaviour by which an attack is made on software or information in order to benefit from it in any form whatsoever'. Computer crimes can also be defined as 'technical crimes that arise in secret, committed by intelligent criminals possessing tools of technical knowledge, aimed at undermining the right to information, with their attacks targeting stored computer data and information transmitted through information systems and networks'.

- **Artificial Intelligence:**

No unified definition of this term has yet been agreed upon. However, artificial intelligence can be defined as 'those systems capable – using technology – of making various decisions

through self-control, generating specific content, predicting, and even providing recommendations and guidance'.

From this definition, it becomes clear that the use of artificial intelligence in committing cybercrime is also closely linked to technology. These are pre-eminently technical crimes that rely on intelligence and the speed of data linkage to achieve their goal. This may surpass human intelligence in some situations, making an individual or institution vulnerable to electronic fraud.

- **Cybersecurity:**

In the age of development and technology, societies – both individuals and institutions – have become deeply and profoundly linked to information networks due to their need to maximise the benefits and facilities these networks offer for managing various tasks effectively across different fields and specialisations, whether educational, professional, personal, etc. This means these networks collect, process, and store a vast amount of user data (digital information). The problem of protecting this data arises as a fundamental issue, as it is an integral part of any society's national security.

On this basis, cybersecurity is defined as 'the continuous effort to protect those networks and data from unauthorised use, which can cause harm either on a personal or public level. Hence, the need to protect this data and information (identity, computer data, etc.) becomes paramount, as user safety and national security may be threatened by hacking and unauthorised use'.

Cybersecurity can also be defined as 'a set of technical and organisational measures aimed at protecting systems, networks, and data from cyberattacks. This includes the use of protection systems, data encryption, and the application of appropriate security policies to ensure the confidentiality and integrity of information'.

- **Digital Space:**

Digital space is defined as 'the domain created within the computer environment and information network using software. This concept is not fixed in terms of the definitions addressed to it, and sometimes the meaning depends on the context in which it is used. Generally, it can be said that digital space is an electronic environment, area, or space, used by people, containing digital resources, where communication takes place electronically'.

3. Sociological Approaches Explaining the Phenomenon:

Through these theories, we will show how these approaches explain the phenomenon of cybercrime in light of the artificial intelligence revolution, by projecting the concepts and terms of each theory in a procedural and applied manner based on certain evidence and examples from social reality.

3.1 Crime Opportunity Theory:

Opportunity theory is among the most prominent theories explaining criminal acts. Although the theory emerged in the 1970s through researchers Marcus Felson and Lawrence Cohen (1979), it remains capable of explaining digital crime in our current era. The justification for this is that it is a theory carrying social principles and postulates that enable it to simulate social changes consistent with any contemporary temporal context. Its validity can be justified by its

being a renewed theory in its explanation of the criminal act, moving away from classical explanations of crime based on the premise of 'why does the criminal commit the criminal act?' Instead, the theory shifts the angle of study and research in attempting to understand the nature of criminal behaviour to the question: 'How can circumstances contribute to creating the opportunity to commit a crime?' More precisely, the theory relies on studying and researching the nature of the surrounding circumstances and the victim's routine activity before the behaviour is committed. Criminal behaviour here is achieved when three essential elements are present: the motivated offender, the target (victim), and the absence of protection. From this, we note that opportunity theory – also called rational choice theory or routine activity theory – depends on rational choices that balance cost and profit and the potential risks arising from them.

From the above, it can be said that crime opportunity theory is well suited to explaining the phenomenon of cybercrime, through the interrelationship between the principles on which the theory bases its explanation of crime and the elements of crime in cyberspace (motivated offender, target, absence of protection). The motivated offender is the criminal who is cunning and possesses the skill and tools in digital space (hackers) to trap the victim. The target is the user's sensitive data (bank account, insufficiently protected servers). The absence of protection corresponds in the field of cybercrime to weak security software, lack of encryption, or even the user's weak technical security awareness in digital space. An example of this type of crime in our Algerian society is seen in crimes where victims are people holding electronic cards linked to postal accounts (the gold card). Many people, especially the elderly who lack digital awareness of the dangers of disclosing this type of data through channels such as social media sites (e.g., Facebook), frequently fall victim to this type of crime.

3.2 Social Learning Theory in the Digital Environment:

Learning theory, pioneered by Albert Bandura, is one of the key theories through which the process of acquiring criminal behaviour can be explained. This occurs through stages beginning with the individual observing the behaviour, then imitating it, followed by the reinforcement stage within the social environment. However, what concerns us here is not learning theory and its classical explanation of how behaviour transfers from mere observation to action, but rather how this theory explains crime in its digital (technological) dimension – by which we mean cybercrime.

In learning theory, observation of criminal behaviour often takes place within its classical social framework, such as the social environment, peer groups, television, etc. This constitutes a difference when this theory explains the mechanism by which criminal behaviour transfers from watching digital models on the internet (digital networks, videos, etc.). These videos might depict, for example, fraud operations, hacking methods, or the provision of information. From there, the learning of criminal behaviour from the perspective of learning theory occurs through indirect contact, which multiplies curiosity to imitate. This is because these digital models (films, for instance) influence individuals' perceptions by portraying hackers as inspiring or successful people who achieve quick profits without cost, effort, or risk, in addition

to the esteem they gain in their communities. This is where the reinforcement stage and the consolidation of adopting criminal behaviour occur.

It is also necessary to point out that artificial intelligence's contribution to learning theory has a profound impact on the spread of this type of crime in our digital age (cybercrime). It does so by providing these criminals with ideas and plans that have accelerated the execution process, saved time, and reduced cost and risk, as previously mentioned. Artificial intelligence's contribution has accelerated the learning process through explaining plans, creating tools (via programming), lowering required skill levels (even beginners pose a danger), generating fraudulent messages (deepfakes), and enabling self-learning.

4. The Reality of Crime in Postmodern Societies:

International societies are witnessing rapid and qualitative changes affecting all aspects of life. Perhaps the most prominent manifestation of this change is the transition from a simple lifestyle to a complex lifestyle controlled by technology, which has imposed a digital character on human communication that has, over time, become an integral part of individuals' daily lives. At a time when some voices celebrated the positive side of this transformation and its positive effects on the individual and society, it has become clear over time that this development carries with it extremely serious, unpredictable threats to individuals and institutions. The negative use of information technology has led to the emergence of a new pattern of cross-border criminal behaviour, unconstrained by any specific geographical or temporal field. This new pattern of criminal behaviour takes cyberspace as a fertile environment for trapping victims – a pre-eminently technical crime called cybercrime. It can be said that cybercrime has redefined the identity of crime in the age of technology, necessitating a re-examination of its forms, effects, and even its definition.

Globally, according to reports issued by the US Federal Bureau of Investigation for 2020, statistics reported amounts exceeding $4.2 billion in losses resulting solely from electronic fraud and scams. These figures reflect the degree of danger characterising cybercrime, which threatens individuals and institutions alike. They also express the rapid growth of this phenomenon, especially with the artificial intelligence revolution, which over time will make even a beginner a professional thief. At the local level in Algeria, some studies indicate that 34% of economic institutions have previously been subjected to cyberattacks.

In light of these facts, it is abundantly clear that the world today faces a wave of new criminal threats, which can be described as 'among the most complex issues, as they are committed using the most advanced technical methods, differing from traditional technical crimes, and are characterised by their continuous change and development and the expanding scope of their impact'.

4.1 Forms of Cybercrime Linked to Artificial Intelligence:

The classification of cybercrime varies, as there is no agreed, unified classification. This is due to differences in the degree of development from one society to another. Before discussing some forms of cybercrime, it is necessary to point out that the cybercriminal has distinguishing characteristics that make him a completely different criminal from the traditional one, whether

in terms of the tools each uses in the criminal act or even the method of targeting the victim. The cybercriminal is a pre-eminently technical criminal, as he employs specific techniques to help him circumvent information systems to breach the firewall. From this simple definition, we can proceed to explain some types of cybercrime related to the use of artificial intelligence:

- **Crimes affecting systems and information security:** These are crimes aimed at destroying or accessing private or sensitive data through unauthorised entry. It can also be said that these are crimes that seek to threaten data integrity, whether data belonging to individuals or institutions, etc.
- **Crimes targeting the computer:** This type of crime aims at pure technical destruction of infrastructure, in order to steal data. Among the methods used is the dissemination of malicious types of viruses and software (ransomware) – a type of virus that encrypts files and then demands sums of money to decrypt them – or, for example, denial-of-service (DDoS) attacks. Also among the examples of these crimes is hacking, which, as mentioned above, is unauthorised entry seeking espionage or the theft of information and data.
- **Crimes depending on the type of content:** This type of crime relies on content published on websites. Among its well-known tools is pornographic content that focuses on the immoral aspect. It can be said that this crime falls within the scope of electronic blackmail crimes by threatening individuals with immoral private photos or videos – something we often hear about.
- **Crimes concerning money or people:** These are hacking crimes, specialising in fraud, embezzlement, document forgery, and attempts to access individuals' data. Their tools also include spreading false, misleading news and rumours, violating others' privacy, and using information immorally to serve interests, among others.

This classification represents the forms of cybercrime in general, which national and international efforts have sought to establish as a reliable division when discussing cybercrime and attempting to tighten the net on it and reduce its destructive effects. From the above, what can be confirmed is that artificial intelligence has significantly contributed to changing the structure and identity of criminal behaviour in the age of artificial intelligence – a very advanced stage of technological development in the modern era.

The impact of artificial intelligence on cybercrime has not only changed the structure of criminal behaviour in terms of methods of commission but has also changed the nature of the effort expended by the criminal to achieve his goals. It has moved the criminal from mere physical behaviour relying on strength and human intelligence to technical effort relying on technology and complex algorithms characterised by targeting precision, difficulty of tracking, a daily expanding number of victims, and shortcomings in legal legislation. These tools, which humans once thought were directed towards production and addition, have in our current era become tools that are, to say the least, extremely dangerous, as they excel at forgery, social engineering, the use of malicious software, complex algorithms, etc.

5. Cybercrime and Its Impact on Social Security:

Regardless of its form – whether traditional or new – crime has a qualitative impact on the individual and society. This impact has social, psychological, security, economic, institutional, and familial repercussions.

- **Social and psychological impact on family stability:** This aspect affects the material stability of the family. For example, if a family member

(the breadwinner) is subjected to electronic fraud, this may lead to the loss of the family's savings. Such incidents can give rise to tensions and family disputes with economic dimensions, negatively affecting the psychological aspect. Perhaps the most prominent incidents in this field also include the crime of honour-related electronic blackmail, which can escalate to family crimes, even murder. Thus, electronic crimes have a social and psychological dimension that may negatively affect family structures in general.

- **Impact on the security and economy of institutions:** According to statistics from 2021, an increase was recorded in the number of people who were

victims of electronic fraud through online shopping, causing damage valued at 1.5 billion Algerian dinars (equivalent to $11 million USD). In the same year, other reports also showed statistics issued by the National Centre for Cybersecurity indicating that 70% of citizens feel that government institutions are unable to protect their data. This is clearly reflected, in their view, in their caution and anxiety when dealing digitally with government institutions.

Collectively, these crimes, in addition to crimes that may extend to other fields, can sometimes lead to a shaking of trust between individuals and government institutions when we speak of crime in its macro-sociological dimension, regardless of its specialisation (especially economic and financial). This reflects negatively on the reputation, activity, and economy of these institutions over time, in addition to its effect and reflection on the individual (micro-sociological). Regardless of the level of this impact, threat, and reach that characterises cybercrime, caution must be exercised and the matter taken seriously – internationally, regionally, and nationally. Human society today faces a danger of the highest level, among whose characteristics is that it is cross-border and self-developing (artificial intelligence). Therefore, everyone's efforts must be combined as an international responsibility to combat and reduce the seriousness of the situation in a manner that ensures the safety of bodies and users.

6. Mechanisms for Combating and Preventing Cybercrime in the Age of Artificial Intelligence:

The international and national (Algerian) community is making great efforts to find ways to achieve and ensure adequate protection from the dangers of cybercrime. Despite these dangers being highlighted and warned against, the efforts made have not been able to contain these risks for several reasons, perhaps the most prominent being the rapid development of hacking, scamming, and fraud techniques, which have come to rely heavily on artificial intelligence tools. This has caused the danger to increase and the number of victims to multiply. Today's initiatives to combat cybercrime stand between a complex war (intelligence vs intelligence).

Therefore, it is very difficult for traditional methods of confrontation to have the ability to deter these threats.

Hence, through what has been discussed, we have chosen to point to a number of proposals that could reduce the seriousness of cybercrime, including:

- **Education and awareness:** Through awareness campaigns organised in the form of workshops and training courses, whose subject matter involves

teaching individuals the principles and fundamentals that can help them protect themselves from deceptions (suspicious links or calls) that could put their personal data at risk.

- **Encouraging individuals to use protection programmes to achieve personal security:** (installing them on computers), and alerting them to carry out

necessary updates to these programmes in a timely manner, so they can protect themselves from the cyber risks that surround them.

- **Ensuring the security of institutions:** Conducting training courses for employees on cybersecurity, and ensuring the use of security software to close

security gaps to protect data and individuals' lives.

- **Establishing partnerships between sectors (public and private):** This benefits institutions through cooperation and coordination of efforts that can

contribute to developing strategies to confront and deter electronic crime (exchanging information and expertise).

- **The legal aspect:** Traditional laws for combating crime are no longer reliable in confronting electronic crime. Therefore, legislative authorities must

seek to adapt laws that suit the nature or structure of crime in the current age. Perhaps among the important chapters in this regard is allocating a specific section of laws to punish any act or behaviour that uses technology to violate users' data.

- **Improving verification and tracking methods:** Perhaps among the most prominent characteristics of cybercrime is that it is a cross-border crime, and

its traces are difficult to follow in a world characterised by complexity and the ability to disguise (IP addresses). Therefore, care must be taken to train security personnel in the use of tracking and investigation tools so they can uncover the identity and location of the cybercriminal.

7. Findings of the Study:

This research paper came to address the subject of cybercrime and whether artificial intelligence has affected the structure of criminal behaviour in general. Through the readings presented, discussed, analysed, and researched in an attempt to answer this question, it has been concluded that the structure of criminal behaviour has indeed changed. As shown in the sociological approaches, the criminal in the modern era has come to rely in his behaviour on the principle of assessing losses and profits. Technology and the internet have not only changed the structure of criminal behaviour but have also made the cybercriminal more intelligent, more precise in targeting the victim, and less wasteful in committing the crime. What has further changed the identity of criminal behaviour is the artificial intelligence revolution, which has

become a source of support in terms of information, ideas, and even advanced technology. We now hear of hacking crimes, destroying programmes and websites with viruses, and electronic warfare – terms that did not exist before.

This transformation in general has left behind social-psychological, economic, and politico-security effects on societies and governments internationally (e.g., WikiLeaks). The principle has become that everyone is targeted and threatened without exception, which has pushed countries towards coordination and cooperation to combine everyone's efforts in an attempt to reduce the danger and coordinate to find solutions and close gaps. What has further complicated the mission is the artificial intelligence revolution, which has reduced the burdens on cybercriminals. Methods have evolved, the target has become more visible, and traditional laws do not suit the nature of (criminal) behaviour. This places the international community before a particular challenge that can be described as a war of intelligence versus intelligence.

References

1. Al-Dosouqi, T. I. (2008). *Information security (technical, legislative and criminal aspects)*. Alexandria, Egypt: New University House.
2. Al-Roumi, M. A. (2003). *Crimes against computers and the internet*. Alexandria: University Publications House.
3. Al-Sahafi, R. bint A. A. (2020). Cybercrimes. *The Comprehensive Multidisciplinary Electronic Journal, (24)*. Jeddah, Saudi Arabia.
4. Arab Administrative Development Organization. (n.d.). *The impact of electronic crimes on Arab individuals and societies* [Statistical report].
5. Boudiar, A., & Tabbal, R. (2024). *Cybercrime and its effects on the individual and society in the age of technology*. Journal of Human and Social Sciences Researcher, 16(1). University of 20 August 1955 Skikda, Algeria.
6. Djerboua, N. (2021). *Electronic crime and its impact on social security*. Laboratory Notebooks Journal, 16(2). Algeria.
7. Jamaoui, N. (2021). *Electronic crime and its impact on social security*. Laboratory Notebooks Journal, 16(2). Algeria. (Note: Duplicate entry of Djerboua, N. – retained once as per APA uniqueness rule)
8. National Centre for Cybersecurity. (2021). *Cybersecurity report in Algeria*.
9. Raddad, A. (2024, May). *The reality of crime in the postmodern era*. Police Journal (Research and Studies), (158).
10. Saudi Authority for Data and Artificial Intelligence. (2024, April). *Artificial intelligence for executives series* (2nd ed., Vol. 1). Saudi Arabia.
11. Tashour, M. (2015, December). *Digital spaces as a foundation for reading in light of modern technologies*. Information Sciences Journal, (4). University of Constantine 2, Algeria.

Foreign references:

1. Bertino, E & .Sandhu, R .**Cybersecurity: Concepts, Challenges and Opportunities** .Computer, 43(10). 2010.
2. Thomas J. Holt, **Cybercrime and Digital Forensics an Introduction**, Routledge, USA, 2022.