

The Role of Cybersecurity in Establishing the Modernization of Criminal Justice

دور الأمن السيبراني في تكريس عصبة القضاء الجزائري

Boubaaya Abdelghani

Faculty of Law, University of Bejaia

Research Laboratory on the Effectiveness of Legal Norm

Abdelghani.boubaaya@droit.univ-bejaia.dz

Date of submission:02/04/2025 Date of final acceptance:24/07/2025 Date of publication :September

Abstract:

Modern technology is one of the key pillars supporting the idea of modernizing criminal justice due to the specificity of its tools and characteristics, aligning with efforts to improve judicial services. However, its impact on rights and freedoms has necessitated the utilization of cybersecurity mechanisms to balance the protection of these rights with the establishment of criminal justice modernization. This study aims to explore cybersecurity's contributions to the modernization of criminal justice in light of the provisions of information laws and those related to the modernization of the justice sector in Algeria.

Keywords: Cybersecurity; modernization of criminal justice; electronic data; modern technology; rights and freedoms.

ملخص:

تعد التكنولوجيا الحديثة من أهم المرتكزات الداعمة لتجسيد فكرة عصبة القضاء الجزائري لخصوصية وسائلها وخصائصها، ما يتوافق مع التوجهات الرامية لتحسين الخدمات القضائية، غير أن انعكاساتها على الحقوق والحريات استدعى تسخير آلية الأمن السيبراني للموازنة بين حماية هذه الأخيرة وتكريس فكرة العصبة الجزائرية، وتستهدف هذه الدراسة البحث في مساهماته في عصبة القضاء الجزائري، وذلك على ضوء مضامين القوانين المعلوماتية وتلك المتعلقة بعصبة قطاع العدالة في الجزائر.

الكلمات المفتاحية: الأمن السيبراني؛ عصبة القضاء الجزائري؛ المعطيات الإلكترونية؛ التكنولوجيا الحديثة؛ الحقوق والحريات.

Introduction:

Criminal justice is one of the most important components of the justice sector, as it is the body responsible for protecting property and both material and moral rights on one hand, and due to its procedural and substantive specificity on the other. Procedurally, it is characterized by procedural mechanisms that often conflict with the rights and freedoms of individuals during the exercise of its powers of prosecution and trial. Substantively, it is concerned with adjudicating cases and disputes of a criminal nature, highlighting the effective role of criminal justice in establishing the directions of criminal policy, which has been further reinforced by modern technological developments.

In this context, the nature of criminal court judgments is subjective in terms of their content; they often include criminal data that is legally protected due to its sensitivity and seriousness. With the implementation of the idea of modernizing criminal justice, the importance of protecting this information has increased due to its connections with the digital environment. The comprehensive nature of technology across various stages of litigation raises the possibility of infringing upon the digital rights and freedoms of individuals and the judicial system, necessitating a balance between protecting these rights and employing technology in the modernization of criminal justice.

Supporting this argument is the view that technology and digital judicial procedural practices may pose a threat to the integrity and sanctity of judicial data. Therefore, it is essential to link the idea of protecting this data with technology, which has called for the provision of technological mechanisms to secure and ensure judicial protection. This is embodied in the emergence of the concept of cybersecurity as a means to protect digital rights and freedoms, which fosters confidence in digital criminal justice and emphasizes procedural diversity.

Regarding the importance of the topic of cybersecurity, it is considered relatively modern, having been the subject of study by researchers and specialists in legal and technological fields. However, it has not addressed the role of cybersecurity in modernizing criminal justice, despite the issue's significant importance from both legal and technological perspectives. This study seeks to explore the role of cybersecurity in the modernization of criminal justice and to demonstrate the modern relationship between the judiciary and technology.

Through this study, we aim to illustrate the extent of the legislator's interest in establishing cybersecurity in the modernization of the justice sector in general and the criminal system in particular, as well as its implications for developing criminal policy in both its procedural and substantive aspects. We also aim to shed light on the foundations of cybersecurity and its effects on individuals' privacy, while highlighting the obstacles to effectively establishing cybersecurity.

The issue of cybersecurity within criminal justice raises numerous challenges, often stemming from the lack of a specific and independent law that adequately regulates it, in addition to some concerns centered around the effectiveness of cybersecurity in Protecting Rights and Freedoms and Establishing the Idea of Modernizing Criminal Justice.

We attempt through this study to answer the following question:

To what extent does cybersecurity contribute to the modernization of the criminal justice system?

To address this question, we have decided to divide the study into two sections: we will first clarify the nature of cybersecurity (1), and then discuss its role in establishing the idea of modernizing criminal justice (2).

To enrich this study and cover many of its aspects, we relied on the descriptive method to describe the status of cybersecurity concerning criminal justice and its implications for rights and freedoms. We also employed the inductive analytical method to explore and analyze the texts related to the study topic. Additionally, we included the deductive and comparative methods as tools for reasoning and comparison, in light of the contents of laws related to cybersecurity and the modernization of the justice sector in Algeria.

1. The Nature of Cybersecurity

The process of modernizing criminal justice relies on several pillars that contribute to its realization, among which modern technology is essential. This technology fundamentally rests on the idea of cybersecurity to ensure its effectiveness in the proper functioning of the criminal authority. Therefore, studying the topic of cybersecurity and its role in supporting the development of the criminal justice system necessitates clarifying its concept and specificity.

1.1. Concept of Cybersecurity

Criminal justice in Algerian legislation is based on several principles that support its functioning, and the principle of cybersecurity is a fundamental pillar for the modernization of the criminal justice system, as a result of the impact of modern technology on the judicial sector. In this paragraph of the study, we aim to define cybersecurity and highlight its specificity.

1.1.1. Definition of Cybersecurity

The structural and functional nature of cybersecurity makes its definition vary depending on the perspective or normative angle from which this security type is viewed. In this paragraph, we seek to clarify its meanings and multiple characteristics.

A) Meaning of Cybersecurity:

As a reflection of the relative modernity of the idea of cybersecurity, its definitions are varied and cannot be confined to a single meaning due to its characteristics and the nature of its tools, which differ among terminological, legal, and jurisprudential definitions.

- Terminological Meaning of Cybersecurity:

Security, in its general sense, refers to the feeling arising from the belief in the ability to confront all risks and control all mechanisms capable of addressing those threats, regardless of their source. It is a general and comprehensive sense of reassurance, indicating a state of lost fear and a sense of psychological and physical safety¹. The term "cyber" denotes everything related to computer culture and science or the digital virtual reality; it is derived from the Greek term "cybernetics," meaning "the internet space".²

- Legal Meaning of Cybersecurity:

Through examining the texts of the Algerian Code of Criminal Procedure and the Law on the Modernization of Justice, it becomes clear that the legislator has not included a legal definition for the mechanism of cybersecurity, merely referencing its forms and aspects. The legislator's concern for cybersecurity protection can be inferred from the provisions of articles 10/2 and 14/2 of the Law on the Modernization of the Justice Sector³, and article 441 bis/2 of Ordinance No 20-04.⁴

However, the legislator addressed the absence of a definition in the Law on the Modernization of the Justice Sector by incorporating a definition in Article 10 of Law 18-04⁵, which defines cybersecurity as: "a set of tools, policies, concepts of security, security mechanisms, guidelines, risk management methods, practices and technologies that can be used to protect electronic communications against any event that may affect the availability, integrity, or confidentiality of stored, processed or transmitted data".

In a similar vein, the legislator included definitions that contribute to understanding the concept of cybersecurity through Article 3 of Law No 18 -07⁶, clarifying the meaning of several terms, including personal data, processing of personal data, and automated processing. It also defined "information" in paragraph four of Article 3 of Law No 21 -09⁷ as: "any event or news, regardless of its source, document, image, audio or visual tape, audiovisual conversation, or telephone call, whose disclosure may affect the relevant authorities".

From this reading of the key texts related to cybersecurity, it is evident that the legislator considered the meanings of informational terms and their conceptual specificity, ensuring a qualitative formulation of the texts related to cybersecurity, avoiding ambiguity and interpretive or practical issues. This has implications for judicial practice and delineates the scope of cybersecurity protection through the establishment of legal security.

- Jurisprudential Meaning of Cybersecurity:

Cybersecurity refers to the set of measures taken to maintain the confidentiality of electronic information and prevent its breach, ensuring correct access to computing information and preventing it from being placed in an unsafe environment, especially with the acceleration of electronic communications and transactions. From another perspective, cybersecurity is a mix of both physical and non-physical technologies; the former secures programs, applications, networks, and computers, while the latter pertains to data, thus establishing protection against information breaches and controlling the correct access to devices, applications, and networks to protect them from harm arising from cyberspace, whether from states or other cyber actors.⁽⁸⁾

From our viewpoint, cybersecurity can be defined as: a branch of technological sciences based on electronic algorithms that ensure the protection of information systems from attacks that threaten the functions of technological media and the stability of the digital space. From a criminal perspective, it can be defined as: a scientific technological technique that guarantees the informational protection of data with a penal nature against informational threats affecting the privacy of digital rights and freedoms.

In conclusion, through our review of the concept of cybersecurity, we note that it does not exist in complete independence regarding the provision of cybersecurity protection; rather, it coincides with the efforts of legal and judicial security towards establishing modern mechanisms that effectively protect digital rights and freedoms and support the modernization of criminal justice.

B) Characteristics of Criminal Cybersecurity:

Like other forms of security established to ensure the proper functioning of the criminal judiciary, cybersecurity possesses numerous characteristics that distinguish it from traditional security. The connection between modernization and technology necessitated the deployment of a qualitative security that guarantees its effectiveness. This is the role assigned to cybersecurity, which serves as a modern pillar for protecting judicial rights. Among these characteristics, we mention:

- Legitimacy: This characteristic can be inferred from the content of numerous legal amendments related to the modernization of the justice sector. We refer to the texts related to ensuring the necessary protection for various judicial data, which aim at effectively employing technology in various judicial procedures. Including such texts gives both the criminal judge and litigants confidence in electronic criminal justice and enables them to benefit from electronic judicial administrative services.

Furthermore, conferring legitimacy on the concept of cybersecurity bolsters the confidence of litigants and those visiting the judiciary by alleviating fears arising from the potential inadequacy of information security, as well as the risks associated with the use of technology, thereby imparting legitimacy and protection to it. This characteristic thus establishes procedural reliability, allowing electronic criminal procedures to be conducted with full confidence.

- Compulsory (Necessity): Providing cybersecurity within the judiciary is not optional, nor is it a reserve or exception; rather, its presence is inherent and essential for all technological judicial procedures. Its absence exposes litigants' and the judiciary's data to danger, threatens digital rights and freedoms, or renders procedures liable to annulment. Moreover, its loss incurs legal responsibility if it harms rights and freedoms or undermines the sovereignty and dignity of the criminal judiciary.

Based on this, this obligation does not only involve providing cybersecurity; it must also produce its existential effects, meaning it must effectively guarantee the technical protection of all electronically circulated data within the judicial system. The legislator has mandated the necessity

of cybersecurity protection through Article 3 of the Law on the Modernization of the Justice Sector, as well as in Article 441 bis of Ordinance 20-04.

- **Digital (Technological):** Cybersecurity is distinguished from legal or judicial security as it fundamentally relies on digital means, such as the use of technological programs and applications. Additionally, the nature of the training and professionalism of those responsible for ensuring cybersecurity plays a role. Practically, this characteristic can be illustrated by the security measures in place.

The electronic criminal procedures utilizing technological media include protecting electronic evidence, electronic signatures, and various electronic documents issued by the criminal judiciary.

- **Preventive:** This characteristic expresses the purpose and goal of cybersecurity, reflecting the use of technology in modernizing the criminal judiciary. The potential for diminishing rights and freedoms is present; thus, it aims to secure all judicial data from any attacks, whether they result from negligent acts by information employees or from those committed by electronic crime professionals. The nature of technological means necessitates the provision of a qualitative security that corresponds to the scale of threats. It also establishes protection for electronic public prosecution procedures and contributes to ensuring guarantees for fair trial rights.

- **Continuity:** Given the ongoing development of modern technology, the assumption of reliance on it as a means of judicial modernization is increasing, which is reflected in the magnitude of potential technological threats. This automatically necessitates the continuity of cybersecurity to face all potential threats against digital rights and freedoms through the modernization of cybersecurity by harnessing effective cyber mechanisms and expanding the scope of criminalization and punishment for acts that undermine judicial cybersecurity.

1.1.2. The Specificity of Criminal Cybersecurity

Alongside the legislator's interest in establishing cybersecurity protections for rights and freedoms within the justice sector in general, this preventive cyber role has been enhanced more broadly within the criminal judicial system. This is justified by its nature and specific specialization, alongside the nature of the rulings and services arising from this judicial facility, in comparison to civil and administrative bodies. This grants specificity to criminal cybersecurity on one hand and distinguishes it from legal and judicial security on the other.

A) Goal-Oriented Specificity:

Cybersecurity aims to maintain the privacy of criminal data and information, whether that which is exchanged during the exercise of electronic criminal litigation procedures or that which is archived and stored in electronic media. These are considered secrets for individuals that must be protected and not disclosed illegally or exposed to informational crime, thereby reinforcing the preservation of digital rights and freedoms, particularly ensuring the protection of personal life and dignity, especially for those convicted, as well as the confidentiality of their information and criminal records.

Cybersecurity's role is further enhanced within the criminal facility, distinguishing it goal-wise from other legal and judicial security forms. The specialization in criminal justice contributes to the distinctiveness and specificity of cybersecurity, especially at certain criminal bodies (such as military courts, juvenile courts, and national and regional criminal poles), which requires a qualitative cyber protection that effectively prevents and combats cybercrime in a manner consistent with the scale of challenges and technological risks these criminal bodies may face.

B) Mechanism-Specificity:

There is no doubt that cybersecurity possesses specificity in terms of the mechanisms deployed to establish it. It fundamentally relies on technological and digital means, supported by programs and applications managed and operated by experts in the field of informatics or through artificial intelligence technologies. These are foundational elements that require digital prerequisites. The digital nature of cybersecurity necessitated the availability of mechanisms of its

kind to ensure its effectiveness, along with the nature of open-source threats in the digital space and electronic transactions.

From our perspective, we can say that all these indicators and the specific goal-oriented and procedural significances, along with the fundamental differentiation from legal and judicial security, reflect the role of cybersecurity at the level of the criminal judiciary concerning achieving service-oriented goals and procedural judicial practices and embodying the legislative intent directed toward the modernization of the justice sector across its various facilities.

1.2. Requirements of Criminal Cybersecurity

To ensure effective electronic performance and guarantee the effectiveness of cybersecurity, numerous requirements must be met to establish reliable protection for judicial data and achieve the objectives for which this qualitative security model is designed. We attempt to review the most important means and prominent forms of protection it provides.

1.2.1. Means of Criminal Cybersecurity

Securing cyberspace has become a strategy pursued by countries to keep pace with their technological development and reflects their advancement. This is evident in the nature of the means deployed to ensure it. Cybersecurity is considered a strategy and a criterion for securing and modernizing various institutions and facilities of states, including those supporting the establishment of criminal justice, by securing the criminal judicial system to ensure its effectiveness. This requires the integration of various means represented in:

A) Legal Means:

Despite the clear importance and contribution of technology to actualizing and enhancing criminal modernization services, some of its repercussions may potentially detract from rights and freedoms. This necessitates accompanying it with cybersecurity. In accordance with the principle of legality, it is essential to utilize the latter based on laws that include the legitimacy of its use. The law (both procedural and substantive) serves as a fundamental means to keep pace with judicial modernization, starting from its elucidation of cyber terminological concepts.

By virtue of which, administrative and judicial bodies overseeing cybersecurity supervision and effectiveness are established. It also refers to criminal and civil procedures aimed at its protection, thereby cementing legal stability and security.

From another perspective, it contributes to enlightening and guiding the criminal judiciary, advising judges to benefit from laws related to cybersecurity to ensure the legitimate and lawful incorporation of technology within the realm of digital justice on one hand, and to balance the guarantees of the latter with the use of technology on the other. This is done through the proper application of legal and regulatory texts related to cybersecurity, affirming the close connection between legal and cybersecurity.

B) Judicial Means:

The effectiveness of cybersecurity necessitates the availability of judicial means that contribute to increasing its efficiency. This includes procedural and structural means, where the former reflects the allocation of judicial mechanisms to ensure procedural effectiveness in accompanying criminal litigation procedures, while the latter reflects the allocation of rules and structures such as courts and specialized criminal poles for considering cybercrimes, as well as the allocation of qualitative procedures for monitoring cybercriminals and issuing effective penal judgments for the protection of cybersecurity. This highlights the integration between cybersecurity and the principle of judicial security stability.

In this context, from our perspective, the establishment of a cyber court is considered a constructive step and strategy that aims to create a qualitative leap in the field of cybersecurity and combat cybercrime, focusing exclusively on reviewing cyber misdemeanors and felonies according to judicial procedures characterized by specificity that align with the increasing dangers arising from connections to the digital space, with the cyber-criminal judge being the essential and effective factor in ensuring its proper performance.

C) Human Means:

This means includes human resources such as specialized technicians and experts in the field of cybersecurity, forming the information cell supervising the operation of software and technological applications. They activate various mechanisms related to ensuring cybersecurity and guarantee its employment within the criminal judiciary, as well as securing the electronic portal and administrative judicial services related to criminal matters.

In the same context, the authority of the human judge is emphasized, revolving around verifying the availability of cybersecurity before initiating any electronic procedures to protect rights and freedoms and to ensure a fair trial. The judge also contributes to combating cybercrimes by issuing effective criminal judgments against electronic crime. This role is reinforced by the necessity of training the specialized cyber-criminal judge, which ensures effectiveness and productivity reflected in the protection and establishment of cybersecurity.

D) Technological Means:

The nature and characteristics of digital cybersecurity necessitate seeking means of its kind to ensure its effectiveness. It is worth noting that the means of achieving information security is carried out by the competent authority using recognized electronic means, which particularly include everything related to technology (electromagnetic, photovoltaic, digital, optical)⁹. The scope of information security expands to encompass the preservation, protection, and secure transfer of data, in addition to countermeasures according to the McCumber model. Cybersecurity relies on several mechanisms, the most important of which are: electronic signatures, data encryption, and firewall technology¹⁰, some of the key technological standards that information security is based on include the ISO standard, Cobit standard, and Ital standard.¹¹

Thanks to artificial intelligence, legal information can be maintained securely, thereby providing further protection and security. In the future, artificial intelligence could ensure predictive justice¹², as well as assist the intelligent judge and the intelligent defense team (robot lawyer), if modern criminal policy turns to robotic services as a tool for modernizing the criminal judiciary.

1.2.2. Forms of Cybersecurity Protection in Criminal Matters

Based on a review of the Algerian Code of Criminal Procedure and the tracking of various texts related to the modernization of the justice sector, the legislator's reference to forms and shapes of cybersecurity protection is noted. This is discernible from the implications of the terms he used, which affirm procedural protection for cybersecurity. The legislator has also sought to guarantee substantive protection by dedicating texts in the Penal Code and some complementary laws, which include descriptions of informational attacks committed against the effectiveness of cybersecurity.

A) Procedural Criminal Cybersecurity Protection:

Despite the clear contribution of technology to achieving many objectives, of which the modernization of the criminal judiciary is the most important, this is only effectively realized through accompanying cybersecurity that aligns with various stages of criminal justice modernization. We attempt to trace and outline the features of procedural cybersecurity guarantees. The importance of having judicial systems based on digital technology is highlighted, which is referred to as electronic protection of rights related to electronic means.¹³

In addition to the general procedural rules included in the Code of Criminal Procedure related to prosecution and trial, Law No. 09-04 is considered one of the laws containing procedural information security principles, as can be inferred from Articles 3 to 7 and Articles 13 to 17.¹⁴

The legislator emphasized the necessity of safeguarding these principles in Law No. 15-03 concerning the modernization of justice, particularly through its second and third articles, which established key pillars of information protection by creating a central information system for automated data processing.

Besides, also the law incorporates several cybersecurity foundations that emphasize the reliability and confidentiality of electronic communication and the exchange of electronic judicial documents, establishing the principle of electronic documentation. This can be inferred from the

content of Articles 9, 10, and 14. We can observe the joint efforts of the legislator through Article 22 of Law No. 18-07, which aims to establish the National Authority for the Protection of Personal Data, and through the content of Article 52, which guarantees the right to demand precautionary measures against illegal information practices. The judge is tasked with adapting the information security environment for electronic litigation, as stated in Article 441 bis of Order No. 20-04 regarding the use of technological means in judicial procedures.

The legislator's commitment to the ethics of technology is demonstrated by the issuance of Presidential Decree No 20-05¹⁵, followed by the establishment of the National Penal Pole for Combating Crimes Related to Information and Communication Technologies, as per Article 211 bis 22 of Law No. 21-11¹⁶ Criminal proceedings for cybercrimes are subjected to expanded jurisdiction as per Article 211 bis 25 of the same law. The issuance of Presidential Decree No 23-314¹⁷ strengthened the legal alignment with technology through the establishment of the High Commission for Digitization.

It is noteworthy that the legislator did not provide specific provisions regarding the statute of limitations for information crimes affecting the justice sector, as derived from the reading of Article 8 bis of the Code of Criminal Procedure. However, their seriousness necessitates their inclusion in the content of the mentioned article.

B) Substantive Criminal Cybersecurity Protection

The legislator's interest in employing technology to enhance criminal justice is a contributing factor to ensuring the proper functioning of this facility. However, it also carries potential risks, the most prominent of which are information crimes. The legislator has responded to these crimes through numerous laws that collectively form what is referred to as cybersecurity. The judicial authority and its sovereignty can be seen as a target for these crimes. We will outline the texts that establish substantive cybersecurity protection.

Substantive cybersecurity protection pertains to a set of legal texts that specify the forms and elements of criminal acts, along with the various measures and criminal penalties associated with them in accordance with the principle of substantive legality.

By examining Law No 04-15¹⁸, we can infer the legislator's interest in establishing substantive protection by criminalizing behaviors that harm automated data processing systems, detailing the forms of crimes in Articles 394 bis to 394 bis 7. Article 394 bis 3 contains a provision for a doubled penalty if these attacks target entities subject to public law, which includes the judicial authority within these substantive provisions.

In line with this context, the legislator has strengthened cybersecurity through the aforementioned Law No. 09-04, which includes a definition of information crimes in its second article for the purpose of prevention and qualitative combat against such crimes. The law emphasizes the necessity of cybersecurity protection through the content of Articles 17 and 18 of Law No. 15-03 concerning modernization, by criminalizing certain acts that affect electronic signatures¹⁹ and the integrity of electronic documents. This is reflected in Articles 164 and 177 of Law No. 18-04 concerning postal and electronic communications, which include the criminalization of certain attacks on electronic devices and communication facilities.

In conclusion to the same path, Law No. 18-07 mentioned above is one of the most important laws related to data protection, which emphasizes that its processing must be within the framework of respecting human dignity and should not infringe upon individuals' rights, in accordance with Articles 2 and 54 of the law. Article 38 emphasizes the necessity of ensuring confidentiality and complete integrity during processing and taking appropriate measures according to the level of risks and threats. It also includes a statement of cybercrimes from Article 54 to 74, which constitute objective cybersecurity protection.

Order No. 21-09 is among the laws that reflect the ongoing adaptation of the legislator to confront all forms of cybercrime, as it sought to manifest them in Article 37²⁰ applying the principle of deterrence for the category of electronic crime professionals and providing objective

cybersecurity protection that contributes to creating technological immunity aligned with the modernization of criminal justice.

2. The Role of Cybersecurity in the Modernization of Criminal Justice

Undoubtedly, technology plays a significant role in modernizing criminal justice by utilizing it as a tool for litigation and enhancing administrative criminal services, which contributes to the flexibility and simplification of judicial processes. However, this role can only be effective by fostering trust in the use of technology, and perhaps the most prominent factor for its reliability is ensuring protection for personal information related to individuals and the criminal judicial authority, which is the responsibility of cybersecurity to guarantee. This necessitates the showcasing of its contributions and various challenges.

2.1. Contributions of Criminal Cybersecurity

Modern technology is tasked with contributing to realizing the legislator's intention to develop judicial administrative services and ensuring the effective operation of the criminal justice facility, which necessitates enhancing the role of cybersecurity in response to legal and judicial requirements and challenges. In this section of the study, we aim to illustrate the key objectives of criminal cybersecurity and the scope of its applications.

2.1.1. Objectives of Criminal Cybersecurity

As a result of the relative response of modern criminal justice to the increasing demands arising from social and economic developments and the impacts of the digital space, a transition to modern judiciary is necessary, which meets contemporary requirements and helps resolve all difficulties. This can be achieved by employing technology, ensuring its effectiveness, with cybersecurity being one of the most important aspects.

The legislator aims, through the establishment of cybersecurity within judicial bodies, to achieve several objectives aimed at promoting the justice sector and criminal judiciary, which are inferred from the indications of technological employment, and highlighting the paths and goals of cybersecurity, including:

- **Supporting the modernization of the justice sector:** Based on the technological standardization and its significance as one of the main pillars of modernizing the criminal justice sector, ensuring its effectiveness necessitates a cybersecurity framework that provides a secure environment for its utilization. The modernization of this sector through technology is unthinkable without cybersecurity accompaniment, which guarantees the effectiveness of modernization in its criminal aspect and provides quality judicial services.

In this context, it aims to enhance public electronic judicial services, as the administration has adapted to the modern era by transitioning from traditional administration to digital, reflecting on the efficiency and productivity in upgrading public services, notably speeding up transactions using modern means, reducing expenses, and increasing trust among individuals due to the speed and procedural simplification.²¹

- **Establishing guarantees for a fair trial:** Guarantees for a fair trial are among the main pillars of modern criminal policy. With the emergence of digital justice, the legislator is keen to enshrine cybersecurity to ensure reliability regarding electronic trial guarantees and keep pace with various digital procedures²², the principle of speed is considered one of the most important modern constitutional principles and a manifestation of the use of digitization in a judicial context, necessitating a cybersecurity accompaniment to provide a secure space for electronic litigation.

- **Preserving digital rights and freedoms:** This goal has become an obligation for the legislator to strengthen and guarantee, as technology circulates rights and freedoms during the judicial procedural practice. Cybersecurity is tasked with preventing unlawful infringements on these rights, and one of the most prominent rights pertains to individuals' personal data. Therefore, combating cybercrime is one of the most important means established to protect digital rights and freedoms.

In this regard, we refer to the classification criteria for cyber-attacks and their types, which may be based on the method of execution of the attack itself (phishing, denial of service,

backdoors), or the sector of the targeted audience (hacking, theft, espionage), or the ultimate goal intended to be achieved (financial, military, political, economic), or the actors involved (armed forces, cyber armies, organized criminal groups, terrorist groups).²³

- Establishing Reliability in Digital Justice: To provide sufficient guarantees for digital justice and its effectiveness, it is necessary to create a secure electronic space that fosters trust in electronic practices and reinforces data protection. This reality can be realized through the mandatory implementation of cybersecurity, which forms one of the most important pillars of digital trial, as it achieves effectiveness, spreads reliability, and encourages litigants to engage with it, given its ability to support litigants and beneficiaries of judicial services.

- Aligning with International Judicial Systems: The criminal policy pursued by legislators aiming to modernize criminal justice is a result of the global use of technology that has extended to most judicial systems and affected regional and international judicial security. In response to the benefits of technology and the necessity to keep up with the developments of judicial systems while enhancing international judicial cooperation and avoiding its drawbacks, Algerian legislators mandated cybersecurity as a mechanism to support international electronic judicial cooperation and its developments.

- Consolidating Protection of Electronic Judicial Sovereignty: As a consequence of the comprehensiveness of technology across various judicial operations, electronic judicial sovereignty has formed, which we consider (from our perspective) a manifestation of national security, given that it is an extension of state sovereignty. It is a priority to protect it through cybersecurity techniques, which have the capacity to confront all challenges potentially threatening judicial sovereignty. This necessitates employing digital mechanisms to enhance its role in protecting electronic judicial sovereignty.

- Protecting the Electronic Portal of the Ministry of Justice: One of the manifestations of the impacts of technology on justice is the establishment of the electronic portal, aimed at exchanging or extracting various documents electronically (complaints, petition, replies, judgments, and decisions, etc), which may expose it to informational risks. Cybersecurity must address this risk through specialized applications and programs, reflecting on the security of the electronic portal and ensuring the protection of digital judicial rights.

- Countering Electronic Bureaucracy: Denial-of-service viruses are among the risks facing technology in many service areas, including public facilities of all kinds, and the judiciary is one of the bodies expected to be exposed to these attacks, which can halt judicial work in its technological aspect, resulting in a paralysis of administrative and judicial electronic activities, leading to electronic bureaucracy. Cybersecurity intervenes as a mechanism to confront harmful programs and viruses.

2.1.2. Scope of Criminal Cybersecurity

Through the examination of the Code of Criminal Procedure and its most significant amendments related to modernization, it is evident that modern technology has a tangible impact on litigation procedures and guarantees of a fair trial, reflecting on the dimensions of cybersecurity. We attempt to define its scope at the level of the criminal judiciary.

- At the Level of Criminal Litigation:

The electronic public prosecution is considered one of the latest manifestations of modernizing criminal justice, relying in its performance of certain tasks on electronic means, including the exploitation of the electronic portal. The objectives of cybersecurity at this stage are limited to securing electronic documents submitted to the public prosecution and ensuring effective communication with justice agencies, while also protecting all electronic procedures practiced by the prosecution.

In the same context, revolving around the extensions and dimensions of criminal cybersecurity protection, electronic judicial investigations are legislatively covered by cybersecurity, whether related to electronic investigations and their components (such as orders and decisions) or

communication with various judicial bodies or with correctional institutions and security agencies and litigants, where cybersecurity ensures the protection of individuals and guarantees the dignity and immunity of electronic judicial investigations at their various levels.

Its scope expands to include electronic criminal trials, as the presiding judge can utilize various technological techniques in managing them, under a cybersecurity framework that is compatible with technological services. Remote video conferencing technology is among its most prominent applications, where it is conducted under cybersecurity protections that ensure all guarantees of a fair trial. It is inconceivable for it to be held remotely without cybersecurity ensuring and safeguarding the dignity of the court and the rights and freedoms of the parties involved in the public case.

On the other hand, the scope of cybersecurity expands to secure the digital connections and communications between the criminal judiciary and assisting professions through electronic communication platforms as a realization of modernization, such as the electronic platform specific to the bar association and court clerks, among other platforms under construction. The security benefits of cybersecurity also extend to include procedural electronic practices such as electronic appeals and notifications, enhancing the idea of electronic litigation and improving the quality of digital services.

- At the Level of Administrative Criminal Archiving:

The mechanism of electronic storage and archiving is one of the innovative technologies for modernizing criminal justice, considered one of the most important units of the central information system and the electronic portal. Through it, most criminal information is archived in electronic formats, recording and preserving all statements procedures and electronic documents arising from prosecution and trial, including electronic signature and certification data, and data related to the sending and receipt of electronic judicial documents.²⁴

The electronic nature of archiving necessitates the availability of cybersecurity protection to ensure confidentiality and guarantee the safe sending and receiving of various documents, especially those circulated through the electronic portal, such as complaints and petitions, responses, witness statements, security reports, judicial commissions, expert reports, rulings and decisions, electronic appeals, etc. It also aims to combat all cyberattacks in a way that instills trust in electronic archiving and its effectiveness.

2.2. Cybersecurity Challenges in Criminal Justice

Due to the specialized nature of criminal jurisdiction and the specificity of its procedures, the modernization process of criminal justice faces numerous challenges and issues, the most prominent of which is the effective establishment of cybersecurity. Its effectiveness remains relative concerning achieving its objectives, as a result of several obstacles that we will outline in this study, in order to assess the effectiveness of cybersecurity in modernizing the judiciary.

2.2.1. Obstacles to Cybersecurity in Criminal Justice

The guarantee of cybersecurity in criminal justice faces numerous difficulties that limit its role in protecting rights and freedoms, especially digital data and information, whether related to the judicial authority in general or to litigants and their digital identities in particular. These include:

- Legal Difficulties:

Legal texts are considered one of the most important means to establish the effectiveness of cybersecurity; however, the absence of a specific and independent law regarding its contents at the level of criminal justice is one of the obstacles impeding its effectiveness. Conversely, enhancing legal and criminal security specifically positively impacts the productivity of cybersecurity by working towards privatizing an exclusive law with a qualitative and modern formulation that focuses on ensuring the protection of rights and freedoms, especially digital ones, with a proactive and foresight legislative vision for all future challenges stemming from technology, artificial intelligence, and its rapid developments.

- Judicial Difficulties:

The absence of specialized cybersecurity judges hinders the adequate protection of freedoms and rights in the judicial digital space. Additionally, the lack of an independent cyber court with specialized follow-up procedures poses difficulties to the effective establishment of cybersecurity, which negatively affects the nature of criminal rulings related to cybercrime and diminishes their general and specific deterrent strength. The effectiveness of rulings positively influences the productivity of cybersecurity, while a weak deterrent against cybercriminals makes cybersecurity more vulnerable to attacks.

Moreover, the benefit of those convicted of cybercrimes from mitigating circumstances and exemptions encourages recidivism and habitual cybercriminal behavior, affecting the judicial means to support cybersecurity. Furthermore, the absence of limitation periods for cybercrimes poses challenges to its effectiveness. The lack of stability and judicial security negatively impacts cybersecurity, creating an obstacle to the effective progress of the modernization of the criminal system through technology.

- Technological Difficulties:

Due to the ongoing use of technological mechanisms in the modernization process, an increase in cybercrime is anticipated. As technology advances, so does cybercrime. Moreover, infrastructure deficiencies in technological frameworks reduce the effectiveness of cybersecurity, affecting protective mechanisms and necessitating their modernization.

Potential difficulties affecting cybersecurity include the increased use of artificial intelligence technologies and the judicial contributions arising from them, such as predictive justice, smart judges, smart lawyers, metaverse technology, etc. Future technological difficulties may relate to satellite internet and the expansion of cyber wars, which may extend into the judicial domain and its electronic sovereignty.

2.2.2. The Effectiveness of Cybersecurity in the Modernization of Criminal Justice

Cybersecurity is considered a crucial actor in modernizing criminal justice in a manner that aligns with legislative visions and responds to the requirements of modern criminal policy, contributing to a qualitative criminal shift that impacts the achievement of the existential goals of criminal justice at the national and international levels, in integration with other legal and judicial security factors.

Through our overview of some important milestones regarding this field of technology and its connections with justice and the criminal system, it is observed that it possesses relative effectiveness in keeping pace with modernization, based on tangible objectives at the judicial reality level, and its ability to adapt to and confront technological threats despite the challenges and obstacles it faces. However, the existence of a digital criminal justice system cannot be sustained without cybersecurity, which necessitates attention to its modernization and updating.

Conclusion:

At the end of this study, the effective role of cybersecurity in embodying the idea of modernizing criminal judicial justice is evident through procedural security in utilizing technology, ensuring various mechanisms that build trust in digital justice by harnessing technological means to guarantee the achievement of cybersecurity goals. Objectively, cybersecurity acts as a barrier and shield against information crimes threatening criminal justice and the digital rights and freedoms of individuals, reflecting on the establishment of legislative will and its prospects, integrating with legal and judicial security patterns. This study has produced several results and recommendations that we summarize as follows:

(First) Results:

1. The established role of cybersecurity in the modernization of criminal justice, through the objectives outlined in the study.
2. The contribution of cybersecurity to the ethics of technology, preserving rights and freedoms, especially digital ones.

3. The distinction of cybersecurity from other security patterns, despite the existence of functional interconnections between them.
4. The collision of cybersecurity with numerous obstacles and difficulties diminishing its effectiveness and productivity.
5. Legislative and judicial attention to guaranteeing cybersecurity as a technological necessity for modernizing criminal justice.
6. Legislative and judicial concern over the risks of cybersecurity lapses in light of its increasing judicial utilization.
7. The legislator's establishment of relative criminal protection for cybersecurity, aligning with developments in criminal policy.

(Second) Recommendations:

1. The necessity of enshrining the right to cybersecurity in the constitution and establishing qualitative legislation to institutionalize it.
2. The establishment of specialized cybercriminal courts and ensuring the training of specialized cyber judges.
3. The creation of a scientific research center for judicial technology and cybersecurity under the supervision of the Ministry of Justice.
4. Ensuring the comprehensiveness of cybersecurity for all electronic procedures and elevating it to the level of an essential guarantee for fair electronic trials, recognizing its absence as a reason for nullity and compensation.
5. Enhancing the use of artificial intelligence and advanced training for those responsible for its implementation to consolidate cybersecurity.
6. Strengthening the establishment of cybersecurity in military criminal justice due to its functional specificity.
7. Including cybercrimes within the provisions of Article 8 bis of the Algerian Code of Criminal Procedure.
8. Enhancing international cybersecurity cooperation mechanisms and focusing on supporting and protecting electronic judicial sovereignty.

Citations :

¹ Mesika Mohamed: Cyberspace and the Challenges to National Security of States, Journal of Legal and Social Sciences, Ziane Achour University, Djelfa, Algeria, 2022, Vol 07, Issue 04, p. 450.

² Ktaf Suleiman, Boukraine Abdelhalim: Procedural and Substantive Mechanisms to Achieve Cybersecurity, Journal of Governance and Economic Law, Faculty of Law and Political Science, University of Batna, Algeria, 2023, Vol. 03, Issue 02, p. 82.

³ Law No. 15-03, dated February 1, 2015, on the Modernization of the Justice Sector, Official Gazette No. 06, dated February 10, 2015.

⁴ Ordinance No. 20-04, dated August 30, 2020, concerning the use of audiovisual means in judicial procedures, amending and supplementing Ordinance No. 66-155, dated June 8, 1966, which includes the Algerian Code of Criminal Procedure.

⁵ Law No. 18-04, dated May 10, 2018, specifying general rules concerning mail and electronic communications, Official Gazette No. 27, issued on May 13, 2018.

⁶ Law No. 18-07, dated June 10, 2018, concerning the protection of natural persons in the processing of personal data, Official Gazette No. 34, issued on June 10, 2018.

⁷ Ordinance No. 21-09, dated June 8, 2021, concerning the protection of information and administrative documents, Official Gazette No. 45, issued on June 9, 2021.

⁸ Klaa Sharifa: Cybersecurity and the Challenges of Espionage and Electronic Intrusions in the Digital Space, *Journal of Law and Political Sciences*, University of Algiers 3, Algeria, 2022, Vol. 15, Issue 01, p. 298.

⁹ Hazem Hassan El-Gamal, *Criminal Protection of Cybersecurity*, First Edition, Dar Al-Fikr Wa Al-Qanun, Egypt, 2015, p. 66.

¹⁰ Saidi Salima, *Information Security and Its Systems in the Digital Age*, Dar Al-Fikr Al-Jami'i, Egypt, 2017, pp.38, 47.

¹¹ Ibid, pp.131, 136.

¹² Awad Amal Fawzi Ahmed, *Artificial Intelligence as a New Tool for Justice*, First Edition, Arab Democratic Center for Strategic, Political, and Economic Studies, Germany/Berlin, 2023, p.20, and on p/52, the author argues that predictive justice is the use of technology, statistical and mathematical tools to predict criminal acts and potential crimes and employ them in judicial decisions.

¹³ Hussein Ibrahim Khalil and Youssef Sayed Awad: *Litigation through Electronic Means: Theory and Practice Comparative Study in Light of Foreign and Arab Legislation*, Dar Al-Fikr Wa Al-Qanun, Mansoura, Egypt, 2021, p. 58.

¹⁴ See, to Articles 3 to 7 and Articles 13 to 17 of Law No. 09-04, dated August 5, 2009, establishing special rules for the prevention and combating of crimes related to information and communication technologies, Official Gazette No. 47, issued on August 16, 2009.

¹⁵ This ordinance established the National Cybersecurity Council and Agency, tasked with various roles and responsibilities; for more details, refer to Articles 1 to 4 and Articles 17 and 18 of Presidential Decree No. 20-05, dated January 20, 2020, on establishing a national cybersecurity system, Official Gazette No. 04, issued on January 26, 2020.

¹⁶ Ordinance No. 21-11, dated August 25, 2021, on the establishment of a National Judicial Pole for Combating Crimes Related to Information and Communication Technologies, Official Gazette No. 65, issued on August 26, 2021.

¹⁷ See, Article 4 of Presidential Decree No. 23-314, dated September 6, 2023, concerning the establishment and competencies of the Supreme Commission for Digitalization, Official Gazette No. 59, issued on September 10, 2023.

¹⁸ Law No. 04-15, dated November 10, 2004, regarding the definition of crimes affecting automated data processing, Official Gazette No. 71, amending and supplementing the Algerian Penal Code No. 66-156, dated June 8, 1966, Official Gazette No. 49, issued on June 11, 1966.

¹⁹ See, to Article 11 and Articles 66 to 75 of Law No. 15-04, dated February 1, 2015, specifying general rules on electronic signature and certification, Official Gazette No. 06, issued on February 10, 2015.

²⁰ The legislator paid attention to detailing certain cybercriminal acts, including criminalizing unauthorized access to an information system or electronic network or any means of information and communication technologies, see Article 37 of Ordinance 21-09, referenced earlier.

²¹ Zidan Mohamed: Electronic Litigation as a Procedural Mechanism in Facing Emergency Circumstances, the COVID-19 Pandemic as a Model, Algerian Journal of Legal and Political Sciences, University of Algiers, 2021, Vol. 58, Issue 02, p.264.

²² Key guarantees include: electronic publicity, remote electronic attendance, electronic recording, speed principle, etc., along with various procedures such as electronic interrogation and investigation, digital pleading, electronic testimony, and expertise.

²³ Mesika Mohamed, referenced earlier, p. 455.

²⁴ See, to Articles 10 and 14 of Law 15-03, referenced earlier, and Article 441bis/3 of Ordinance 20-04, previously mentioned.

Bibliography:

A- Legislation and Regulatory Texts:

- 1- Ordinance No. 66-155, dated June 8, 1966, concerning the Algerian Code of Criminal Procedure, Official Gazette No. 48, issued on June 10, 1966.
- 2- Ordinance No. 66-156, dated June 8, 1966, concerning the Algerian Penal Code, Official Gazette No. 49, issued on June 11, 1966.
- 3- Law No. 04-15, dated November 10, 2004, regarding crimes affecting automated data processing, Official Gazette No. 71, issued on November 10, 2004, amending Penal Code No. 66-156.
- 4- Law No. 09-04, dated August 5, 2009, establishing special rules for the prevention and combating of information and communication technology-related crimes, Official Gazette No. 47, issued on August 16, 2009.
- 5- Law No. 15-03, dated February 1, 2015, on the Modernization of the Justice Sector, Official Gazette No. 06, issued on February 10, 2015.
- 6- Law No. 15-04, dated February 1, 2015, specifying general rules on electronic signature and certification, Official Gazette No. 06, issued on February 10, 2015.
- 7- Law No. 18-04, dated May 10, 2018, specifying general rules concerning mail and electronic communications, Official Gazette No. 27, issued on May 13, 2018.
- 8- Law No. 18-07, dated June 10, 2018, concerning the protection of natural persons in data processing, Official Gazette No. 34, issued on June 10, 2018.
- 9- Ordinance No. 20-04, dated August 30, 2020, amending and supplementing Ordinance No. 66-155, concerning audiovisual means in judicial procedures, Official Gazette No. 51, issued on August 31, 2020.
- 10- Presidential Decree No. 20-05, dated January 20, 2020, concerning the establishment of a national cybersecurity system, Official Gazette No. 04, issued on January 26, 2020.
- 11- Ordinance No. 21-09, dated June 8, 2021, on protecting information and administrative documents, Official Gazette No. 45, issued on June 9, 2021.
- 12- Ordinance No. 21-11, dated August 25, 2021, on establishing the National Judicial Pole for Cybercrime, Official Gazette No. 65, issued on August 26, 2021.
- 13- Presidential Decree No. 23-314, dated September 6, 2023, on establishing and organizing the Supreme Commission for Digitalization, Official Gazette No. 59, issued on September 10, 2023.

B- Books:

- 1- Hazem Hassan El-Gamal, 2015, Criminal Protection of Cybersecurity, First Edition, Dar Al-Fikr Wa Al-Qanun, Mansoura, Egypt.
- 2- Hussein Ibrahim Khalil, Youssef Awad, 2021.
- 3- Saidi Salima, 2017, Information Security and Its Systems in the Digital Age, Dar Al-Fikr Al-Jami'i, Alexandria, Egypt.

4- Awad Amal Fawzi Ahmed, 2023, Artificial Intelligence as a New Tool for Justice, First Edition, The Democratic Arab Center for Strategic, Political, and Economic Studies, Germany/Berlin.

C- Scientific Articles:

1- Zidan Mohamed, 2021, Electronic Litigation: A Modern Procedural Mechanism in Response to Emergency Situations, Algerian Journal of Legal and Political Sciences, Volume 58, Issue 02, University of Algiers, pp. 257-291, Algeria.

2- Qataf Suleiman, Bouguerine Abdel Halim, 2023, Objective and Procedural Mechanisms Followed to Achieve Cybersecurity (Algeria as a Model), Governance and Economic Law Journal, Volume 03, Issue 02, Faculty of Law and Political Science, University of Batna, pp. 80-93, Algeria.

3- Kallaa Sharifa, 2022, Cybersecurity and the Challenges of Espionage and Electronic Breaches in the Digital Space, Journal of Rights and Political Sciences, Volume 15, Issue 01, University of Algiers, pp 292-314, Algeria.

4- Messika Mohamed, 2022, Cyber Space and National Security Challenges for States, Journal of Legal and Social Sciences, Ziane Achour University, Volume 07, Issue 04, pp. 447-462, Djelfa, Algeria.