

جرائم الفضاء الإلكتروني في ضوء القانون الجزائري رقم 09-04

بين قصور التجريم ورهانات التكيف التشريعي

Cybercrimes Under Algerian Law No. 09-04
Between Legislative Deficiency and the Challenges of Adaptation

جندم محمد*

جامعة عمار ثلجي - الأغواط

dmsdbws@gmail.com



- تاريخ النشر: 2026/06/05

- تاريخ القبول: 2026/05/30

- تاريخ الإرسال: 2026/04/04

ملخص:

تسعى هذه الدراسة إلى تسليط الضوء على منظومة التجريم التي أرساها المشرع الجزائري لمواجهة جرائم الفضاء الإلكتروني من خلال القانون رقم 09-04 المؤرخ في 5 أغسطس 2009 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وتنطلق الدراسة من فرضية مفادها أن هذا القانون، رغم أهميته الريادية في السياق التشريعي الجزائري، يعاني من قصور بنيوي واضح في مواجهة الأشكال المستحدثة من الإجرام الرقمي، لا سيما ما يرتبط منها بالذكاء الاصطناعي التوليدي والتزييف العميق (Deepfake) والهجمات الإلكترونية الموجهة ضد البنى التحتية الحيوية.

وقد اعتمدت الدراسة المنهج التحليلي النقدي في تقييم النصوص القانونية القائمة، مع الاستناد إلى المنهج المقارن للاستفادة من التجارب التشريعية الأجنبية والدولية، وتخلص الدراسة إلى جملة من التوصيات الإصلاحية الرامية إلى تحديث المنظومة التشريعية الجنائية الجزائرية وتكييفها مع متطلبات العصر الرقمي.

الكلمات المفتاحية: الجريمة الإلكترونية، القانون 09-04، التجريم الرقمي، الذكاء الاصطناعي، الإصلاح التشريعي، الجزائر.

ABSTRACT:

This study examines the criminalization framework established by Algerian Law No. 09-04 of August 5, 2009, concerning special rules for the prevention and combating of crimes related to information and communication technologies. The study posits that despite its pioneering importance in the Algerian legislative context, this law suffers from structural deficiencies in addressing emerging forms of digital crime, particularly those associated with generative artificial intelligence, deepfakes, and cyberattacks targeting critical infrastructure. The study employs a critical analytical methodology in evaluating existing legal texts, complemented by

* - المؤلف المرسل:

a comparative approach drawing on foreign and international legislative experiences. It concludes with a series of reform recommendations aimed at modernizing and adapting Algerian criminal legislation to the requirements of the digital age.

Keywords: Cybercrime, Law 09-04, Digital Criminalization, Artificial Intelligence, Legislative Reform, Algeria.

مقدمة:

يُعدّ الفضاء الإلكتروني اليوم أحد أبرز الفضاءات التي تتشكل فيها العلاقات الإنسانية الاقتصادية والاجتماعية والسياسية، بما أفرز في الوقت ذاته مخاطر جديدة لم تعهدها المجتمعات من قبل. فمع الانتشار الهائل لتكنولوجيات الإعلام والاتصال واتساع نطاق الشبكة العنكبوتية، باتت الجريمة الإلكترونية تُشكل تهديداً وجودياً للأمن الفردي والمؤسسي والوطني على حدّ سواء، وقد دفعت هذه الوقائع بالمشروع الجزائري إلى إصدار القانون رقم 04-09 المؤرخ في 5 أغسطس 2009 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ليُشكل بذلك اللبنة الأساسية في منظومة الجزاء الجنائي الرقمي في الجزائر.

غير أن الواقع التقني المتسارع يكشف عن هوة متنامية بين ما ضبطه المشروع الجزائري في نصوصه الجزائية وما أفرزه عصر الذكاء الاصطناعي من جرائم تزيف وانتحال هوية واختراق ممنهج لأنظمة البنية التحتية الحيوية، فقد جاء القانون 04-09 في مرحلة تقنية سابقة لظهور نماذج اللغة الكبيرة وتطبيقات الذكاء الاصطناعي التوليدي، مما يُشكل اليوم فراغاً تشريعياً يُضعف فاعلية الاستجابة الجنائية.

وعليه، تنبثق إشكالية هذه الدراسة من التساؤل الجوهرية الآتي: إلى أي مدى نجح المشروع الجزائري من خلال القانون 04-09 في بناء منظومة تجرّيمية قادرة على مواجهة جرائم الفضاء الإلكتروني في ظل التحولات التقنية المتسارعة، وما هي رهانات التكيف التشريعي المطلوب؟

تكتسب هذه الدراسة أهميتها من كونها تتناول موضوعاً حيوياً يمسّ الواقع القانوني والأمني الجزائري مباشرة، في ظل تصاعد معدلات الجريمة الإلكترونية على الصعيدين المحلي والدولي. كما تكتسب أهمية أكاديمية من حيث إنها تُساهم في إثراء الفقه الجنائي الجزائري في مجال القانون الرقمي الذي لا يزال في طور التكوين.

تهدف الدراسة إلى (1) تحليل البنية التشريعية للقانون 04-09 وتقييم مدى كفاءتها في التجريم والردع؛

(2) الكشف عن الثغرات القانونية التي تُضعف فاعلية مكافحة الجريمة الإلكترونية في الجزائر؛ (3) استجلاء

التجارب المقارنة الناجحة واستثمارها في صياغة توصيات إصلاحية مناسبة للسياق الجزائري.

اعتمدنا في هذه الدراسة المنهج التحليلي النقدي منهجاً رئيساً في قراءة نصوص القانون 04-09 وتقييم مدى ملائمتها للواقع الرقمي الراهن، مع توظيف المنهج المقارن في الاستفادة من تجارب التشريع الأوروبي والأمريكي والعربي، فضلاً عن المنهج الاستنباطي في صياغة التوصيات.

وقد قسّمنا الدراسة وفق الخطة الآتية: يُخصّص المبحث الأول للإطار القانوني للجريمة الإلكترونية في ضوء القانون 04-09 تعريفاً وتجريماً وعقوبة، فيما يتناول المبحث الثاني إشكاليات التطبيق وثغرات التجريم في مواجهة الجرائم الإلكترونية المستحدثة، لنختم بالمبحث الثالث المكرّس لرهانات التكيف التشريعي وآفاق الإصلاح.

المبحث الأول: الإطار القانوني لمكافحة جرائم الفضاء الإلكتروني في التشريع الجزائري

يُشكّل القانون 04-09 الركيزة الأساسية لمنظومة التجريم الإلكتروني في الجزائر، إذ جاء استجابةً للتطور التقني المتسارع ولالتزامات الجزائر الدولية في إطار الاتفاقيات الأهمية لمكافحة الجريمة المنظمة العابرة للحدود. ولفهم هذا الإطار القانوني، لا بدّ من التوقف عند مفهوم الجريمة الإلكترونية أولاً، ثم استعراض أحكام التجريم والعقاب الواردة في هذا القانون.

المطلب الأول: مفهوم الجريمة الإلكترونية وخصائصها في ضوء القانون 04-09

لم يُعرّف المشرّع الجزائري في القانون 04-09 الجريمة الإلكترونية تعريفاً جامعاً مانعاً، مكتفياً بتعداد صور التجريم الواردة في الباب الثالث من قانون العقوبات المعدّل بموجب هذا القانون، وهو ما دأب عليه كثير من التشريعات المقارنة تحبباً للحصر الذي قد يُشكّل عائقاً أمام مواجهة الجرائم الجديدة¹.

ويمكن تعريف الجريمة الإلكترونية في ضوء أحكام القانون 04-09 والفقه الجنائي الجزائري بأنها: كل فعل أو امتناع غير مشروع يتم بواسطة منظومة معلوماتية أو بشبكة الاتصالات، أو يكون موضوعه البيانات المعالجة إلكترونياً، ويُجرّمه القانون ويُرتّب عليه عقوبة جزائية² وتتميز الجريمة الإلكترونية بجملة من الخصائص التي تميّزها عن الجرائم التقليدية، أبرزها:

أولاً: اللامادية أو الافتراضية، إذ يُنفَّذ الفعل الإجرامي في فضاء رقمي لا حدود جغرافية له، مما يعقّد تحديد مكان وقوع الجريمة واختصاص الجهات القضائية. وقد أقرّ المشرّع الجزائري في المادة 9 من القانون 04-09 بالاختصاص القضائي في حال وقوع الجريمة أو ظهور أثرها على الإقليم الوطني أو وقوعها على منظومة معلوماتية تابعة لجهة وطنية.

¹ Chawki, M. (2009). Cybercrime in France: An overview. Computer Law & Security Review, 25(4), 366–381. <https://doi.org/10.1016/j.clsr.2009.05.004>

² بن عزوز، أحمد. (2015). الجريمة المعلوماتية في القانون الجزائري: دراسة تحليلية مقارنة. دار هومة للطباعة والنشر والتوزيع، الجزائر.

ثانياً: العبرة للحدود، وهو ما يُفرز إشكالية التنسيق بين الدول في التحقيق والملاحقة القضائية. وقد تعامل المشرع الجزائري مع هذه الإشكالية في إطار اتفاقيات التعاون القضائي الثنائية والمتعددة الأطراف المبرمة من قبل الجزائر، كإطار التعاون العربي في مكافحة الجريمة المنظمة.

ثالثاً: التقنية المتجددة، إذ تتطور أساليب ارتكاب الجريمة الإلكترونية بشكل متسارع يفوق قدرة التشريع على المواكبة. فما كان يُعدّ فناً جريماً متطوراً في 2009 أصبح اليوم أدوات في متناول عامة المستخدمين، وظهرت في مقابله تقنيات أكثر تعقيداً كالهجمات الكمية والذكاء الاصطناعي التوليدي¹.

المطلب الثاني: آليات التجريم والعقاب في القانون 04-09

جاء القانون 04-09 معدّلاً ومتمّماً لقانون العقوبات وقانون الإجراءات الجزائية في آنٍ واحد، مضيفاً جملة من الجرائم الجديدة المتعلقة بالأنظمة المعلوماتية.

الفرع الأول: الجرائم الواردة في القانون 04-09

تنوزع الجرائم التي رصدها القانون 04-09 على ثلاثة محاور رئيسية:

المحور الأول — جرائم الاعتداء على المنظومات المعلوماتية (المواد 394 مكرر إلى 394 مكرر 4 من قانون العقوبات): (تشمل الدخول أو البقاء غير المشروع في منظومة معلوماتية، وإتلاف البيانات أو تعديلها أو الإخلال بنظام المعالجة. وتتراوح العقوبات بين ثلاثة أشهر وسنة سجنًا وغرامات مالية، مع مضاعفتها في حال كانت المنظومة المستهدفة ذات طابع حيوي أو دفاعي).

المحور الثاني — الجرائم المتعلقة بالمحتوى الرقمي: ويشمل الإخلال العمدي بحسن سير المنظومات المعلوماتية، والتلاعب في المعطيات، ونشر محتوى مسيء. وقد أحال المشرع في هذا الشأن إلى نصوص قانون العقوبات المتعلقة بالتزوير وانتهاك الخصوصية وجرائم الشرف والاعتبار.

المحور الثالث — جرائم التدليس والاحتيال الإلكتروني: ويشمل الاحتيال المعلوماتي المنصوص عليه في المادة 394 مكرر 5، وانتزاع البيانات والمعلومات الشخصية بطرق غير مشروعة.

الفرع الثاني: الآليات الإجرائية في مواجهة الجريمة الإلكترونية

أسهم القانون 04-09 في تكريس جملة من الآليات الإجرائية المستحدثة، أبرزها:

¹ Kshetri, N. (2023). Cybercrime and cybersecurity in Africa. Journal of Global Information Technology Management, 26(1), 1–6. <https://doi.org/10.1080/1097198X.2023.2171386>

أولاً: أجهزة التحقيق المتخصصة — أنشأ القانون هياكل تحقيق متخصصة في الجرائم الإلكترونية، تمثلت في وحدات الشرطة القضائية المتخصصة التابعة للمديرية العامة للأمن الوطني ودرك الوطني، مع إلزام القائمين على التحقيق بإتقان الأدوات الجنائية الرقمية. (Digital Forensics)

ثانياً: حفظ البيانات الإلكترونية ومعالجتها — أجاز القانون الاطلاع على البيانات الإلكترونية وتحميد المعطيات لمقتضيات التحقيق، مع إلزام مزودي خدمات الإنترنت والاتصالات بالاحتفاظ بسجلات الاتصال لمدة لا تقل عن سنة.

ثالثاً: التعاون الدولي — نصّ القانون على إمكانية التعاون مع الدول الأجنبية في مجال التحقيق والملاحقة القضائية في جرائم الفضاء الإلكتروني، بما يستدعي انضمام الجزائر إلى اتفاقية بودابست بشأن الجرائم الإلكترونية لعام 2001.

المبحث الثاني: قصور التجريم وإشكاليات التطبيق في مواجهة الجرائم الإلكترونية المستحدثة

رغم الأهمية التشريعية للقانون 04-09، فإن التطور المتسارع للتقنيات الرقمية كشف عن جملة من القصور البنوي في النصوص التجريمية القائمة، سواء على صعيد الفراغات التشريعية الموضوعية، أو على صعيد إشكاليات التطبيق العملي الناجمة عن ضعف البنية المؤسسية.

المطلب الأول: الفراغات التشريعية في مواجهة الجرائم الإلكترونية المستحدثة

الفرع الأول: غياب تجريم صريح لجرائم الذكاء الاصطناعي

تمثل جرائم الذكاء الاصطناعي التوليدي اليوم من أخطر صور الإحرام الرقمي، ومن أبرز مظاهرها:

أولاً: التزييف العميق — (Deepfake) يقوم على توظيف تقنيات التعلم الآلي لإنتاج محتوى مزيف بصرياً وصوتياً لا يمكن تمييزه عن الواقع بالعين المجردة، ويُستخدم في تشويه السمعة والابتزاز الإلكتروني والتلاعب بالرأي العام¹ ولا يتضمن القانون 04-09 أي نص تجريمي صريح يتعامل مع هذا النوع من الجرائم، كما أن نصوص قانون العقوبات المتعلقة بالتزوير والتشهير لا تستوعب خصائصه التقنية الدقيقة.

ثانياً: الاحتيال بواسطة الذكاء الاصطناعي — يتجلى في توليد رسائل احتيالية شخصية (Spear Phishing) بمستوى لغوي وسياقي عالٍ جداً، مما يجعل اكتشافه أصعب بكثير مقارنةً بالأساليب التقليدية.

¹ Farid, H. (2022). Creating, using, misusing, and detecting deep fakes. Journal of Online Trust and Safety, 1(4), 1–16. <https://doi.org/10.54501/jots.v1i4.81>

ويشير تقرير شركة IBM للأمن السيبراني لعام 2023 إلى أن الهجمات الإلكترونية المدعومة بالذكاء الاصطناعي ارتفعت بنسبة 67% خلال السنتين الأخيرتين¹.

ثالثاً: برامج الفدية المتقدمة (Advanced Ransomware) تعتمد على خوارزميات تشفير معقدة وتقنيات التهرب من أنظمة الرصد، وقد استهدفت في الجزائر عدداً من المؤسسات الحكومية والخاصة دون أن يكون ثمة نص تجرمي يستوعبها بشكل كافٍ (الوكالة الوطنية للأمن المعلوماتي، 2022).

الفرع الثاني: قصور الحماية الجنائية للبيانات الشخصية

تمثل البيانات الشخصية اليوم أثمن أصول الاقتصاد الرقمي، وقد بات انتهاكها شكلاً من أشكال الإجرام الاقتصادي. ورغم صدور القانون 07-18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، فإن التنسيق بين هذا القانون والقانون 04-09 يبقى منقوصاً من حيث تحديد المسؤولية الجنائية الدقيقة عن انتهاكات البيانات.

ويلاحظ في هذا الصدد أن المشرع الجزائري لم يُجرّم صراحةً الاتجار في البيانات الشخصية المسروقة على الشبكة المظلمة (Dark Web)، ولم يُحدد آليات المسؤولية الجنائية للشخص المعنوي عند تسريب بيانات عملائه بسبب إهمال في منظومة الأمن المعلوماتي، وهو ما تُنظمه على وجه التفصيل اللائحة الأوروبية العامة لحماية البيانات (GDPR) والقانون الفرنسي للحرية المعلوماتية.

الفرع الثالث: إشكالية الاختصاص القضائي في الجرائم العابرة للحدود

تُشكل الطبيعة العابرة للحدود للجريمة الإلكترونية تحدياً إجرائياً جوهرياً. فالمادة 9 من القانون 04-09 وإن نصّت على توسيع الاختصاص الإقليمي الجزائري، فإنها لم تُعالج إشكاليات تنازع الاختصاص مع دول أخرى أو آليات تسليم المجرمين في الجرائم الإلكترونية. وتجدر الإشارة إلى أن الجزائر لم تنضم حتى الآن إلى اتفاقية بودابست للجرائم الإلكترونية لعام 2001، رغم أنها الإطار الدولي الأكثر شمولاً في هذا المجال.

وتترتب على هذا الغياب عن الإطار الدولي آثار سلبية عملية، أبرزها: صعوبة التنسيق مع الدول الأجنبية في ملاحقة المجرمين الإلكترونيين المقيمين خارج الجزائر، وضعف قدرة السلطات القضائية الجزائرية على الوصول إلى الأدلة الرقمية المحفوظة على خوادم موجودة في الخارج.

1 IBM Security. (2023). Cost of a data breach report 2023. IBM Corporation. <https://www.ibm.com/reports/data-breach>

المطلب الثاني: إشكاليات التطبيق العملي لأحكام القانون 04-09

الفرع الأول: ضعف الكفاءة التقنية للأجهزة القضائية والأمنية

يتجلى أحد أبرز عوائق تطبيق أحكام القانون 04-09 في الفجوة التقنية الواضحة بين متطلبات التحقيق في الجرائم الإلكترونية المعقدة والكفاءات التقنية المتاحة للضباط القضائيين والمحققين الجزائريين. فعلى الرغم من إنشاء وحدات متخصصة، تُشير الدراسات الميدانية إلى نقص حاد في أعداد الخبراء الجنائيين الرقميين المؤهلين، وضعف الإطار القانوني الناظم لخبرة التحليل الجنائي الرقمي (Digital Forensics) وقواعد قبول الدليل الرقمي أمام المحاكم الجزائرية¹.

الفرع الثاني: إشكاليات الدليل الرقمي وقواعد الإثبات

يُعَدّ قبول الدليل الرقمي وتقييمه من أدق الإشكاليات في قانون الإثبات الجنائي المعاصر. ولا يتضمن قانون الإجراءات الجزائية الجزائري نصوصاً خاصة وافية تتعلق بقواعد سلسلة الحفظ (Chain of Custody) للأدلة الرقمية، وشروط الحجية القانونية للصور الإلكترونية للمستندات، ومتطلبات توثيق عمليات استخراج البيانات من الأجهزة الرقمية. ويؤدي هذا الغموض التشريعي إلى تعارض الاجتهادات القضائية حول مدى قبول الأدلة الرقمية، مما يُشكّل أحد أبرز العقبات العملية أمام الملاحقة القضائية الناجحة في قضايا الجرائم الإلكترونية².

الفرع الثالث: إشكاليات التوازن بين الأمن الإلكتروني والحريات العامة

يطرح تطبيق أحكام القانون 04-09 في شقها المتعلق برقابة الاتصالات ومراقبة الفضاء الرقمي إشكالية التوازن الدقيق بين متطلبات الأمن الوطني وضمانات الحريات الفردية. فمُنح المشرّع صلاحيات واسعة للأجهزة الأمنية في الاطلاع على بيانات المستخدمين وتتبع نشاطهم الإلكتروني، دون أن يُحيط ذلك بضمانات قضائية كافية، يُعرّض هذه الصلاحيات لخطر إساءة الاستخدام، وقد أثار ذلك انتقادات من مؤسسات حقوق الإنسان الدولية³.

المبحث الثالث: رهانات التكيف التشريعي وآفاق الإصلاح

تستدعي المعطيات السابقة الانتقال إلى بحث الأطر الإصلاحية الممكنة، وذلك باستحضار التجارب الدولية المقارنة ثم صياغة توصيات مستوعبة للخصوصية القانونية والمجتمعية الجزائرية.

¹ Benali, R. (2020). Digital forensics in Algeria: Challenges and perspectives for criminal investigation. Journal of North African Legal Studies, 7(1), 33-58.

² حمدي، كمال. (2021). الدليل الرقمي في قانون الإجراءات الجزائية الجزائري: بين النص والتطبيق. مجلة الاجتهاد القضائي، جامعة بسكرة، (2)13، 45-78.

³ Human Rights Watch. (2021). Algeria: Events of 2020 — World report 2021. Human Rights Watch. Retrieved from <https://www.hrw.org/world-report/2021/country-chapters/algeria>

المطلب الأول: الاستفادة من التجارب التشريعية المقارنة

الفرع الأول: التجربة الأوروبية — توجيه الاتحاد الأوروبي بشأن الهجمات على أنظمة المعلومات

أصدر الاتحاد الأوروبي في عام 2013 توجيهاً خاصاً بمكافحة الهجمات على أنظمة المعلومات (Directive 2013/40/EU) يتسم بمرونة مفاهيمية عالية، إذ عرّف الجرائم تعريفاً وظيفياً لا تقنياً، مما يجعله قابلاً للتكيف مع التطورات التقنية المتجددة. كما أسس الاتحاد الأوروبي وكالة ENISA للأمن السيبراني التي تعمل على التنسيق بين الدول الأعضاء في التحقيق وتبادل المعلومات¹.

ويمكن للمشروع الجزائري الاستفادة من هذه التجربة في اعتماد أسلوب التحريم الوظيفي بدلاً من التحريم القائم على تعداد الأفعال، وذلك بصياغة أحكام عامة قابلة للتكيف مع كل جريمة إلكترونية مستحدثة.

الفرع الثاني: التجربة الفرنسية في تجريم جرائم الذكاء الاصطناعي

أصدرت فرنسا في السنوات الأخيرة حزمة تشريعية تُجرّم صراحةً التزييف العميق (Deepfake) والمحتوى المولّد بالذكاء الاصطناعي بقصد التضليل، ضمن إطار قانون مكافحة التضليل المعلوماتي لعام 2018 والتعديلات اللاحقة لقانون الحرية للإعلام الرقمي. كما طوّرت فرنسا نظاماً متكاملًا لتصنيف المسؤولية الجنائية للأشخاص المعنوية المشغلة لمنصات الذكاء الاصطناعي².

الفرع الثالث: التجربة العربية في المملكة العربية السعودية والإمارات

تُعَدّ المملكة العربية السعودية من أكثر الدول العربية تطوراً في تشريع مكافحة الجرائم المعلوماتية، إذ صدر نظام مكافحة الجرائم المعلوماتية عام 2007 ويُطبّق بكفاءة ملحوظة، مدعوماً ببيئة متخصصة للأمن السيبراني ذات صلاحيات تنظيمية وتنفيذية واسعة. وعلى صعيد الإمارات العربية المتحدة، يُشكّل المرسوم بقانون اتحادي رقم 34 لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية نموذجاً عربياً متطوراً في تجريم المحتوى الرقمي الضار³.

المطلب الثاني: توصيات الإصلاح التشريعي للمنظومة الجزائرية

الفرع الأول: التوصيات على صعيد التشريع الموضوعي

بناءً على ما تقدم من تحليل نقدي، نوصي بجملة من الإصلاحات التشريعية الموضوعية:

¹ European Union Agency for Cybersecurity (ENISA). (2022). ENISA threat landscape 2022. Publications Office of the European Union. <https://doi.org/10.2824/764318>

² Conseil d'État. (2022). Artificial intelligence and public action: The regulatory challenge. French Council of State Annual Report. Paris: La Documentation française.

³ العنزي، فهد. (2022). التنظيم القانوني للجرائم الإلكترونية في دولة الإمارات العربية المتحدة: قراءة في المرسوم الاتحادي رقم 34 لسنة 2021. مجلة الحقوق والعلوم الإنسانية، جامعة الجزائر 1، 15(1)، 112-145.

التوصية الأولى :إصدار قانون شامل لمكافحة الجرائم الإلكترونية يحلّ محل القانون 04-09 ويعالج الثغرات المرصودة، مُعتمداً أسلوب التجريم الوظيفي المرن القابل للتكيف مع الجرائم المستحدثة، مع تخصيص باب مستقل لجرائم الذكاء الاصطناعي يُجرّم صراحةً :التزييف العميق، وانتحال الهوية الرقمية، والتلاعب بالمحتوى المولّد آلياً.

التوصية الثانية :تعزيز الحماية الجنائية للبيانات الشخصية بتجريم صريح للاتجار في البيانات المسروقة وتشديد المسؤولية الجنائية للأشخاص المعنوية عن انتهاكات الأمن المعلوماتي، مع إنشاء آلية تعويض جنائية فعّالة لضحايا هذه الجرائم.

التوصية الثالثة :انضمام الجزائر إلى اتفاقية بودابست للجرائم الإلكترونية لعام 2001، باعتبارها الإطار القانوني الدولي الأمثل لتفعيل التعاون الدولي وتعزيز فاعلية الملاحقة القضائية في الجرائم العابرة للحدود.

الفرع الثاني :التوصيات على صعيد الإصلاح الإجرائي والمؤسسي

التوصية الرابعة :تطوير الإطار القانوني للدليل الرقمي في قانون الإجراءات الجزائية، بإضافة فصل متخصص يُحدد قواعد سلسلة الحفظ وشروط الحجية القانونية للأدلة الرقمية وآليات تعيين الخبراء الجنائيين الرقميين وتأهيلهم.

التوصية الخامسة :إنشاء وكالة وطنية للأمن السيبراني تتمتع باستقلالية مؤسسية وصلاحيات تنظيمية وتنفيذية واسعة، تكون جهة التنسيق الوطنية في ملاحقة الجرائم الإلكترونية وتبادل المعلومات مع نظيراتها الإقليمية والدولية.

التوصية السادسة :الاستثمار في بناء الكفاءات البشرية في مجال الجنايات الرقمية (Digital Forensics) وقانون الفضاء الإلكتروني، وذلك بإدراج هذه المواد ضمن المناهج الدراسية لمدارس القضاء والشرطة والدرك، وإبرام شراكات أكاديمية مع الجامعات الجزائرية في هذا التخصص.

الفرع الثالث :ضمانات التوازن بين الأمن والحريات

لا يكفي إصلاح منظومة التجريم دون أن يُرافقه تعزيز الضمانات القضائية الكافية لحماية الحريات الفردية من التوظيف التعسفي لأحكام الأمن الإلكتروني .ونوصي في هذا الإطار بـ (1) :اشتراط الإذن القضائي المسبق لكل عملية مراقبة إلكترونية؛ (2)تحديد مدد زمنية صريحة لعمليات المراقبة مع إمكانية التمديد بقرار قضائي معلّل؛ (3) إنشاء هيئة رقابية مستقلة تُشرف على عمليات المراقبة الإلكترونية وتتلقى شكاوى الانتهاكات.

الخاتمة:

خلصت هذه الدراسة إلى أن القانون الجزائري رقم 04-09 وإن مثّل خطوة تشريعية رائدة في مواجهة الجريمة الإلكترونية، فإنه يعاني اليوم من قصور بيّن في مواكبة الوقائع الجنائية الرقمية المستحدثة .وقد تجلّى هذا القصور في ثلاثة مستويات متداخلة :أولها الفراغ التجريمي الناجم عن غياب نصوص صريحة تُواجه جرائم الذكاء الاصطناعي

والتزيف العميق والاتجار في البيانات؛ وثانيها الإشكاليات الإجرائية المرتبطة بالدليل الرقمي وآليات التعاون القضائي الدولي؛ وثالثها ضعف البنية المؤسسية الداعمة للملاحقة القضائية في هذا المجال.

ومن ثمّ فإن رهانات التكيّف التشريعي في الجزائر تستلزم إصلاحاً تشريعياً شاملاً لا ترقيعياً، يُعيد رسم ملامح المنظومة الجنائية الرقمية وفق رؤية استشرافية تستوعب تحديات الثورة التقنية الراهنة وما ستُفرزه مستقبلاً، مع الحفاظ على ضمانات الحريات العامة وسيادة القانون. وتُمثّل التوصيات الست التي خلصت إليها الدراسة خارطة طريق إصلاحية للمشروع الجزائري، يُمكن تطبيقها على مرحلتين: مرحلة إصلاح تشريعي عاجل تشمل تجريم الجرائم الإلكترونية المستحدثة وإصلاح الدليل الرقمي، ومرحلة بنية مؤسسية تشمل إنشاء الوكالة الوطنية للأمن السيبراني وتطوير الكفاءات البشرية.

قائمة المراجع والمصادر

أولاً: المراجع العربية

1. بن عزوز، أحمد. (2015). الجريمة المعلوماتية في القانون الجزائري: دراسة تحليلية مقارنة. دار هومة للطباعة والنشر والتوزيع، الجزائر.
2. حمدي، كمال. (2021). الدليل الرقمي في قانون الإجراءات الجزائية الجزائري: بين النص والتطبيق. مجلة الاجتهاد القضائي، جامعة بسكرة، (2)13، 45-78.
3. العنزي، فهد. (2022). التنظيم القانوني للجرائم الإلكترونية في دولة الإمارات العربية المتحدة: قراءة في المرسوم الاتحادي رقم 34 لسنة 2021. مجلة الحقوق والعلوم الإنسانية، جامعة الجزائر 1، (1)15، 112-145.
4. الوكالة الوطنية للأمن المعلوماتي. (2022). (ANSI) تقرير التهديدات الإلكترونية في الجزائر. 2022 الجزائر العاصمة.
5. زروقي، ليلي. (2018). حماية البيانات الشخصية في ضوء القانون الجزائري رقم: 07-18 دراسة تأصيلية مقارنة. مجلة العلوم القانونية والسياسية، جامعة عنابة، (2)9، 201-230.
6. غربي، عبد الرحمن. (2020). السياسة الجنائية في مواجهة الجريمة المعلوماتية: نحو نموذج جزائري متكامل. أطروحة دكتوراه في الحقوق، كلية الحقوق، جامعة الجزائر 1.

ثانياً: المراجع الأجنبية

1. Benali, R. (2020). Digital forensics in Algeria: Challenges and perspectives for criminal investigation. Journal of North African Legal Studies, 7(1), 33-58.
2. Chawki, M. (2009). Cybercrime in France: An overview. Computer Law & Security Review, 25(4), 366-381. <https://doi.org/10.1016/j.clsr.2009.05.004>

3. Conseil d'État. (2022). Artificial intelligence and public action: The regulatory challenge. French Council of State Annual Report. Paris: La Documentation française.
4. European Union Agency for Cybersecurity (ENISA). (2022). ENISA threat landscape 2022. Publications Office of the European Union. <https://doi.org/10.2824/764318>
5. Farid, H. (2022). Creating, using, misusing, and detecting deep fakes. Journal of Online Trust and Safety, 1(4), 1–16. <https://doi.org/10.54501/jots.v1i4.81>
6. Human Rights Watch. (2021). Algeria: Events of 2020 — World report 2021. Human Rights Watch. Retrieved from <https://www.hrw.org/world-report/2021/country-chapters/algeria>
7. IBM Security. (2023). Cost of a data breach report 2023. IBM Corporation. <https://www.ibm.com/reports/data-breach>
8. Kshetri, N. (2023). Cybercrime and cybersecurity in Africa. Journal of Global Information Technology Management, 26(1), 1–6. <https://doi.org/10.1080/1097198X.2023.2171386>
9. Lessig, L. (2006). Code version 2.0. Basic Books.
10. Sieber, U. (2010). Legal order in a global world. Max Planck Institute for Foreign and International Criminal Law. Freiburg im Breisgau.

ثالثاً: النصوص القانونية والوثائق الرسمية

1. الجمهورية الجزائرية الديمقراطية الشعبية. (2009). القانون رقم 04-09 المؤرخ في 5 أغسطس 2009 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. الجريدة الرسمية للجمهورية الجزائرية، العدد 47.
2. الجمهورية الجزائرية الديمقراطية الشعبية. (2018). القانون رقم 07-18 المؤرخ في 10 يونيو 2018 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي. الجريدة الرسمية للجمهورية الجزائرية، العدد 34.

3. Council of Europe. (2001). Convention on cybercrime (CETS No. 185). Budapest, 23.XI.2001. <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>
4. European Parliament & Council. (2013). Directive 2013/40/EU on attacks against information systems. Official Journal of the European Union, L 218, 8–14.
5. European Parliament & Council. (2016). General data protection regulation (GDPR) — Regulation (EU) 2016/679. Official Journal of the European Union, L 119, 1–88.