وزارة التعليم العالي والبحث العلمي
جامعة المجاهد عبد الحفيظ بوالصوف- ميلة
كلية الحقوق

القسم: الحقوق
التخصص: قانون جنائي

الرقم التسلسلي:.....
الرمز:.....

الحماية القانونية من جرائم التزوير الرقمي في التشريع الجزائري

مذكرة ضمن متطلبات نيل شهادة الماستر

اعداد الطالبتين:
دعاس منال
حبيلة جازية

اشراف الأستاذة:
د. بغدادي ايمان

السنة الجامعية: 2026/2025

وزارة التعليم العالي والبحث العلمي
جامعة المجاهد عبد الحفيظ بوالصوف- ميلة
كلية الحقوق

القسم: الحقوق
التخصص: قانون جنائي

الرقم التسلسلي:.....
الرمز:.....

الحماية القانونية من جرائم التزوير الرقمي في التشريع الجزائري

مذكرة ضمن متطلبات نيل شهادة الماستر

اعداد الطالبتين:
دعاس منال
حبيلة جازية

اشراف الأستاذة:
د.بغدادي ايمان

أعضاء لجنة المناقشة

الاسم واللقب	الانتماء	الرتبة العلمية	صفته في اللجنة
د. منصور نورة	جامعة عبد الحفيظ بوالصوف- ميلة	أستاذ محاضر - ب -	رئيسا
د. ايمان بغدادي	جامعة عبد الحفيظ بوالصوف- ميلة	أستاذ محاضر - ب -	مشرفا ومقررا
د. شوقي حفياني	جامعة عبد الحفيظ بوالصوف- ميلة	أستاذ محاضر - ب -	عضوا مناقشا

السنة الجامعية: 2026/2025

بِسْمِ ٱللَّهِ ٱلرَّحْمَٰنِ ٱلرَّحِيمِ

قُل رَبِّ زِدْنِي عِلْمًا

سورة طه : 114

شكر وتقدير

بسم الله الرحمن الرحيم

بكل تواضع وامتنان نُقدّم أصدق عبارات الشكر والتقدير والعرفان لكل من أسهم – بقربه أو بعده – في إنجاز هذا العمل وإخراجه إلى حيز الوجود.

فإلى أستاذتنا لمشرفة الأستاذة بغدادي إيمان

نُقدّم لها أسمى آيات الإمتنان والتقدير لقد كانت لنا طوال مسار هذا البحث نبراساً يهدي خطانا ومرشدةً تُضيء لنا دروب التحليل القانوني بعلمها الواسع وصبرها الجمّ، لقد آمنت بقدراتنا حينما كنا نبحث عن ثقتنا بأنفسنا، ومنحتنا من وقتها وخبرتها الكثير، فكانت لنا بحق قدوةً في الأمانة العلمية والصرامة البحثية، شكراً لها على كل تَوجيهِ، وعلى كل ملاحظة بناءة، وعلى كل لحظة من لحظات الإشراف التي شكّلت دون شك حجر الزاويةِ في هذا المشروع.

وإلى السادة أعضاء لجنة المناقشة

نُقدّم لهم خَالص الشكر والتقدير على تكرَمهم بقبول مناقشة هذا العمل، وعلى ما سيبذلونه من جهد نقديٍ بناء يثري البحث ويكمل مساره، نتطلّع بكل احترام وتقديرٍ إلى ملاحظاتهم القيمة التي ستكون بلا ريب – مصدر إثراء علمي لنا.

وإلى كل من وقف إلى جانبنا

نَوجّه عبارات الشكر والعرفان لكل من ساعدنا – من قريب أو من بعيد – في رحلة هذا البحث الطويلة، لكل من قَدّم لنا يد العون، أو شاركنا فكرةً، أو رافقنا بكلمةٍ طيبَةٍ، أو سهّل لنا أمراً، أو شاركنا همّ التفكير والتحليل. لقد كان هذا العمل – كما كل عملٍ علميٍّ حقّ – نتاج جهدٍ جماعيٍّ يَتجاوز حدود الكاتبين، فكان لدعمكم وتشجيعكم الأثر الأعظم في بلوغنا هذه المرحلة.

والحمد لله ربِّ العالمين.

إهـداء

إلى روح والدي رحمه الله،
الذي غادر الدنيا قبل أن يقرأ في عيني فرحة التخرج،
لكنه لم يغب يوما عني.
أنت يا أبي أول من علمني أن العلم نور،
وأن الكرامة تبني بالمعرفة والمثابرة.
هذه الصفحات شاهدة على أن حلمك لم يمت،
وأن ابنتك قد وصلت إلى ما كنت تتمناه لها.
رحمك الله، وجعل الجنة دار مثواك،
وألحقني بك في دار كرامته.

♥

وإلى أمي، يا من حولت الحياة بعد رحيله
إلى أنغام من الأمل والصبر.
أنت لم تكوني مجرد أم،
بل كنت لنا أبا وأما، وسندا لا يتزعزع، وملاذا لا يضام.
شكرا لأنك أمنت بي حين شككت بنفسي،
وشكراً لأنك ضحيت بسنوات عمرك لأن أبني مستقبلي.
هذا النجاح لك، كما كل نجاح سأهديه لك ما حييت.

♥

وإلى إخوتي،
شكراً لأنكم كنتم لي ظهراً وقوة.
شكراً لأن فرحتكم بي لم تكن مجاملة،
بل كانت حقيقة تشبه قلوبكم النقية.

♥

إلى كل من ذكرتهم،
وإلى كل من شاركني هذا الطريق بقلب صادق...
أهدي هذا العمل بكل ما في قلبي
من حب وامتنان ووفاء لا ينتهي.

منال

إهـداء

أهدي هذا العمل إلى أبي،
شكرا لأنك آمنت بي منذ البداية،
ولأنك كنت أول من صفق لي حين لم يكن أحد يرى ما أراه.
هذا النجاح لك يا أبي،
كما كل ما سأصبحه في حياتي.

♥

وإلى أمي،
يا من جعلت من البيت مدرسة من الحب والدفء.
شكرا لأنك كنت لي ملاذا حين تثقل الدنيا،
ولأنك علمتيني أن الضعف ليس عيبا،
بل العيب في أن نتوقف.
هذا العمل لك.
بكل ما فيه من جهد وإصرار تعلمته منك.

♥

وإلى إخوتي،
أنتم لم تكونوا مجرد إخوة،
بل كنتم فريقي الأول.
شكرا على الضحك في لحظات ضعفي،
وعلى الصمت في لحظات حزني.

♥

وإلى كل من ساندني،
إلى الذين قدموا لي يد العون بلا منة،
والذين آمنوا بقدراتي حين شككت بها،
والذين كانوا لي نورا في نفق هذا الطريق الطويل.
شكرا لأنكم لم تكونوا مجرد "محيط"،
بل كنتم جزءاً من هذا الإنجاز.

♥

إلى كل من ذكرتهم...
أهدي هذا العمل بصدق قلبي،
مؤمنة بأن لا نجاح بينى وحده،
وأن الحب الحقيقي هو الذي يحول المستحيل إلى حقيقة.
والحمد لله.

جازيـة

المقدمة

يشهد العالم اليوم تحولاً رقمياً شاملاً غيّر من طبيعة العلاقات الاجتماعية والاقتصادية والقانونية، حيث أصبح الاعتماد على المحررات الإلكترونية والمعاملات الرقمية بديلاً أساسياً عن الوسائل التقليدية، ومع هذا التطور، برزت ظاهرة التزوير الرقمي كإحدى أخطر الجرائم المستجدة التي تستهدف النزاهة والموثوقية التي تقوم عليها الأنظمة المعلوماتية، ولم يعد التزوير مقتصراً على المحررات الورقية، بل امتد ليشمل البيانات والمعطيات المخزنة إلكترونياً، والتوقيعات الرقمية، ووسائل الدفع الإلكتروني، مما خلق تحديات غير مسبوقة أمام النظم القانونية، وقد حاول التشريع الجزائري مواكبة هذا التحول من خلال سن نصوص جزائية ومدنية تنظم المحرر الإلكتروني وتجرم التلاعب بالأنظمة الرقمية، غير أن هذا الإطار لا يزال يحتاج إلى استقراء نقدي في ظل التطورات التقنية المتسارعة.

أهمية الموضوع:

على المستوى النظري، تسهم هذه الدراسة في إثراء المكتبة القانونية العربية والجزائرية ببحث متخصص يقع في منطقة التقاء القانون الجنائي بالقانون الرقمي، حيث إن التزوير الرقمي يطرح إشكاليات نظرية تتعلق بتعريف الجريمة وأركانها وطبيعة الضرر في الفضاء الافتراضي، وعلى المستوى العملي، تقدم الدراسة قراءة نقدية للسياسة التشريعية والعقابية المعتمدة، وتضع بين يدي القضاة والمحامين والباحثين إطاراً تحليلياً يساعد على فهم آليات تجريم التزوير الرقمي ومكافحته، مع اقتراح حلول عملية لتجاوز الثغرات التي تعترض الملاحقة الفعلية لهذه الجرائم.

أسباب اختيار الموضوع:

الأسباب الموضوعية:

من الأسباب الموضوعية التي دفعت إلى اختيار هذا الموضوع: حداثته وارتباطه الوثيق بالتحول الرقمي الذي تشهده الجزائر في مجالات الإدارة الإلكترونية والتجارة الإلكترونية والخدمات البنكية الرقمية. كما أن هذا الموضوع يثير إشكاليات عملية جمة تتعلق بصعوبة ضبط الأدلة الرقمية وإثباتها، وتحديد الاختصاص القضائي في الجرائم العابرة للحدود، وعلى الصعيد التشريعي رغم صدور نصوص مهمة لا يزال هناك نقص في الدراسات المتخصصة التي تتناول هذا الموضوع بشكل استقرائي وتحليلي.

الأسباب الذاتية:

أما الأسباب الذاتية، فتتمثل في رغبة الباحث في التعمق في دراسة الجرائم المعلوماتية كمجال حديث من القانون الجنائي، وإيمانه بضرورة مواكبة التطورات التقنية بردع قانوني فعال يحمي المجتمع من مخاطر الجريمة الرقمية.

أهداف الموضوع:

يهدف هذا البحث إلى إبراز الإطار القانوني لجرائم التزوير الرقمي في التشريع الجزائري من خلال تحليل النصوص الجزائية المنظمة لهذا النوع من الجرائم، ودراسة أركانها المادية والمعنوية، وتقييم السياسة العقابية المعتمدة في هذا المجال، مع الوقوف على التعديلات الأخيرة التي مست النصوص الجنائية ومدى انعكاسها على فعالية الحماية القانونية، كما يسعى البحث إلى تقييم الآليات الإجرائية والمؤسساتية المكلفة بمكافحة هذه الجرائم، وتحديد مدى كفاية الخبرة القضائية والتعاون الدولي في مجال الملاحقة والإثبات.

حدود الدراسة:

تقتصر هذه الدراسة من حيث الحدود المكانية على الجمهورية الجزائرية، نظراً لما تمثله من نموذج تشريعي وقضائي يجمع بين الخصوصية القانونية الوطنية والانفتاح على المعايير الدولية في مجال الجرائم المعلوماتية، أما من حيث الحدود الزمانية، فيغطي البحث الفترة الممتدة من بداية التنظيم الجزائي للجرائم المعلوماتية إلى غاية السنة الحالية، وهي فترة شهدت تفعيل آليات الحماية الجزائية من التزوير الرقمي وتطور الإطار التشريعي المنظم للمحرر الإلكتروني والتوقيع الإلكتروني.

صعوبات الدراسة:

لم تخلُ دراسة هذا الموضوع من صعوبات، أبرزها ندرة المراجع المتخصصة باللغة العربية التي تتناول التزوير الرقمي في التشريع الجزائري بشكل خاص، وسرعة تطور التقنيات الرقمية التي تجعل بعض المعلومات القانونية عرضة للتجديد المستمر، فضلاً عن قلة الاجتهادات القضائية المنشورة في هذا المجال، وقد تم تجاوز هذه الصعوبات بالاعتماد على المصادر الأجنبية المترجمة، والاطلاع على الأدبيات القانونية المقارنة، فضلاً عن الاستعانة بالنصوص التشريعية والتنظيمية الأصلية والاتفاقيات الدولية ذات الصلة.

اشكالية الدراسة:

تتمحور الإشكالية العامة للبحث حول التساؤل التالي: إلى أي حد وفّر التشريع الجزائري حماية قانونية كافية وفعالة من جرائم التزوير الرقمي، وهل النصوص الجزائية والإجرائية الحالية قادرة على مواجهة التحديات التقنية والإجرامية المستجدة في هذا المجال؟

الأسئلة الفرعية:

- ما هي ماهية التزوير الرقمي وخصائصه المميزة عن التزوير التقليدي؟
- ما هي شروط الاعتراف بالقيمة القانونية للمحرر الإلكتروني في الجزائر؟
- ما هي الأركان القانونية لجريمة التزوير الرقمي في ظل النصوص الجزائية الحالية؟
- ما هي طبيعة العقوبات المقررة ومدى ملاءمتها لخطورة هذه الجرائم؟
- ما هي الآليات الإجرائية المتاحة لضبط الأدلة الرقمية وإثباتها؟
- ما هو دور الخبرة القضائية والمعلوماتية في كشف التزوير الرقمي؟
- ما هي الآليات المؤسساتية والدولية المكلفة بمكافحة هذه الظاهرة؟

المنهج المعتمد:

يتبع هذا البحث منهجاً تحليلياً يقوم على دراسة النصوص القانونية وتحليل مضمونها وتفكيك أحكامها، إلى جانب المنهج الوصفي في عرض المفاهيم والأركان والإجراءات، والمنهج المقارن في بعض المحاور التي تستدعي الاطلاع على التجارب التشريعية الأجنبية والاتفاقيات الدولية، وذلك بهدف الوصول إلى نتائج علمية دقيقة تسهم في تطوير الإطار القانوني الجزائري.

تقسيم الدراسة:

ينقسم هذا البحث إلى فصلين رئيسيين: يتناول الفصل الأول الإطار الموضوعي لجريمة التزوير الرقمي في القانون الجزائري، من خلال ثلاثة مباحث، يخصص الأول منها لدراسة ماهية التزوير الرقمي ومحله، فيما يعنى الثاني بالأركان القانونية للجريمة، ويتناول الثالث النظام العقابي المقرر لها.

أما الفصل الثاني فيركز على الآليات الإجرائية والمؤسساتية لمكافحة التزوير الرقمي، وينقسم بدوره إلى ثلاثة مباحث، الأول يتناول إجراءات البحث والتحري، والثاني يعالج مسائل الإثبات والملاحقة القضائية، في حين يخصص الثالث للآليات المؤسساتية والتعاون الدولي.

الفصل الأول

الاطار المفاهيمي لجريمة التزوير الرقمي في القانون الجزائري

يشهد العالم المعاصر تحولاً رقمياً متسارعاً أعاد تشكيل البنية الاجتماعية والاقتصادية والقانونية للعلاقات البشرية، إذ أضحت المعطيات الرقمية والمحررات الإلكترونية محوراً أساسياً في التعاملات المدنية والتجارية والإدارية، ومع هذا التحول برزت جرائم معلوماتية جديدة تستهدف النزاهة والثقة في النظام الرقمي، تُعدّ جريمة التزوير الرقمي من أخطرها وأكثرها تعقيداً نظراً لما تُحدثه من خلخلة في اليقين القانوني الذي تستند إليه المحررات الإلكترونية كوسيلة إثبات.

وقد اقتضت طبيعة هذه الجريمة تدخلاً تشريعياً خاصاً يتجاوز الأطر التقليدية التي كانت تحكم جريمة التزوير في المحررات الورقية، إذ استوجب الأمر مواكبة التطور التكنولوجي بإقرار نصوص جنائية تتصدى للسلوكيات الإجرامية المستحدثة، وفي هذا الإطار سارع المشرع الجزائري إلى وضع قواعد جنائية خاصة بجرائم المعلوماتية بموجب القانون رقم 09-04 المتعلق بالجريمة المعلوماتية، كما أسس لنظام المحرر الإلكتروني والتوقيع الإلكتروني بالقانون رقم 15-04 المؤرخ في 01 فيفري 2015، مما مكّن من الاعتراف بالقيمة القانونية للمحررات الرقمية وبالتالي توفير الحماية الجنائية لها ضد أشكال التلاعب والتزييف.

غير أن التحدي القانوني يظل قائماً في تحديد الأركان الموضوعية والشكلية لهذه الجريمة وفي ضبط العناصر المكونة لها في ظل خصوصية الوسيلة الإلكترونية التي تتميز بالسرعة والخفاء والانتقال عبر الحدود، مما يفرض إعادة النظر في المفاهيم الكلاسيكية للركن المادي والركن المعنوي والعلاقة السببية بينهما، كما يطرح النظام العقابي المقرر لهذه الجريمة إشكاليات تتعلق بملاءمة العقوبات لخطورة السلوك الإجرامي، ومدى فعالية التدابير الوقائية والتكميلية في الحد من انتشار هذه الظاهرة.

من هذا المنطلق يكتسي الفصل الأول أهمية بالغة في مذكرة البحث، إذ يرمي إلى تفكيك البناء القانوني لجريمة التزوير الرقمي وتحليل عناصرها العقابية انطلاقاً من التشريع الجزائري، ويهدف إلى رسم الإطار الموضوعي الذي تتحرك فيه هذه الجريمة، من خلال تحديد ماهيتها ومحلها والأركان المكونة لها، بما يمهد لدراسة الضمانات الإجرائية والآليات القضائية المقررة لمكافحتها في الفصول الموالية، فالإحاطة الدقيقة بالبنية الداخلية لهذه الجريمة وتمييزها عن الجرائم المعلوماتية الأخرى المجاورة يشكل شرطاً أساسياً لإعمال النصوص الجزائية على نحو سليم، ولتطوير استراتيجيات قانونية فعالة في مواجهة هذا النوع من الجريمة التي باتت تمثل تهديداً حقيقياً للأمن المعلوماتي والاستقرار الاقتصادي والاجتماعي.

المبحث الاول: ماهية التزوير الرقمي في التشريع الجزائري

تقتضي الدراسة الرصينة لجريمة التزوير الرقمي عدم الاكتفاء بالنظر اليها كجريمة تقنية بحتة، بل كاعتداء صارخ على "الثقة الرقمية" التي تسعى الدولة الجزائرية لتوطيدها، فبعد ان كان التزوير ينصب على المحررات الرقمية الملموسة، اضحى اليوم يستهدف الكيانات الافتراضية والبيانات المشفرة، وهو ما فرض على المشرع اعادة تكييف اركان هذه الجريمة بما يتلائم مع الطبيعة غير المادية للوسائط الحديثة.[1]

ان المشرع الجزائري، ومن خلال مجموعة من النصوص القانونية الصادرة في عام 2024، لاسيما القانون رقم 24-06 المؤرخ في 28 أفريل 2024 المعدل والمتمم للأمر رقم 66-156 المؤرخ في 8 جوان 1966 المتضمن قانون العقوبات، وضع حجر الاساس للاعتراف الكامل بالتعاملات الالكترونية، و هو ما استتبع بالضرورة تشديد الحماية الجنائية عليها بموجب القانون رقم 24-02 المؤرخ في 26فيفري2024 المتعلق بمكافحة التزوير واستعمال المزور، هذا الاخير لم يعد يفرق في العقاب بين تزوير المحرر الرقمي وتزوير المعطيات الرقمية، طالما ان النتيجة واحدة وهي تغيير الحقيقة لاحداث ضرر[2]، كما ان القانون رقم 26-02 المؤرخ في 17فيفري2026 المتعلق بالخدمات العامة لخدمات الثقة للمعاملات الالكترونية والتعريف الالكتروني جاء ليضفي صبغة "السيادة" على هذه الحماية، معتبرا ان سلامة البيانات الرقمية جزء لا يتجزأ من الامن القومي.

بناءا على ذلك، سنحاول في هذا المبحث فك التداخل المفاهيمي حول مفهوم التزوير الرقمي، وبيان محله الذي يميزه عن التزوير التقليدي، مع استعراض بعض صوره في الواقع العملي.

المطلب الاول: مفهوم التزوير الرقمي

يشكل ضبط "مفهوم التزوير الرقمي" حجر الزاوية في بناء الحماية الجنائية للمعلومات، اذ لم يعد التزوير مجرد عبث بمداد القلم او كشط للورق، بل اصبح سلوكا تقنيا يستهدف "البيانات" في جوهرها الرقمي، و تبرز الصعوبة المنهجية في تحديد هذا المفهوم نظرا لتعدد التسميات واختلاف الزوايا الفقهية والتشريعية في النظر

[1] خالد تومي، **تأثير الرقمنة على الثقة الرقمية في القانون الجزائري**، مجلة الحقوق و لعلوم السياسية، جامعة محمد لمين دباغين سطيف2، مجلد11، العدد1، سنة 2024، ص210.

[2] فتيحة معمري، **تحديات الامن السيبراني والسيادة الرقمية في ظل التشريع الجزائري الحديث**، مجلة الحقوق والعلوم السياسية، جامعة خنشلة، مجلد9، عدد2، جوان 2021، ص114.

اليه؛ فبينما يراه البعض امتدادا للتزوير التقليدي باليات حديثة، يعتبره المشرع الجزائري –خاصة في ظل التعديلات الاخيرة بموجب القانون رقم 24–06– جريمة قائمة بذاتها تستهدف سلامة الانظمة المعلوماتية.[1]

وعليه، سنعمل في هذا المطلب على تفكيك العناصر المكونة لهذا المفهوم من خلال ثلاثة فروع؛ نخصص الأول منها لتعريفه فقهيا وقانونيا، ثم ننتقل في الفرع الثاني لبيان خصائصه الجوهرية التي تميزه عن التزوير الرقمي، لنختم في الفرع الثالث بتحديد تقاطعاته وعلاقاته بالجرائم المعلوماتية الاخرى التي نصت عليها الترسانة القانونية الجزائرية الحديثة لعام 2026.

الفرع الاول: تعريف التزوير الرقمي

إنَّ تحديد حقيقة التزوير الرقمي يستوجب منا الانطلاق من التأصيل المفاهيمي لمصطلح "التزوير" في أصله اللغوي، وصولاً إلى صياغة تعريف اصطلاحي يواكب التحول الرقمي الذي شهده القانون الجزائري، وهو ما سنفصله وفق الآتي.

اولا: المدلول اللغوي

التزوير لغةً مصدره زور، بمعنى ساعده على تزوير الوثائق: تزييفها، تلفيقها، الاتيان بوثائق غير أصلية، ويقصد به تغيير الحقيقة ماديا أو معنويا بقصد الغش في سند او وثيقة من شأنه احداث ضرر، اي بمعنى اخر تقليد الشيء مع ادعاء أن هذا المزور هو الأصل مع انه ليس كذلك.[2]

ثانيا: المدلول الاصطلاحي

يقصد بالتزوير اضفاء مظهر غير حقيقي على الشيء بما يخالف حقيقته الاصلية، وذلك من خلال تغييره أو تحريفه أو تحسين صورته على نحو يؤدي الى تضليل الغير وحمله على الاعتقاد بصحته، ويتجسد التزوير في عادة صور، من أبرزها تزوير الوثائق والمحررات الرسمية أو العرفية، وكذلك الادلاء بشهادة الزور، حيث يتم تقديم معلومات أو بيانات غير مطابقة للحقيقة بقصد اظهارها بصورة صحيحة، كما قد يتحقق التزوير بادخال تعديل أو تغيير على الشيء في ذاته، سواء باعادة صياغته أو تزيينه بما يجعله مخالفا لواقعه الحقيقي.[3]

---

[1] عبد العزيز بن خدة، **الخصوصية الاجرامية لجرائم التزوير في المحررات الالكترونية**، مجلة الفقه و القانون، جامعة الوادي، مجلد10، عدد3، سنة2023، ص154.

[2] **معجم المعاني الجامع**، "تزوير"، تاريخ الاطلاع 12 مارس2026، على الساعة 22:02، عبر الرابط: https://www.almaany.com/ar/dict/ar-ar/تزوير/.

[3] بساحة سليمة، **جريمة التزوير الالكتروني**، مذكرة ماستر في القانون القضائي، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس، مستغانم، 2025، ص 03.

ويرتبط مفهوم التزوير في معناه اللغوي بمعاني التزيين والتحسين، أي اظهار الشيء في صورة حسنة رغم عدم مطابقته للحقيقة، كما يدل لفظ "الزور" على الميل والانحراف عن الحق، ومنه أطلق على الكذب والباطل لكونه خروجا عن الحقيقة وتزييفا لها.[1]

ثالثا: التعريف الفقهي للتزوير

تعددت اجتهادات الفقه في تحديد مفهوم التزوير، غير أنها تتفق في جوهرها على أنه فعل يقوم على تغيير الحقيقة في محرر أو واقعة معينة بقصد الغش، وبطريقة من شأنها أن تؤدي الى الحاق الضرر بالغير فقد عرفه بعض الفقه بأنه تغيير للحقيقة في محرر باحدى الطرق التي يحددها القانون، وذلك بقصد الغش و بما يمكن أن يترتب عنه ضرر، كما عرف أيضا بأنه تحريف للحقيقة في محرر يتعلق بواقعة أعد هذا المحرر لاثباتها، متى تم هذا التغيير بقصد الغش وكان من شأنه احداث ضرر للغير.[2]

كما ذهب بعض الفقه الى تعريف التزوير بأنه تغيير للحقيقة في محرر تغييرا متعمدا يتضمن قصدا جنائيا، ويتم باحدى الوسائل التي نص عليها القانون، بحيث يؤدي هذا التغيير الى الحاق الضرر أو احتمال وقوعه[3]، ويتضح من هذه التعريفات أن جوهر جريمة التزوير يتمثل في المساس بسلامة المحررات والثقة التي يوليها الأفراد لها في المعاملات القانونية.

ومع التطور التكنولوجي واتساع نطاق التعاملات الالكترونية، لم يعد التزوير مقتصرا على المحررات التقليدية، بل امتد ليشمل المحررات الالكترونية والبيانات الرقمية ووسائل الدفع الحديثة، فقد أصبح من الممكن ارتكاب التزوير عن طريق التلاعب بالمعلومات أو تعديل البيانات الواردة في المستندات الالكترونية أو وسائل الدفع الالكترونية، مثل الشيكات الالكترونية وغيرها من أدوات الدفع الرقمية المنتشرة في المعاملات الحديثة[4].

كما ظهرت أنظمة حديثة لتحويل الأموال تعتمد على الوسائط الالكترونية، مثل أنظمة التحويل عبر الشبكات المعلوماتية أو بطاقات الدفع الالكترونية أو العملات الرقمية، وهي بدورها قد تكون محلا لجريمة التزوير الرقمي، وتتحقق هذه الجريمة عادة من خلال ادخال بيانات غير صحيحة، أو تعديل المعلومات المخزنة في النظام المعلوماتي، أو تغيير التوقيع الالكتروني، أو حذف بعض العبارات الجوهرية من المستند الالكتروني بما يؤدي الى تغيير مضمونه الحقيقي أو اخفاء معلومات مؤثرة في قيمته القانونية[5].

---

[1] **المرجع نفسه**، ص03.

[2] محمود نجيب حسني، **شرح قانون العقوبات–القسم الخاص**، الطبعة السادسة، دار النهضة العربية، القاهرة، سنة 1989، ص312 .

[3] Garçon émile**, Code pénal annoté**, Tome 02, Librairie du Recueil Sirey, Paris, 1956, p425.

[4] محمد سعيد نمور، **جرائم الحاسوب والانترنت**، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، سنة 2010، ص 147.

[5] احمد فتحي سرور، **الوسيط في قانون العقوبات–القسم الخاص**، الطبعة الرابعة، دار النهضة العربية، القاهرة، سنة 2006، ص 455.

وفي هذا السياق عرف الفقيه علي عبد القادر القهوجي التزوير الالكتروني بأنه تغيير للحقيقة يرد على مخرجات الحاسوب، سواء تجسدت في مستندات ورقية مطبوعة أو بيانات رقمية محفوظة على دعامة الكترونية، شريطة أن يكون لهذا المحرر أثر في اثبات حق أو ترتيب أثر قانوني[1]، أما الفقه الفرنسي فقد عرف التزوير في المحررات بأنه تغيير للحقيقة في الوقائع التي أعد المحرر لاثباتها، متى تم ذلك بقصد الغش وكان من شأنه احداث ضرر، وهو التعريف الذي تبناه جانب معتبر من الفقه الفرنسي والمصري في دراساتهم القانونية المتعلقة بجريمة التزوير[2].

رابعا: التعريف القانوني للتزوير الرقمي في ظل التوجه التشريعي الحديث

ان المشرع الجزائري لم يعط تعريفا محددا لجريمة التزوير وانما اشار اليها من خلال الافعال المادية في النصوص القانونية حيث عبر عنها كما يلي:"...كل من قلد أو زور أو زيف..."،"...أو من استعمل..."،"...كل من زاد من قيمة..."،"...كل من قلد أو اصدر...أو باع أو روج أو وزع..."،"...كل من وضع توقيعا أو أحدث تغييرا أو انتحل شخصية أو اصطنع اتفاقية أو ادرج شروطا أو اسقطها، أو ادلى بتصريح كاذب"، هذه كلها مصطلحات أدرجها المشرع الجزائري في تعريف جريمة التزوير، بحيث يتضح لنا جليا أن التزوير هو تغيير الحقائق بقصد الغش أو الكذب سواء أكان هذا التغيير في النقود أو الأختام والطوابع والدمغات والعلامات أو المحررات والوثائق والشهادات، و سواء أكان هذا التغيير بالكتابة أو بالرسوم أو بالاشارات والرموز أو الشكل العام، وغالبا ما يلجأ الجاني الى مثل هذه الافعال لتحقيق المصلحة الخاصة له.[3]

ان تكييف التزوير الرقمي كجريمة قائمة بذاتها في التشريع الجزائري يجد أساسه في كون "البيان المعلوماتي" قد أضحى يتمتع بنفس الحجية القانونية الذي يتمتع بها المحرر الورقي، فبالاستناد الى المادة 394 مكرر 1 من قانون العقوبات التي تنص على: "...كل من أدخل بطريق الغش معطيات في نظام المعالجة الالية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها."[4]، وبقراءة تحليلية لنصوص القانون رقم 24-02 المؤرخ في 26 فيفري 2024 المتعلق بمكافحة التزوير واستعمال المزور، يظهر ان المشرع قد وسع من مفهوم

---

[1] علي عبد القادر القهوجي، **قانون العقوبات-القسم الخاص**، الطبعة الأولى، الدار الجامعية، الاسكندرية، سنة 2003، ص 389.

[2] Jean Pradel, **Droit pénal spécial**, 16e édition, Cujas, paris, 2011, p 503.

[3] اية الوصيف، **جرائم التزوير في القانون الجزائري**، موقع محاماة نت، بتاريخ 12 أكتوبر 2019، اطلع عليه بتاريخ 9 مارس 2026، الساعة 02:37، عبر الرابط: https://www.mohamah.net.

[4] المادة 394 مكرر 1 من الامر رقم 66-156 المؤرخ في 8 جوان 1966 المتضمن قانون العقوبات ، المعدل والمتمم بموجب القانون رقم 24-06 المؤرخ في 28 افريل 2024 ، الجريدة الرسمية للجمهورية الجزائرية ، العدد 30، مؤرخ في 30 أفريل 2024.

الركن المادي لجريمة التزوير؛ فلم يعد يشترط "الافراغ المادي" للحقيقة على دعامة ورقية، بل اعتبر ان مجرد ادخال معطيات وهمية، أو تعديل بيانات صحيحة داخل نظام معالجة الية، هو فعل كاف لقيام الجريمة.[1]

ويكمن الفرق الجوهري من الناحية القانونية في ان التزوير الرقمي هو "تزوير معنوي" بطبيعته، لانه ينصب على محتوى المعلومة الرقمية لا على هيكلها المادي، وهو ما دفع المشرع بموجب التعديلات لعام 2024و2026 الى تشديد الرقابة الاجرائية على وسائل الدفع الالكتروني والتوقيعات الرقمية، معتبرا أن أي مساس بسلامة هذه البيانات يعد تقويضا للثقة الرقمية التي تعد امتدادا للثقة العامة التقليدية[2]، وقد عرفته اتفاقية مجلس أوروبا للجرائم الالكترونية (2001) في المادة 7 بأنه:" ادخال، أو اتلاف بيانات كومبيوتر، بشكل يجعل بيانات غير أصلية تبدو أصلية بقصد اعتبارها أو استخدامها لأغراض قانونية، بغض النظر عما اذا كانت تلك البيانات قابلة للقراءة والفهم بشكل مباشر أم لا[3]"، وعليه يمكننا تعريف التزوير عموما بأنه: "تشويه وتغيير متعمد للحقيقة في الأقوال أو الأفعال بهدف الاضرار بالغير".[4]

الفرع الثاني: الخصائص المميزة للتزوير الرقمي عن التزوير التقليدي

بالرغم من اشتراك التزوير الرقمي مع التزوير التقليدي في "العلة" وهي تغيير الحقيقة، الا أن الأول ينفرد بخصائص ذاتية مستمدة من طبيعة الوسط الذي يقع فيه، وهو "الفضاء السيبراني"، ان خروج الجريمة من حيز الماديات الملموسة الى حيز النبضات الالكترونية أضفى عليها سمات فنية واجرائية معقدة؛ فبينما يترك التزوير الورقي اثار مادية يمكن كشفها بالخبرة الفنية التقليدية (كالكشط والمحو المادي)، يتميز التزوير الرقمي ب"اللامادية" وسهولة طمس الأدلة.[5]

هذه الخصوصية هي التي جعلت من مكافحته أمرا يتجاوز الأساليب التقليدية للضبط القضائي، مما دفع المشرع الجزائري في تعديلات 2024 و2026 الى اقرار اليات اجرائية خاصة تتماشى مع سرعة التنفيذ وصعوبة اثبات الأثر، والطبيعة العابرة للحدود التي تصبغ هذا النوع من الجرائم[6]، وعليه سنعمل في هذا الفرع على تحليل ابرز هذه الخصائص التي تمنح التزوير الرقمي خطورته الاجرامية المستحدثة.

---

[1] عبد الرزاق بن خيرة، **الحماية الجنائية للمحررات الالكترونية في ظل القانون 04-15 والقوانين المكملة له**، مجلة المفكر، جامعة بسكرة مجلد 16، العدد 2، سنة 2021، ص 142،

[2] قانون رقم 24-02 المؤرخ في 26 فيفري 2024، يتعلق بمكافحة التزوير واستعمال المزور، ج.ر، عدد 15، 29 فيفري 2024,

[3] Council of Europe**, Convention on Cybercrime (Budapest Convention),** 2001, Article 7.

[4] جمال نجيمي، **جرائم التزوير في قانون العقوبات الجزائري**، دار هومة، الطبعة الثانية، الجزائر، 2014، ص07.

[5] محمد بودالي، **الجريمة المعلوماتية في القانون الجزائري**، مجلة الفقه و القانون، جامعة الوادي، المجلد11، العدد01، سنة 2012، ص95.

[6] قانون رقم 24-02 المؤرخ في 26 فيفري 2024، يتعلق بمكافحة التزوير و استعمال المزور، ج.ر، عدد 15، 29 فيفري 2024,

اولا: تعدد وتنوع مراحل الاعتداء على الحقيقة الرقمية

تنفرد جريمة التزوير الرقمي بخاصية اجرائية وفنية دقيقة، وهي امكانية تحقق ركنها المادي في أي مرحلة من مراحل تشغيل نظام المعالجة الالية للبيانات، فخلافا للتزوير التقليدي الذي يقع عادة على المحرر بعد اكتماله أو أثناء صياغته المادية، فان النسق الرقمي يسمح يسمح للجاني بالتدخل في ثلاث محطات أساسية:

1. مرحلة الادخال(Input): وتعتبر من أكثر المراحل شيوعا، حيث يتم تغذية النظام بمعلومات غير صحيحة أو اغفال ادخال بيانات جوهرية، وهو ما يعرف "بالتزوير المعنوي الرقمي"، و مثال ذلك قيام الموظف المختص بادراج أسماء وهمية في قاعدة بيانات الرواتب أو المنح، مما يؤدي الى توليد مخرجات (صكوك أو كشوف) مزورة في محتواها رغم سلامة شكلها التقني.

2. مرحلة المعالجة البرمجية (Processing): وتتمثل في التلاعب بالخوارزميات أو التعليمات البرمجية التي تقوم بتحليل البيانات؛ حيث يتم توجيه النظام لاعطاء نتائج مخالفة للحقيقة (مثل تعديل معادلة حسب الفوائد البنكية لتعمل لصالح الجاني)، وهنا يكون التزوير منصبا على "العملية المنطقية" للنظام ذاته.

3. مرحلة الاخراج (Output): وتتحقق عند التلاعب بالنتائج النهائية التي تظهر على الشاشة أو التي يتم طباعتها، من خلال اعتراض تدفق البيانات قبل وصولها الى وسيط الاخراج النهائي وتبديلها بمعطيات مزورة، مما يفقد المحرر الالكتروني مصداقيته و حجيته القانونية.

ان هذا التعدد في نقاط الاختراق يمنح التزوير الرقمي "مرونة جرمية" تجعل من الرقابة التقنية و التدقيق المعلوماتي أمرا بالغ الصعوبة، حيث يمتزج الفعل الجرمي بالعمليات التقنية المشروعة للنظام، مما يستوجب تتبع الأثر الرقمي (Log Files) في كل مرحلة على حدة لاثبات واقعة تغيير الحقيقة.[1]

علاوة على ما سبق، فان خطورة التزوير في مراحل المعالجة الالية تكمن في خاصية "التخفي والاندماج التقني"؛ اذ غالبا ما يمتزج فعل تغيير الحقيقة بالعمليات البرمجية المشروعة للنظام، مما يجعل الجريمة غير مرئية حتى بالنسبة للمستخدمين المتخصصين[2]، فخلافا للتزوير التقليدي الذي يترك أثرا ماديا كالكشط أو

[1] عمر عبد السلام حسن الجبوري، **جريمة تزوير الالكتروني في تشريع الاردني دراسة مقارنة**، رسالة ماجستار، جامعة شرق الاوسط، كلية الحقوق، 2017، الأردن، ص17.

[2] بلقاسم بوزيدي، **السياسة الجنائية لمواجهة جرائم التزوير المعلوماتي في التشريع الجزائري**، مجلة الدراسات الحقوقية، جامعة سعيدة، المجلد08، العدد02، ص418.

التحشير، فان التلاعب في مرحلة المعالجة (Processing) قد يتم عبر "أكواد برمجية" مؤقتة تحذف تلقائيا بعد أداء مهمتها الجرمية، و هو ما يمنح الجاني القدرة على تضليل الرقابة القضائية والتقنية لفترات زمنية طويلة.[1]

هذا و تجدر الاشارة الى أن المشرع الجزائري، ومن خلال القوانين الحديثة لاسيما القانون رقم 24-02 المؤرخ في 26 فيفري 2024 المتعلق بمكافحة التزوير واستعمال المزور، أدرك أن تتبع هذه المراحل يتطلب "تفتيشا رقميا" دقيقا يمتد ليشمل قواعد البيانات و سجلات النظام (Log Files)، بالنظر الى أن التزوير الرقمي في أي مرحلة من هذه المحطات يعد مساسا مباشرا بسلامة ومصداقية المعطيات، و هو ما يجعل وصف الجريمة يتراوح بين التزوير المعلوماتي و المساس بأنظمة المعالجة الالية وفقا للمادة 394 مكرر 1 من قانون العقوبات.[2]

ثانيا: انعدام الأثر المادي الملموس للفعل الجرمي

تتمثل السمة الأبرز لهذا الجرم في كونه يستهدف محلاً "غير ملموس"، فبينما يقع التزوير التقليدي على دعامة مادي (ورق)، ينصب التزوير الرقمي على "نبضات الكترونية" مشفرة داخل نظام المعالجة الآلية [3]، ومن وجهة نظرنا، فإن هذه الخاصية تمنح الجاني ميزة "الخفاء التقني"؛ إذ يمكنه تحريف الحقيقة دون ترك أثر مادي مرئي (المحو)، مما يجعل الدليل الرقمي دليلاً هشا وقابلاً للتغيير بسرعة فائقة إذا لم يتم ضبطه وفق معايير فنية صارمة.

وعليه، فان هذه الخاصية تفرض تحديا مزدوجا امام جهات التحقيق؛ فمن جهة، لا يمكن معاينة التزوير بالعين المجردة، و من جهة اخرى، فان استخراج الدليل يتطلب فحصا فنيا معمقا لسجلات النظام (System Logs) للكشف عن اي تعديلات غير مشروعة طرأت على البيانات الأصلية، وهذا ما دفع المشرع الجزائري في القوانين الحديثة (خاصة القانون24-02) الى التأكيد على دور الخبرة الرقمية كالية وحيدة لتعويض غياب الاثر المادي الملموس في هذا النوع من الجرائم.[4]

---

[1] عبد العزيز بن خدة، **الخصوصية الاجرامية لجرائم التزوير في المحررات الالكترونية**، مجلة الفقه والقانون، جامعة الوادي، المجلد10، العدد03، ص159.

[2] المادة 394 مكرر 1 من الامر رقم 66-156 المؤرخ في 8 جوان 1966 المتضمن قانون العقوبات ، المعدل والمتمم بموجب القانون رقم 24-06 المؤرخ في 28 افريل 2024 ، الجريدة الرسمية للجمهورية الجزائرية ، العدد 30 ، 30 أفريل 2024,

[3] زيدان زبيحة ، **الجريمة المعلوماتية في التشريع الجزائري و الدولي** ، دار الهدى ، د.ط، الجزائر ، 2011، ص58.

[4] بلقاسم بوزيدي، **السياسة الجنائية لمواجهة جرائم التزوير المعلوماتي في التشريع الجزائري**، مجلة الدراسات الحقوقية، جامعة سكيكدة، المجلد08، العدد02، ص420.

ثالثا: تفرد شخصية المجرم و دوافعه

ترتكب جريمة التزوير الالكتروني بوسائل تقنية، و لذلك يحتاج مرتكبيها الى خبرة و لتخصص في المجال الالكتروني لانه سيتعامل مع جهاز الكمبيوتر، و نظام المعالجة الالية للبيانات، فقد يكون هذا المجرم الالكتروني من الموظفين المتخصصين في مجال الحاسب الالي وهم يحتلون المرتبة الأولى بين مجرمي المعلوماتية، أو من القراصنة أو من المحترفين وهم أشخاص يستغلون الحاسب الالي و لكن بشكل غير قانوني وهم فئتين الهاكرز القراصنة الهواة والكراكرز وهم القراصنة المحترفون.[1]

رابعا: خاصية العبور للحدود الوطنية (عولمة الجريمة)

على خلاف التزوير الورقي الذي يظل مرتبطاً بالحيز الجغرافي لوجود الوثيقة، يتسم التزوير الرقمي بطابع "كوني"؛ إذ يمكن تنفيذ الركن المادي للجريمة من دولة، بينما تتحقق النتيجة الإجرامية في نظام معلوماتي بدولة أخرى، وما نلاحظه في هذا الصدد، أن المشرع الجزائري في القانون 24-06 المؤرخ في 28 أفريل 2024 قد فطن لخطورة هذه الخاصية، حيث اعتبر أن المساس بالأنظمة المعلوماتية الوطنية يعد مساساً بالسيادة الرقمية، وهو ما يبرر بسط الاختصاص القضائي الجزائري على جرائم قد يكون فاعلها خارج الحدود الوطنية، تكريساً لمبدأ عالمية العقاب في الفضاء الافتراضي.[2]

الفرع الثالث: تمييز التزوير الرقمي عن الجرائم المعلوماتية الاخرى

تتقاطع جريمة التزوير الرقمي مع طائفة من الجرائم المعلوماتية المستحدثة في قانون العقوبات، إلا أنَّ هذا التقاطع لا يعني الوحدة؛ بل تحتفظ كل جريمة بذاتية مستقلة من حيث الركن المادي والقصد الجنائي، وسنحاول تبيان هذا التمايز من خلال النقاط الآتية:

أولا: التمييز بين جريمة التزوير الرقمي و جريمة الاحتيال المعلوماتي

يعرف التزوير الرقمي بأنه:" الادخال أو التغيير أو الحذف أو اخفاء بيانات الحاسوب عن عمد ودون حق، مما يؤدي الى بيانات غير أصلية، بهدف اعتبارها أو التصرف بناء عليها لأغراض قانونية كما لو كانت أصيلة."[3] ، وقد نصت هذه الجريمة المادة 394 مكرر1 من قانون العقوبات الجزائري (الامر 66-156

[1] بساحة سليمة، **جريمة التزوير الالكتروني**، مذكرة ماستر في القانون القضائي، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس، مستغانم، 2025، ص10 .

[2] المادة 2 من القانون رقم 24-06 المؤرخ في 28 افريل 2024 ، المعدل و المتمم للامر 66-156 المتضمن قانون العقوبات ، الجريدة الرسمية للجمهورية الجزائرية ، العدد 30 ، 30 أفريل 2024.

[3] اية بن ميسية، **الجريمة الالكترونية واليات مكافحتها في التشريع الجزائري**، مذكرة ماستر في القانون الجنائي، معهد الحقوق، المركز الجامعي عبد الحفيظ بوالصوف ميلة، 2025، ص35.

المؤرخ في 8 جوان 1966 المعدل و المتمم) التي جاء فيها:" يعاقب بالحبس من ستة (6) أشهر الى ثلاث (3) سنوات وبغرامة من 500.000 دج الى 2.000.000 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الالية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها."[1]

أما الاحتيال المعلوماتي فيعرف بأنه:" كل فعل احتيالي يتم باستخدام تقنيات المعلومات و الاتصال بهدف الحصول على منافع مالية أو معنوية غير مشروعة."[2] ، وقد نظمته المادة 394 مكرر 2 من قانون العقوبات الجزائري التي نصت على :" يعاقب بالحبس من شهرين الى ثلاث سنوات و بغرامة من 1.000.000 دج الى 5.000.000 دج لكل من قام عمدا و بطريق الغش بتصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية."[3]

من خلال استقرائنا للمعايير الفاصلة بين الجريمتين، يمكننا القول ان وجه الاختلاف الجوهري يكمن في "المصلحة المحمية"؛ فبينما يهدف التزوير الرقمي الى حماية "صدقية المعطيات" وصحتها كهدف بذاته، نجد أن الاحتيال المعلوماتي يتجاوز ذلك ليجعل من المعطيات مجرد وسيلة لاستهداف "الأموال والمصالح المالية" للضحية.

ويظهر هذا الاحتيال جليا في الركن المادي؛ حيث يقتصر التزوير على العمليات التقنية الماسة بالبيانات (تغيير، حذف)، بينما يتسع الاحتيال ليشمل أفعالا تداولية (نشر، اتجار، توفير)، كما يمتد الخلاف ليشمل النتيجة الاجرامية؛ فالتزوير يكتمل بجرد خلق واقعة رقمية للحقيقة، في حين أن الاحتيال يتطلب بالضرورة وقوع ضرر مالي أو معنوي بالغير، ولا يفوتنا ملاحظة التباين في السياسة العقابية، حيث نجد أن المشرع رفع سقف الغرامة المالية في جريمة الاحتيال بشكل ملحوظ مقارنة بالتزوير، نظرا للطبيعة النفعية لهذه الجريمة.[4]

بالرغم من وضوح النصوص النظرية، الا أننا نرى من خلال هذا التحليل وجود تداخل اجرامي دقيق؛ فالتزوير الرقمي غالبا ما يمثل "مرحلة تمهيدية" أو وسيلة ضرورية لتنفيد جريمة الاحتيال المعلوماتي، هذا

---

[1] المادة 394 مكرر 1 من الامر رقم 66-156 المؤرخ في 8 جوان 1966 المتضمن قانون العقوبات ، المعدل والمتمم بموجب القانون رقم 24-06 المؤرخ في 28 افريل 2024 ، الجريدة الرسمية للجمهورية الجزائرية ، العدد 30 ، سنة2024.

[2] **مقال: بحث و دراسة حول الجرائم الالكترونية وأنواعها والاجراءات القانونية لمكافحتها**، صادر عن الموقع السوري للاستشارات والدراسات القانونية، اطلع عليه بتاريخ 15 مارس 2026، على الساعة 20:55، الرابط:www.syrianalaw.net

[3] المادة 394 مكرر2، من الامر رقم 66-156 المؤرخ في 8 جوان 1966 المتضمن قانون العقوبات ، المعدل والمتمم بموجب القانون رقم 24-06 المؤرخ في 28 افريل 2024 ، الجريدة الرسمية للجمهورية الجزائرية ، العدد 30 ، 30 أفريل 2024.

[4] شيخ سناء وشيخ محمد زكرياء، **مكافحة الجرائم الالكترونية في القانون الجزائري** ، تم الاطلاع عليه يوم 16 مارس 2026، على الساعة 00:06، متاح على الرابط:https://wameedalfiker.com

التداخل يطرح اشكالا قضائيا في التكييف القانوني عند وقوع ضرر مالي ناتج عن تزوير بيانات؛ فهل نطبق نص المادة 394 مكرر 1 باعتبارها "الوسيلة"، أم المادة 394 مكرر 2 باعتبارها "الغاية"؟[1]

ان هذا الاشكال لا يقتصر على التشريع الوطني فحسب، بل هو محل نقاش دولي؛ حيث حاولت اتفاقية بودابست (2001) فض هذا النزاع عبر المادتين 7و8، مفرقة بين التزوير المتعلق بالحاسوب (Computer-related Forgery) والاحتيال المتعلق به (Computer-related Fraud)، وهو المنهج الذي سار عليه المشرع الفرنسي أيضا في المادتين 323-3 من قانون عقوباته، مع تشديده للعقوبات المالية لتصل الى 150.000 يورو[2]، وفيما يخص موقف الجزائر من هذا الاطار الدولي، تجدر الاشارة الى أن الدولة الجزائرية لم تصادق على اتفاقية بودابست (2001) حتى الان، ويعود عدم الانضمام الى تحفظات تتعلق بالسيادة الوطنية، خاصة ما يتعلق بالوصول العابر للحدود الى البيانات المخزنة، مفضلة بذلك الاعتماد على ترسانتها القانونية الخاصة أو التوجه نحو صياغة اتفاقية أممية شاملة تضمن توازنا أكبر بين مكافحة الاجرام وحماية الخصوصية.

ومنه يمكن القول أن المشرع الجزائري، ومن خلال القانون 09-04 المؤرخ في 5 أوت 2009 والمتعلق بالوقاية من الجرائم المرتبطة بتكنولوجيا الاعلام والاتصال ومكافحتها، حاول ارساء قواعد وقائية متينة، الا أن الحاجة تبقى قائمة لتدقيق المصطلحات المتعلقة ب"الغش المعلوماتي" لفك الارتباط بين التزوير كوسيلة والاحتيال كغاية، تفاديا لأي لبس في التكييف القضائي يخدم الجاني على حساب الضحية[3].

ثانيا: التمييز بين جريمة التزوير الرقمي وجريمة المساس بأنظمة المعالجة الالية للبيانات

عند النظر في ماهية التزوير الرقمي، نجد أنه ينصرف أساسا الى "تزييف الحقيقة الرقمية"؛ حيث يعرف بأنه الادخال أو التغيير أو الحذف أو الاخفاء العمدي لبيانات الحاسوب بهدف خلق بيانات غير أصيلة يعتد بها قانونا كأنها صحيحة، وقد جسد المشرع الجزائري هذا المفهوم في المادة 394 مكرر 1 من قانون العقوبات (المعدل بالقانون 24-06)، معاقبا بالحبس من سنة الى 3 سنوات كل من عبث بالمعطيات بطريق الغش، مبررا بذلك خطورة المساس بصدقية البيانات[4].

---

[1] بوبكر رشيدة، **المرجع السابق**، ص 45.

[2] **Convention on Cybercrime (Budapest Convention),** 2001, Articles 7 &8 ; Code pénal français, Articles 323-1 à 323-3.

[3] القانون 09-04 المؤرخ في 5 أوت 2009 المتعلق بالوقاية من الجرائم المرتبطة بتكنولوجيات الاعلام والاتصال لمكافحتها، الجريدة الرسمية، العدد 47، الصادر بتاريخ 16 أوت 2009.

[4] المادة 394 مكرر 1 من الأمر رقم 66-156 المؤرخ في 8 جوان 1966 المتضمن قانون العقوبات ، المعدل والمتمم بموجب القانون رقم 24-06 المؤرخ في 28 أفريل 2024 ، الجريدة الرسمية للجمهورية الجزائرية ، العدد 30 ، الصادر بتاريخ 30 أفريل 2024.

أما جريمة المساس بأنظمة المعالجة الالية للبيانات أو ما يعرف بالولوج غير المشروع فتعرف بأنها:" كل فعل يهدف الى الدخول أو البقاء عن طريق الغش في كل جزء من منظومة للمعالجة الالية للمعطيات، بما في ذلك محاولات الولوج والتدخل في طريقة سير المنظومة."[1]، وقد نظمها القانون الجزائري في المادتين 394 مكرر و 394 مكرر 1 من قانون العقوبات اللتان نصتا على:" يعاقب بالحبس من ستة (6) أشهر الى سنتين (2) وبغرامة من 60.000 دج الى 200.000 دج، كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الالية للمعطيات أو يحاول ذلك، تضاعف العقوبة اذا ترتب على ذلك حذف أو تغيير المعطيات المنظومة، واذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة، تكون العقوبة الحبس من سنة (1) الى ثلاث (3) سنوات والغرامة من 100.000 دج الى 300.000 دج."[2]

من خلال تحليلنا للمادة الاجرامية للجريمتين، يمكننا استخلاص فوارق جوهرية، فمن حيث المصلحة المحمية، نجد أن التزوير الرقمي يحمي "صحة وسلامة المعطيات"، بينما يحمي المساس بالنظام "سرية وسلامة المنظومة" في حد ذاتها، ويظهر هذا التباين جليا في النتيجة الاجرامية؛ فالتزوير يكتمل بحدوث تزييف في البيانات دون اشتراط تعطل النظام، في حين أن جريمة المساس بالنظام تقتضي بالضرورة حدوث اختراق أو اعاقة أو اتلاف فعلي للمنظومة[3]، كما نلاحظ اختلافا في السياسة العقابية؛ حيث جعل المشرع الجزائري عقوبة التزوير الأساسية أشد من عقوبة الولوج الأساسي للنظام، وهو توجه يختلف عن بعض التشريعات المقارنة كالقانون الفرنسي الذي يشدد في عقوبات الولوج والبقاء غير المشروع في المواد 323- ومايليها[4]، وهذا يعكس تقدير المشرع الجزائري بأن خطر تزييف المعطيات الرقمية وما يترتب عليه من ضياع للحقوق أشد جسامة من مجرد الولوج غير المرخص.[5]

بالرغم من هذا الفصل النظري، الا أننا نرى وجود فجوة في التطبيق القضائي ناتجة عن التداخل بين المرحلة التمهيدية والتنفيذية؛ فالولوج غير المشروع يمثل عادة "المعبر الضروري" لارتكاب التزوير الرقمي، وان استخدام المشرع لعبارة "بطريق الغش" في الجريمتين يضاعف من صعوبة التمييز، خاصة وأن عقوبة التزوير الرقمي من حيث الغرامة هي أشد بكثير من غرامة تخريب النظام، مما يظهر بوضوح أن المشرع يولي حماية

[1] مكري ايمان، **الجريمة الالكترونية في التشريع الجزائري**، رسالة ماجستير، جامعة الجزائر3، سنة 2016، ص67.

[2] المادة 394 مكرر و ما يليها من الأمر رقم 66-156 المؤرخ في 8 جوان 1966 المتضمن قانون العقوبات ، المعدل والمتمم بموجب القانون رقم 24-06 المؤرخ في 28 أفريل 2024 ، الجريدة الرسمية للجمهورية الجزائرية ، العدد 30 ، الصادر بتاريخ 30 أفريل 2024.

[3] سيق الدين الخليفي واخرون، **حماية المعطيات الشخصية في زمن الذكاء الاصطناعي**، ماستر قانون العقود والانظمة العقارية، كلية العلوم القانونية والاقتصادية والاجتماعية، ماي 2025، ص 38.

[4] **Code pénal français**, Articles 323-1 & 323-3 (modifiér par le loi n° 2015-912 du 24 juillet 2015).

[5] يوسف حمداني، **تطور الجرائم الالكترونية في الجزائر**، مجلة القانون والمجتمع، العدد 45، 2025، ص 34.

"أصالة البيانات" ثقلا ماليا كبيرا[1]، ويؤيد هذا الطرح التوجه الدولي في اتفاقية بودابست (2001)، التي فصلت بين التزوير والولوج والتخريب[2]، وهو المنهج الذي نأمل أن يكرسه الاجتهاد القضائي الجزائري لفك هذا التداخل وتجنب العقوبات المزدوجة على فعل اجرامي واحد.

ثالثا: تمييز جريمة التزوير الرقمي بين جرائم الهوية الرقمية

من وجهة نظرنا، يمثل التزوير الرقمي ذروة الاعتداء المادي على الحقيقة الرقمية، حيث يستهدف الجاني هنا "البيان" في ذاته لجعله ناطقا بغير الحقيقة، وقد حسم المشرع الجزائري هذا المفهوم في المادة 394 مكرر 1 من قانون العقوبات (الأمر 66-156 المعدل بالقانون 24-06)[3]، حيث يبرز هذا النص القانوني بوضوح أن المصلحة المحمية هنا هي "أصالة المعطيات"؛ فالتزوير يكتمل بمجرد تغيير الحقيقة في النظام المعلوماتي بطريقة احتيالية، مما ينتج عنه بيانات غير أصيلة يعتد بها قانونا، وبتحليلنا لهذا النص، نجد أن المشرع الجزائري قد شدد العقوبة المالية في التعديل الأخير لتصل الى 2.000.000 دج، وهو ما يعكس جسامة الضرر الناتج عن تزييف الأدلة الرقمية في المعاملات القانونية.[4]

على خلاف التزوير، تذهب جرائم الهوية الرقمية لاستهداف "الذات الانسانية" في تمظهرها الافتراضي؛ فهي تشمل سرقة الهوية وانتحال الشخصية الرقمية، ومن خلال ملاحظاتنا البحثية، نرى أن المشرع الجزائري لم يفرد لها نصا مستقلا تحت هذا المسمى، بل عالج مظاهرها عبر نصوص عامة في قانون العقوبات، لاسيما المادة 249 المتعلقة بانتحال الصفة، والتي تنص على: "كل من انتحل اسم الغير، في ظروف أدت الى قيد حكم في صحيفة السوابق القضائية لهذا الغير أو كان من الجائز أن تؤدي الى ذلك، يعاقب بالحبس من سنة(1) الى خمس (5) سنوات وبغرامة من 100.000 دج الى 500.000 دج، دون الاخلال باتخاد اجراءات المتابعة ضده بشأن جناية التزوير اذا اقتضى الحال ذلك."[5]

[1] سارة العبيدي، **المرجع السابق**، ص68.

[2] **Convention on Cybercrime (Budapest Convention),** 2001, Articles 2-5-7.

[3] المادة 394 مكرر 1 من الأمر رقم 66-156 المؤرخ في 8 جوان 1966 المتضمن قانون العقوبات ، المعدل والمتمم بموجب القانون رقم 24-06 المؤرخ في 28 أفريل 2024 ، الجريدة الرسمية للجمهورية الجزائرية ، العدد 30 ، الصادر بتاريخ 30 أفريل 2024.

[4] Zerrouki Assia & Hamel Mohamed, **"Cybercrime Follow-up Procedures : A Comparative Study of Algeria and Qatari Legislation"**, Journal of Legal Studies, University og Ghardaia, 2024, P 45.

[5] المادة 249 من الأمر رقم 66-156 المؤرخ في 8 جوان 1966 المتضمن قانون العقوبات ، المعدل والمتمم بموجب القانون رقم 24-06 المؤرخ في 28 أفريل 2024 ، الجريدة الرسمية للجمهورية الجزائرية ، العدد 30 ، الصادر بتاريخ 30 أفريل 2024.

من خلال المقارنة التحليلة، أستطيع استخلاص معيار جوهري للتمييز: فالتزوير الرقمي هو اعتداء على "الشيء" (البيانات)، بينما جرائم الهوية هي اعتداء على "الشخص" (المركز القانوني)، في التزوير تكون الضحية هي "الثقة العامة في البيانات"، بينما في جرائم الهوية تكون الضحية هي "الانسان في هويته وخصوصيته".[1]

كما نسجل ملاحظة نقدية حول تداخل الجريمتين، فالتزوير الرقمي قد يكون "الوسيلة" (مثل تزوير توقيع الكتروني) بينما سرقة الهوية هي "الغاية" (تقمص شخصية صاحب التوقيع)، ويؤيد هذا الطرح التوجه الدولي في اتفاقية بودابست، حيث فصلت المادة 7 التزوير عن الاحتيال والسرقة المرتبطة بالهوية[2]، وبمقارنة ذلك مع القانون الفرنسي، نجد تمايزا واضحا بين المادة 323-3 (تزوير البيانات) والمادة 226-4-1 (سرقة الهوية)[3]، وهو ما يدفعنا للقول بأن القانون الجزائري لا يزال يعتمد على "تشتت النصوص" بدلا من "وحدة المفهوم" في حماية الهوية الرقمية.

رابعا: تمييز جريمة التزوير الرقمي عن جريمتي القمار وغسل الأموال عبر الانترنت

أدى اتساع رقعة الفضاء السيبراني الى ظهور أنماط اجرامية مستحدثة تتداخل فيما بينها من حيث الوسيلة التقنية، لكنها تختلف في وجودها القانوني، ومن أبرز هده الجرائم نجد القمار الالكتروني وغسل الأموال، واللذان يرتبطان بعلاقة وطيدة مع التزوير المعلوماتي كأداة تنفيذية أو وسيلة لاخفاء المصدر غير المشروع.[4]

جريمة القمار عبر الانترنت تتمثل في ممارسة ألعاب الحظ والمراهنات باستخدام شبكات الاتصال الالكترونية، حيث يتم ايداع الأموال الناتجة عن أعمال غير مشروعة في شركات مالية أو بنوك، ثم يخضع غاسل الأموال لمرحلة التقييم والتمويه عبر اجراء عمليات لاخفاء الأصل غير المشروع للأموال، وأخيرا مرحلة الادماج التي تهدف الى اضفاء الشرعية على تلك الأموال واعادتها للمجرمين في شكل عوائد نظيفة وغير خاضعة للضرائب[5]، أما جريمة غسيل الأموال عبر الانترنت فتتمثل في اخفاء أو تمويه مصادر الأموال غير المشروعة باستخدام التقنيات الرقمية، حيث تساعد شبكة الانترنت القائمين بعمليات غسيل الأموال بتوفير عدة مميزات منها السرعة الشديدة وتخطي الحواجز الحدودية بين الدول وتفادي القوانين التي قد تضعها الدول من

[1] Zerrouki Assia & Hamel Mohamed**, Op.cit,** P 50.

[2] **Convention on Cybercrime (Budapest Convention),** 2001, Articles 7 & 8.

[3] **Code pénal français**, Articles 323-3 & 226-4-1(modifiér par le loi n° 2014-617 du 13 juin 2014).

[4] بساحة سليمة، **المرجع السابق**، ص16 .

[5] شهيرة بولحية، **الاحتيال الالكتروني**، مجلة الدراسات القانونية والاقتصادية، جامعة باتنة 1، الجزائر، العدد 04، ديسمبر 2019، ص38.

أجل اعاقة هذا النشاط، وكذا تشفير عملياتهم ما يعطيها قدر كبير من السرية وخاصة في تسهيل مرتكبي جرائم غسيل الأموال نقلها الى أي مكان في العالم من أجل استثمارها في اقليم أي دولة من دولة[1].

من خلال التحليل، تتبين لنا أوجه التشابه بين هذه الجرائم في كونها تستخدم نظام المعالجة الالية للمعطيات كوسيلة أو كغاية، وفي العنصر النفسي (القصد الجنائي والعلم)، وفي طريقة الاجرام التي تكون بطريق الغش أو التدليس، كما أنها تستهدف جميعها الاضرار بالاقتصاد الوطني سواء كان ذلك بتزييف بيانات مالية أو بممارسة قمار غير مشروع أو باخفاء مصادر أموال مشبوهة، غير أن الاختلاف الجوهري يكمن في موضوع الجريمة فالتزوير يستهدف المعطيات ذاتها بينما القمار يستهدف الأموال عبر الممارسات الاحتمالية، وغسيل الأموال يستهدف اخفاء المصدر غير المشروع للأموال، ويظهر الاختلاف أيضا في الوسيلة الاجرامية فالتزوير يتم عبر التلاعب التقني بالبيانات، والقمار عبر مواقع الكترونية مخصصة، وغسيل الأموال عبر تحويلات مصرفية الكترونية معقدة، كما يختلفان في المرحلة الاجرامية فالتزوير قد يكون وسيلة لاعداد بيانات القمار أو غسيل الأموال، والقمار قد يكون مصدرا للأموال المغسولة، لكنها تظل جرائم مستقلة يجمعها التداخل في بعض الحالات دون التطابق.[2]

المطلب الثاني: محل جريمة التزوير الرقمي (المحرر الالكتروني)

يتمثل المحل في الجريمة الالكترونية بصفة عامة، وفي جريمة التزوير الرقمي بصفة خاصة، في الاعتداء على قيمة اجتماعية تستوجب حماية القانون الجنائي، فالمحل ليس مجرد شيء مادي يمس به، بل هو مصلحة قانونية يقرها النظام القانوني ويحميها، وفي ظل الثورة الرقمية، تعددت المحلات التي تستوجب الحماية الجنائية، حيث لم تعد الجريمة مقتصرة على الاعتداء على الأشخاص أو الأموال المادية، بل تعدتها الى المعطيات الرقمية والأنظمة المعلوماتية والتواقيع الالكترونية، وقد اهتم المشرع الجزائري بحماية هذه المحلات الثلاثة في اطار مكافحة جريمة التزوير الرقمي، اما بموجب نصوص خاصة في قانون العقوبات، أو بموجب نصوص أخرى في التشريعات الموازية، وسنتناول في هذا المطلب هذه الحالات الثلاثة على النحو التالي:

[1] حسين فريجة، **الجرائم الالكترونية والانترنت**، مجلة المعلوماتية، السعودية، العدد 36، أكتوبر 2011، ص 5.

[2] Zerrouki Assia & Hamel Mohamed, **Op.cit**, P 52.

الفرع الأول: تعريف المحرر الالكتروني في التشريع الجزائري

يقتضي البحث في الجريمة المعلوماتية ضبط المحل الذي ترد عليه هذه الجرائم، وهو "المحرر الالكتروني" كبديل حديث للمحرر الورقي، ومن خلال استقرائنا للمنظومة التشريعية الوطنية، تبرز الرؤية التحليلة التالية:

أولا: المفهوم القانوني للمحرر الالكتروني

من خلال دراستنا للتشريع الجزائري، أجد أن المشرع لم يضع تعريفا موحدا وصريحا للمحرر الالكتروني في نص واحد، بل اكتفى بتبيان مفهومه عبر نصوص متفرقة تتعلق بالاثبات الالكتروني ومواكبة الثورة الرقمية[1]، ففي ظل التطور التكنولوجي المتسارع أصبح العالم يعتمد بشكل متزايد على الوسائل الرقمية في جميع جوانب الحياة، بما في ذلك المعاملات القانونية، مما اضطر المشرع الجزائري الى تكييف قوانينه لمواكبة هذا التحول[2]، ومن وجهة نظرنا، فان هذا الاكتفاء بالتعريفات المتفرقة يعد اشكالية تشريعية تستدعي اصدار نص موحد يجمه بين هذه التعريفات لضمان الاستقرار القانوني.

يمكن تعريف المحرر الالكتروني في التشريع الجزائري بأنه أي رسالة بيانات تتضمن معلومات يتم انشاؤها، دمجها، تخزينها، ارسالها، أو استقبالها كليا أو جزئيا بوسيلة الكترونية، رقمية، أو بأي وسيلة أخرى مشابهة[3]، هذا التعريف الواسع يهدف الى استيعاب التطورات التكنولوجية المستمرة وضمان شمولية القانون لمختلف أشكال الوثائق الرقمية، حيث يعد هذا المحرر من حيث القيمة الاثباتية معادلا للمحرر الورقي بشرط الالتزام بشروط محددة تضمن سلامته وموثوقيته[4]، وفي تحليلنا الشخصي، أرى أن هذا التعريف الشامل يعد ايجابية تشريعية تسمح بتطوير القانون مواكبة للتقنيات الناشئة دون الحاجة الى تعديلات متكررة.

---

[1] رحال علي، **حجية المحررات الالكترونية في الاثبات على ضوء التشريع الجزائري والتشريع المقارن**، مجلة طبنة للدراسات العلمية الأكاديمية، المجلد 04، العدد02، نوفمبر 2021 ، ص300.

[2] محمد طلعت يدك، **الحجية القانونية لتوثيق المحرارات الالكترونية: دراسة مقارنة**، مجلة جيل الأبحاث القانونية المعمقة، مركز جيل البحث العلمي، مصر، العدد 50، ص71 ومابعدها.

[3] المادة 378 مكرر من القانون رقم 08-09 المؤرخ في 25 فيفري 2008، المتضمن قانون الاجراءات المدنية والادارية المعدل والمتمم بالقانون رقم 22-13 المؤرخ في 12 جويلية 2022، الجريدة الرسمية، العدد48، الصادر بتاريخ 17 جويلية 2022.

[4] حنان براهيمي، **المحررات الالكترونية كدليل اثبات**، مجلة المفكر، جامعة محمد خيضر بسكرة، المجلد08، العدد01، ماي2013، ص136.

ثانيا: الأساس التشريعي والاعتراف القانوني

لقد أقر المشرع الجزائري من خلال عدة قوانين بحجية المحررات الالكترونية، فقد نصت المادة 323 مكرر 1 من القانون المدني الجزائري على أنه: "يعتبر الاثبات بالكتابة في الشكل الالكتروني كالاثبات بالكتابة على الورق، بشرط امكانية التأكد من هوية الشخص الذي أصدرها، وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها"[1]، هذا النص يضع الأساس للاعتراف العام بالمحررات الالكترونية ويساوي بينها وبين المحررات الورقية التقليدية من حيث الحجية، ومن وجهة نظرنا فان هذا التساوي بين الكتابة الالكترونية والكتابة على الورق يعد تطورا تاريخيا في قانون الاثبات الجزائري، الا أنه يثير اشكالية تتعلق بمدى قدرة القضاء على التحقق من تحقق الشروط المذكورة في النص.

كما أصدر المشرع القانون 15-04 المؤرخ في 1 فيفري 2015 المتعلق بالتوقيع والتصديق الالكتروني، والذي يحدد القواعد العامة لضمان موثوقية هذه الأدوات الرقمية، وقد عزز من هذا الاتجاه القانون رقم 18-05 المؤرخ في 10 ماي 2018 المتعلق بالتجارة الالكترونية، والذي يوسع من نطاق استخدام المحررات الالكترونية في المعاملات التجارية[2]، وفي تحليلنا المقارن، نجد أن المشرع الجزائري قد اتبع منهج التدرج التشريعي حيث بدأ بالاطار العام ثم تخصص في مجالات محددة، وهذا المنهج يضمن مرونة التطبيق لكنه قد يحدث تناقضات بين النصوص.

أما في مجال الاجراءات، فقد عرفت المادة 378 مكررا من قانون الاجراءات المدنية والادارية (القانون04-15) المحرر الالكتروني بأنه: "أي محرر ينتج أو يحفظ أو يرسل أو يستقبل بوسائل الكترونية"، مما يؤكد على شمولية التعريف واتساع نطاقه[3]، ومن ملاحظتنا التحليلية فان هذا التعريف الاجرائي أوسع من التعريف المدني، مما قد يحدث لبسا في التكييف القانوني يستدعي توحيد التعريفات.

[1] المادة 323 مكرر1 ، الامر رقم 75-58 المؤرخ في 26 سبتمبر 1975، المتضمن القانون المدني المعدل والمتمم بموجب القانون رقم 05-10 المؤرخ في 20 جوان 2005، الجريدة الرسمية، العدد 44، 2005.

[2] القانون رقم 15-04 المؤرخ في 1 فيفيري 2015، المتعلق بالتوقيع والتصديق الالكتروني، الجريدة الرسمبة، العدد06، الصادر بتاريخ 10 فيفري 2015.

[3] القانون رقم 18-05، المؤرخ في 10 ماي2018، المتعلق بالتجارة الالكترونية، الجريدة الرسمية، العدد28، الصادر بتاريخ 16 ماي 2018.

ثالثا: خصائص المحرر الالكتروني

يميز المحرر الالكتروني عن المحرر الورقي بخصائص تقنية وقانونية متعددة تميزه كوسيلة اثبات حديثة، فمن الناحية التقنية يتميز المحرر الالكتروني بأنه محمول على دعامة الكترونية وليس على ورق، مما يجعله عرضة لعمليات تقنية معقدة تضمن سلامته من التلاعب وصحة نسبته لصاحبه[1]، وهذه الخاصية التقنية تعد جوهرية في تمييز المحرر الالكتروني، حيث ان الوساط الالكترونية تختلف اختلافا جوهريا عن الوسائط الورقية من حيث الية التخزين والاسترجاع والتعديل.

ومن الناحية القانونية، يتميز المحرر الالكتروني بأنه يخضع لنظام قانوني خاص ينظمه مجموعة من النصوص التشريعية المتفرقة، بدءا من القانون المدني ومرورا بقانون التوقيع الالكتروني وانتهاء بقانون التجارة الالكترونية[2]، وهذا التعدد التشريعي يشكل خاصية قانونية تميز المحرر الالكتروني عن المحرر الورقي الذي يخضع أساسا لأحكام القانون المدني.

كما يتميز المحرر الالكتروني بخاصية القابلية للتكرار والنسخ دون فقدان للجودة، وهو ما لايتوفر في المحرر الورقي الذي يتأثر بالعوامل البيئية والزمنية[3]، غير أن هذه الخاصية تثير اشكالية قانونية تتعلق بتحديد الأصل من النسخة، مما يستدعي اليات تقنية خاصة للتمييز بينهما.

وتتميز أيضا بخاصية السرعة في التداول والارسال عبر شبكات الاتصال الالكترونية، مما يجعله أداة فعالة في التعاملات التجارية والادارية السريعة[4]، لكن هذه السرعة تقابلها مخاطر أمنية تتعلق باحتمال التدخل غير المشروع أو الاعتراض أثناء النقل، مما يستدعي تدابير تقنية وحماية قانونية اضافية.

وأخيرا، يتميز المحرر الالكتروني بخاصية الاعتماد على التوقيع الالكتروني كبديل عن التوقيع اليدوي، حيث يعتبر التوقيع الالكتروني الصادر عن سلطة تصديق معتمدة معادلا قانونا للتوقيع التقليدي[5]، وهذه

---

[1] المادة 378 مكرر من القانون رقم 08-09 المؤرخ في 25 فيفري 2008، المتضمن قانون الاجراءات المدنية والادارية المعدل والمتمم بالقانون رقم 22-13 المؤرخ في 12 جويلية 2022، الجريدة الرسمية، العدد48، الصادر بتاريخ 17 جويلية 2022..

[2] فضيلة يسعد، **القوة الثبوتية للتوقيع الالكتروني في التشريع الجزائري**، مجلة العلوم الانسانية، جامعة20 أوت1955 سكيكدة، المجلد 30، العدد52، ديسمبر2019، ص460.

[3] أميمة لعروسي، **حجية المحرر الالكتروني، مجلة القانون والأعمال الدولية**، منشور بتاريخ 22أفريل2020، تم الاطلاع يوم 21 مارس2026 ، على الساعة 16:53، على الرابط: https://www.droitetentreprise.com

[4] محمد سعيد عبد المولى، **الاثبات بالمحررات الالكترونية**، موقع حماة الحق للمحاماة والاستشارات القانونية، نشر بتاريخ 27أكتوبر 2021، تم الاطلاع عليه يوم 21 مارس 2026، على الساعة 17:10، على الرابط: https://jordan-lawyer.com

[5] حسين فريجة، **المرجع السابق**، ص05.

الخاصية تعد حجز الزاوية في منظومة المحرر الالكتروني حيث انها تضمن النسب والصفة والارادة للمحرر، وهي العناصر الأساسية لصحة أي محرر.

الفرع الثاني: شروط الاعتراف بالقيمة القانونية للمحرر الالكتروني

لم يكتفِ المشرع الجزائري بالاعتراف النظري بالمحرر الإلكتروني، بل أحاطه بمجموعة من الضوابط الجوهرية التي تضمن سلامته وموثوقيته، ومن وجهة نظرنا، فإنَّ هذه الشروط هي التي تحدد "محل الجريمة"؛ فالمحرر الذي يفتقد لهذه الشروط قد لا يرقى لمرتبة السند القانوني المحمي من التزوير، ويمكن حصر هذه الشروط في النقاط الآتية:

أولا: الشروط الموضوعية المتصلة بماهية المحرر الالكتروني في النظام القانوني الجزائري

تنبثق القيمة القانونية للمحرر الالكتروني في التشريع الجزائري من مدى قدرته على محاكاة الوظائف التقليدية للورقة، وهو ما يفرض توافر جملة من الشروط الجوهرية التي تخرجه من مجرد كونه فيضا من البيانات الرقمية الى كونه "سندا قانونيا" يعتد به أمام المحاكم الجزائرية[1]، ومن وجهة نظرنا كباحثين، فان هذه الشروط تمثل "الهيكل الوجودي" للمحرر في النظام القانوني الجزائري، وتتمثل فيما يلي:

1. تجسيد المضمون في شكل كتابة الكترونية قابلة للادراك

ان الكتابة هي جوهر المحرر، وفي المجال الرقمي لايشترط أن تكون الكتابة بخط اليد، بل يكفي أن تكون مجموعة من الرموز أو الحروف أو الأرقام المخزنة الكترونيا، غير أن الشرط الجوهري هنا هو "القابلية للقراءة والادراك"، بمعنى أن تكون هذه البيانات قابلة للاسترجاع والعرض على الشاشة أو الطباعة في أي وقت، وقد عرف المشرع الجزائري في المادة 2/ج من القانون رقم 09-04 المؤرخ في 05 أوت 2009 "المعطيات المعلوماتية" بأنها:"أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها"[2]، فالمحرر الذي لا يمكن قراءته أو الذي يتلاشى بمجرد اغلاق النظام لا يتمتع بأي قيمة قانونية لأنه يفتقد لشرط الثبات النسبي، وهو ما يتطلب وجود "الدعامة الحافظة" الامنة التي يحميها المشرع الجزائري من خلال نصوصه الجنائية.

[1] عمارة فتيحة، **جريمة التزوير الالكتروني**، مجلة القانون والمجتمع، كلية الحقوق والعلوم السياسية، جامعة سعيدة، الجزائر، المجلد 07، العدد 01، سنة 2019، ص12.

[2] المادة 2 القانون رقم 09-04 المؤرخ في 05 أوت2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47، سنة 2009.

2. امكانية نسبة المحرر لكاتبه (الصلة بالفاعل)

لا يمكن الاعتراف بالمحرر الالكتروني في النظام القانوني الجزائري ما لم تكن هناك وسيلة قانونية وتقنية لربطه بشخص معين (طبيعي أو معنوي)، هذه "النسبية" هي التي تضفي الصبغة القانونية على التصرف، اذ لا يمكن تصور وجود التزام قانوني دون وجود ملتزم محدد[1]، ونرى أن هذا الشرط هو العتبة الأولى لمواجهة جريمة التزوير الرقمي المنصوص عليها في المادة 394 مكرر من قانون العقوبات الجزائري المعدل و المتمم بالقانون 24-06[2]؛ اذ ان أي غموض في تحديد هوية منشىء المحرر يجرده من حجيته في الاثبات ويجعله مجرد معلومات مجهولة المصدر، ولقد أكد المشرع الجزائري في المادة 2/و من القانون 09-04 على أهمية "الاتصالات الالكترونية" التي تشمل "أي تراسل أو ارسال أو استقبال علامات أو اشارات أو كتابات أو صور أو أصوات أو معلومات"، مما يؤكد ضرورة النسبة بين المرسل والمحرر[3].

3. اتجاه الارادة لاحداث أثر قانوني

يجب أن يتضمن المحرر الالكتروني تعبيرا واضحا عن الارادة يهدف الى انشاء، تعديل، أو انهاء مراكز قانونية[4]، فالمسودات الالكترونية أو المراسلات العابرة التي لا تحمل طابع الالتزام لا تعد محررات قانونية محمية، وهنا يبرز دور التحليل القانوني في التمييز بين "الوعاء المعلوماتي" و"المحرر القانوني"؛ فالاخير هو الذي يرتب حقوقا وواجبات قابلة للتنفيذ أمام القضاء، وقد لاحظنا ان المادة 2/ج من القانون 09-04 تفرق بين "المعطيات المعلوماتية" كتمثيل للمعلومات، وبين "المنظومة المعلوماتية" كأداة للمعالجة، مما يعني أن الاعتراف القانوني يتطلب وجود ارادة منظمة عبر نظام معلوماتي يهدف الى احداث أثر قانوني محدد[5].

ثانيا: الشروط الشكلية والتقنية لضمان الحجية والاستمرارية في المشرع الجزائري

بمجرد توافر الشروط الموضوعية، ينتقل البحث "صحة" هذا المحرر واستمرارية سلامته، وهي شروط تقنية في مظهرها وقانونية في أثرها، تضمن عدم العبث بالحقيقة الرقمية:

---

[1] عمارة فتيحة، **المرجع السابق**، ص22.

[2] المواد 394 و394 مكرر و394 مكرر 1 و394 مكرر2 من القانون رقم 24-06 المؤرخ في 28 أفريل2024 لمعدل و المتمم لقانون العقوبات، الجريدة الرسمية، العدد30، سنة 2024.

[3] المادة 2 القانون رقم 09-04 المؤرخ في 05 أوت2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47، سنة 2009.

[4] عمارة فتيحة، **المرجع السابق**، ص140.

[5] المادة 2 القانون رقم 09-04 المؤرخ في 05 أوت2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47، سنة 2009.

أ. شرط السلامة وعدم التعديل (تكامل البيانات)

تعتمد القيمة القانونية للمحرر الالكتروني في النظام الجزائري على ضمان عدم تعرضه لأي تحريف أو تغيير منذ لحظة انشائه وحتى وقت الاحتجاج به[1]، فالمحرر الالكتروني بطبيعته الرقمية يتسم بالسيولة وسهولة التعديل، مما يفرض استخدام تقنيات (مثل التشفير أو التوقيع الرقمي) تضمن "تجميد" البيانات، وقد نصت المادة 394 مكرر/2 من قانون العقوبات الجزائري المعدل و المتمم بالقانون 24-06 على أنه: "تضاعف العقوبة اذا ترتب على ذلك حذف أو تغيير المعطيات المنظومة"، مما يدل على أن المشرع الجزائري يعتبر تغيير المعطيات جريمة مضاعفة تستوجب عقوبة مشددة[2]، وان اي تغيير يطال "البيانات الجوهرية" للمحرر يعد تزويرا ينسف قيمته القانونية بالكامل، بينما قد لا تؤثر التغييرات التقنية الطفيفة (مثل تغيير نوع الخط أو التنسيق) على جوهر المحرر.

ب. اقتران المحرر بالتوقيع الالكتروني المؤمن

يعتبر التوقيع الالكتروني الركن الركين في الاعتراف بحجية المحرر في النظام القانوني الجزائري، فهو الذي يقوم مقم الامضاء اليدوي في المحررات الرقمية[3]، ويشترط في هذا التوقيع أن يكون "مؤمنا"، أي مرتبطا بالموقع وحده، وتحت سيطرته الكاملة، وبحيث يسمح بكشف أي تعديل لاحق يطرأ على المحرر، ولقد عرف المشرع الجزائري التوقيع الالكتروني في القانون رقم 15-04 (المتعلق بالمعاملات الالكترونية) والمرسوم التنفيذي 16-135 بأنه: "معطى ينجم عن استخدام أسلوب معين يتيح التعرف على هوية مرتكب التوقيع، ويضمن نسبة هذا التوقيع اليه، ويحمي المحرر من أي تغيير أو تزوير"[4]، ونعتقد أن التوقيع ليس مجرد اجراء شكلي، بل هو "ختم الأمان" الذي يحول البيانات من مجرد "كلام مرسل" الى "حجة قانونية" قاطعة، وقد أوجد المشرع الجزائري "الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها" بموجب المواد 13 و14 للاشراف على ضمانات التوقيع الالكتروني والتحقق من صحته[5].

---

[1] عمارة فتيحة، **المرجع السابق**، ص92.

[2] المواد 394 و394 مكرر و394 مكرر 1 و394 مكرر2 من القانون رقم 24-06 المؤرخ في 28 أفريل2024 لمعدل و المتمم لقانون العقوبات، الجريدة الرسمية، العدد30، سنة 2024.

[3] امال قارة، **الحماية الجنائية للمعلوماتية في التشريع الجزائري**، الطبعة الثانية، دار هومة، الجزائر، 2010، ص115.

[4] المرسوم التفيذي رقم 16-135 المؤرخ في 25 ماي 2016 المتعلق بالتوقيع الالكتروني، الجريدة الرسمية، العدد 32، الصادر بتاريخ 29 ماي 2016.

[5] المادة 2 القانون رقم 09-04 المؤرخ في 05 أوت2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47، سنة 2009.

ج. معيار الضرر وعلاقة المحرر بالحماية الجنائية الجزائرية

لكي يكتسب المحرر حماية القانون الجزائري (خاصة ضد التزوير)، يجب أن يكون العبث به مؤديا الى وقوع ضرر[1] ، فالمشرع الجزائري سواء في قانون العقوبات (المواد 394 ومابعدها) أو في القانون 09-04، يربط بين الاعتراف بالقيمة القانونية وبين حماية هذه القيمة من "تغيير الحقيقة" الذي يلحق ضررا بالغير، لذا فان المحرر الذي لا يترتب على تغييره اي ضرر مادي أو معنوي، تضعف قيمته كدليل اثبات قانوني أمام المحاكم الجزائرية، وقد نصت المادة 394 مكرر1 من قانون العقوبات المعدل والمتمم بموجب القانون 24-06 على معاقبة كل من "أدخل بطريق الغش معطيات في نظام المعالجة الالية أو أزال أو عدل" بعقوبة الحبس والغرامة، مما يدل على أن المشرع الجزائري يرى أن العبث بالمحرر الالكتروني يستوجب العقاب فقط اذا ادى الى وقوع ضرر محدد[2].

ثالثا: الاطار الاجرائي والتحديات التطبيقية في الجزائر

ومن خلال ما تقدم، يتبين لنا أن الاعتراف بالقيمة القانونية للمحرر الالكتروني في مذكرتنا هذه ليس مجرد مسألة تقنية، بل هو نظام متكامل يزاوج بين ثبات المضمون (الشروط الموضوعية) وأمان الوسيلة (الشروط الشكلية)[3]، غير أن الممارسة العملية في الجزائر لا تزال تواجه عراقيل عدة تعيق التكريس الفعلي لهذه الوسيلة في المعاملات اليومية، يبرز ذلك في محدودية اللجوء اليها أمام الجهات القضائية، وضعف انتشارها في العقود والصفقات رغم تطور المنظومة الرقمية[4].

ويعود ذلك الى تحديات متعلقة بالثقة، الوعي القانوني، والجاهزية التقنية، فبالرغم من الاطار التشريعي الذي وضعه المشرع الجزائري من خلال القانون 09-04 والقانون 15-04 والمرسوم 16-135 المؤرخ في 25 أبريل 2016 الذي يحدد طبيعة وتكوين وعمل السلطة الحكومية للتصديق الالكتروني، فان تحقيق التوازن بين حماية حقوق المتعاملين والانفتاح على التقنية يتطلب تدخلا تشريعيا مرنا يراعي خصوصية البيئة الرقمية دون

[1] امال قارة، **المرجع السابق**، ص168.

[2] المواد 394 و394 مكرر و394 مكرر 1 و394 مكرر2 من القانون رقم 24-06 المؤرخ في 28 أفريل2024 لمعدل و المتمم لقانون العقوبات، الجريدة الرسمية، العدد30، سنة 2024.

[3] عمارة فتيحة، **المرجع السابق**، ص22.

[4] عمارة فتيحة، **المرجع السابق**، ص12.

الاخلال بضمانات الاثبات التقليدي المنصوص عليها في القانون 08-09 المتضمن قانون الاجراءات المدنية والادارية[1].

الفرع الثالث: التوقيع الالكتروني كهدف لعمليات التزوير

نظرا للتطور المعلوماتي المتسارع الذي تشهده الجزائر في اطار التحول الرقمي الشامل، بات التوقيع الالكتروني يمثل ركيزة أساسية من ركائز الثقة في المعاملات الرقمية، سواء كانت مدنية أو تجارية أو ادارية، اذ يعوض التوقيع التقليدي اليدوي في العديد من التعاملات الحديثة، غير أن هذا التطور التقني، رغم ما يحمله من ايجابيات في تسهيل الاجراءات وتسريعها، قد فتح المجال أمام ظواهر اجرامية جديدة تستهدف هذه الوسيلة الحديثة للتعبير عن الارادة، خاصة من خلال عمليات التزوير والتزييف الالكتروني التي تستغل الثغرات التقنية والقانونية، ومن هنا نرى أن المشرع الجزائري قد استدعى الأمر وضع اطار قانوني متكامل يجمع بين التنظيم والتجريم والحماية، ليس فقط لتقنين استخدام التوقيع الالكتروني، بل أيضا لحمايته كقيمة قانونية مستقلة من الاعتداءات الجرمية، واذ نتناول هذا الفرع، فاننا نسعى الى تفكيك المنظومة القانونية الجزائرية المتعلقة بحماية التوقيع الالكتروني من عمليات التزوير، من خلال دراسة الأسس القانونية لهذا التوقيع، وتحليل طبيعة الجريمة المعلوماتية المتمثلة في تزويره، واستعراض الاليات القانونية والعقابية التي أقرها المشرع، وذلك في سياق منهجي يهدف اللى ابراز مدى فعالية التشريع الجزائري في مواجهة هذا النوع من الجرائم الرقمية المتطورة.

أولا: الأساس القانوني للتوقيع الالكتروني وتميزه التنظيمي في النظام القانوني الجزائري

يبدو لنا، ونحن نستشرف النصوص التشريعية المنظمة لهذا المجال، أن المشرع الجزائري قد أرسى قواعده الأولى عبر القانون رقم 15-04 المؤرخ في 1 فيفري 2015 المتعلق بالتوقيع الالكتروني والتصديق الالكتروني[2] ، والذي يعد النص الجوهري والأساسي الذي حدد القواعد العامة لانشاء التوقيع الالكتروني والتصديق الالكتروني والاعتراف القانوني بهما في مختلف المعاملات، وقد نص هذا القانون في نصوصه التحضيرية على تعريف دقيق ومفصل للتوقيع الإلكتروني، إذ عرّفه في المادة 2 بأنه: "بيانات في شكل

[1] القانون رقم 08-09 المؤرخ في 25 فيفري 2008، يتضمن قانون الاجراءات المدنية والادارية، الجريدة الرسمية، العدد23، الصادرة بتاريخ 27 أبريل 2008.

[2] القانون رقم 15-04 المؤرخ في 1 فيفري2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، الجريدة الرسمية، العدد 06، الصادر بتاريخ 10 فيفري2015.

الكتروني، مرفقة أو مرتبطة منطقيا ببيانات الكترونية أخرى، تستعمل كوسيلة توثيق" [1]، مما يُؤسّس لتمييز قانوني حاسم ودقيق بين نوعين رئيسيين من التوقيعات الإلكترونية: التوقيع الإلكتروني العادي، والتوقيع الإلكتروني الموصوف، ونلاحظ أن هذا التمييز يكتسب أهمية بالغة في سياق حماية التوقيع من التزوير، نظراً لما يُمنحه التوقيع الموصوف من حجية قانونية أقوى وأكثر متانة، إذ يُنشأ بموجب شهادة تصديق إلكترونية معتمدة تصدر عن جهة موصوفة تضمن هوية الموقّع بشكل أكثر صرامة وموثوقية[2].

كما أن المشرع الجزائري قد أكّد على الحجية القانونية للتوقيع الإلكتروني من خلال القانون رقم 10-05 المتمم لقانون الإثبات المدني والتجاري [3]، والذي اعترف بالتوقيع الإلكتروني كوسيلة من وسائل الإثبات الإلكتروني، مُعادلاً بينه وبين التوقيع اليدوي التقليدي في حال استيفائه للشروط القانونية المنصوص عليها صراحة في النصوص التنظيمية[4]، ونستنتج من هذا الاعتراف القانوني أن المشرع قد سعى إلى دمج التوقيع الإلكتروني في المنظومة القانونية التقليدية، مما يُضفي عليه الشرعية القانونية الكاملة في المنازعات القضائية ويُعزز من مصداقيته القانونية، غير أن هذا الاعتراف المتزايد بالحجية يجعل من التوقيع الإلكتروني هدفاً استراتيجياً للمجرمين الرقميين الذين يسعون إلى تزويره للاستيلاء على حقوق الغير أو التلاعب بالمعاملات القانونية.

ثانيا: طبيعة جريمة تزوير التوقيع الالكتروني واطارها التجريمي في التشريع الجزائري

غير أن الاعتراف القانوني المتزايد بهذا النوع الحديث من التوقيعات قد جعله هدفاً مباشراً ومحورياً لعمليات التزوير والتقليد من قبل المجرمين الإلكترونيين، مما استدعى من المشرع الجزائري وضع إطار تجريمي خاص ومتطور يحمي هذا التوقيع من الاعتداءات الرقمية المتنوعة.

وعلى خلاف الاعتقاد الشائع، فان امكانية التزوير في المحررات الورقية قد تبدو أيسر وأسهل، بينما يتطلب تزوير المحرر الالكتروني دراية وخبرة تقنية عالية جدا لاختراق أنظمة التشفير والتوثيق الرقمي، وأمام هذا التحدي التقني نجد ان الجهود التي تبذل اليوم والأبحاث والأفكار التي تطرح تهدف أساسا الى توظيف أحدث التقنيات لتوفير حماية قصوى وضمان أمن استخدام شبكة الانترنت ونظم المعلومات، بغية رفع نسبة الدقة في

---

[1] شيخ سناء وشيخ محمد زكرياء، **مكافحة الجرائم الالكترونية في القانون الجزائري** ، تم الاطلاع عليه يوم 24 مارس 2026، على الساعة 00:06، متاح على الرابط:https://wameedalfiker.com

[2] عجابي الياس، **الطبيعة القانونية للتوقيع الالكتروني**، مجلة دراسات وأبحاث، جامعة الجلفة ، المجلد 01، العدد 01، ص255.

[3] مطلق بن مقحص بن مطلق السهلي، **حجية التوقيع الالكتروني في الاثبات**، مجلة ابن خلدون للدراسات والأبحاث، المجلد 03، العدد 07، جويلية 2023، ص10.

[4] **مدى حجية التوقيع الالكتروني في الاثبات في التشريع الجزائري: دراسة على ضوء أحكام القانون 15-04**، تم الاطلاع عليه يوم 24 مارس 2026، على الساعة 00:49، على الرابط: https://platform.almanhal.com

التحقق من شخصية القائم بالتصرف القانوني، خاصة في مجال التجارة الالكترونية الذي يعتمد بشكل كلي على الثقة الرقمية[1].

وقد تحقق ذلك بصدور القانون رقم 09-04 المؤرخ في 5 أوت 2009 المتعلق بالوقاية من الجرائم المعلوماتية [2]، والذي يُعدّ بحق الدرع الجنائي الأساسي والأول في هذا المجال، إذ صنّف المشرع في مواد هذا القانون تزوير التوقيع الإلكتروني كجريمة معلوماتية مستقلة بذاتها، متجاوزاً بذلك مفهوم المخالفات التقنية البحتة أو المخالفات الإدارية إلى إدراكه كفعل إجرامي ذات طبيعة جنائية واضحة تستوجب التدخل القضائي والقانوني الرادع[3].

ونرى أن المشرع قد تبنى في هذا السياق رؤية شاملة ومتكاملة للحماية الجنائية، حيث شملت أفعال التزوير المجرّمة بموجب أحكام هذا القانون تزوير أو تعطيل أو إتلاف وسيط إلكتروني أو محرر إلكتروني، أو إنشاء توقيع مزيف أو تعديله أو تغييره بأي شكل من الأشكال، أو حتى استخدامه للاحتيال على الغير أو الإضرار به[4]، ونؤكد أن هذا الاتساع في دائرة الأفعال المجرمة يُبيّن مدى حرص المشرع على حماية سلامة المستندات الإلكترونية وهوية الموقّعين من الاعتداءات الرقمية المتطورة، مستنداً في ذلك إلى مفهوم واسع للجرائم الإلكترونية يتجاوز الفعل المادي التقليدي ليشمل الأفعال الافتراضية والاعتداءات على البيانات الرقمية.

ثالثا: منظومة الحماية الوقائية والاليات التنفيذية والعقابية

وفي سياق متصل ومكمل، فإننا نلاحظ أن المشرع الجزائري قد أولى اهتماماً بالغاً واستباقياً بالآليات الوقائية التي تسبق وقوع الجريمة، من خلال تنظيم دور" مؤدي خدمات التصديق الإلكتروني "الذين يُشكّلون الركيزة الأساسية والحجر الزاوي في منظومة الحماية الشاملة، وذلك بموجب أحكام القانون15-04 ، حيث يتولى هؤلاء المؤديون إصدار شهادات التصديق الإلكترونية الموصوفة التي تضمن هوية الموقّع بشكل قاطع وتُؤكد صدور التوقيع عن الشخص فعلاً وليس عن غيره[5]، ونرى أن هذه الآلية التقنية-القانونية المتطورة تُشكّل خط

---

[1] ايمان بغدادي، **التوقيع الالكتروني كبديل للتوقيع التقليدي في التجارة الالكترونية**، مجلة الاقتصاد الدولي والعولمة، جامعة زيان عاشور بالجلفة، المجلد 02، العدد 04، تم النشر بتاريخ 01 ديسمبر 2019، ص20.

[2] القانون 09-04 المؤرخ في 5 أوت 2009، المتعلق بالوقاية من الجرائم المرتبطة بتكنولوجيات الاعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47، الصادر بتاريخ 16 أوت 2009.

[3] فيصل محمودي، **"المحامي فيصل محمودي يوضح مفهوم الجرائم الالكترونية بنظر القانون'**، فيديو يوتيوب على قناة Echorouk News، تم النشر يوم 12 جانفي 2026، تم الاطلاع عليه بتاريخ 24 مارس2026، على الساعة 17:45، على الرابط: https://www.youtube.com/watch?v=jC6e05PxCQq.

[4] غلاب عبد الحق، **خصوصية جريمة تزوير التوقيع الالكتروني في التشريع الجزائري**، مجلة الدراسات القانونية والسياسية، جامعة عمار ثليجي الأغواط، المجلد 08، العدد 01، جانفي 2022، ص496.

[5] **مقال: التصديق الالكتروني (Electronic certification)**، صادر عن الموقع الرسمي لسلطة ضبط البريد والاتصالات الالكترونية، تم الاطلاع يوم 24 مارس 2026، على الساعة 01:40، على الرابط: https://www.arpce.dz/en/big-folders/electronic-certification.

دفاع أولاً وأساسياً ضد عمليات التزوير، حيث تضع عبء الإثبات القانوني على من يدّعي خلاف ما تثبته وسائل التصديق المعتمدة رسمياً، مما يُقلل بشكل كبير من فرص التلاعب بالبيانات والتزوير[1].

كما أن السلطة الوطنية للتصديق الإلكتروني(ANCE) ، التابعة لوزارة البريد والمواصلات، تُشرف بشكل مباشر ودقيق على إصدار هذه الشهادات وتُراقب عمل مؤدي الخدمات، مما يضمن وجود هيئة عمومية موثوقة لإصدار الشهادات ويُعزز من الثقة العامة في النظام الرقمي الجزائري[2]، أما على المستوى العقابي، فقد جاءت العقوبات المقررة في القانون 09-04 بشكل رادع يتناسب مع خطورة الجريمة الإلكترونية وآثارها الاجتماعية والاقتصادية، حيث نصّ القانون على عقوبات سالبة للحرية تتراوح بين ستة أشهر إلى خمس سنوات حبساً، بالإضافة إلى غرامات مالية مالية ثقيلة تصل إلى خمسمائة ألف دينار جزائري، وذلك حسب نوع الضرر الناتج عن عملية التزوير وطبيعة الفعل المرتكب[3].

ونستخلص من هذا التدرج العقابي الدقيق أن المشرع قد سعى جاهداً إلى تحقيق الردع العام والخاص في آن واحد، من خلال فرض عقوبات سالبة للحرية والمال معاً، مما يُشكّل عائقاً قانونياً كبيراً أمام المجرمين المحتملين، غير أننا نؤكد على أن فعالية هذه العقوبات تظل مرتبطة بمدى تطور آليات الكشف والتحقيق في الجرائم الرقمية التي تتطلب خبرات تقنية عالية وكوادر متخصصة[4]، وخلاصة القول، فإن التشريع الجزائري قد قطع شوطاً كبيراً وجاداً في بناء منظومة قانونية متكاملة ومتينة تجمع بين الحماية التنظيمية والحماية الجنائية والحماية الإثباتية، تبقى في حاجة مستمرة وماسة إلى التحديث واليقظة لمواكبة التطورات التقنية السريعة في أساليب الاحتيال والتزوير الإلكتروني[5].

---

[1] السائح ايمان، **الحماية القانونية للتوقيع الالكتروني**، منشورات المجلة المغربية للدراسات والاستشارات القانونية، جامعة محمد الأول وجدة، العدد 01، سنة 2016، ص45.

[2] **مقال: التوقيع والتصديق الالكترونيين**، صادر عن الموقع الرسمي لوزارة البريد والمواصلات السلكية واللاسلكية ، تم الاطلاع عليه يوم 24 مارس 2026، على الساعة 2:04، على الرابط: https://www.mpt.gov.dz

[3] المادة 11 من قانون 09-04 المؤرخ في 5 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47، سنة 2009.

[4] **مصالح شرطة مكافحة الجرائم الالكترونية تسجل 567 قضية تتعلق بجرائم الانترنت**، صادر عن الموقع الرسمي للشرطة الجزائرية، تم الاطلاع عليه يوم 24 مارس 2026، على الساعة 2:13، على الرابط: https://www.algeriepolice.dz

[5] سعيد بن لحرش، **الحماية الجزائية للتوقيع الالكتروني**، مذكرة ماستر في الحقوق تخصص قانون أعمال، جامعة زيان عاشور، الجلفة، 2021، ص15.

المطلب الثالث: صور التزوير الرقمي في الواقع العملي

لا يتخذ التزوير الرقمي شكلاً واحداً في الواقع التطبيقي، بل يتلون بتطور الوسائل التقنية المستخدمة، وهو ما يجعله يتجاوز المفهوم الكلاسيكي للتزوير المادي،ومن خلال تتبعنا للثقافة الجنائية الرقمية الحديثة، يمكن رصد أهم هذه الصور فيما يلي:

الفرع الأول: تزوير البيانات والمعطيات المخزنة

نستهلُّ بحثنا في هذا الفرع بالإشارة إلى أن التحول الرقمي الذي تشهده الجزائر في مختلف مناحي الحياة الاقتصادية والإدارية والاجتماعية، قد ولَّد تحديات قانونية معقدة تقتضي استجابات تشريعية مبتكرة وشاملة، فمع تزايد الاعتماد على الأنظمة الحاسوبية وقواعد البيانات الإلكترونية في تخزين ومعالجة المعلومات الحساسة والحيوية، برزت ظاهرة تزوير البيانات والمعطيات المخزنة كإحدى أخطر الجرائم المعلوماتية التي تُهدِّد النسيج الاقتصادي والأمني للدولة[1]، ومن هنا، نسعى في هذا الفرع إلى تفكيك المنظومة القانونية الجزائرية المتعلقة بهذه الجريمة، عبر الوقوف على المفهوم القانوني الدقيق لها، والأسس التشريعية المواجهة لها، والعقوبات والآليات الرقابية المقررة، وذلك بغية تقديم رؤية تحليلية نقدية تستجيب لمتطلبات البحث العلمي.

أولا: المفهوم القانوني لجريمة تزوير البيانات والمعطيات المخزنة بين التقليدي والرقمي

نؤكد أن التشريع الجزائري قد تبنى تعريفاً واسعاً وشاملاً للتزوير يتجاوز النطاق التقليدي المحدود في المحررات الورقية والوثائق المادية، ليشمل كذلك البيانات والمعطيات المخزنة إلكترونياً[2]، فقد تضمن المشرع الجزائري في نصوصه أن تزوير البيانات يشمل أي تغيير متعمد للحقيقة في سجل أو محرف، سواء كان ذلك ورقياً أو رقمياً، بهدف الإضرار بالغير أو تحقيق منفعة غير مشروعة[3]، كما نلاحظ أن المشرع قد فرَّق في نصوصه بين التزوير التقليدي الذي يركز على الوثائق المادية كالشهادات الإدارية والعقود والمحررات الرسمية والعرفية، وبين التزوير الرقمي الذي يمتد إلى تعديل البيانات في قواعد البيانات الحاسوبية، وتزييف الهويات الرقمية، والتلاعب في المعاملات الإلكترونية[4].

---

[1] **مقال: الجزائر: اقرار قانون جديد يتصدى لجرائم تزوير الوثائق**، الصادر عن موقع العربي الجديد، تم الاطلاع عليه يوم 25 مارس 2026، على الساعة 22:25، على الرابط: https://www.alaraby.co.uk.

[2] أمينة داودي، **هذه عقوبة تزوير الوثائق الادارية والشهادات**، الصادر عن موقع النهار أنلاين، بتاريخ 11 أكتوبر 2023، تم الاطلاع عليه بتاريخ 25 مارس 2026، على الساعة 22:33، على الرابط: https://www.ennaharonline.com

[3] محمد العيداني ، يوسف زروق، **حماية المعطيات الشخصية في الجزائر على ضوء القانون رقم 18-07 (المتعلق بحماية الاشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي)**، مجلة معالم للدراسات القانونية والسياسية، المركز الجامعي تندوف، المجلد 02، العدد 03، ديسمبر 2018، ص 120.

[4] نزيهة علال، **الاطار القانوني لحماية المعطيات ذات الطابع الشخصي في الفضاء الالكتروني في ظل القانون 18-07**، مجلة دائرة البحوث والدراسات القانونية والسياسية، المركز الجامعي مرسلي عبد الله – تيبازة، المجلد04، العدد09، جوان 2020، ص70.

نرى أن هذا التوسع المفاهيمي الذي أدخله المشرع الجزائري يُعدُّ خطوة متقدمة وضرورية في مواكبة التطورات التكنولوجية الراهنة، إذ يعكس وعياً تشريعياً عميقاً بالتحولات الهيكلية في طبيعة الوثائق والمعاملات، غير أننا نلاحظ أن هذا التعريف الواسع قد يثير إشكالية في التمييز الدقيق بين التزوير الرقمي وبين جرائم الحاسوب الأخرى كالقرصنة والاختراق، مما يقتضي من القضاء الجزائري جهداً تفسيرياً كبيراً لتحديد معايير التمييز بين هذه الأنواع [1]، كما نعتقد أن التركيز على عنصر "الاضرار بالغير" كركن معنوي في الجريمة قد يُضعف الحماية القانونية في حالات التزوير التي لا ينتج عنها ضرر مباشر فوري، ولكنها تشكل خطراً محتملاً على النظام العام الرقمي.

ثانيا: الأساس القانوني والتشريعي المتكامل لمواجهة الجريمة

نُبرز أن الجزائر قد اعتمدت منظومة تشريعية متكاملة ومتشعبة تستهدف مواجهة جرائم تزوير البيانات بشكل خاص والجرائم الإلكترونية بشكل عام، ففي مقدمة هذه التشريعات يأتي قانون العقوبات الجزائري الذي يُعد الأساس العقابي في هذا المجال، حيث ينص صراحة على عقوبات مشددة للتزوير تتراوح بين الحبس من خمس إلى عشر سنوات في المحررات الإدارية مثل الشهادات والرخص، وتصل إلى أعلى درجات العقوبات في حال ارتباط التزوير ببيانات مالية أو حاسوبية[2].

كما نتطرق إلى القانون 18-07 المتعلق بحماية المعطيات ذات الطابع الشخصي الصادر بتاريخ 10 جوان2018 ، الذي يُعتبر حجر الزاوية في حماية البيانات الشخصية في الجزائر، إذ يهدف إلى حماية الحياة الخاصة للأفراد وحقوقهم وكرامتهم في سياق معالجة البيانات [3]، وقد نص هذا القانون على ضرورة الحصول على موافقة صريحة من الأفراد قبل معالجة بياناتهم، كما أحدث السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي (ANPDP) كجهة مستقلة للرقابة والتنظيم[4].

إضافة إلى ذلك، نجد قانون مكافحة التزوير واستعمال المزور(رقم 24-02 المعدل والمتمم بالقانون 15-07)، الذي يهدف إلى توسيع نطاق الجرائم ليشمل الوثائق الإلكترونية والمعاملات الرقمية، مع فرض

---

[1] بوحديد فارس، قرانة عادل، **مهام السلطة الوطنية لحماية المعطيات الشخصية في التشريع الجزائري**، مجلة العلوم القانونية والاجتماعية، جامعة زيان عاشور الجلفة كلية الحقوق والعلوم السياسية، المجلد06، العدد02، جوان 2021، ص18.

[2] أمينة داودي، **هذه عقوبة تزوير الوثائق الادارية والشهادات**، الصادر عن موقع النهار أنلاين، بتاريخ 11 أكتوبر 2023، تم الاطلاع عليه بتاريخ 25 مارس 2026، على الساعة 22:33، على الرابط: https://www.ennaharonline.com

[3] القانون رقم 18-07 المؤرخ في 10 جوان 2018 المعدل والمتمم بالقانون رقم 25-11 المؤرخ في 24 جويلية 2025، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية، العدد 34، الصادر بتاريخ 10 جوان 2018.

[4] **السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي**، الصادر عن الموقع الرسمي للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي ، تم الاطلاع يوم 25 مارس 2026، على الساعة 23:07، على الرابط: https://anpdp.dz

عقوبات صارمة تصل إلى ثلاثين سنة حبساً في حال تعلق التزوير ببيانات حيوية أو وثائق سفر[1]، كما لا يفوتنا الإشارة إلى القوانين الإلكترونية الأخرى كالقانون 05-01 والقانون 09-04 المعدل، اللذين ينصان صراحة على معاقبة الفعل الإلكتروني المتمثل في تعديل البيانات المخزنة في الأنظمة الحاسوبية أو الشبكات[2].

نرى أن هذا التكامل التشريعي يعكس رؤية استباقية من المشرع الجزائري لبناء جدار قانوني حصين يحمي الفضاء الرقمي الوطني، غير أننا نلاحظ وجود تداخل في الاختصاصات بين هذه النصوص، مما قد يؤدي إلى صعوبة في تحديد النص القانوني الأنسب للمتابعة في حالات معينة[3]، فمثلاً، عندما يتعلق الأمر بتزوير بيانات شخصية مخزنة إلكترونياً، قد يقع الالتباس بين تطبيق قانون العقوبات العام وقانون 18-07 الخاص، كما نعتقد أن غياب نص صريح في قانون العقوبات يجرم "تزوير البيانات" كجريمة مستقلة بعنوان محدد قد يخلق ثغرة في الحماية الجنائية، حيث ما زال الاعتماد على الفصول العامة المتعلقة بالتزوير في المحررات، مما يستدعي إدخال تعديلات جوهرية على قانون العقوبات لمواكبة الخصوصية الرقمية.

ثالثا: العقوبات المقررة والآليات الرقابية والوقائية

نُجمِع في هذا العنصر أن العقوبات في التشريع الجزائري تتفاوت بحسب طبيعة البيانات المزورة ونوع الجريمة والصفة القانونية للجاني، فقد تتراوح العقوبات بين الحبس والغرامات المالية الكبيرة، وتصل في حالات التزوير الخطيرة للبيانات الحيوية من قبل موظفين عموميين إلى السجن المؤبد[4]، وقد وضع المشرع جدولاً تفصيلياً للعقوبات يميز بين تزوير المحررات العامة والخاصة، والمحررات التجارية، والوثائق الإدارية، مع تشديد العقوبات في حالات معينة.

كما نؤكد على الدور المحوري الذي تضطلع به السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي (ANPDP) في الإشراف على تطبيق قوانين حماية البيانات الشخصية، وضمان مطابقة معالجة البيانات للأحكام القانونية، وتلقي الشكاوى وتقديم الإرشادات، فضلاً عن دورها في الدفاع عن خصوصية الأفراد في

---

[1] **مقال: صدور قانون مكافحة التزوير واستعمال المزور في الجريدة الرسمية**، الصادر عن موقع الجزائر الان، بتاريخ 13 مارس 2024، تم الاطلاع عليه بتاريخ 25 مارس 2026، على الساعة 23:14، على الرابط: https://algeriemaintenant.dz

[2] شهيرة مسعود، **الجريمة الالكترونية في التشريع الجزائري**، مذكرة ماستر تخصص قانون عام، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس مستغانم، 14 جويلية 2021، ص 35.

[3] **قرار صادر عن المحكمة العليا**، غرفة الجنح والمخالفات، ملف رقم 1185414، المؤرخ في 20 جويلية 2023، قضية (ع.م) ومن معه ضد (د.م) والنيابة العامة، منشور على الموقع الالكتروني للمحكمة العليا، تم الاطلاع عليه يوم 25 مارس 2026، على الساعة 23:30، على الرابط: https://www.coursupreme.dz

[4] اية الوصيف، **جرائم التزوير في القانون الجزائري**، موقع محاماة نت، بتاريخ 12 أكتوبر 2019، اطلع عليه بتاريخ 25 مارس 2026، الساعة 23:44، عبر الرابط: https://www.mohamah.net.

الفضاء الرقمي[1]، أما على مستوى الآليات الوقائية، فقد سعت الجزائر إلى تعزيز قدراتها في مجال الأمن السيبراني من خلال تحديث الأنظمة وتدريب الكوادر وتطبيق أفضل الممارسات الدولية لمكافحة الجرائم الإلكترونية[2].

نرى أن التدرج في العقوبات يعكس فلسفة تشريعية رصينة تأخذ بعين الاعتبار مبدأ تناسب العقوبة مع الجريمة، غير أننا نعتقد أن غياب التفاصيل الإجرائية الدقيقة لتطبيق هذه العقوبات قد يُضعف فعاليتها، فمثلاً، رغم أن قانون 18-07 ينص على إنشاء ANPDP ، إلا أن فعالية هذه الهيئة تبقى مرهونة بمدى استقلاليتها المالية والإدارية، وقدرتها على التدخل الفوري في حالات الانتهاك[3] كما نلاحظ أن المشرع قد اهتم بالعقوبات الرادعة على حساب الوقاية والتوعية، حيث تظهر الوثيقة اهتماماً محدوداً بالبرامج التوعوية للمواطنين بمخاطر تزوير البيانات، وعليه، نرى ضرورة تطوير استراتيجية وطنية شاملة تجمع بين الحماية القانونية والتقنية والتربوية لمواجهة هذه الظاهرة.

ختاماً، نستنتج أن التشريع الجزائري قد وضع منظومة قانونية متينة تستهدف حماية الأفراد والمؤسسات من جريمة تزوير البيانات، مع الحفاظ على التوازن بين تسهيل المعاملات الرقمية وضمان أمن المعلومات، غير أن هذه المنظومة تظل بحاجة إلى مراجعة دورية لمواكبة التطورات التكنولوجية المتسارعة.

الفرع الثاني: تزوير المواقع الالكترونية والبريد الالكتروني

نستهلُّ بحثنا في هذا الفرع بالإشارة إلى أن التحول الرقمي المتسارع الذي تشهده الجزائر في مختلف مناحي الحياة الاقتصادية والإدارية والاجتماعية، قد أدى إلى انتشار واسع للمواقع الإلكترونية والبريد الإلكتروني كوسائل أساسية للتواصل والتعاملات التجارية والإدارية، مما ولَّد ظاهرة جنائية جديدة تمثلت في تزوير هذه الوسائل الرقمية بهدف الاحتيال والخداع والتضليل[4]، فقد أصبحت جرائم تزوير المواقع الإلكترونية والبريد الإلكتروني من أخطر الجرائم المعلوماتية التي تهدد الأمن الاقتصادي والاجتماعي للأفراد والمؤسسات على حد سواء، نظراً لسهولة ارتكابها وصعوبة كشفها وسرعة انتشارها عبر الحدود الإلكترونية، وقد سعت الجزائر إلى

---

[1] قرانة عادل، بوحديد فارس، **مهام السلطة الوطنية لحماية المعطيات الشخصية في التشريع الجزائري**، مجلة العلوم القانونية والاجتماعية، جامعة زيان عاشور الجلفة، المجلد 06، العدد 02، جوان 2021، ص 1059.

[2] طباش عزالدين، **الحماية الجزائية للمعطيات الشخصية في التشريع الجزائري دراسة في ظل القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي**، المجلة الأكاديمية للبحث القانوني، العدد 02، 2018، ص 29.

[3] **الأحكام الجديدة في قانون مكافحة التزوير واستعمال المزور: تعزيز الردع وحماية الثقة العامة**، موقع وكالة الأنباء الجزائرية، 30 جوان 2024، تم الاطلاع عليه يوم 25 مارس 2026، على الساعة 23:56، على الرابط: https://www.aps.dz/ar/algerie/164434-2024-06-30-14-15-54.

[4] القانون رقم 09-04 المؤرخ في 5 أوت 2009، المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47، سنة 2009.

مواكبة هذه التطورات من خلال سن قوانين وآليات تستهدف مكافحة هذه الظواهر التي تهدد الأفراد والمؤسسات على حد سواء [1]، ومن هنا، نسعى في هذا الفرع إلى تفكيك المنظومة القانونية الجزائرية المتعلقة بهذه الجرائم، عبر الوقوف على المفهوم القانوني الدقيق لها، والأسس التشريعية المواجهة لها، والعقوبات والآليات الوقائية المقررة، وذلك بغية تقديم رؤية تحليلية نقدية تستجيب لمتطلبات البحث العلمي.

أولا: المفهوم القانوني وتكييف جريمة تزوير المواقع والبريد الإلكتروني

نؤكد أن التشريع الجزائري لم يضع تعريفاً مستقلاً وصريحاً ومباشراً لجريمة "تزوير المواقع الالكترونية" أو "تزوير البريد الالكتروني" بشكل منفصل، وإنما يندرج مفهوم هذه الأفعال تحت قوانين أوسع تتعلق بالجرائم الإلكترونية والتزوير بشكل عام[2]، ففيما يخص تزوير المواقع الإلكترونية، يُقصد به إنشاء موقع إلكتروني يحاكي موقعاً أصيلاً رسمياً أو تجارياً بهدف تضليل المستخدمين والاحتيال عليهم، سواء كان ذلك لسرقة البيانات الشخصية(Phishing التصيد الاحتيالي) أو لجمع الأموال وهمياً دون تقديم الخدمات أو المنتجات، أو نشر معلومات مضللة أو أخبار كاذبة[3]، وتتضمن صور تزوير المواقع إنشاء صفحات تسجيل دخول وهمية لخدمات البريد أو البنوك لسرقة بيانات الاعتماد، وإنشاء مواقع إخبارية مزيفة لنشر معلومات مضللة، وتقليد مواقع التسوق الإلكتروني لخداع المستهلكين وجمع أموالهم دون تقديم منتجات أو خدمات[4].

أما تزوير البريد الإلكتروني فيتمثل في إرسال رسائل إلكترونية وهمية تبدو وكأنها صادرة من جهات موثوقة (حكومية أو بنكية أو شركات شحن) بهدف خداع المستلم للكشف عن معلومات حساسة أو تنفيذ إجراءات معينة تضره، ويُعرف أيضاً بـ "الانتحال" أو "التصيد الاحتيال"(Phishing) [5] ، وتتضمن تكتيكات تزوير البريد الإلكتروني التصيد الاحتيالي (phishing) وإرسال رسائل بريد إلكتروني احتيالية تبدو وكأنها من مصدر موثوق لخداع الضحايا للكشف عن معلومات شخصية أو مالية، وانتحال الشخصية (spoofing) وتغيير عنوان المرسل في رسالة إلكترونية لتبدو وكأنها قادمة من شخص أو كيان آخر، وهجمات الرئيس التنفيذي BEC)

---

[1] **مدونة: كيف تبدأ مشروع تجارة الكترونية في الجزائر: الدليل الشامل**، افاكت (Evact)، تم الاطلاع عليه يوم 27 مارس 2026، على الساعة 17:32، على الرابط: https://evact.net

[2] عمارة فتيحة، **المرجع السابق**، ص 170.

[3] أحمد محمد محروس عبدالعال، **التزوير الاكتروني بين التشريع التقليدي واليات المواجهة الحديثة**، المجلة الأكاديمية للأبحاث والنشر العلمي، الاصدار 70، فيفري 2025، ص 54.

[4] عزة خولة، ربيع شيماء، **اليات مكافحة الجرائم الالكترونية في التشريع الجزائري**، مذكرة ماستر تخصص قانون الاعلام الي والانترنت، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الابراهيمي برج بوعريريج، سنة 2024، ص 41.

[5] شيخ سناء، شيخ محمد زكرياء، **مكافحة الجرائم الالكترونية في القانون الجزائري**، مقال بحثي منشور على منصة وميض الفكر، تم الاطلاع عليه بتاريخ 27 مارس 2026، على الساعة 18:07، على الرابط: https://wameedalfiker.com

(Scams وانتحال شخصية مسؤول في شركة لتنفيذ تعليمات مزيفة لتحويل أموال أو الكشف عن معلومات سرية[1].

نرى أن هذا الغياب التشريعي لتعريف مستقل ومحدد وصريح لتزوير المواقع الإلكترونية والبريد الإلكتروني يُعدُّ إشكالية قانونية جوهرية وخطراً على فعالية الحماية الجنائية، إذ يجعل التكييف القانوني لهذه الأفعال يعتمد بشكل كبير على اجتهاد القضاء في تطبيق النصوص العامة المتعلقة بالتزوير والاحتيال والاعتداء على أنظمة المعلومات [2]، كما نلاحظ أن الخلط بين مفهومي "تزوير المواقع" و"تزوير البريد" في النصوص القانونية قد يؤدي إلى صعوبة في تحديد الاختصاص القضائي والعقوبة المناسبة لكل جريمة على حدة، مما يستدعي من المشرع الجزائري إدخال تعديلات تشريعية تفرق بين هذه الأنواع من الجرائم الإلكترونية بشكل صريح ومحدد ومستقل .كما نعتقد أن التركيز على عنصر "الاحتيال" كركن أساسي في الجريمة قد يُضعف الحماية القانونية في حالات التزوير التي لا يتوافر فيها عنصر الخداع المباشر، ولكنها تشكل خطراً على النظام الاقتصادي الرقمي والثقة في المعاملات الإلكترونية.

ثانيا: الأساس القانوني والتشريعي المتكامل لمواجهة الجريمة

نُبرز أن الجزائر قد اعتمدت منظومة تشريعية متكاملة ومتشعبة تستهدف مواجهة جرائم تزوير المواقع الإلكترونية والبريد الإلكتروني بشكل خاص والجرائم الإلكترونية بشكل عام، تتمثل في مجموعة من النصوص القانونية التي تتكامل وتتداخل فيما بينها:

1. القانون 09-04 المؤرخ في 05 أوت 2009 المتعلق بالوقاية من الجرائم المرتبطة بتكنولوجيات المعلومات والاتصال، والذي يُعد الحجر الأساس في مكافحة الجرائم الإلكترونية بالجزائر، حيث يعرف الجريمة الإلكترونية بأنها كل فعل يستهدف المنظومات المعلوماتية، ويجرم الوصول غير المصرح به إلى الأنظمة المعلوماتية، وتشويه البيانات، ويُطبق أحكامه على تزوير المواقع الإلكترونية[3]، ويضع هذا القانون إطاراً قانونياً عاماً للجرائم المتعلقة بالمعلوماتية، حيث يجرم الوصول غير المصَّرح به إلى الأنظمة المعلوماتية وتغيير المعلومات والبيانات، ويحدد العقوبات التي تلحق بالأفعال التي تلحق ضرراً بالممتلكات أو الاقتصاد باستخدام الوسائل الإلكترونية[4].

---

[1] أحمد محمد محروس عبدالعال، **المرجع السابق**، ص56.

[2] عمار حشمان، **الجريمة المعلوماتية في التشريع الجزائري**، مذكرة ماستر تخصص ادارة التحقيقات الاقتصادية والمالية، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، جامعة قاصدي مرباح ورقلة، السنة الجامعية 2019/2018، ص60.

[3] القانون رقم 09-04 المؤرخ في 5 أوت 2009، المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47، سنة 2009.

[4] اية بن ميسية، **المرجع السابق**، ص50.

2. تعديلات قانون العقوبات الجزائري، التي نصت على معاقبة كل من أنشأ أو نشر محتوى رقمياً يتضمن أفعالاً مزيفة أو اختلاق أغراض تؤدي إلى الضرار بالآخرين، حيث يُعتبر البريد الإلكتروني مستنداً إلكترونياً يمكن أن يخضع لأحكام التزوير[1].

وفي هذا الصدد، نجد أن الاعتداءات على منتوجات الاعلام الالي تشكل الركن المادي الجوهري لتحقق الجريمة المعلوماتية؛ فهي تعد من أخطر صور الغش المعلوماتي نظرا لما تكتسيه وسيلة الحاسب الالي من خطورى تقنية، وبالرغم من أن المشرع الجزائري قد اقتدى بنظيره الفرنسي في اخضاع أفعال التزوير المعلوماتي للنصوص العامة للتزوير، الا أن واقع الممارسة يكشف عن فرق شاسع بين نصوص قانون العقوبات الجزائري والفرنسي في هذا المضمار، وعليه تبرز الحاجة الملحة لتجاوز القواعد التقليدية وعصرنتها من خلال ادراج نص خاص ومستقل بالتزوير المعلوماتي في قانون العقوبات الجزائري بما يضمن دقة التكييف وتفعيل الردع[2].

3. القانون 24-02 المؤرخ في 26 فيفري 2024 المتعلق بمكافحة التزوير واستعمال المزور، والذي يُعدُّ خطوة مهمة لتوسيع نطاق التجريم ليشمل المستندات الإلكترونية بشكل صريح، بما في ذلك المواقع الإلكترونية والبريد، مع تشديد العقوبات على التزوير الاقتصادي الذي يمس بالاقتصاد الوطني[3]، ويوسع هذا القانون نطاق التزوير ليشمل المستندات الإلكترونية بشكل صريح، بما في ذلك المواقع الإلكترونية والبريد، ويحدد عقوبات مشددة للتزوير تصل إلى عشر سنوات سجن، كما يتناول القانون "العملة الرقمية" والمزورات، ويغطي حالات التصيد الاحتيالي (phishing) عبر البريد والمواقع المزيفة التي يؤثر فيها التزوير على الاقتصاد[4].

4. الأمر 04/15 المتعلق بالتوقيع الإلكتروني والتصديق، الذي يحدد قواعد التوقيع الإلكتروني ويجرم استخدامه بشكل مشروع أو تزويره، مما يؤثر مباشرة على سلامة المعاملات الإلكترونية التي تتم عبر المواقع والبريد الإلكتروني، ويُعتبر تزوير التوقيع الإلكتروني جريمة خطيرة تقوض الثقة في المعاملات الرقمية[5].

---

[1] مسعود شهيرة، **الجريمة الالكترونية في التشريع الجزائري**، مذكرة ماستر تخصص قانون عام، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس مستغانم، جويلية 2021، ص67.

[2] ايمان بغدادي، **أثر تعديل قانون العقوبات الجزائري في التصدي للجريمة الالكترونية**، مجلة افاق للبحوث والدراسات، المركز الجامعي ايليزي، المجلد 02، العدد 02، جويلية 2019، ص190.

[3] **مقال: الاحكام الجديدة في قانون مكافحة التزوير واستعمال المزور محور يوم دراسي بالجزائر العاصمة**، جريدة هورايزون (Horizons)، 30 جوان 2024، تم الاطلاع عليه بتاريخ 27 مارس 2026، على الساعة 18:48، على الرابط: https://www.horizons.dz

[4] مصطفاوي أسامة، **التزوير في المستندات الالكترونية في القانون الجزائري**، مذكرة ماستر تخصص الادارة الالكترونية، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف بالمسيلة، سنة 2025، ص42.

[5] راضية مشري، **جريمة تزوير التوقيع الالكتروني في التشريع الجزائري**، حوليات جامعة قالمة للعلوم الاجتماعية والانسانية، جامعة 8 ماي 1945 قالمة، المجلد 19، العدد 20، جوان 2017، ص127.

نرى أن هذا التكامل التشريعي يعكس وعياً متزايداً لدى المشرع الجزائري بخطورة الجرائم الإلكترونية وتطور أساليب ارتكابها، غير أننا نلاحظ وجود تداخل كبير في الاختصاصات بين هذه النصوص، مما قد يؤدي إلى ازدواجية في الملاحقة القضائية أو الغموض في تحديد النص الأنسب للتطبيق [1]، كما نعتقد أن القانون 24-02 الجديد، رغم أهميته في توسيع نطاق التزوير ليشمل المستندات الإلكترونية، إلا أنه لم يعالج بشكل كافٍ وصريح خصوصية جرائم التصيد الاحتيالي (phishing) والاحتيال الإلكتروني المتطور التي تتزايد يومياً، مما يستدعي إصدار نصوص خاصة تجرم هذه الظاهرة بشكل مستقل ومفصل، كما نرى أن غياب التعريف الصريح لـ "الموقع الإلكتروني المزيف" و"البريد الإلكتروني المزور" في النصوص القانونية يجعل القضاء الجزائري في حاجة ماسة إلى جهود تفسيرية وتوضيحية من المجلس الأعلى للقضاء لتوحيد الممارسة القضائية في هذا المجال.

ثالثا: العقوبات المقررة والآليات الوقائية والرقابية

نُجمِع في هذا العنصر أن العقوبات في التشريع الجزائري تتفاوت بحسب جسامة الجريمة والضرر الناتج عنها، وتتناسب طردياً مع خطورة الجريمة وتأثيرها على الاقتصاد الوطني والمعاملات الرقمية:

ففي ظل القانون 09-04 وقانون العقوبات: تتراوح عقوبات السجن بين ثلاث إلى سبع سنوات في الحالات التي ينتج عنها إضرار جسيم، وتصل إلى خمس سنوات في حالات الاعتداء على الشرف، وتصل الغرامات إلى 500,000 دينار جزائري وقد تزداد لتصل إلى مليون دينار في الحالات الأكثر خطورة[2]، كما يمكن مصادرة الأجهزة والوسائل المستخدمة في ارتكاب الجريمة [3].

أما في ظل القانون24-02 : فقد ارتقت العقوبات إلى السجن لمدة تصل إلى عشر سنوات في حالات التزوير الاقتصادي الإلكتروني الذي يمس بالاقتصاد الوطني، مثل تزوير موقع بنكي للاحتيال، مع الحفاظ على العقوبات المالية المشددة[4]، كما يجرم القانون أفعال التزوير المتعلقة بالتوقيع الإلكتروني والمفاتيح الرقمية، ويُعامل بصرامة في المعاملات الرقمية[5].

نرى أن التدرج في العقوبات يعكس فلسفة تشريعية رصينة تأخذ بعين الاعتبار مبدأ تناسب العقوبة مع الجريمة والضرر الناتج عنها، غير أننا نعتقد أن العقوبات المالية قد لا تكون رادعة بما فيه الكفاية في ظل

---

[1] يزيد بوحليط، **الجرائم الالكترونية والوقاية منها في القانون الجزائري**، د.ط، دار الجامعة الجديدة، الاسكندرية، سنة 2019، ص55.

[2] عزة خولة، ربيع شيماء، **المرجع السابق**، ص52.

[3] مزيان كمال، **المرجع السابق**، ص 37.

[4] **مقال: الاحكام الجديدة في قانون مكافحة التزوير واستعمال المزور محور يوم دراسي بالجزائر العاصمة**، جريدة هورايزون (Horizons)، 30 جوان 2024، تم الاطلاع عليه بتاريخ 27 مارس 2026، على الساعة 18:48، على الرابط: https://www.horizons.dz

[5] راضية مشري، **المرجع السابق**، ص134.

الربحية العالية لهذه الجرائم، وخاصة تلك التي تستهدف البنوك والمؤسسات المالية الكبرى أو الأفراد من ذوي الدخل المرتفع[1] ، كما نلاحظ أن المشرع الجزائري لم يولِ اهتماماً كافياً بالآليات الوقائية والتقنية والتوعوية، حيث تركز النصوص بشكل كبير على الجانب العقابي والرادع على حساب التوعية والتثقيف الرقمي للمواطنين وتعزيز الوعي الأمني السيبراني، وعليه، نرى ضرورة تطوير استراتيجية وطنية شاملة تجمع بين الحماية القانونية والتقنية والتربوية والتوعوية لمواجهة ظاهرة تزوير المواقع والبريد الإلكتروني، تشمل إنشاء وحدات متخصصة في الشرطة القضائية للتحقيق في الجرائم الإلكترونية، وتعزيز التعاون الدولي نظراً للطبيعة العابرة للحدود لهذه الجرائم، ومواكبة التطور التكنولوجي السريع في مجالات الذكاء الاصطناعي والتقنيات الرقمية الجديدة[2].

ختاماً، نستنتج أن التشريع الجزائري قد وضع منظومة قانونية متينة تستهدف حماية الأفراد والمؤسسات من جرائم تزوير المواقع الإلكترونية والبريد الإلكتروني، مع الحفاظ على التوازن بين تسهيل المعاملات الرقمية وضمان أمن المعلومات، غير أن هذه المنظومة تظل بحاجة إلى مراجعة دورية ومستمرة لمواكبة التطورات التكنولوجية المتسارعة والتحديات الجديدة التي تفرضها الجرائم الإلكترونية المعقدة.

الفرع الثالث: تزوير البطاقات البنكية ووسائل الدفع الالكتروني

نستهلُّ بحثنا في هذا الفرع بالإشارة إلى أن التحول الرقمي المتسارع الذي تشهده الجزائر في مختلف مناحي الحياة الاقتصادية والمصرفية قد أدى إلى انتشار واسع للبطاقات البنكية ووسائل الدفع الإلكتروني كأدوات حيوية في النظام المصرفي والاقتصادي اليومي، مما ولَّد ظاهرة جنائية معقدة تمثلت في تزوير هذه الوسائل الرقمية بهدف الاحتيال وسرقة الأموال والممتلكات،[3] فقد أصبحت جرائم تزوير البطاقات البنكية ووسائل الدفع الإلكتروني من أخطر الجرائم المعلوماتية التي تهدد الثقة في المعاملات الرقمية وتُلحق أضراراً جسيمة بالأفراد والمؤسسات المالية على حد سواء، نظراً لسهولة ارتكابها وتطور أساليب المجرمين في التلاعب بالبيانات المصرفية والتقنيات الحديثة[4]، ومن هنا، نسعى في هذا الفرع إلى تفكيك المنظومة القانونية الجزائرية المتعلقة بهذه الجرائم، عبر الوقوف على الأسس التشريعية المواجهة لها، وأنواع البطاقات المستهدفة، والآليات الوقائية والعقوبات والمسؤوليات المقررة، وذلك بغية تقديم رؤية تحليلية نقدية تستجيب لمتطلبات البحث العلمي الرصين.

---

[1] عمار حشمان، **المرجع السابق**، ص71.

[2] شيخ سناء، شيخ محمد زكرياء، **مكافحة الجرائم الالكترونية في القانون الجزائري**، مقال بحثي منشور على منصة وميض الفكر، تم الاطلاع عليه بتاريخ 27 مارس 2026، على الساعة 18:07، على الرابط: https://wameedalfiker.com

[3] فريد مشري واخرون، **الحماية القانونية لوسائل الدفع الالكتروني –الجزائر نموذجا–** ، مداخلة في ملتقى وطني بعنوان: المستهلك والاقتصاد الرقمي: ضرورة الانتقال وتحديات الحماية، المركز الجامعي عبد الحفيظ بوالصوف–ميلة، يومي 23 و24 افريل 2018، ص02.

[4] كوثر سعدي، رضوان بن صاري، **حماية وسائل الدفع الالكتروني The Electronic Payment Protection**، مجلة الدراسات القانونية، جامعة يحي فارس بالمدية ، سنة 2023، تم الاطلاع عليه يوم 28 مارس 2026، على الساعة 12:54، على الرابط: https://theses-algerie.com/artivle/details/35728.

أولا: الأساس القانوني والتشريعي المتكامل لمواجهة جريمة التزوير

نؤكد أن الجزائر قد بنت منظومة قانونية متعددة الأبعاد ومتكاملة تستهدف معالجة قضية تزوير البطاقات البنكية ووسائل الدفع الإلكتروني، تتمثل في مجموعة من النصوص القانونية التي تتكامل وتتداخل فيما بينها لتوفير حماية شاملة:

1. القانون 09-04 المؤرخ في 05 أوت 2009 المتعلق بالوقاية من الجرائم المرتبطة بأنظمة المعلومات، والذي يُعد حجر الزاوية في مكافحة تزوير البطاقات البنكية في الجزائر، فقد نص هذا القانون على عقوبات صارمة تتراوح بين الحبس من ثلاث إلى سبع سنوات وغرامة مالية تصل إلى خمسمائة ألف دينار جزائري (500,000د.ج) في حال الوصول غير المصَّرح به إلى أنظمة الدفع الإلكتروني أو تزوير البيانات والبطاقات .كما يغطي هذا القانون عمليات الاحتيال عبر الإنترنت وتقليد البطاقات المصرفية مثل بطاقات CIB والبطاقة الذهبية، مما يوفر إطاراً عاماً لحماية الأنظمة المعلوماتية المصرفية[1].

2. القانون 18-05 المؤرخ في 10 ماي 2018 المتعلق بالتجارة الإلكترونية، الذي يهدف إلى تنظيم المعاملات الرقمية وتوفير بيئة آمنة للمستهلكين، فقد تضمنت مواده من 27 إلى 29 ضمانات واضحة وصريحة تفرض على البنوك التزامات باتجاه تأمين التحويلات المالية وحماية المستهلكين من سرقة البطاقات أو استخدامها للاحتيال، مع عقوبات جنائية مشددة تصل إلى السجن خمس سنوات وغرامة تصل إلى مليون دينار جزائري (1,000,000د.ج) في حال التلاعب بالبطاقات أو استخدامها للاحتيال[2].

3. القانون 15-04 المؤرخ في 18 فيفري 2015 المتعلق بالتوقيع الإلكتروني والتصديق، الذي يعزز الحماية القانونية للدفع الإلكتروني عبر الاعتراف بالتوقيع الإلكتروني كدليل قانوني قاطع، وقد نص هذا القانون على معاقبة تزوير التوقيع الإلكتروني بالحبس الذي يتراوح بين سنة وثلاث سنوات وغرامة تصل إلى ثلاثمائة ألف دينار جزائري (300,000د.ج)، مما يُطبق بشكل مباشر على عمليات الدفع الإلكتروني التي تعتمد على التحقق الرقمي والتوقيع الإلكتروني في المعاملات البنكية[3].

4. الأمر رقم 66-156 المؤرخ في 08 جوان 1966 (القانون الجنائي الجزائري)، وخاصة المواد 368 المتعلقة بالاحتيال، والمادة 374 المتعلقة بالتزوير في العمليات التجارية، والمادة 303 المتعلقة بحماية الوثائق . تطبق هذه النصوص على أشكال الاحتيال المنطوي على التزوير في البطاقات البنكية، حيث تتراوح العقوبات

---

[1] غزالي نزيهة، **الاليات القانونية لحماية وسائل الدفع الالكتروني في التشريع الجزائري**، مجلة البحوث السياسية والادارية، جامعة محمد لمين دباغين سطيف 2، المجلد 06، العدد 01، ص 288.

[2] قمراوي حفيظة، **الحماية القانونية لبطاقة الدفع الالكتروني في التشريع الجزائري**، اطروحة دكتوراه تخصص قانون الاعمال المقارن، كلية الحقوق والعلوم السياسية، جامعة وهران2 محمد بن أحمد، سنة 2025، ص255.

[3] غزالي نزيهة، **المرجع السابق**، ص289.

بين الحبس من سنتين إلى خمس سنوات وغرامة تُعادل ضعف القيمة المسروقة، مما يوفر غطاءً قانونياً واسعاً ومكملاً لمكافحة هذه الجرائم[1].

نرى أن هذا التكامل التشريعي يعكس وعياً متزايداً وناضجاً لدى المشرع الجزائري بخطورة الجرائم المعلوماتية المستهدفة للقطاع المصرفي والمالي، غير أننا نلاحظ وجود تداخل كبير في الاختصاصات بين هذه النصوص القانونية، مما قد يؤدي في الممارسة العملية إلى ازدواجية في الملاحقة القضائية أو الغموض في تحديد النص الأنسب للتطبيق على حالة معينة[2].

كما نعتقد أن القانون 18-05 ، رغم أهميته النوعية في حماية المستهلكين، إلا أنه لم يحدد بشكل كافٍ ودقيق الآليات التقنية الإلزامية التي يجب على البنوك اعتمادها لحماية البطاقات البنكية، مما يترك مجالاً واسعاً للاجتهاد القضائي والتفسيرات المتباينة، كما نرى أن غياب نص صريح ومحدد يجرم "تزوير البطاقة البنكية" كجريمة مستقلة ومنفصلة في القانون الجنائي يجعل التكييف القانوني يعتمد على نصوص عامة قد لا تتوافق تماماً مع خصوصية الجريمة الإلكترونية المعقدة والمتطورة.

ثانيا: أنواع البطاقات البنكية المستهدفة بالتزوير والآليات التقنية للحماية

نُبرز أن هناك عدة أنواع شائعة ومختلفة من البطاقات البنكية في الجزائر تُعتبر أدوات حيوية في النظام المصرفي وتساهم بشكل كبير في تسهيل المعاملات اليومية للمواطنين، وتتمثل في الأنواع التالية:

1. بطاقات CIB (البنوك بين البطاقات)، وهي البطاقات الأساسية والمحورية في النظام المصرفي الجزائري التي تتيح إجراء المعاملات والتحويلات المالية بين مختلف البنوك المحلية الجزائرية[3].

2. البطاقة الذهبية، وهي بطاقة يصدرها بريد الجزائر تهيمن على حصة كبيرة من السوق المصرفية وتُستخدم على نطاق واسع في عمليات السحب النقدي والدفع الإلكتروني[4].

3. البطاقات الدولية مثل Visa وMasterCard، التي تصدرها العديد من البنوك الجزائرية وتتميز بكونها تتيح للمستخدمين إجراء معاملات مالية عالمية، وتأتي هذه البطاقات عادةً مزودة بشريحة ذكية ورقم سري لتعزيز مستوى الأمان[5].

---

[1] غولم بونفلة، **أثر اليقظة الاستراتيجية على الأداء المتميز للمؤسسات الاقتصادية: دراسة حالة عينة من المؤسسات الجزائرية**، أطروحة دكتوراه تخصص ادارة الأعمال، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة 08 ماي 1945 قالمة، سنة 2021، ص40.

[2] وليد لعماري، **الضمانات القانونية ضد مخاطر استخدام وسائل الدفع الالكتروني**، مجلة العلوم القانونية والسياسية، جامعة الشهيد حمه لخضر الوادي، المجلد 11، العدد 01، جانفي 2020، ص 56.

[3] فريد مشري واخرون، **الحماية القانونية لوسائل الدفع الالكتروني –الجزائر نموذجا–** ، مداخلة في ملتقى وطني بعنوان: المستهلك والاقتصاد الرقمي: ضرورة الانتقال وتحديات الحماية، المركز الجامعي عبد الحفيظ بوالصوف–ميلة، يومي 23 و24 افريل 2018، ص04.

[4] فريد مشري واخرون، **المرجع نفسه**، ص04.

[5] فريد مشري واخرون، **المرجع السابق**، ص04.

ومن حيث الآليات الوقائية والتقنية، نؤكد أن الجهود الجزائرية تتضمن مجموعة من التدابير المتطورة :

الشريحة الذكية (PIN): تزود معظم البطاقات البنكية حالياً بشريحة ذكية تتطلب إدخال رقم سري سرير، مما يزيد من صعوبة التزوير والاستخدام غير المصرح به[1].

كلمات المرور لمرة واحدة (OTP): تُستخدم كطبقة أمان إضافية للتحقق من هوية المستخدم في المعاملات عبر الإنترنت[2].

الرسائل النصية القصيرة (SMS): ترسلها البنوك للعملاء عند إجراء أي عملية باستخدام بطاقاتهم لاكتشاف أي نشاط مشبوه فوراً[3].

رقم التحقق CVV2 : وهو الرقم المكون من ثلاثة أو أربعة أرقام الموجود على ظهر البطاقة والذي يضيف طبقة أمان أخرى للمعاملات عبر الإنترنت [4].

نرى أن تنوع البطاقات البنكية في الجزائر يعكس تطوراً إيجابياً ومتقدماً في الخدمات المصرفية الرقمية، غير أننا نلاحظ أن البطاقة الذهبية لبريد الجزائر، رغم انتشارها الواسع بين فئات عريضة من المستخدمين، إلا أنها قد تكون أكثر عرضة للتزوير والاحتيال نظراً لاعتمادها الكبير من قبل شرائح اجتماعية قد لا تكون على دراية كافية بالإجراءات الأمنية والوقائية اللازمة [5].

كما نعتقد أن غياب توحيد المعايير الأمنية بين البطاقات المحلية (CIB) والبطاقات الدولية (Visa/MasterCard) قد يخلق ثغرات أمنية يستغلها المحتالون والمجرمون الإلكترونيون، مما يستدعي من بنك الجزائر إصدار تعليمات رقابية أكثر صرامة تلزم جميع المصارف باعتماد أعلى معايير الأمان الذكي والتشفير . كما نرى ضرورة تعزيز الوعي الرقمي لدى المستخدمين بشكل أكبر وأشمل، حيث أن الرسم البياني التحليلي أسفله يشير بوضوح إلى أن الوعي المستهلكي يتطلب تحسيناً مستمراً ودائماً لمواكبة سرعة الاحتيال وتطور أساليبه.

---

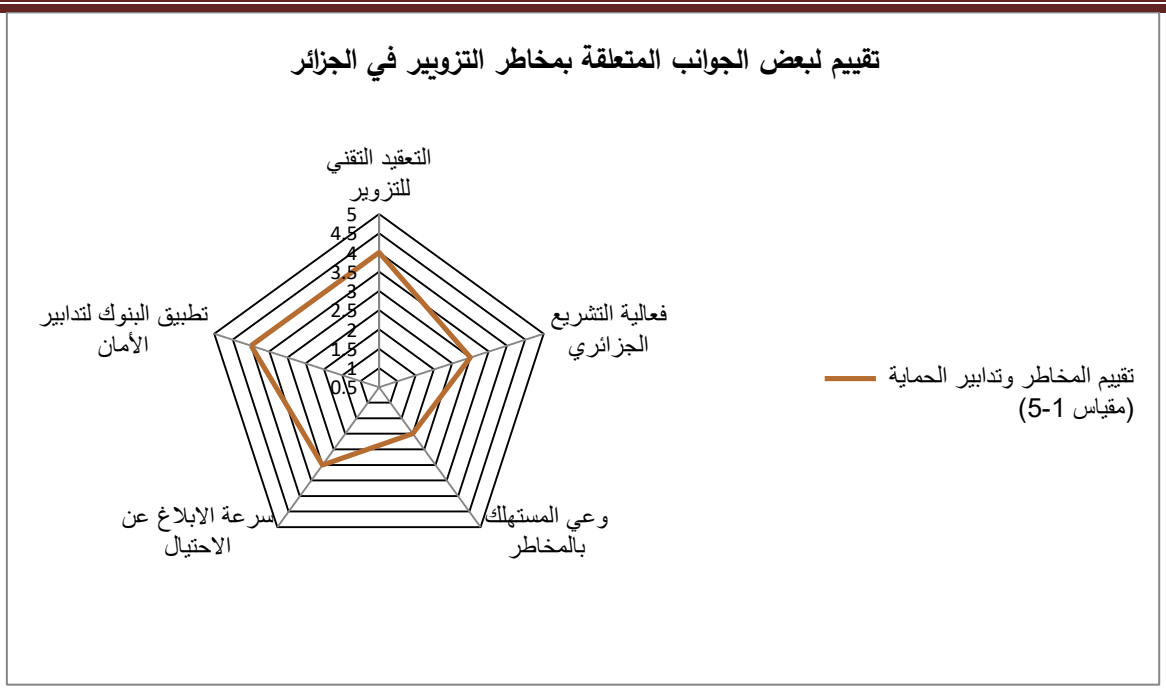
[1] مروة ظافري، نهى ياسمين يونس، **حماية المستهلك من مخاطر الدفع الالكتروني**، مذكرة ماستر تخصص قانون أعمال، كلية الحقوق والعلوم السياسية، جامعة 20 أوت 1955 سكيكدة، جوان 2023، ص 48.

[2] مروة ظافري، نهى ياسمين يونس، **المرجع نفسه**، ص48.

[3] مروة ظافري، نهى ياسمين يونس، **المرجع السابق**، ص48

[4] مروة ظافري، نهى ياسمين يونس، **المرجع السابق**، ص48

[5] بوجمعة شهرزاد، عيشاوي امال، **مظاهر الحماية القانونية لوسائل الدفع الالكتروني في التشريع الجزائري**، مجلة البحوث والدراسات القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة البليدة 2 –لونيسي علي، المجلد 13، العدد 01، جانفي 2024، ص40.



المصدر: من اعداد الطالبتين، بالاعتماد على التقديرات والتحديات الحالية، 2026.

ثالثا: العقوبات الجنائية والمسؤولية المدنية والمداولات القضائية

نُجمِع في هذا المطلب أن العقوبات والمسؤوليات في التشريع الجزائري تتفاوت وتتدرج بحسب جسامة الجريمة ونوعها والضرر الناتج عنها:

من حيث العقوبات الجنائية: تتراوح العقوبات بين الحبس من ثلاث إلى سبع سنوات وغرامات مالية تصل إلى مليون دينار جزائري، مع إمكانية مصادرة الأجهزة والوسائل المستخدمة في ارتكاب الجريمة [1].

ومن حيث المسؤولية المدنية: يلزم القانون البنوك بتعويض الضرر الناتج عن التزوير إذا ثبت إهمالها في تطبيق تدابير الأمان والحماية اللازمة، مع تحديد سقف قانوني للمسؤولية البنكية بمبلغ خمسين ألف دينار (50,000د.ج) في حال الإبلاغ الفوري عن الحادثة خلال مدة أربع وأربعين ساعة (48ساعة) [2].

ما تُعرَّف المسؤولية الجنائية للأشخاص الطبيعية والاعتبارية المتورطين في عمليات التزوير، سواء كانوا مزورين أو مستخدمين أو متواطئين، وقد تمتد هذه المسؤولية إلى الحدود الدولية في حال ارتباط التزوير باتفاقيات دولية انضمت إليها الجزائر مثل اتفاقية بودابست لسنة 2001.[3]

[1] بنك الجزائر، تعليمات رقم 01-25، المؤرخة في 02 مارس 2025، المتعلقة بشروط الترخيص بتأسيس واعتماد بنك ومؤسسة مالية، الجزائر، سنة 2025.

[2] بوزينة امنة امحمدي، **النظام القانوني للتعامل ببطاقة الائتمان المتداولة في البنوك الجزائرية**، مجلة القانون، معهد العلوم القانونية والادارية، المركز الجامعي أحمد زبانة بغليزان، العدد 08، جوان 2018، ص37.

[3] حسينة شرون، عبد الحليم بن مشري، **الحماية القانونية لبطاقات الدفع الالكترونية** ، مجلة الاجتهاد القضائي، جامعة محمد خيضر بسكرة، المجلد 12، العدد 01، مارس 2019، ص75.

نرى أن التدرج في العقوبات يعكس فلسفة تشريعية رصينة تأخذ بعين الاعتبار مبدأ تناسب العقوبة مع الجريمة والضرر الناتج عنها، غير أننا نعتقد أن سرعة الإبلاغ المحددة في القانون (48ساعة) قد تكون قصيرة جداً ومجحفة بالنسبة للمستخدمين الذين لا يتابعون حساباتهم البنكية باستمرار أو الذين يقعون ضحية الاحتيال في فترات الإجازات أو العطل، مما قد يحرمهم من حق التعويض المشروع[1].

كما نرى أن السقف المالي المحدد للمسؤولية (50,000دينار) قد لا يكون كافياً ولا عادلاً لتغطية الخسائر الكبيرة التي قد يتكبدها المستخدمون في حالات الاحتيال المعقدة والمتطورة، مما يستدعي مراجعة هذا السقف بما يتناسب مع التضخم الاقتصادي وطبيعة المخاطر الرقمية المتزايدة .كما نلاحظ أن المشرع الجزائري لم يولِ اهتماماً كافياً بالجانب الوقائي والتوعوي، حيث تركز النصوص بشكل كبير على الجانب العقابي والزجري على حساب التوعية والتثقيف المصرفي للمواطنين.

ختاماً، نستنتج أن التشريع الجزائري قد وضع منظومة قانونية متينة ورصينة تستهدف حماية الأفراد والمؤسسات من جرائم تزوير البطاقات البنكية ووسائل الدفع الإلكتروني، مع الحفاظ على التوازن بين تسهيل المعاملات الرقمية وضمان أمن المعلومات والممتلكات، غير أن هذه المنظومة تظل بحاجة إلى مراجعة دورية ومستمرة لمواكبة التطورات التكنولوجية المتسارعة والتحديات الجديدة التي تفرضها الجرائم الإلكترونية المعقدة والمتطورة.

المبحث الثاني: الأركان القانونية لجريمة التزوير الرقمي

يشكل مبحث الأركان القانونية لجريمة لتزوير الرقمي محورا أساسيا في دراسة الجرائم المعلوماتية، اذ يتناول البنية التشريعية التي تقوم عليها المسؤولية الجنائية في هذا النوع من الجرائم، وقد اقتضت طبيعة الجريمة الرقمية المستحدثة تطويرا ملحوظا في النظرية القانونية التقليدية، خاصة فيما يتعلق بعناصر قيام الجريمة وأركانها المكونة[2].

لقد أدرك المشرع الجزائري مبكراً ضرورة مواكبة التطور التكنولوجي الهائل في مجال نظم المعلومات والاتصالات، فسعى إلى إرساء قواعد قانونية خاصة تحمي الأنظمة المعلوماتية والبيانات الرقمية من الاعتداءات التي تطالها، ويعد القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المتضمن تعديل قانون العقوبات، والذي أضاف قسماً خاصاً بـ"المساس بأنظمة المعالجة الآلية للمعطيات"، الحجر الأساس في هذا المجال[3].

---

[1] **المديرية العامة للضرائب تحذر المواطنين من منصات الدفع الالكترونية غير الرسمية**، صادر عن موقع أخبار بلا حدود، منشور في مارس 2026، تم الاطلاع عليه يوم 28 مارس 2026، على الساعة 22:47، على الرابط: https://unlimited-news

[2] عمار فتيحة، **جريمة التزوير الالكتروني**، مجلة القانون والمجتمع، جامعة أدرار، المجلد 07، العدد 01، جوان 2019، ص 170.

[3] القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، المعدل و المتمم للأمر رقم 66-156 والمتضمن قانون العقوبات، الجريدة الرسمية، العدد 71، الصادرة بتاريخ 10 نوفمبر 2004.

إن جريمة التزوير الرقمي تختلف جوهرياً عن الجريمة التقليدية من حيث الوسيلة المستخدمة والمحل المادي والنتائج المترتبة عليها .ففي حين يقتصر التزوير التقليدي على المحررات الورقية، يمتد التزوير الرقمي ليشمل البيانات الإلكترونية والمعلومات المخزنة أو المعالجة أو المنقولة عبر الأنظمة المعلوماتية[1].

ومع التطور المستمر في أساليب الاختراق والتلاعب بالبيانات، أصدر المشرع الجزائري القانون رقم 24-06 المؤرخ في 28 أفريل 2024 المعدل والمتمم لقانون العقوبات، والذي جاء ليعزز الحماية الجزائية في ظل التحول الرقمي المتسارع، وقد تضمن هذا التعديل أحكاماً جديدة تهم مكافحة جرائم التزوير بشكل عام، مع مراعاة الخصوصيات الرقمية للجرائم المعلوماتية[2].

ومن ثم، يقتضي دراسة هذه الجريمة تفكيكاً دقيقاً لأركانها القانونية الثلاثة: الركن الشرعي الذي يحدد محل الحماية الجنائية، والركن المادي الذي يتمثل في السلوك الإجرامي ونتيجته، والركن المعنوي المتمثل في القصد الجنائي، وقد اكتسبت هذه الأركان خصوصية مميزة في ظل البيئة الرقمية، مما استدعى تطوير مقاربات فقهية جديدة تستوعب طبيعة هذه الجرائم العابرة للحدود[3].

المطلب الأول: الركن الشرعي (محل الحماية)

لا يمكن تكييف أي سلوك إجرامي في الفضاء الرقمي دون الاستناد إلى قاعدة قانونية واضحة تكرس مبدأ الشرعية الجنائية ،وبالنسبة لجريمة التزوير الرقمي، فقد أدرك المشرع الجزائري أنَّ النصوص التقليدية المتعلقة بتزوير المحررات الورقية لم تعد كافية لمواجهة التلاعب بالنبضات الإلكترونية والمعطيات الافتراضية ،ومن هذا المنطلق، استحدث المشرع منظومة قانونية متكاملة تبدأ بتحديد "محل الحماية" المتمثل في النظام المعلوماتي، وصولاً إلى تجريم الأفعال التي تمس بصحة البيانات، وهو ما يستدعي منا البحث في ماهية هذا النظام كركيزة شرعية أولى للجريمة.

الفرع الأول: النظام المعلوماتي أو نظام المعالجة الالية للمعطيات

يُعدّ تحديد المفهوم القانوني للنظام المعلوماتي، أو ما يُطلق عليه في المصطلح التقني "نظام المعالجة الآلية للمعطيات"، من المسائل الأكاديمية والعملية المحورية التي تؤسس لكل منهج علمي رصين في مجال قانون الجرائم الإلكترونية بصفة عامة، والتزوير الرقمي بصفة خاصة؛ ذلك أن هذا النظام لا يمثل مجرد بيئة تقنية محايدة، بل يشكل في الوقت ذاته محلاً مادياً للاعتداء الجنائي ووسيلة تنفيذية للجرائم المعلوماتية، مما

---

[1] نجيمي جمال، **جرائم التزوير في قانون العقوبات الجزائري**، د.ط، دار هومة للطباعة والنشر، الجزائر، د.ت.ن، ص269.

[2] القانون رقم 24-06 المؤرخ في 28 أفريل 2024، المعدل و المتمم للأمر رقم 66-156 والمتضمن قانون العقوبات، الجريدة الرسمية، العدد 30، الصادرة بتاريخ 30 أفريل 2024.

[3] شيخ سناء، شيخ محمد زكرياء، **مكافحة الجرائم الالكترونية في القانون الجزائري**، مقال بحثي منشور على منصة وميض الفكر، تم الاطلاع عليه بتاريخ 2 أفريل 2026، على الساعة 18:47، على الرابط: https://wameedalfiker.com

يفرض على الباحث الوقوف المستفيض على طبيعته القانونية، وحدوده الموضوعية، وعلاقته بالمكونات المادية وغير المادية، ومدى نجاعة التشريع الجزائري في استيعاب هذه الثنائية المعقدة، وقد حاول المشرع الجزائري استقراء هذا المفهوم في نصوص قانون 09-04 المؤرخ في 05 أوت 2009 المتعلق بالوقاية من الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال ومكافحتها[1]، لكن هذا الاستقراء ظل محل نقاش نظري وتطبيقي، مما يستدعي تفكيكاً منهجياً لأبعاده المختلفة.

أولا: المفهوم القانوني للنظام المعلوماتي بين البعد التقني والحماية الجنائية

يُعرّف التشريع الجزائري في إطاره التقني "نظام المعالجة الآلية للمعطيات" بأنه: "مجموعة متكاملة من الأجهزة المادية (كالحواسيب والخوادم والمعدات الطرفية) والعناصر غير المادية (كالبرامج والتطبيقات والبيانات والمعلومات المشفرة والوصلات)، التي تتيح معالجة البيانات واستخراج النتائج" [2]، وهذا التعريف الوارد ضمن نصوص قانون 09-04 يكشف عن اختيار المشرع الجزائري اعتماد مفهوم تقني شامل ينظر إلى النظام كوحدة متكاملة(Unité intégrée) ، لا كمجرد مجموعة من المكونات المنفصلة؛ فالحماية الجنائية هنا لا تقتصر على الحاسوب كمادة، بل تمتد لتشمل البرامج والمعطيات والوصلات التي تؤلف منظومة المعلومات بكاملها[3].

ويتجلى من هذا التحديد أن المشرع قد سعى إلى تجاوز النظرة التقليدية المادية المجردة، ليؤسس لحماية جزائية شاملة تستهدف البيئة الرقمية ككيان مستقل، وهو ما يمثل تحولاً نوعياً في الفلسفة الجنائية؛ إذ إن الجرائم المعلوماتية، ومنها التزوير الرقمي، لا ترتكز على الاعتداء المادي المباشر على الأشياء المحسوسة، بل على المساس بالمنظومة الرقمية بوصفها بنية تحتية معلوماتية[4]، وقد أكدت المحكمة العليا الجزائرية في أحكامها المتعلقة بإثبات التحريف في الوثائق الإدارية الرقمية، على ضرورة تحديد طبيعة المحرر وتاريخ صدوره وطريقة التحريف المتبعة، مما يعكس إدراك القضاء العالي لهذه الطبيعة المركبة للنظام المعلوماتي[5].

---

[1] القانون رقم 09-04 المؤرخ في 5 أوت 2009، المتعلق بالوقاية من الجرائم المرتبطة بتكنولوجيات الاعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47، الصادر بتاريخ 16 أوت 2009.

[2] المحامية مروة أبو العلا، **بحث متميز حول خصوصية الجرائم الالكترونية في التشريع الجزائري والتشريعات المقارنة**، منشور على موقع محاماة نت، بتاريخ 20 أفريل 2018، تم الاطلاع عليه بتاريخ 2 أفريل 2026، على الساعة 19:07، على الرابط: https://mohamah.net.

[3] يعيش تمام شوقي، خليفة محمد، **نظام المعالجة الالية للمعطيات الالكترونية كأساس للحماية الجزائية في التشريع الجزائري**، مركز جيل البحث العلمي، بتاريخ 16 أوت 2018، تم الاطلاع عليه بتاريخ 2 أفريل 2026، على الساعة 19:14، على الرابط: https://jilrc.com.

[4] القانون رقم 09-04 المؤرخ في 5 أوت 2009، المتعلق بالوقاية من الجرائم المرتبطة بتكنولوجيات الاعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47، الصادر بتاريخ 16 أوت 2009.

[5] قرار صادر عن المحكمة العليا، الغرفة الجزائية، ملف رقم 1185414، المؤرخ في 20 جويلية 2023، قضية (ع.م) ومن معه ضد (د.م) والنيابة العامة، منشور عبر الموقع الرسمي للمحكمة العليا، تم الاطلاع عليه بتاريخ 2 أفريل 2026، على الساعة 19:23، على الرابط: https://coursupreme.dz

ثانيا: ثنائية المحل والأداة في طبيعة النظام المعلوماتي

إن ما يميز التحليل القانوني للنظام المعلوماتي في سياق التزوير الرقمي هو الثنائية الوظيفية التي يؤديها؛ فمن جهة، يشكل النظام محلاً مادياً للجريمة (Objet matériel de l'infraction) عندما يكون الهدف المباشر للاعتداء هو المساس بسلامته الوظيفية، سواء كان ذلك عن طريق الدخول غير المشروع إليه، أو التلاعب بالبيانات المخزنة فيه، أو الحذف أو الإتلاف غير المشروع[1]، وقد نص قانون 09-04 صراحة على تجريم كل مساس بالنظام المعلوماتي، معتبراً أن هذا المساس يمسّ بالنظام بذاته، بغض النظر عن المكونات المادية المحددة[2].

ومن جهة أخرى، يؤدي النظام المعلوماتي دور الوسيلة أو الأداة (Moyen ou instrument) لارتكاب جرائم التزوير؛ فالحاسوب والشبكات المعلوماتية يمكن استخدامها في إنشاء بيانات كاذبة، أو تزوير رموز وبرامج، أو إنشاء توقيعات إلكترونية مزورة، أو حتى تزوير بطاقات ائتمان رقمية، وهنا يبرز التشابك المعقد بين النظام كهدف والنظام كوسيلة، حيث يصعب في كثير من الحالات فصل الاعتداء على النظام نفسه عن استخدامه في ارتكاب أفعال تزوير تستهدف أنظمة أخرى أو بيانات مخزنة فيها[3].

وقد لاحظنا أن المشرع الجزائري قد دمج بين هاتين الوظيفتين في نصوص موحدة، فعاقب في آن واحد على الاعتداء المباشر على النظام (الدخول غير المشروع، التخريب، الحذف)، وعلى استخدام النظام في ارتكاب أفعال التزوير الرقمي؛ وهو ما يعكس إدراكاً عميقاً للطبيعة المركبة للجرائم المعلوماتية التي لا يمكن فصل فيها بين الوسيلة والهدف، ويؤكد المحامي فيصل محمود في الفيديو التوضيحي المتعلق بمفهوم الجرائم الإلكترونية في التشريع الجزائري، على أن هذا التكامل بين المحل والأداة هو ما يميز النظام الجزائري عن النظم التقليدية، مما يستدعي تطوير آليات تحقيق وإثبات متخصصة[4].

ثالثا: مكافحة التزوير الرقمي في إطار النظام المعلوماتي

لقد اهتم المشرع الجزائري بتجريم التزوير الرقمي على النحو الذي يتلاءم مع خصوصية النظام المعلوماتي، فلم يقتصر على تطبيق القواعد العامة للتزوير المنصوص عليها في قانون العقوبات (المواد 191

---

[1] بوضياف اسمهان، **الجريمة الالكترونية والاجراءات التشريعية لمواجهتها في الجزائر**، مجلة الاستاذ الباحث للدراسات القانونية والسياسية، العدد 11، ماي 2018، ص 357.

[2] بوضياف اسمهان، **المرجع السابق**، ص358.

[3] عمار حشمان، **الجريمة المعلوماتية في التشريع الجزائري**، مذكرة الماستر، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، جامعة قاصدي مرباح، ورقلة، 02 جويلية 2019، ص 37.

[4] فيصل محمودي، **"المحامي فيصل محمودي يوضح مفهوم الجرائم الالكترونية بنظر القانون"**، فيديو يوتيوب على قناة Echorouk News، تم النشر يوم 12 جانفي 2026، تم الاطلاع عليه بتاريخ 2 أفريل 2026، على الساعة 21:00، على الرابط: https://www.youtube.com/watch?v=jC6e05PxCQq

إلى198)، بل استحدث نصوصاً خاصة تتناول التزوير في البيئة الرقمية .فقانون 09-04 يجرم تزوير البيانات والمعطيات في أنظمة المعالجة الآلية، بينما يتناول قانون 15-04 المتعلق بالتوقيع الإلكتروني والتصديق، تزوير التوقيعات الإلكترونية واستخدامها بشكل غير مشروع، مؤكداً على أن التوقيع الإلكتروني يتمتع بنفس الحجية القانونية للتوقيع اليدوي، وبالتالي يستحق نفس الحماية الجنائية[1].

أما قانون 18-07 المؤرخ في 25 جويلية 2018 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، فيضيف بعداً آخر للحماية، إذ يعالج جانباً محدداً من جوانب التزوير الرقمي المتمثل في تزوير البيانات الشخصية المعالجة آلياً، مما يعكس اهتماماً متزايداً بحماية البيانات ذات الطابع الشخصي كجزء لا يتجزأ من النظام المعلوماتي[2]، وتتفاوت العقوبات المقررة بحسب خطورة الجريمة وطبيعة النظام المستهدف؛ ففي حالة تزوير التوقيع الإلكتروني، تصل العقوبة إلى خمس سنوات حبساً وغرامة قدرها 500.000 دينار جزائري [3]، بينما تصل في حالة التزوير في الوثائق الرسمية الرقمية إلى عشر سنوات سجناً طبقاً للمادة 195 من قانون العقوبات[4].

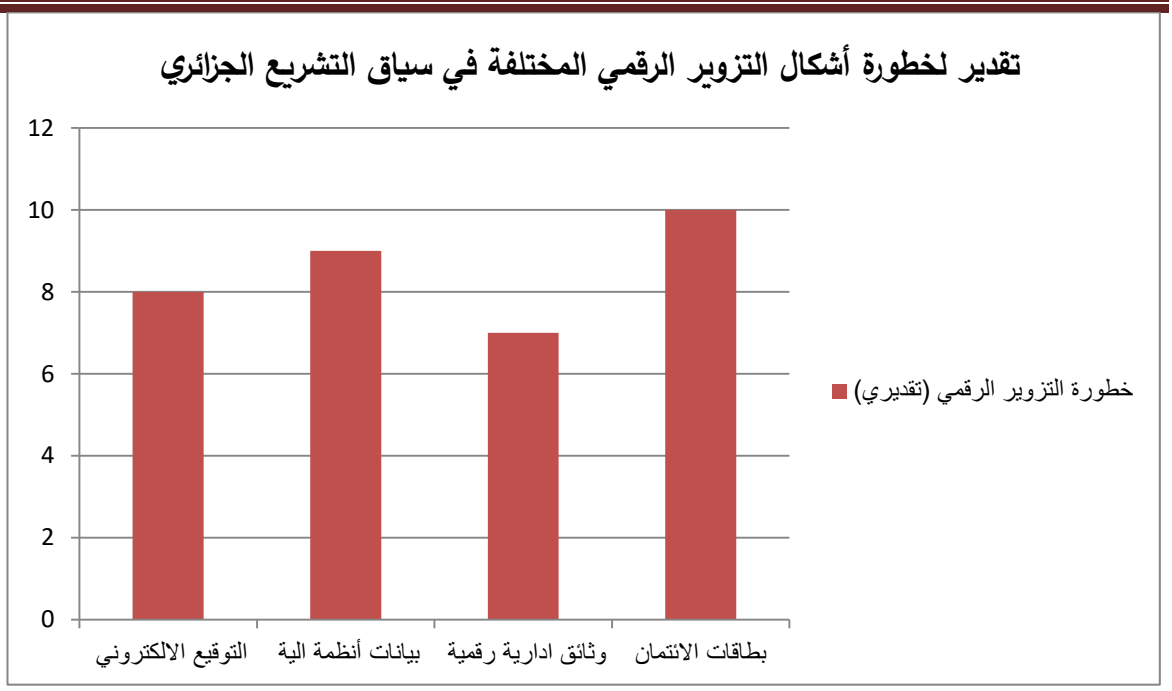
من خلال التمحيص في النصوص القانونية الجزائرية المتعلقة بالنظام المعلوماتي، يتبين لنا أن المشرع الجزائري قد قطع شوطاً مهماً في استيعاب خصوصية البيئة الرقمية، لكنه ظل في كثير من الأحيان مرتبطاً بالقواعد التقليدية للتزوير المنصوص عليها في قانون العقوبات .فالنصوص الخاصة بقانون09-04 ، رغم شموليتها، تفتقر أحياناً إلى الدقة التقنية المطلوبة في تحديد ماهية" النظام "بحد ذاته، مما قد يثير إشكاليات في التطبيق القضائي، خاصة فيما يتعلق بتحديد اللحظة التي يتحول فيها النظام من كونه مجرد أداة للتواصل إلى كونه محلاً للاعتداء الجنائي.

[1] القانون رقم 15-04 المؤرخ في 1 فيفري 2015، المتعلق بالقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، الجريدة الرسمية، العدد 06، الصادر في 10 فيفري 2015.

[2] القانون رقم 18-07 المؤرخ في 10 جوان 2018، المتعلق بحماية الاشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية، العدد 34، الصادر في جوان 2018.

[3] المادتين 56 و57 من القانون رقم 18-07 المؤرخ في 10 جوان 2018، المتعلق بحماية الاشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية، العدد 34، الصادر في جوان 2018.

[4] مصطفاوي أسامة، **التزوير في المستندات الالكترونية في القانون الجزائري**، مذكرة ماستر تخصص الادارة الالكترونية، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف بالمسيلة، السنة الجامعية 2025/2024، ص47.



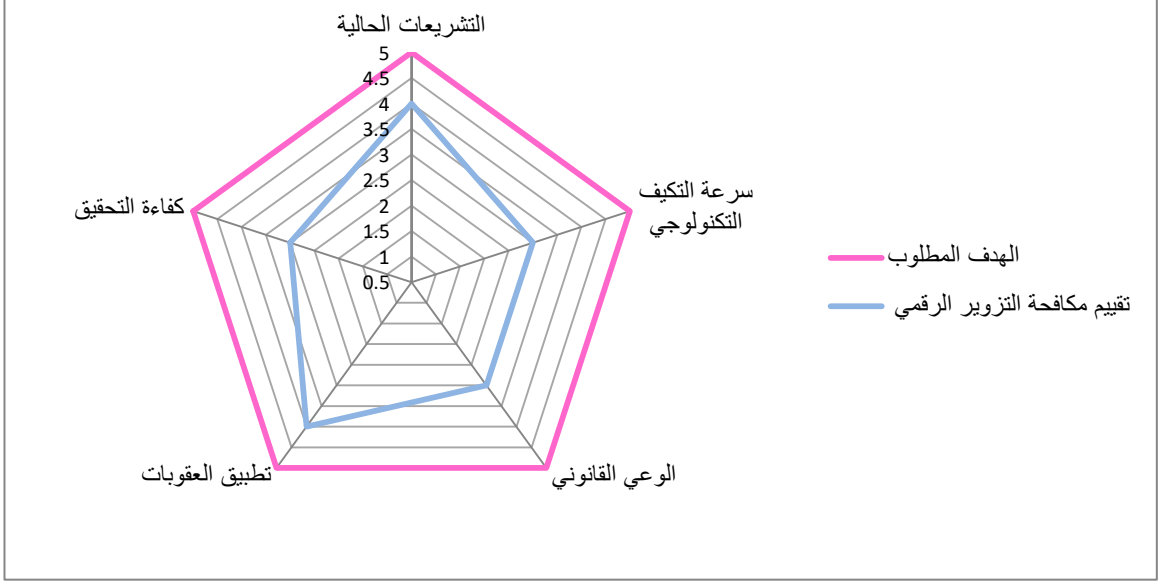
المصدر: من اعداد الطالبتين بالاعتماد على مقتضيات القانون رقم 04-09، 2026.

كما أن الرسم البياني أعلاه الذي يوضح تقدير خطورة أشكال التزوير الرقمي، يكشف عن أن بطاقات الائتمان تحظى بأعلى درجات الخطورة(10/10) ، تليها بيانات أنظمة الآلية(9/10) ، ثم التوقيع الإلكتروني (8/10)، ثم الوثائق الإدارية الرقمية(7/10) ؛ وهذا التصنيف يطرح تساؤلات جوهرية حول مدى تلاؤم العقوبات المقررة مع هذه الخطورة، حيث نلاحظ أن العقوبات المقررة لتزوير التوقيع الإلكتروني (5سنوات) أقل مما قد تقتضيه خطورة هذا النوع من الجرائم على الثقة في المعاملات الإلكترونية.

علاوة على ذلك، يظهر من الرسم البياني الرداري المقارن أسفله بين الوضع الحالي والهدف المنشود في مكافحة التزوير الرقمي، أن هناك فجوات كبيرة في مجالات كفاءة التحقيق وتطبيق العقوبات والوعي القانوني، مقارنة بالتشريعات الحالية، وهو ما يؤكد ضرورة إحداث هيئة وطنية للرقابة ومتابعة الجرائم الإلكترونية بشكل مستقل، مع تطوير البنية التحتية التكنولوجية وتدريب الكوادر القضائية والأمنية على آليات التحقيق الرقمي[1].

[1] سعيدة بوزنون، **مكافحة الجريمة الالكترونية في التشريع الجزائري، مجلة العلوم الانسانية**، جامعة منتوري بقسنطينة، المجلد 30، العدد 05، ديسمبر 2019، ص50.

مقارنة بين الوضع الحالي لمكافحة التزوير الرقمي في الجزائر والهدف المنشود.



المصدر: من اعداد الطالبتين بالاعتماد على مخرجات الدراسة، 2026.

الفرع الثاني: البيانات الرقمية ذات الحجية الرقمية

يُعدّ مفهوم الحجية الرقمية من المفاهيم المحورية التي تشكّل ركيزة الأساس في النظام القانوني الحديث، خاصة في ظل التحول الرقمي المتسارع الذي تشهده الجزائر ومساعيها نحو بناء اقتصاد رقمي موثوق؛ إذ تمثل هذه الحجية القوة القانونية والإثباتية التي تُمنح للبيانات والمحررات الإلكترونية، مما يجعلها معادلة للمحررات التقليدية الورقية في إثبات الحقوق والالتزامات، ونظراً لطبيعة البيانات الرقمية القابلة للتعديل والتزييف بسهولة نسبية، فقد اقتضى الأمر من المشرع الجزائري وضع إطار قانوني دقيق يضمن صحة هذه البيانات وسلامتها ومصدرها، مع توفير ضمانات تقنية وقانونية تحول دون الطعن فيها أو التلاعب بها، وفي هذا الفرع، سنحاول تفكيك المفهوم القانوني للحجية الرقمية، مستقصين أركانها وشروطها في التشريع الجزائري، ومدى فعالية النصوص القانونية في تحقيق التوازن بين تسهيل المعاملات الإلكترونية وحمايتها من جرائم التزوير الرقمي.

أولا: المفهوم القانوني للحجية الرقمية وطبيعتها القانونية

تُعرّف الحجية الرقمية في إطارنا القانوني بأنها القوة القانونية والإثباتية الممنوحة للبيانات والمعلومات والمحررات الإلكترونية، بما يجعلها قابلة لإثبات الحقوق والالتزامات أمام المحاكم والإدارات بذات القوة المقررة للمحررات الورقية التقليدية[1]، ونلاحظ أن المشرع الجزائري قد تبنى في قانون 15-04 المتعلق بالتوقيع

[1] القانون رقم 15-04 المؤرخ في 1 فيفري 2015، المتعلق بالقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، الجريدة الرسمية، العدد 06، الصادر في 10 فيفري 2015.

الإلكتروني والتصديق مفهوماً واسعاً للحجية الرقمية، لم يقتصر على مجرد الاعتراف الشكلي بالمحرر الإلكتروني، بل امتد ليشمل الآلية التقنية التي تضمن ربط البيانات بالشخص الطبيعي أو المعنوي بشكل لا يقبل التنازع أو الانكار، وهو ما يُعرف بالتوقيع الإلكتروني الموثوق[1].

وتتميز الحجية الرقمية عن نظيرتها الورقية بأنها قائمة على التحقق التقني (Vérification technique) أكثر من اعتمادها على الشكليات المادية، إذ يكفي لإثبات صدور المحرر الإلكتروني التحقق من صحة التوقيع الإلكتروني وسلامة البيانات منذ إنشائها وحتى عرضها، وهو ما يستلزم بنية تحتية تقنية معقدة تتمثل في مقدمي خدمات التصديق والتوقيع الإلكتروني المعتمدين من قبل الهيئة المنظمة [2]، وقد أكدت الدراسات على أن هذا التحول نحو الحجية الرقمية يمثل ثورة في قواعد الإثبات القانونية، حيث أصبحت البيانات الرقمية ذاتها، بمجرد استيفائها الشروط القانونية، حجة قاطعة يصعب دحضها إلا بدليل تقني مضاد[3].

ثانيا: الأساس القانوني للحجية الرقمية ومرتكزاتها التشريعية

يستند الاعتراف القانوني بالحجية الرقمية في التشريع الجزائري إلى مجموعة من النصوص القانونية المتكاملة، يأتي في مقدمتها قانون 15-04 الصادر في 2005 (المعدل والمتمم) المتعلق بالتوقيع الإلكتروني والتصديق، والذي يُعدّ القانون الأم في هذا المجال[4]، وقد نص هذا القانون صراحة على أن المحررات الإلكترونية والتوقيعات الإلكترونية التي تستوفي شروط الصحة القانونية تتمتع بالحجية نفسها المقررة للمحررات والتوقيعات الورقية، مع مراعاة الخصوصيات التقنية التي تميز البيئة الرقمية[5]، كما أسهم قانون 24-02 المتعلق بمكافحة التزوير واستعمال المزور، الصادر في2024 ، في تعزيز هذه الحجية من خلال إقرار عقوبات مشددة

[1] المواد4،5،7 المتعلقة بالتوقيع الالكتروني الموثوق من القانون رقم 15-04 المؤرخ في 1 فيفري 2015، المتعلق بالقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، الجريدة الرسمية، العدد 06، الصادر في 10 فيفري 2015.

[2] القانون رقم 25-11 المؤرخ في 24 جويلية 2025 المعدل والمتمم للقانون رقم 18-07 المؤرخ في 10 جوان 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية، العدد 48، الصادر بتاريخ 24 جويلية 2025.

[3] يوسف مسعودي، رحاب أرجيلوس، **مدى حجية التوقيع الالكتروني في الاثبات في التشريع الجزائري (دراسة على ضوء أحكام القانون 15-04)**، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المركز الجامعي لتامنغست بأدرار، المجلد 06، العدد 01، جانفي 2017، ص83.

[4] القانون رقم 15-04 المؤرخ في 1 فيفري 2015، المتعلق بالقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، الجريدة الرسمية، العدد 06، الصادر في 10 فيفري 2015.

[5] القانون رقم 15-04 المؤرخ في 1 فيفري 2015، المتعلق بالقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، الجريدة الرسمية، العدد 06، الصادر في 10 فيفري 2015.

على تزوير البيانات الرقمية ذات الحجية القانونية، مما يخلق ردعاً جنائياً يحمي مصداقية المحررات الإلكترونية.[1]

أما قانون 25-11 المؤرخ في 24 جويلية 2025 (الموافق لـ 28 محرم1447) المتعلق بحماية البيانات الشخصية، فقد أضاف بعداً جديداً للحجية الرقمية، إذ اعتبر البيانات الشخصية التي تتم معالجتها رقمياً محمية بموجب قواعد خاصة، وألزم مقدمي الخدمات الإلكترونية بالتقيد بمعايير دقة وصحة هذه البيانات، مما يعني أن الحجية الرقمية هنا لا تقتصر على الإثبات، بل تمتد لتشمل الحماية الجنائية للبيانات من التلاعب أو التزوير[2]، وقد أوضحت الوكالة الجزائرية للأنباء (APS) في تقاريرها أن هذه التشريعات الثلاثة تشكل منظومة متكاملة لبناء الثقة الرقمية في الجزائر[3].

ثالثا: شروط الحجية الرقمية وضمانات صحتها

نرى أن الحجية الرقمية في التشريع الجزائري لا تكون مطلقة أو آلية، بل هي مشروطة بتحقق متطلبات تقنية وقانونية دقيقة، نتلخصها فيما يلي:

أ. التوقيع الإلكتروني الموثوق(Signature électronique qualifiée) ، والذي يجب أن يتم إنشاؤه بواسطة وسائل تقنية آمنة غير قابلة للاختراق، وأن يكون مرتبطاً بالمُوقّع بشكل فريد وغير قابل للنقل.

ب. سلامة البيانات(Intégrité des données) ، بمعنى أن تكون البيانات محمية ضد أي تعديل أو تغيير غير مصرح به منذ إنشائها.

ج. التصديق الإلكتروني (Certification électronique) الذي تقدمه جهات معتمدة من قبل الهيئة المنظمة للبريد والاتصالات(ARPCE) ، والذي يضمن هوية المُوقّع وصحة مفاتيح التوقيع[4].

كما نلاحظ أن المشرع قد اشترط قواعد بيانات موحدة (Bases de données unifiées) للتحقق السريع من صحة الوثائق والمحررات الإلكترونية، وهو ما يعزز من درجة الحجية ويقلل من فرص نجاح عمليات التزوير[5]،

---

[1] القانون 24-02 المؤرخ في 26 فيفري 2024، المتعلق بمكافحة التزوير واستعمال المزور، الجريدة الرسمية، العدد 15، الصادر بتاريخ 29 فيفري 2024.

[2] القانون رقم 25-11 المؤرخ في 24 جويلية 2025، المتعلق بحماية الاشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية، العدد 48، الصادر بتاريخ 24 جويلية 2025.

[3] **مجلس الأمة: المصادقة على القانون المحدد للقواعد العامة المتعلقة بخدمات الثقة للمعاملات الالكترونية**، وكالة الأنباء الجزائرية، منشور بتاريخ 21 جانفي 2026، تم الاطلاع عليه يوم 3 أفريل 2026، على الساعة 01:07، على الرابط: https://aps.dz.

[4] المادة 4 المتعلقة بشروط صحة التوقيع الالكتروني من القانون رقم 15-04 المؤرخ في 1 فيفري 2015، المتعلق بالقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، الجريدة الرسمية، العدد 06، الصادر في 10 فيفري 2015.

[5] المادة 5 المتعلقة بقواعد البيانات الموحدة للتحقق من صحة الوثائق من القانون رقم 15-04 المؤرخ في 1 فيفري 2015، المتعلق بالقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، الجريدة الرسمية، العدد 06، الصادر في 10 فيفري 2015.

وقد أكدت مجلة القانون والأعمال (Droit et Entreprise) على أن هذه الشروط مجتمعة تهدف إلى تحقيق الأمن القانوني (Sécurité juridique) في الفضاء الرقمي، وجعل البيانات الرقمية ذات حجية قاطعة في التعاملات الإدارية والتجارية [1].

رابعا: علاقة الحجية الرقمية بحماية البيانات الشخصية

تتجلى أهمية الحجية الرقمية في بعدها المتعلق بحماية البيانات الشخصية، حيث إن البيانات ذات الطابع الشخصي إذا ما تمت معالجتها رقمياً فإنها تكتسب حجية قانونية تتطلب حماية خاصة .وقد نص قانون 11-25على أن تقديم معلومات كاذبة أو مضللة في البيانات الشخصية المعالجة رقمياً يُعدّ جريمة جنائية، مما يؤكد على أن الحجية الرقمية هنا مزدوجة :فهي من جهة أداة إثبات للحقوق، ومن جهة أخرى محل لحماية جنائية مشددة[2].

ونرى أن هذا التداخل بين الحجية الرقمية وحماية البيانات الشخصية يخلق منظومة وطنية لحوكمة البيانات(Gouvernance des données) ، تهدف إلى ترسيخ سيادة الدولة الرقمية وضمان تبادل آمن للبيانات بين الإدارات المختلفة، مع منع حالات التزوير الرقمي التي قد تمس بهذه البيانات [3]، وقد أوضحت دراسات منشورة في موقع المركز الجامعي للبحث العلمي (CERIST) أن هذا النهج يعكس إدراكاً عميقاً لدى المشرع الجزائري بأن الحجية الرقمية لا يمكن أن تتحقق دون بيئة آمنة محمية من الاختراق والتزوير[4].

من خلال ما تقدم، نؤكد أن التشريع الجزائري قد قطع شوطاً كبيراً في إرساء قواعد الحجية الرقمية، لكننا نلاحظ أن هناك تحديات تطبيقية لا يزال العمل جارياً لتجاوزها؛ فالرسم البياني (الشكل الراداري) المقارن لتأثير القوانين المختلفة على مكافحة التزوير يظهر أن قانون 24-02 يتفوق في مجال تعزيز الحجية القانونية وتغطية أنواع التزوير، بينما يظل قانون 15-04 أقل فعالية في مجال سرعة التحقق مقارنة بالمعايير الدولية.

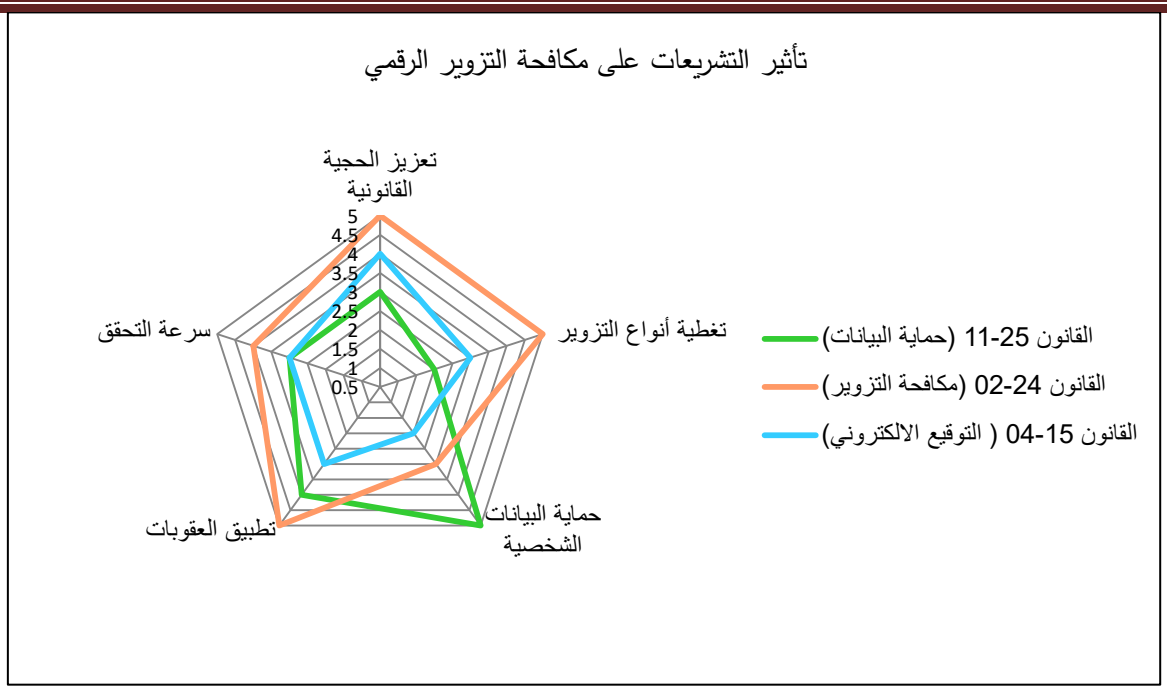
---

[1] يوسف مسعودي، رحاب أرجيلوس، **المرجع السابق**، ص85.

[2] القانون رقم 25-11 المؤرخ في 24 جويلية 2025، المتعلق بحماية الاشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية، العدد 48، الصادر بتاريخ 24 جويلية 2025.

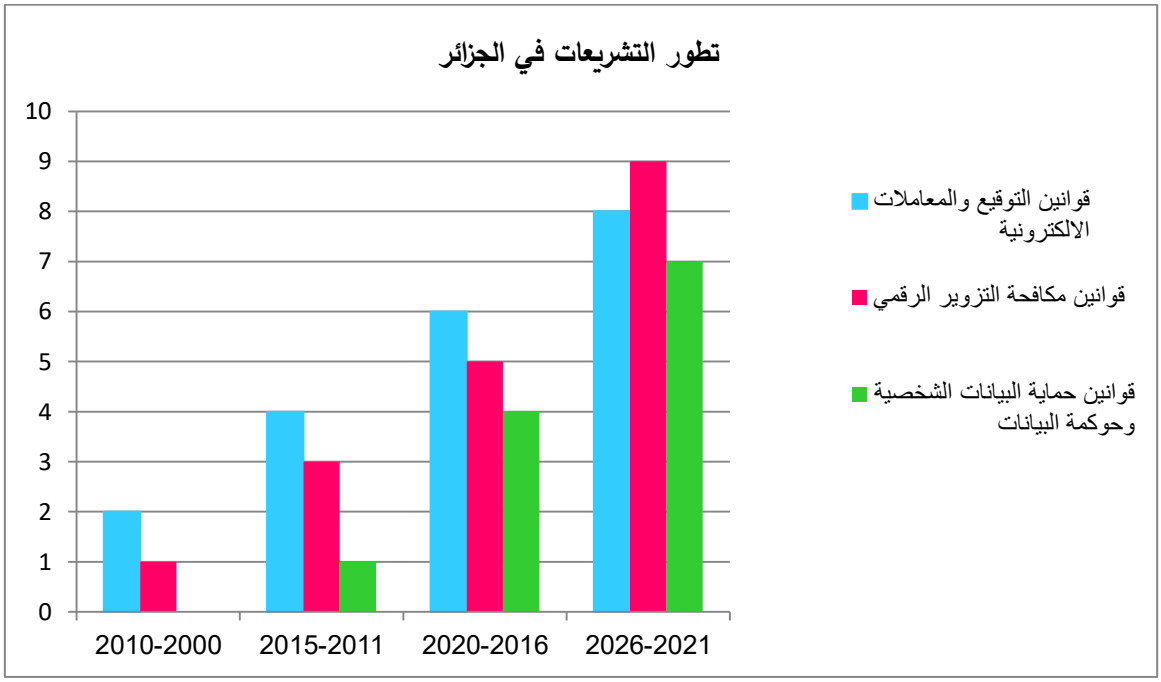
[3] **كلمة الوزير الأول خلال اشرافه على وضع المنظومة الوطنية لحوكمة البيانات حيز الخدمة**، منشور على الموقع مصالح الوزير الأول، بتاريخ 9 فيفري 2026، تم الاطلاع عليه يوم 3 أفريل 2026، على الساعة 1:39، على الرابط: https://premier-minister.gov.dz.

[4] بهادي عبد القادر، الصادق عبد القادر، **الحق في خصوصية البيانات الشخصية عبر المجال الرقمي وسبل حمايتها في التشريع الجزائري**، مجلة الحقيقة، جامعة احمد دراية بأدرار، المجلد 24، العدد 02، 05 ماي 2025، ص 21.



المصدر: من اعداد الطالبتين بالاعتماد على مخرجات الدراسة، 2026.

كما أن الرسم البياني الشريطي يوضح تطور التشريعات عبر الفترات (2010-2000، 2015-2020، 2016-2026، 2021) حيث نلاحظ ارتفاعاً ملحوظاً في قوانين مكافحة التزوير الرقمي وقوانين حماية البيانات في الفترة الأخيرة.



المصدر: من اعداد الطالبتين بالاعتماد على مخرجات الدراسة، 2026.

ونرى ضرورة تطوير البنية التحتية التقنية بشكل أكبر، وإنشاء سجل وطني موحد للمحررات الإلكترونية ذات الحجية، مع تكثيف التوعية القانونية للمواطنين بأهمية الحفاظ على سلامة بياناتهم الرقمية، كما نؤكد على ضرورة مواكبة التطور التكنولوجي السريع بتعديلات تشريعية مستمرة، خاصة في مجال الذكاء الاصطناعي والعقود الذكية، لضمان استمرار فعالية الحجية الرقمية في مواجهة أشكال التزوير المتطورة[1].

الفرع الثالث: المصلحة المحمية من تجريم التزوير الرقمي

يُعدّ التزوير الرقمي من الجرائم المعلوماتية الناشئة التي فرضتها متطلبات العصر الرقمي، والتي أصبحت تُشكّل تهديداً جوهرياً للمنظومة القانونية والاقتصادية والاجتماعية في المجتمعات المعاصرة، وقد اقتضى التصدي لهذا النوع من الجرائم تجاوز المنظور الجنائي التقليدي القائم على مفهوم التزوير المادي، إلى بلورة منظومة قانونية متكاملة تتناول خصوصيات الجريمة الرقمية وانعكاساتها المتعددة الأبعاد، وقد ارتكز المشرع الجزائري في هذا المسعى على حماية مصالح جوهرية تتجاوز مجرد معاقبة الفاعل، لتشمل صيانة الثقة في الفضاء الرقمي، وضمان سلامة المحررات الإلكترونية، وحماية أمن الدولة والمجتمع، ودعم الاقتصاد الرقمي، وتعزيز حجية الأدلة الرقمية في الإثبات، ومن ثم، يتعين التوقف عند هذه المصالح المحمية تحليلاً وتفصيلاً، لما لذلك من أهمية نظرية وتطبيقية في فهم الفلسفة التشريعية الجزائرية لمكافحة التزوير الرقمي.

أولا: صيانة الثقة في المعاملات الإلكترونية

تُشكّل الثقة في المعاملات الإلكترونية الركيزة الأساسية التي قام عليها المشرع الجزائري في تجريمه للتزوير الرقمي، إذ باتت المعاملات الإلكترونية جزءاً لا يتجزأ من الحياة اليومية للأفراد والمؤسسات على حد سواء، وقد أدرك المشرع أن غياب الثقة في هذه المعاملات يُعيق عجلة التقدم الرقمي، ويُشلّ الانتقال نحو الاقتصاد الرقمي المنشود، ومن هنا، جاء التجريم ليضمن أن المشاركة في معاملة رقمية ما يمكن الاعتماد على صحتها، وأن الأطراف المتعاقدة تتعامل بيانات ومعلومات مؤمنة، بما يشمل حماية خصوصية المستخدمين وسلامة البنية التحتية المعلوماتية [2].

ويتجلى هذا الهدف بوضوح في النصوص القانونية التي تُجرّم التلاعب بالبيانات والوثائق الإلكترونية، حيث يهدف المشرع إلى بناء بيئة رقمية آمنة وموثوقة تُشجع الأفراد والشركات على الانخراط في المعاملات

[1] سعيدة بوزنون، **المرجع السابق**، ص55.

[2] معمري ايمان، فضيلة شعبان، **مدى مواجهة المشرع الجزائري للجرائم الالكترونية "جريمة التزوير الالكتروني نموذجا"**، مداخلة في ملتقى:الدكتوراه الدولي متعدد الاختصاصات، جامعة الشهيد حمه لخضر الوادي، من 23 الى 26 فيفري 2020، ص12.

الإلكترونية دون خوف من الاحتيال أو التزوير .وقد أسهمت هذه التشريعات في خلق مناخ قانوني يضمن للمتعاملين في الفضاء الرقمي الحماية اللازمة لممتلكاتهم وحقوقهم[1].

نرى أن هذا الهدف يُعدّ من الأهداف الاستباقية في السياسة التشريعية الجزائرية، إذ يسعى المشرع من خلاله إلى خلق مناخ استثماري رقمي جاذب، ونلاحظ أن التحدي يكمن في مدى فعالية التطبيق العملي في ظل تطور أساليب الاحتيال الرقمي.

ثانيا: ضمان صحة المحررات والمعلومات الرقمية

تُعتبر صحة ومصداقية المحررات الإلكترونية والتوقيعات الرقمية من الأمور ذات الأهمية البالغة في الإثبات القانوني، إذ إن المحررات الرقمية تُعدّ بمثابة الوسيلة الأساسية لإثبات الحقوق والالتزامات في المعاملات المعاصرة، وقد أدرك المشرع الجزائري أن التزوير الرقمي يُهدد حقوق الأفراد والمؤسسات، وقد يؤدي إلى إنشاء مستندات مزورة تبدو أصلية، مما يُربك العدالة ويُعرّض الحقوق للضياع[2].

ولمواجهة هذا الخطر، تضمنت التشريعات الجزائرية نصوصاً تضمن أن المحررات الرقمية تعكس الحقيقة وتتعرض للتغيير بآلية مصرح بها قانوناً، مما يعزز من حجيتها في الإثبات ويجعلها موثوقة في النزاعات القانونية، وقد تجلى ذلك في القوانين المعدلة والمتممة، والتي وسّعت من نطاق التجريم لتشمل الأشكال الرقمية للتزوير، بما في ذلك التلاعب بالبيانات وتزوير التوقيعات الإلكترونية[3].

نرى أن هذا الهدف يُمثّل جوهر الحماية القانونية في مجال الإثبات الرقمي، ونلاحظ أن المشرع قد استلهم التجارب المقارنة، غير أن الصياغة القانونية لازالت بحاجة إلى مزيد من الدقة في تحديد معايير الصحة الرقمية.

---

[1] رياض/خ، **قانون مكافحة جرائم التزوير في الجريدة الرسمية**، جريدة البلاد، بتاريخ 13 مارس 2004، تم الاطلاع عليه يوم 3 أفريل 2026، على الساعة 20:16، على الرابط: https://elbilad.net

[2] **مقال: التنظيم القانوني للجريمة الالكترونية في التشريع الجزائري**، مجلة الفكر القانوني والسياسي، جامعة ابن خلدون تيارت، ردمد: 2588-2112، تم الاطلاع عليه عبر منصة مركز المعرفة الرقمي، بتاريخ 3 أفريل 2026، على الساعة: 20:24، على الرابط: https://ddl.ae

[3] **مجلس الأمة: المصادقة على نص قانوني بمكافحة التزوير واستعمال المزور**، الاذاعة الجزائرية، تم النشر يوم 30 جانفي 2024، تم الاطلاع عليه يوم 3 افريل 2026، على الساعة 20:28، على الرابط: https://news.radioalgerie.dz

ثالثا: حماية أمن الدولة والمجتمع

تمتدّ آثار التزوير الرقمي لتطال أمن الدولة والمجتمع بشكل مباشر، إذ يمكن أن يؤدي التلاعب بالوثائق الرسمية مثل جوازات السفر والهويات إلى تهديد الأمن القومي، ويسمح للمجرمين بالتهرب من العدالة، كما يمكن أن تكون تداعيات التزوير الرقمي أبعد من مجرد خسائر مالية، لتصل إلى المساس باستقرار المجتمع وحماية مصالحه العليا[1].

ولهذا، تضمن التشريع الجزائري حماية الأمن السيبراني وأمن المجتمع من خلال نصوص تُجرّم الاعتداء على الأنظمة المعلوماتية والتلاعب بالوثائق الرقمية ذات الصلة بالأمن الوطني، وقد أولى المشرع اهتماماً خاصاً بمكافحة الجرائم المنظمة والجماعية التي تستخدم التزوير الرقمي وسيلة لارتكاب جرائم أكثر خطورة، مما يعكس حرصه على صيانة النظام العام وحماية المجتمع من المخاطر الرقمية[2].

نرى أن هذا الهدف يُجسّد الطابع الاحترازي في السياسة الجنائية الجزائرية، ونلاحظ أن التنسيق الدولي يظلّ ضعيفاً في هذا المجال، ويحتاج إلى اتفاقيات تُسهّل تبادل المعلومات في قضايا التزوير الرقمي العابر للحدود.

رابعا: دعم الاقتصاد الرقمي وحماية المستهلكين

يسعى المشرع الجزائري، من خلال تجريم التزوير الرقمي، إلى بناء قانونية بيئة رقمية آمنة تُشجع الأفراد والشركات على الانخراط في المعاملات الإلكترونية دون خوف من الاحتيال، فالهدف لا يقتصر على معاقبة المزوّرين، بل يتعداه إلى خلق مناخ اقتصادي يحافظ على الثقة اللازمة لازدهار الاقتصاد الرقمي[3].

كما يلعب التجريم دوراً محورياً في حماية المستهلكين من العمليات الاحتيالية التي تستغل الثغرات الرقمية، إذ يضمن للمواطنين الحماية من وقوعهم ضحايا لهذه الجرائم، وقد تجلى ذلك في التشريعات التي تُجرّم التزوير في المعاملات التجارية الإلكترونية، والتي تهدف إلى حماية الحقوق المالية للمتعاملين وضمان نزاهة السوق الرقمي[4].

---

[1] أحمد محروس عبد العال، **المرجع السابق**، ص19.

[2] **جريمة تزوير المحررات في التشريع الجزائي الجزائري**، منشورات جامعة الدكتور مولاي الطاهر بسعيدة، كلية الحقوق والعلوم السياسية، تم الاطلاع عليه بتاريخ 3 أفريل 2026، على الساعة 20:36، على الرابط: https://budsp.univ-saida.dz/doc_num.php?explnum_id=2701

[3] عثمان لحياني، **الجزائر تتجه الى اصدار قانون جديد للحد من جرائم التزوير**، العربي الجديد، منشور بوم 29 ماي 2023، تم الاطلاع عليه يوم 3 أفريل 2026، على الساعة 28:42، على الرابط: https://www.alaraby.co.uk

[4] Rayan Khiari, Hayette Selmani, **Electronic Forgery As a Manifestation of Degital Corruption**, Journal of Legal Studies and Researches, volume 11, number 1, 15 january 2026, P 20.

نرى أن هذا الهدف يُمثّل التقاطعة بين القانون الجنائي والقانون الاقتصادي، ونلاحظ أن المشرع قد اقتصر في كثير من الأحيان على النصوص الجنائية، دون إقرار آليات مدنية فعالة لتعويض الضحايا.

خامسا: تعزيز حجية الأدلة الرقمية في الإثبات

يُعدّ التوقيع الإلكتروني والمحررات الرقمية من أهم وسائل الإثبات في العصر الرقمي، وقد حرص المشرع الجزائري على تعزيز حجيتها القانونية من خلال نصوص تضمن سلامتها وموثوقيتها، فالقانون رقم 15-04 المتعلق بالتوقيع الإلكتروني قد أسّس لنظام قانوني يُعطي للتوقيع الإلكتروني حجية قانونية كاملة، مكافئة للتوقيع اليدوي في كثير من الحالات[1] .

وقد تضمنت التعديات اللاحقة، وخاصة القانون رقم 18-07 المتعلق بمكافحة التزوير، نصوصاً تُجرّم تزوير التوقيع الإلكتروني والتلاعب بالمحررات الرقمية، مما يعكس اهتمام المشرع بتعزيز منظومة الإثبات الرقمي وضمان نزاهتها، ويُعدّ هذا الهدف من الأهداف المركزية في السياسة التشريعية الجزائرية، إذ يُسهم في بناء نظام قانوني مواكب للتطور التكنولوجي[2].

نرى أن هذا الهدف يُمثّل إنجازاً تشريعياً مهماً، ونلاحظ أن التحدي يكمن في انتشار استخدام التوقيع الإلكتروني المعتمد، والذي يظلّ محدوداً في الجزائر.

سادسا: ضمان نزاهة الخدمات الحكومية الرقمية

مع التحول الرقمي للإدارات العمومية، أصبحت نزاهة الخدمات الحكومية الإلكترونية من المصالح المحمية بقوة القانون، فالتزوير الرقمي في هذا السياق يمكن أن يُعرقل سير المرافق العامة ويُضر بالمصالح العامة، ولذا، تضمنت التشريعات الجزائرية نصوصاً خاصة بمكافحة التزوير في الوثائق الإدارية الإلكترونية، مع تشديد العقوبات في حالات تورط موظفين عموميين.[3]

وقد عكس قانون 2023 المتعلق بتشديد العقوبات على جرائم التزوير التزام الدولة بتوفير بيئة رقمية آمنة وموثوقة، حيث تصل العقوبات إلى السجن المؤبد في الحالات الخطيرة التي تمس بالأمن الجماعي أو تتضمن تورط منظمات إجرامية أو موظفين عموميين [4].

---

[1] سويلم فضيلة، **ضوابط التسويق الالكتروني في التشريع الجزائري**، مجلة القانون والعلوم السياسية، المركز الجامعي صالحي أحمد بالنعامة، المجلد 09، العدد 01، تاريخ النشر 30 أفريل 2023، ص 162.

[2] **المجلس الشعبي الوطني: المصادقة على مشروع القانون المتعلق بمكافحة التزوير واستعمال المزور**، الاذاعة الجزائرية، تم النشر يوم 21 ديسمبر 2023، تم الاطلاع عليه يوم 3 افريل 2026، على الساعة 21:23، على الرابط: https://news.radioalgerie.dz

[3] بوضياف اسمهان، **المرجع السابق**، ص373.

[4] سعيدة بوزنون، **المرجع السابق**، ص 58.

نرى أن هذا الهدف يُجسّد مبدأ النزاهة الإدارية في العصر الرقمي، ونلاحظ أن الفعالية تقتضي إقرار آليات رقابية تقنية تُمكّن من كشف التلاعب في الوقت الفعلي.

سابعا: العلاقة التكاملية بين المصالح المحمية

يُبرز المخطط الذهني المُرفق بالوثيقة العلاقة المعقدة بين المصالح المختلفة التي يحميها التشريع الجزائري من التزوير الرقمي، إذ تتداخل هذه المصالح وتتكامل فيما بينها لتشكل منظومة حماية شاملة، فالمصلحة المحمية من تجريم التزوير الرقمي لا تقتصر على جانب واحد، بل تمتد لتشمل الثقة في المعاملات الإلكترونية، وصحة المحررات الرقمية، وأمن الدولة والمجتمع، والاقتصاد الرقمي، والأمن السيبراني، والهوية الشخصية، والحفاظ على أمن الدولة.[1]

وتتجلى هذه العلاقة التكاملية في النصوص القانونية التي تُعالج التزوير الرقمي باعتباره جريمة مركبة، تُصيب عدة مصالح في آن واحد، مما يستدعي ردعاً تشريعياً متناسباً مع خطورة الفعل الإجرامي وانعكاساته المُتعددة، وقد عكس المشرع الجزائري هذا التكامل في صياغة النصوص القانونية، حيث تتضمن المواد الجنائية حماية متكاملة للمصالح المذكورة [2].

نرى أن هذا التكامل يُمثّل منهجاً علمياً في صياغة السياسة الجنائية، ونلاحظ أنه يحتاج إلى آليات تنسيقية بين مختلف الوزارات والأجهزة المعنية.

المطلب الثاني: الركن المادي للجريمة

لا تكتمل الجريمة قانوناً بمجرد النص عليها في الركن الشرعي، بل لا بد من تجسيدها في أرض الواقع من خلال ركن مادي قوامه سلوك إجرامي يمس بسلامة المعطيات المعلوماتية، ويتميز الركن المادي في التزوير الرقمي بكونه "سلوكا تقنيا" بامتياز، لا يتطلب بالضرورة وجود مجهود عضلي أو ملامسة مادية للمحرر، بل يكفي فيه التلاعب بالرموز الرقمية لتغيير الحقيقة التي أعد المحرر لإثباتها.

الفرع الأول: السلوك الاجرامي (تغيير الحقيقة بالوسيلة الرقمية)

يُعدّ الركن المادي من الأركان الأساسية التي تقوم عليها الجريمة في النظرية القانونية العامة، وهو يتجسد في السلوك الإجرامي المادي الصادر عن الإنسان سواء أكان إيجابياً أم سلبياً، وفي سياق جريمة التزوير الرقمي، يكتسب هذا الركن أهمية بالغة نظراً لطبيعة الوسيلة المستخدمة في ارتكاب الجريمة، إذ إن التطور التكنولوجي قد أفرز أساليب جديدة للاعتداء على الحقيقة تختلف جوهرياً عن الأساليب التقليدية، وقد حرص المشرع الجزائري على تحديد ماهية هذا السلوك الإجرامي بشكل دقيق، معتبراً أن الركن المادي في التزوير

[1] يوسف مسعودي، لرحاب أرجيلوس، **المرجع السابق**، ص95.

[2] مصطفاوي أسامة، **المرجع السابق**، ص 53.

الرقمي يتمثل في" تغيير الحقيقة بالوسيلة الرقمية"، مما يستلزم الوقوف عند خصائص هذا السلوك وعناصره وأشكاله لتحديد نطاق التجريم بدقة، وذلك في إطار المنظومة القانونية التي نظمتها القوانين رقم 09-04 و-05 18ونص المادة 195 مكرر من القانون الجنائي.

أولا: تعريف السلوك الإجرامي في التشريع الجزائري

يُعرّف الركن المادي لجريمة التزوير الرقمي في التشريع الجزائري بأنه" تغيير الحقيقة بالوسيلة الرقمية"، وهو تعريف يتجاوز المفهوم التقليدي للتزوير المقصور على المحررات المادية الورقية ليشمل كل أشكال التلاعب بالبيانات والمعلومات والمستندات الإلكترونية، فالسلوك الإجرامي هنا يقوم على فعل مادي ملموس يهدف إلى إظهار واقع مغاير للحقيقة، سواء كان ذلك عن طريق إنشاء محرر إلكتروني مزيف أو التلاعب في محتوى مستند إلكتروني موجود، ويشترط المشرع في هذا السلوك أن يكون متعمداً ومقصوداً، أي أن يصدر عن قصد جنائي يهدف إلى تحقيق فائدة غير مشروعة أو استخدام المحرر المزور، مما يميزه عن الأخطاء التقنية غير المقصودة [1].

وقد تناولت النصوص القانونية الجزائرية هذا السلوك في عدة مواد، أبرزها المادة 195 مكرر من القانون الجنائي التي تجرم "الحذف أو الإضافة أو التغيير في سجل أو وثيقة إلكترونية بقصد الاحتيال"، والمادة 244 المتعلقة بتزوير التوقيع، مما يعكس اهتماماً تشريعياً بتحديد الأفعال المكونة للجريمة بشكل دقيق وشامل[2].

نرى أن هذا التعريف يعكس مرونة المشرع الجزائري في مواكبة التطور التكنولوجي، إذ إن إطلاق مصطلح "الوسيلة الرقمية" يشمل كل التقنيات الحديثة والمستجدة دون حصرها في نصوص محددة، مما يضمن استمرارية النص القانوني وفعاليته في مواجهة أساليب الاحتيال المستجدة.

ثانيا: أشكال السلوك الإجرامي في التزوير الرقمي

يستقرئ التحليل القانوني للنصوص الجزائرية ثلاثة أشكال رئيسية للسلوك الإجرامي في التزوير الرقمي:

أ. التلاعب بالبيانات الإلكترونية: ويشمل التعديل أو الحذف أو الإضافة في بيانات إلكترونية موجودة، مثل تغيير قواعد البيانات المالية أو السجلات الإلكترونية أو العقود الرقمية، وقد نصت على هذا الشكل المادة 195مكرر من القانون الجنائي الجزائري[3] .

---

[1] مريم عيسات، **تزوير التوقيع الالكتروني**، مذكرة ماستر تخصص قانون الدولة والمؤسسات، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، سنة 2017، ص 49.

[2] راضية مشري، **جريمة تزوير التوقيع الالكتروني في التشريع الجزائري**، حوليات جامعة قالمة للعلوم الاجتماعية والانسانية، جامعة 8 ماي 1945 قالمة، المجلد 19، العدد 20، جوان 2017، ص130.

[3] رياض/خ، **قانون مكافحة جرائم التزوير في الجريدة الرسمية**، منشور على موقع البلاد نت، بتاريخ 13 مارس 2024، تم الاطلاع عليه يوم 6 أفريل 2026، على الساعة 21:11، على الرابط: https://www.elbilad.net

ب. إنشاء مستندات إلكترونية غير صحيحة: وهو إنشاء وثائق إلكترونية مزيفة من العدم تبدو أصلية، مثل تصميم وثيقة إلكترونية بالكامل تحاكي الواقع، أو إنشاء فواتير وهمية، أو شهادات جامعية مزورة إلكترونياً، وهذا الشكل يمثل التزوير الإيجابي الصرف[1].

ج. تزييف التوقيعات الرقمية: ويتمثل في إنشاء توقيع إلكتروني مزيف أو تقليد توقيع إلكتروني مشروع لتوثيق وثائق غير صحيحة، وتجرم هذه الحالة صراحة المادة 244 من القانون الجنائي، وهي من أخطر أشكال التزوير الرقمي لما للتوقيع الإلكتروني من حجية قانونية في الإثبات[2].

نرى أن هذا التصنيف يعكس شمولية المشرع الجزائري في معالجة مختلف صور التزوير الرقمي، مع ملاحظة أن هذه الأشكال قد تتداخل فيما بينها في الجريمة الواحدة، مما يستلزم الاعتناء بالتكييف القانوني الصحيح عند التطبيق.

ثالثا: تمييز السلوك الإجرامي في التزوير الرقمي عن التقليدي

رغم اشتراك التزوير الرقمي والتقليدي في الهدف الجنائي المتمثل في تغيير الحقيقة، إلا أن السلوك الإجرامي في النوع الأول يتميز بخصائص تقنية وقانونية جوهرية، ففي التزوير التقليدي، يقتصر السلوك على المحررات المادية الورقية ويتطلب مهارات يدوية في التقليد والتزييف، بينما في التزوير الرقمي، يمتد السلوك ليشمل البيانات الإلكترونية والتوقيعات الرقمية، ويتطلب معرفة تقنية متخصصة في البرمجيات وأنظمة الحماية الإلكترونية[3].

وتتجلى هذه الاختلافات في الرادار البياني المقارن ، حيث يظهر أن التزوير الرقمي يتفوق في أبعاد التلاعب بالبيانات وتزييف التوقيعات واستخدام الوسائل التقنية، بينما يبقى الضرر وإحداث الوثائق المزورة عنصراً مشتركاً بين النوعين، كما أن التزوير الرقمي يتسم بسرعة الانتشار عبر الشبكات الإلكترونية وسهولة النسخ والتداول، مما يجعل أثره الضار أشد وطأة على الثقة في المعاملات الرقمية[4].

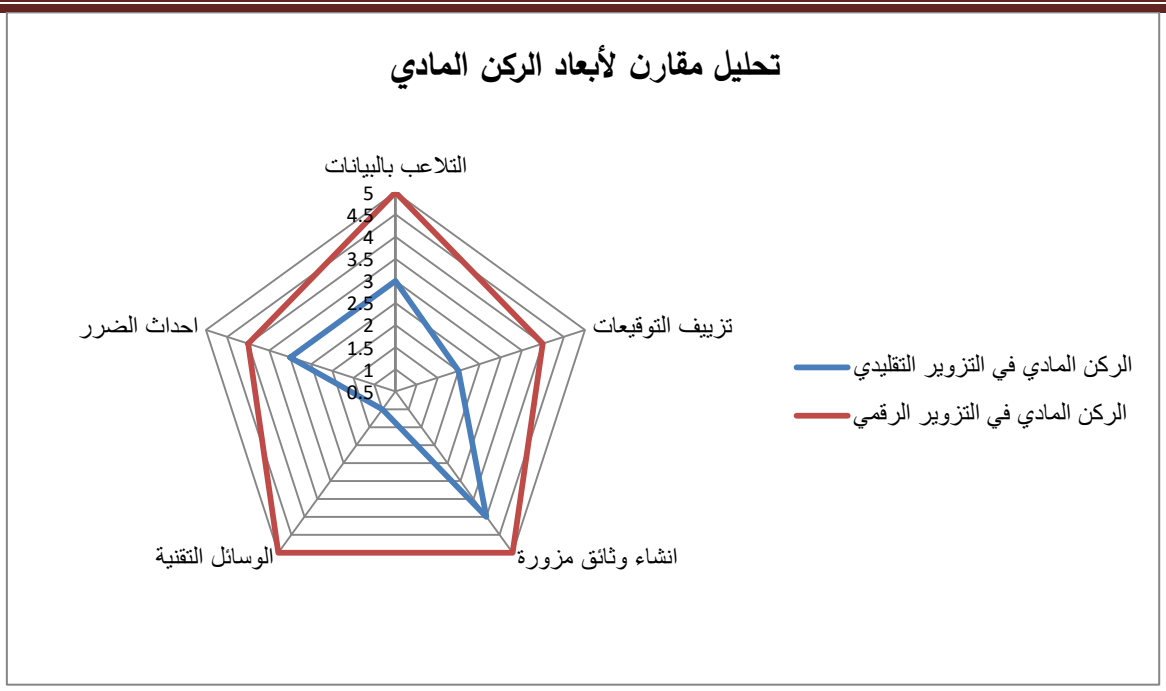
---

[1] مينا فايق، **جرائم التزوير في المحررات الرسمية والعرفية**، منشور على موقع الدكتور مينا فايق، بتاريخ 9 سبتمبر 2025، تم الاطلاع عليه يوم 6 أفريل 2026، على الساعة 21:20، على الرابط: https://menafayq.com

[2] غلاب عبد الحق، **خصوصية جريمة تزوير التوقيع الالكتروني في التشريع الجزائري**، مجلة الدراسات القانونية والسياسية، جامعة عمار ثليجي الأغواط، المجلد 8، العدد 01، ص497.

[3] سفران الشمراني، **جريمة التزوير في النظام السعودي**، منشور على موقع مكتب المحامي والمستشار القانوني سفران مشبب الشمراني، بتاريخ 15 ماي 2025، تم الاطلاع عليه يوم 6 أفريل 2026، على الساعة 21:30، على الرابط:https://lawyesafran.com

[4] **جريمة التزوير في القانون المغربي والعقوبات**، موقع محامي بهيئة الدار البيضاء CLF AVOCAT، تم الاطلاع عليه يوم 6 أفريل 2026، على الساعة 21:36، على الرابط: https://calavpcat.ma



المصدر: من اعداد الطالبتين بالاعتماد على مخرجات الدراسة، 2026.

نرى أن هذا التمييز ضروري لتحديد الاختصاص القضائي والقواعد الإجرائية المطبقة، خاصة في ظل عدم اكتمال بعض النصوص القانونية في التعامل مع الخصائص التقنية للتزوير الرقمي مقارنة بالتقليدي.

الفرع الثاني: النتيجة الاجرامية (احتمال وقوع ضرر)

يُعدّ الركن المادي في الجريمة عموماً، والجريمة الرقمية خصوصاً، مرتكزاً على عنصرين أساسيين هما: السلوك الإجرامي والنتيجة الإجرامية، وفي سياق جريمة التزوير الرقمي، تكتسب النتيجة الإجرامية أهمية خاصة نظراً لطبيعة الفعل الإجرامي الذي يُحدث تغييراً في الحقيقة الرقمية دون أن يترتب عليه بالضرورة ضرر فعلي مادي ملموس في كل الحالات، وقد اختار المشرع الجزائري، في إطار مواكبته للتطور التكنولوجي، اعتماد "احتمال وقوع الضرر" كأساس للتجريم والعقوبة، مما يعكس فلسفة وقائية تحمي المجتمع من المخاطر المحتملة للجريمة الرقمية قبل وقوعها فعلياً، ومن ثم، يتعين التوقف عند هذا المفهوم وتحليل أركانه وأنواعه وآليات إثباته، لما له من انعكاسات جوهرية على تحديد نطاق المسؤولية الجنائية وتقدير العقوبة المناسبة في التشريع الجزائري.

أولا: مفهوم الضرر المحتمل في النظرية الجنائية والتشريع الجزائري

يُقصد بالضرر المحتمل في جريمة التزوير الرقمي، ذلك الضرر الذي يُحدثه الفعل الإجرامي بمجرد ارتكابه، دون اشتراط وقوعه فعلياً أو تحقق خسارة مادية ملموسة، فالمشرع الجزائري قد استند في تجريمه للتزوير الرقمي إلى مبدأ الوقاية من المخاطر، معتبراً أن مجرد احتمال وقوع الضرر كافٍ لاكتمال الركن المادي

للجريمة، ويُعكس هذا المفهوم عمقاً فهماً لطبيعة الجرائم الإلكترونية، التي قد لا تترك آثاراً مادية ظاهرة في لحظة ارتكابها، لكنها تشكل تهديداً حقيقياً لاستقرار المعاملات الرقمية وثقة المتعاملين فيها[1].

وتجدر الإشارة إلى أن هذا المفهوم يختلف جوهرياً عن الضرر الفعلي المُشترط في بعض الجرائم التقليدية، إذ إن المشرع يكتفي في التزوير الرقمي بالإضرار الاحتمالي بالنظام القانوني والثقة العامة، مما يُوسع من نطاق الحماية الجنائية ويجعلها أكثر فعالية في مواجهة السرعة الفائقة لانتشار الجرائم الرقمية، وقد أكدت النصوص القانونية، وخاصة القانون رقم 24-02 المتعلق بمكافحة التزوير واستعمال المزور، على أن الجريمة تُعتبر مكتملة بمجرد ارتكاب الفعل الإجرامي المُحدث للتغيير في الحقيقة الرقمية، دون انتظار وقوع الضرر الفعلي[2].

نرى أن هذا التوجه التشريعي يُمثل تطوراً نوعياً في السياسة الجنائية الجزائرية، إذ ينتقل من مبدأ الردع بعد وقوع الجريمة إلى مبدأ الوقاية من المخاطر المحتملة، ونلاحظ أن اعتماد الضرر المحتمل كأساس للتجريم يُساعد على تجاوز الإشكاليات الإثباتية المرتبطة بالإثبات الفعلي للضرر في الفضاء الرقمي، حيث قد يكون من الصعب تحديد الخسارة المادية الفعلية في وقت مبكر.

ثانيا: أنواع الضرر المحتمل في جريمة التزوير الرقمي

يمكن تصنيف الضرر المحتمل في جريمة التزوير الرقمي في التشريع الجزائري إلى ثلاثة أنواع رئيسة، تختلف في طبيعتها وآثارها ومدى تأثيرها على المجتمع والفرد:

أ. الضرر المادي المحتمل: ويشمل الخسائر المالية التي قد تلحق بالأفراد أو المؤسسات نتيجة تزوير مستندات مالية رقمية أو بيانات بنكية أو عقود إلكترونية، فالتزوير في سجل إلكتروني أو محو بيانات مخزنة قد يؤدي إلى خسائر اقتصادية كبيرة، حتى وإن لم تتحقق هذه الخسائر فعلياً في لحظة اكتشاف الجريمة، وقد يمتد هذا الضرر إلى إتلاف أنظمة المعلومات أو تعطيلها، مما يُحدث اضطراباً في السير العادي للمعاملات الرقمية[3].

ب. الضرر المعنوي المحتمل: ويتعلق بالاعتداء على السمعة والثقة، سواء ثقة الأفراد أو المؤسسات في الوثائق الرسمية والمعاملات الرقمية، فتزوير التوقيع الإلكتروني مثلاً يُقوض الثقة في النظم الرقمية التي يعتمد

---

[1] رياض/خ، **قانون مكافحة جرائم التزوير في الجريدة الرسمية**، منشور على موقع البلاد نت، بتاريخ 13 مارس 2024، تم الاطلاع عليه يوم 6 أفريل 2026، على الساعة 21:11، على الرابط: https://www.elbilad.net

[2] **الاحكام الجديدة في قانون مكافحة التزوير واستعمال المزور محور دراسي بالجزائر العاصمة**، وكالة الأنباء الجزائرية، منشور بتاريخ 30 جوان 2024، تم الاطلاع عليه يوم 6 أفريل 2026، على الساعة 22:07، على الرابط: https://www.aps.dz/ar/algerie/164434

[3] معمري ايمان، فضيلة شعبان، **مدى مواجهة المشرع الجزائري للجرائم الالكترونية "جريمة التزوير الالكتروني نموذجا"**، مداخلة في ملتقى الدكتوراه الدولي متعدد الاختصصات، جامعة الشهيد حمة لخضر الوادي، من 23 الى 26 فيفري 2020، ص39.

عليها الاقتصاد الرقمي كأساس لعمله، ويفتح الباب أمام الاحتيال وسرقة الهوية وجرائم سيبرانية أخرى، ويُعد هذا النوع من الضرر من أخطر أنواع الضرر المحتمل، لأنه يُهدد الأساس المعنوي للتعاملات الإلكترونية[1].

ج. الضرر الاجتماعي المحتمل: وهو ذلك الضرر الذي يمس المجتمع ككل، خاصة عندما يستهدف التزوير وثائق هوية رقمية أو سجلات مدنية أو خدمات حكومية إلكترونية، فالتلاعب في الوثائق الرقمية للدولة قد يؤدي إلى اضطراب في تقديم الخدمات العامة أو تهديد الأمن القومي أو زعزعة الثقة في المؤسسات العامة، ويُعد هذا الضرر أشد خطورة لأنه يمتد آثاره ليشمل المصلحة العامة والأمن الجماعي[2].

نرى أن هذا التصنيف يُظهر الشمولية التي يتسم بها المشرع الجزائري في حماية المصالح المختلفة من جريمة التزوير الرقمي، ونلاحظ أن التشريع الجزائري قد نجح في تغطية جميع جوانب الضرر المحتمل، مما يعكس إدراكاً عميقاً لطبيعة الجريمة الرقمية المتعددة الأبعاد.

ثالثا: الضرر المحتمل كأساس للتجريم في النظام القانوني الجزائري

يستمد التجريم في جريمة التزوير الرقمي في الجزائر أساسه من مبدأ "احتمال وقوع الضرر"، وهو ما يُميز هذه الجريمة عن كثير من الجرائم التقليدية التي تشترط وقوع الضرر الفعلي لاكتمال أركانها، فالمشرع الجزائري، ومن خلال القوانين رقم 09-04 المتعلق بمكافحة الجرائم الإلكترونية، والقانون رقم 15-04 المتعلق بالتوقيع الإلكتروني، والقانون رقم 24-02 المؤرخ في 26 فيفري 2024 المتعلق بمكافحة التزوير واستعمال المزور، قد أكد على أن الجريمة تُعتبر مكتملة بمجرد ارتكاب الفعل الإجرامي المُحدث للتغيير في الحقيقة الرقمية، دون انتظار وقوع الضرر الفعلي[3].

وقد استند المشرع في ذلك إلى طبيعة الجريمة الرقمية التي تتسم بالسرعة في الانتشار والصعوبة في الرقابة، مما يقتضي تدخلاً قانونياً مبكراً قبل تحقق النتائج الخطيرة، فالفعل الإجرامي بمجرد ارتكابه يُحدث تغييراً في الوضعية القانونية للمحرر الرقمي، ويُنشئ حالة من عدم الاستقرار في المعاملات الإلكترونية، مما يكفي لاعتباره ضرراً محتملاً يستوجب العقاب[4].

نرى أن هذا المبدأ يُعدّ من المبادئ الحديثة في القانون الجنائي الجزائري، التي تتجاوز النظرية التقليدية للجريمة، ونلاحظ أن اعتماد الضرر المحتمل يُعطي القانون مرونة أكبر في مواجهة التطورات التكنولوجية المتسارعة، حيث إن المشرع لا يحتاج إلى انتظار وقوع كارثة مالية أو اجتماعية فعلية لمعاقبة الفاعل.

---

[1] عمارة فتيحة، **جريمة التزوير الالكتروني**، مجلة القانون والمجتمع، جامعة أدرار، المجلد 7، العدد 1، منشور بتاريخ 01 جوان 2019، ص 174.

[2] راضية مشري، **المرجع السابق**، ص135.

[3] أحمد محمد محروس عبد العال، **المرجع السابق**، ص51.

[4] مصطفاوي أسامة، **المرجع السابق**، ص 69.

رابعا: العلاقة بين الضرر المحتمل وتحديد العقوبة

تتأثر العقوبات المقررة لجريمة التزوير الرقمي في التشريع الجزائري بدرجة احتمال وقوع الضرر وخطورته، حيث نصت المادة 194 مكرر من القانون العقوبات المعدل على عقوبة الحبس من سنة إلى خمس سنوات وغرامة مالية لجرائم التزوير في الوثائق الإلكترونية أو التوقيعات الإلكترونية، وتزداد شدة العقوبة عندما يمس الضرر المحتمل بالأمن الجماعي أو الاقتصاد الوطني، حيث تصل العقوبة إلى الحبس من ثلاث سنوات إلى عشر سنوات في الحالات التي يكون فيها الضرر المحتمل أكبر، مثل التزوير في أختام الدولة أو توقيعاتها الرقمية أو الوثائق ذات الصلة بالأمن القومي[1].

كما يعاقب المشرع على استعمال المزور بنفس عقوبة التزوير، مما يعكس إدراكاً لاستمرار الضرر المحتمل حتى بعد ارتكاب فعل التزوير الأصلي، وقد أكد القانون رقم 24-02 على ضرورة تكييف العقوبة وفقاً لطبيعة الضرر المحتمل، سواء كان مادياً أو معنوياً أو اجتماعياً، مع مراعاة ظروف التشديد والتخفيف المنصوص عليها في القانون العقوبات[2].

نرى أن هذا التدرج في العقوبات يُعكس دقة المشرع الجزائري في معايرة العقوبة مع خطورة الفعل الإجرامي واحتمال الضرر الناتج عنه، ونلاحظ أن المشرع قد أولى اهتماماً خاصاً بالحالات التي يكون فيها الضرر المحتمل ممتداً ليشمل المصلحة العامة، مما يُظهر حرصاً على حماية الأمن القومي في ظل التحول الرقمي.

خامسا: آليات إثبات الضرر المحتمل في الممارسة القضائية

تُعدّ إثبات الضرر المحتمل في جريمة التزوير الرقمي من أبرز التحديات القضائية التي تواجه السلطات الجزائرية، نظراً للطبيعة غير المادية لهذا الضرر، وتعتمد السلطات القضائية على عدة آليات لإثبات هذا العنصر، منها الاعتماد على الخبرة التقنية المتخصصة في مجال الجرائم الإلكترونية، حيث يقوم خبراء تقنيون بالكشف عن آثار الفعل الإجرامي في الأنظمة الرقمية وتحديد مدى احتمالية وقوع الضرر الناتج عنه، كما يتم الاعتماد على الأدلة الإلكترونية مثل السجلات الرقمية والبيانات الوصفية التي تُظهر محاولات الولوج غير المشروع أو التغيير في البيانات[3].

---

[1] مروى بن بوزيد، نجوى هداج، **الحماية الجنائية لبطاقات الدفع الالكتروني من التزوير**، مذكرة ماستر تخصص قانون اعلام الي والانترنت، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الابراهيمي برج بوعريريج، 12 جوان 2025، ص62.

[2] مريم عيسات، **المرجع السابق**، ص51.

[3] **مجلس الأمة: المصادقة على نص قانوني بمكافحة التزوير واستعمال المزور**، الاذاعة الجزائرية، تم النشر يوم 30 جانفي 2024، تم الاطلاع عليه يوم 6 افريل 2026، على الساعة 22:36، على الرابط: https://news.radioalgerie.dz

وفي هذا الإطار، يلعب التفتيش الإلكتروني دوراً حيوياً في جمع الأدلة اللازمة لإثبات الضرر المحتمل، مع مراعاة الضوابط القانونية المنصوص عليها في قانون الإجراءات الجزائية، كما تسعى السلطات إلى استخدام تقنيات التشفير والحماية الرقمية كوسائل وقائية لتقليل احتمالية وقوع الضرر، مما يُساعد فيما بعد على إثبات محاولة التزوير قبل تحقق الضرر الفعلي[1].

نرى أن هذه الآليات تتطلب تكويناً مستمراً للقضاة والمحامين في مجال التكنولوجيا الرقمية، ونلاحظ أن الفعالية في إثبات الضرر المحتمل تقتضي تطوير البنية التحتية التقنية للعدالة الجنائية الجزائرية، وإنشاء وحدات متخصصة للخبرة الجنائية الرقمية تكون مؤهلة لتحليل الأدلة الإلكترونية وتحديد مدى الضرر المحتمل.

الفرع الثالث: العلاقة السببية في الجريمة الرقمية

تُعدّ العلاقة السببية من المبادئ الأساسية في النظرية القانونية الجنائية، التي يترتب عليها تحديد نطاق المسؤولية الجنائية ونسبة النتائج الضارة للفاعل، وفي سياق الجرائم الرقمية، تكتسب هذه العلاقة أهمية خاصة نظراً لطبيعة هذه الجرائم غير المادية والمترامية الأطراف، والتي قد يصعب فيها ربط الفعل الإجرامي بالنتيجة الضارة بشكل مباشر وواضح، وقد اضطر المشرع الجزائري، في إطار سعيه لمواكبة التطور التكنولوجي المتسارع، إلى تطوير منظومة قانونية تتصدى لإشكاليات إثبات العلاقة السببية في الفضاء الرقمي، مع مراعاة خصوصيات هذا النوع من الجرائم التي تتميز بالغموض والسرعة في الانتشار وصعوبة تحديد الفاعل الحقيقي، ومن ثم، يتعين الوقوف عند تحليل ماهية هذه العلاقة وشروطها وآليات إثباتها في التشريع الجزائري، لما لذلك من انعكاسات جوهرية على تحديد المسؤولية الجنائية في الجرائم الإلكترونية.

أولا: ماهية العلاقة السببية في الجرائم الرقمية

تعني العلاقة السببية في جوهرها وجود رابط سببي مباشر بين الفعل الذي قام به المتهم ووقوع النتيجة الإجرامية الضارة، بحيث لا تُنسب النتيجة للفاعل بشكل كامل إلا بوجود هذا الرابط الحتمي، وتُطبق هذه العلاقة في الجرائم الإلكترونية كما تُطبق في الجرائم التقليدية، إذ إن المبدأ السببي يظل قائماً بغض النظر عن طبيعة الوسيلة المستخدمة في ارتكاب الجريمة[2].

وقد عرّف التشريع الجزائري الجريمة الرقمية بأنها كل فعل إجرامي يتم باستخدام وسيلة إلكترونية، مثل الاختراق والاحتيال الإلكتروني، ويشمل ذلك مجموعة واسعة من الأفعال التي تستهدف أنظمة المعلومات والبيانات الخصوصية بواسطة الحاسوب وشبكة الإنترنت، وفي هذا السياق، تُعدّ العلاقة السببية شرطاً أساسياً

[1] اية بن ميسية، **المرجع السابق**، ص76.

[2] فريدة عيادي، **الجريمة المعلوماتية في التشريع الجزائري**، المجلة الجزائرية للعلوم القانونية والسياسية، جامعة بن يوسف بن خدة الجزائر، المجلد 55، العدد 2، منشور يوم 15 جوان 2018، ص 234.

لتقرير المسؤولية الجنائية عن المساس بأنظمة البيانات، فمثلاً إذا أدى فعل الاختراق إلى تعطيل النظام أو سرقة البيانات، يُعتبر الرابط السببي متحققاً، ويستتبع إيقاع العقوبة المحددة على مرتكبها[1].

نرى أن هذا المفهوم يعكس استمرارية المبادئ القانونية الكلاسيكية في مواجهة الجرائم المعاصرة، ونلاحظ أن التشريع الجزائري قد نجح في تطبيق مبدأ العلاقة السببية على الجرائم الإلكترونية دون إخلال بجوهره، مع مراعاة التحول الرقمي في وسائل الإثبات.

ثانيا: تحديات إثبات العلاقة السببية في الجرائم الرقمية

يواجه تطبيق مبدأ العلاقة السببية في الجرائم الرقمية تحديات كبيرة، تفرضها طبيعة هذه الجرائم التي تتسم بالغموض والسرعة في الانتشار والمترامية الأطراف المادية غير الطبيعة، وتتمثل أبرز هذه التحديات في صعوبة تحديد الفاعل الحقيقي نظراً لإمكانية إخفاء الهوية في الفضاء الرقمي، وسرعة انتشار الجريمة عبر الشبكات العنكبوتية، إضافة إلى التعقيدات التقنية التي تستدعي تفسيرات قضائية متعمقة[2].

كما تفرض الجرائم غير العمدية، التي قد يقرها المشرع الجزائري، تعقيداً أكثر في إثبات العلاقة السببية، حيث يجب الربط بين التقصير أو الإهمال والنتيجة الضارة، مع ضرورة تطبيق مفهوم السببية على الأفعال التي ترتكب باسم أو بحساب الكيان الفاعل وليس الأشخاص الطبيعيين[3].

إضافة إلى ذلك، تواجه الجرائم المرتكبة باستخدام الذكاء الاصطناعي تحديات خاصة في إثبات العلاقة السببية، إذ إن النصوص الصريحة التي تنظم السببية في هذه الحالات قد لا توجد، مما يتطلب تفسيراً للمادة 18مكرر من قانون العقوبات، خاصة في الحالات التي تتسبب فيها آليات مستقلة بأضرار دون تدخل عوامل خارجية، حيث يكون الفعل السببي للضرر فيه معقداً[4].

نرى أن هذه التحديات تستلزم تطويراً مستمراً للقدرات التقنية والقانونية للقضاة والخبراء، ونلاحظ أن السرعة المتسارعة للتطور التكنولوجي تجعل من الصعب على النصوص القانونية مواكبة كل مستجدات الجريمة الرقمية.

ثالثا: آليات التحقيق وإثبات العلاقة السببية

تمثل آليات التحقيق الإلكتروني جزءاً أساسياً في إثبات العلاقة السببية في الجرائم الرقمية في الجزائر، حيث يتم الاستعانة بآليات جمع الأدلة الرقمية وتحليلها، وتعتبر الأدلة الرقمية، مثل سجلات الدخول والبصمات

[1] راضية مشري، **المرجع السابق**، ص136.

[2] يزيد بوحليط، **المرجع السابق**، ص 100.

[3] اية بن ميسية، **المرجع السابق**، ص77.

[4] التجاني ايمان واخرون، **المسؤولية الجزائية عن الاستخدام غير المشروع للذكاء الاصطناعي**، مذكرة ماستر تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية جامعة قاصدي مرباح ورقلة، السنة الجامعية 2024/2023، ص 55.

الرقمية والشبكة ومسارات النشاط، حاسمة في إثبات السببية، ويتطلب جمعها وتحليلها خبرة متخصصة في الطب الشرعي الرقمي لضمان صحتها وقبولها في المحاكم[1].

كما يلعب الخبراء القضائيون المتخصصون في تكنولوجيا المعلومات دوراً حيوياً في مساعدة القضاة على فهم التعقيدات التقنية للجرائم الرقمية وتحديد الروابط السببية بين الأفعال والنتائج، إذ إن خبرتهم ضرورية لترجمة التعقيدات التكنولوجية إلى مفاهيم قانونية واضحة[2].

نرى أن فعالية هذه الآليات تتوقف على جودة التكوين المستمر للقضاة والمحامين في المجال الرقمي، ونلاحظ ضرورة تطوير البنية التحتية للخبرة القضائية في الجزائر لمواكبة التطورات التقنية.

المطلب الثالث: الركن المعنوي (القصد الجنائي)

تعد جريمة التزوير الرقمي من الجرائم العمدية التي لا يُتصور وقوعها عن طريق الخطأ غير العمدي أو الإهمال؛ إذ تتطلب انصراف نية الجاني بوعي وإدراك نحو العبث بالحقيقة المخزنة اليا، ويقوم الركن المعنوي في هذه الجريمة على "القصد الجنائي" بشقيه العام (العلم والإرادة) والخاص (نية استعمال المحرر المزور) وهو ما يمنح السلوك طابعه الجرمي ويخرج الأخطاء البرمجية العفوية من دائرة التجريم.

الفرع الأول: القصد الجنائي العام (العلم والارادة)

يُعدّ القصد الجنائي العام من الأركان الأساسية التي تقوم عليها المسؤولية الجنائية في النظرية القانونية العامة، وهو يتمثل في العلم والإرادة اللذين يوجدان في قلب الفعل الإجرامي، وفي سياق جريمة التزوير الرقمي، تكتسب هذه العناصر أهمية بالغة نظراً للطبيعة التقنية المعقدة للجريمة، التي تقتضي دراية خاصة بالوسائل الإلكترونية وإدراكاً واضحاً للنتائج القانونية المترتبة على تغيير الحقيقة في المحررات الرقمية، وقد حرص المشرع الجزائري، في إطار سعيه لمواكبة التطور التكنولوجي المتسارع، على تحديد مفهوم القصد الجنائي العام في جريمة التزوير الرقمي بشكل دقيق، معتمداً على عنصري العلم والإرادة كأساس للتجريم والعقوبة، وذلك في ضوء القوانين رقم 24-02 و 09-04و18-07.

أولاً: مفهوم القصد الجنائي العام في التزوير الرقمي

يتألف القصد الجنائي العام في جريمة التزوير الرقمي من عنصرين رئيسيين لا غنى عنهما لإدانة المتهم، هما: العلم والإرادة، فالعلم يقتضي أن يكون الجاني مدركاً تمام الإدراك لطبيعة الفعل الإجرامي الذي يرتكبه، أي علمه بأنه يقوم بتغيير الحقيقة في بيانات أو مستندات رقمية، سواء كان ذلك بتعديل أو تزييف أو

[1] **مجلس الأمة: المصادقة على نص قانوني بمكافحة التزوير واستعمال المزور**، الاذاعة الجزائرية، تم النشر يوم 30 جانفي 2024، تم الاطلاع عليه يوم 6 افريل 2026، على الساعة 22:36، على الرابط: https://news.radioalgerie.dz

[2] اية بن ميسية، **المرجع السابق**، ص78.

إنشاء محرر مزور، ويشمل هذا العلم الوعي بأن التعديل يمس بالحجية القانونية للمحرر الرقمي المعترف به قانوناً، مما يجعل الفعل يتجاوز مجرد الفعل المادي ليدخل في دائرة الجريمة[1].

أما الإرادة فتعني توجه النية نحو ارتكاب الفعل الإجرامي، بحيث يكون تصرف الجاني طوعياً وغير ناتج عن إكراه، وتتجه إرادته نحو تحقيق غرض غير مشروع، سواء كان ذلك بالحصول على حقوق للغير أو تضليل الجهات الرسمية أو الإضرار بالغير، وقد شددت التشريعات الجزائرية، وخاصة القانون رقم 24-02 المتعلق بمكافحة التزوير واستعمال المزور، على ضرورة توافر هذه الإرادة لإدانة الجاني، مما يعكس مبدأ قانون العقوبات الجزائري في معاقبة القصد الجنائي العام[2].

نرى أن هذا التعريف يعكس دقة المشرع الجزائري في تمييز الجريمة الرقمية عن الخطأ الفني غير المقصود، ونلاحظ أن توافر العلم والإرادة معاً يضمن عدم إدانة الأشخاص الذين يقعون في أخطاء تقنية غير متعمدة.

ثانياً: عنصر العلم في القصد الجنائي الرقمي

يتمثل عنصر العلم في القصد الجنائي الرقمي بإدراك الجاني لطبيعة فعله الإجرامي ونتائجه القانونية، ففي جريمة التزوير الرقمي، يجب أن يكون الجاني على دراية تامة بأنه يغير الحقيقة في مستند إلكتروني أو بيانات رقمية، وأن هذا التغيير سيؤدي إلى جعل المحرر غير صحيح قانوناً، ويشمل هذا العلم الوعي بالقيمة القانونية للمحرر الرقمي، خاصة في ظل اعتراف القانون رقم 18-07 المتعلق بالتوقيع الإلكتروني والشهادة الإلكترونية بقوة المحررات الرقمية المساوية للمحررات التقليدية[3].

كما يمتد هذا العلم ليشمل الإدراك بالنتائج الضارة المترتبة على الفعل، سواء كانت مادية كالحصول على مال غير مستحق، أو معنوية كالمساس بسمعة الغير أو ثقة الجمهور في المعاملات الرقمية، وقد تضمنت النصوص القانونية الجزائرية، وخاصة المادة المتعلقة بالتزوير في الوثائق الإلكترونية، صراحة اشتراط العلم بتغيير الحقيقة كركن أساسي للجريمة[4].

---

[1] راضية مشري، **المرجع السابق**، ص 137.

[2] **الاحكام الجديدة في قانون مكافحة التزوير واستعمال المزور محور دراسي بالجزائر العاصمة**، وكالة الأنباء الجزائرية، منشور بتاريخ 30 جوان 2024، تم الاطلاع عليه يوم 7 أفريل 2026، على الساعة 15:30، على الرابط: https://www.aps.dz/ar/algerie/164434

[3] رياض/خ، **قانون مكافحة جرائم التزوير في الجريدة الرسمية**، منشور على موقع البلاد نت، بتاريخ 13 مارس 2024، تم الاطلاع عليه يوم 7 أفريل 2026، على الساعة 15:36، على الرابط: https://www.elbilad.net

[4] فراجي عماد الدين، **التزوير وأحكامه في الجزائر على ضوء القانون المستحدث 24-02**، موقع ResearchGate، منشور بتاريخ افريل 2024، تم الاطلاع عليه يوم 7 أفريل 2026، على الساعة 15:41، على الرابط: https://researchgate.net

نرى أن هذا العنصر يُعد حجر الزاوية في إثبات الجريمة الرقمية، إذ إن إخفاء النوايا الكامنة وراء الأفعال التقنية يجعل من الصعب على المحكمة تحديد وجود القصد الجنائي دون دلائل مادية على العلم.

ثالثاً: عنصر الإرادة في القصد الجنائي الرقمي

تعني الإرادة في سياق التزوير الرقمي توجه النية المباشرة والواعية نحو ارتكاب الفعل الإجرامي، بقصد تحقيق غرض غير مشروع، فالجاني يجب أن يكون قد توجهت إرادته نحو تغيير الحقيقة في الوثيقة الرقمية أو التوقيع الإلكتروني، بهدف استخدامها في أغراض إجرامية كالاحتيال أو الاستيلاء على حقوق الغير أو تضليل الجهات الرسمية، وقد أكد القانون رقم 24-02 على ضرورة توافر هذه الإرادة المباشرة، حيث نص صراحة على معاقبة من يقوم بالتزوير بقصد الاحتيال أو المساس بالحقوق[1].

وتتجلى الإرادة أيضاً في اختيار الوسيلة الإلكترونية لارتكاب الجريمة، سواء كان ذلك من خلال برامج التعديل الرقمي أو التزييف العميق (Deepfakes) أو الاختراق الإلكتروني، مما يعكس وعياً كاملاً بوسائل الجريمة وأهدافها، وقد لاحظت المحاكم الجزائرية في أحكامها المتعلقة بالجرائم الإلكترونية على ضرورة إثبات توجه الإرادة نحو النتيجة الإجرامية الضارة[2].

نرى أن الإرادة المباشرة تُميز بين الجريمة الرقمية والسلوك غير المؤاخذ عليه قانوناً، ونلاحظ أن التشريع الجزائري قد ركز على النية المباشرة رغم أن بعض الحالات قد تستدعي القصد الجنائي غير المباشر.

رابعاً: تحديات إثبات القصد الجنائي في البيئة الرقمية

تواجه إثبات القصد الجنائي في جريمة التزوير الرقمي تحديات معقدة، تفرضها طبيعة البيئة الإلكترونية وسرعة التطور التكنولوجي، فالأدلة الرقمية، مثل السجلات الإلكترونية والبصمات الرقمية والبيانات الوصفية (Metadata)، تلعب دوراً حاسماً في كشف النوايا الكامنة وراء الفعل، إلا أنها قابلة للتغيير والتعديل بسهولة، مما يجعل عملية الجمع والتحليل تقع على عاتق الشرطة العلمية المتخصصة[3].

كما أن ظهور تقنيات الذكاء الاصطناعي والتعلم الآلي، مثل تقنيات التزييف العميق(Deepfakes) ، قد عقد مهمة إثبات العلم والإرادة، حيث يمكن للجاني أن يدعي عدم العلم بأن المحتوى مزور، أو أنه استخدم أداة

---

[1] **موسى قرومي: جريمة التزوير واستعمال المزور أخذت ابعادا خطيرة**، الاذاعة الجزائرية، تم النشر يوم 30 جوان 2024، تم الاطلاع عليه يوم 7 افريل 2026، على الساعة 15:53، على الرابط: https://news.radioalgerie.dz

[2] شعباني نوال، **مظاهر تفعيل قواعد مكافحة جرائم التزوير المقررة بموجب القانون رقم 24-02 المتعلق بمكافحة التزوير واستعمال المزور**، المجلة النقدية للقانون والعلوم السياسية، جامعة مولود معمري تيزي وزو، المجلد 20، العدد 01، منشور بتاريخ 30 جوان 2025، ص 599.

[3] ألجية قريب، **دور الشرطة العلمية في اثبات جريمة التزوير في المحررات**، مذكرة ماستر تخصص قانون جنائي وعلوم جنائية، كلية الحقوق، جامعة الجزائر1- بن يوسف بن خدة، سنة 2025، ص59.

إجرامية دون قصد إجرامي، وقد تتطلب هذه الحالات تطوير آليات قانونية وتقنية جديدة لمواجهة الأساليب المتطورة[1].

نرى أن هذه التحديات تستلزم تطويراً مستمراً لقدرات الأجهزة الأمنية والقضائية في مجال التحليل الجنائي الرقمي، ونلاحظ ضرورة إنشاء وحدات متخصصة للخبرة القضائية في مجال الذكاء الاصطناعي.

خامساً: العلاقة بين القصد الجنائي والعقوبات المقررة

تنص التشريعات الجزائرية على عقوبات صارمة تتناسب مع خطورة القصد الجنائي في جريمة التزوير الرقمي .فقد نص القانون رقم 24-02 على عقوبات تتراوح بين الحبس من سنة إلى خمس سنوات وغرامات مالية كبيرة، وتشدد هذه العقوبات في حالات تعلق الفعل ببيانات حساسة أو وثائق رسمية للدولة، حيث قد تصل العقوبة إلى عشر سنوات حبساً[2].

ويرتكز تقدير العقوبة على درجة قسوة القصد الجنائي، فكلما كانت الإرادة موجهة نحو أهداف أكثر خطورة كالمساس بالأمن القومي أو تضليل القضاء، زادت شدة العقوبة .كما يعاقب القانون على استعمال المزور بنفس عقوبة التزوير، مما يعكس استمرار الخطورة الجنائية للقصد حتى بعد ارتكاب الفعل الأصلي[3].

نرى أن هذا التدرج في العقوبات يعكس حكمة المشرع في معايرة العقوبة مع درجة الخطورة النفسية للجاني، ونلاحظ أن التشريع الجزائري قد أولى اهتماماً خاصاً بحماية الوثائق الرسمية الإلكترونية.

الفرع الثاني: القصد الجنائي الخاص (نية استعمال المحرر المزور)

يُعدّ القصد الجنائي الخاص من العناصر المميزة لجريمة التزوير بشكل عام، والتزوير الرقمي بشكل خاص، إذ يتجاوز بذلك مجرد تغيير الحقيقة في المحرر ليشمل النية المحددة في استعمال هذا المحرر المزور في أغراض إجرامية معينة، وقد اهتم المشرع الجزائري بهذا الركن المعنوي الخاص اهتماماً بالغاً، نظراً لما يمثله من حجر زاوية في تمييز جريمة التزوير عن المخالفات التقنية البسيطة أو الأخطاء غير المقصودة في التعامل مع الوثائق الإلكترونية، وفي ظل التحول الرقمي المتسارع، أصبحت مسألة إثبات نية استعمال المحرر المزور تحدياً قضائياً وتقنياً معقداً، يتطلب تطوير آليات إثباتية متخصصة تتواءم مع طبيعة الفضاء الإلكتروني، ومن ثم، يتعين الوقوف عند تحليل هذا القصد الخاص، وشروط تحققه، وكيفية إثباته في التشريع الجزائري، مع بيان مدى تكيف النصوص القانونية مع خصوصيات البيئة الرقمية.

---

[1] **التزوير الالكتروني يهدد الثقة الرقمية في عصر الذكاء الاصطناعي**، منشور على موقع البديل ABC، تم الاطلاع عليه يوم 7 أفريل 2026، على الساعة 16:05، على الرابط: https://elbadilabc-ar.dz

[2] مريم عيسات، **المرجع السابق**، ص 55.

[3] **أنواع وأمثلة على الجرائم الالكترونية**، منشور على موقع قانون تك، بتاريخ 17 جوان 2025، تم الاطلاع عليه يوم 7 أفريل 2026، على الساعة 16:17، على الرابط: https://www.9anon4dz.com

أولاً: ماهية القصد الجنائي الخاص وتميزه عن القصد العام

يتمثل القصد الجنائي الخاص في جريمة التزوير الرقمي، وفقاً للتشريع الجزائري، في "نية استعمال المحرر المزور"، وهو ذلك العنصر الحاسم الذي يميز جريمة التزوير عن مجرد فعل تغيير الحقيقة في المحرر الرقمي، فبينما يكتفي القصد العام بالعلم والإرادة في ارتكاب فعل التغيير، يتطلب القصد الخاص توجيه النية نحو استخدام المحرر المزور في معاملة معينة أو لتحقيق غرض غير مشروع، سواء كان ذلك في معاملات إدارية أو مصرفية أو قانونية[1].

وهذا يعني أن مجرد إعداد أو تعديل محرر إلكتروني دون وجود نية واضحة لاستعماله في أغراض إجرامية قد لا يرتقي إلى جريمة التزوير الكاملة، بل قد يبقى في دائرة المحاولة أو الإعداد لارتكاب الجريمة، وقد نصت المادة 303 من قانون العقوبات الجزائري، ضمن المواد المتعلقة بالتزوير من 303 إلى309 ، على ضرورة توافر هذه النية الخاصة لاكتمال الجريمة، وهو ما يُطبق أيضاً على التزوير الرقمي في ضوء أحكام قانون 09-04 المتعلق بالجرائم الإلكترونية[2].

نرى أن هذا التمييز بين القصد العام والخاص يحمل أهمية قانونية جوهرية في تحديد نطاق المسؤولية الجنائية، إذ إنه يضمن عدم إدانة الأشخاص الذين قد يقومون بتعديلات تقنية على وثائق رقمية دون نية استخدامها بشكل مزور، ونلاحظ أن المشرع الجزائري قد حافظ على هذا المبدأ الكلاسيكي رغم التحول الرقمي.

ثانياً: نية استعمال المحرر المزور في البيئة الرقمية

تكتسب نية استعمال المحرر المزور طابعاً خاصاً في البيئة الرقمية، حيث إن إثباتها تتطلب دلائل تقنية دقيقة تفوق متطلبات الإثبات في التزوير التقليدي، ففي التزوير الورقي، قد تكفي قرائن مادية كحيازة المحرر المزور أو تقديمه لجهة رسمية لإثبات النية، بينما في الفضاء الرقمي، تتطلب الإثبات تحليل سجلات الوصول (Logs)، وعناوينIP ، ورسائل البريد الإلكتروني، وسجلات التصفح، لتحديد ما إذا كان الجاني قد وجه فعلاً نحو استخدام المحرر المزور في معاملة معينة[3].

وقد وسع الفقه والقضاء الجزائري مفهوم "الاستعمال" ليشمل في البيئة الرقمية مجرد تقديم الوثيقة المزورة في منظومة إلكترونية، أو إرسالها عبر شبكات الاتصالات، أو حتى حفظها في أجهزة إلكترونية بقصد التقديم

---

[1] راضية مشري، **المرجع السابق**، ص138.

[2] **جريمة التزوير التقليدي في القانون الجزائري**، مدونة الحقوق والعلوم السياسية (APP-ON)، منشور بتاريخ 22 أكتوبر 2013، تم الاطلاع عليه يوم 7 أفريل 2026، على الساعة: 16:57، على الرابط: https://www.app-on.com/2013/10/blog-post9260.html

[3] أحمد محمد محروس عبد العال، **المرجع السابق**، ص52.

لاحقاً، وقد أكدت المحكمة العليا في أحكامها المتعلقة بالتزوير ضرورة إثبات توجه النية نحو الغرض المحدد من الاستعمال، سواء كان الحصول على منفعة مالية أو تضليل جهة رسمية أو الإضرار بالغير[1].

نرى أن التوسع في تفسير "الاستعمال" في الفضاء الرقمي يعكس مرونة القضاء الجزائري في مواكبة التطور التكنولوجي، إذ إن مجرد نقل الملف المزور عبر الشبكات الإلكترونية يُعدّ استعمالاً فعلياً يحقق ركن القصد الخاص، ونلاحظ أن هذا التوسع يستلزم حذراً في التكييف القانوني لضمان عدم المساس بالحريات الرقمية.

ثالثاً: إشكاليات إثبات القصد الخاص في التزوير الرقمي

تواجه نية استعمال المحرر المزور في التزوير الرقمي إشكاليات جسيمة تتعلق بطبيعة الأدلة الرقمية وقابليتها للتغيير والتعديل، فالنية كعنصر نفسي داخلي يصعب إثباته مباشرة، ويقتضي الاستناد إلى قرائن ظرفية مستمدة من البيئة الرقمية، مثل تحليل البيانات الوصفية (Metadata) المرتبطة بالمحرر، أو سجلات تعديل الملفات، أو محتوى الرسائل الإلكترونية المتبادلة بين الأطراف[2].

كما أن التطور التكنولوجي، وظهور تقنيات الذكاء الاصطناعي في إنشاء المحتوى المزور (Deepfakes)، قد عقد مهمة إثبات النية، حيث يمكن للمتهم أن يدعي أن المحتوى الرقمي قد أُنشئ للاستخدام الشخصي أو للتجربة التقنية دون نية تقديمه رسمياً، وقد شدد الفقه الجزائري على ضرورة توفر أدلة تقنية دامغة تثبت توجه الإرادة نحو الاستعمال المزور، خاصة في ظل غياب نصوص صريحة في التشريع الجزائري تُعرف استعمال المحرر الرقمي بشكل تفصيلي مقارنة بالمحررات الورقية[3].

نرى أن هذه الإشكاليات تستلزم تطوير قدرات الخبرة القضائية الرقمية في الجزائر، ونلاحظ أن الاعتماد على الخبراء التقنيين أصبح ضرورة ملحة لتحليل الأدلة الرقمية واستخلاص النية الخاصة منها، خاصة في ظل سرعة التطور التقني الذي قد يُفقد النصوص القانونية التقليدية فعاليتها.

رابعاً: العلاقة بين القصد الخاص والعقوبات المقررة

ترتبط شدة العقوبات في جريمة التزوير الرقمي بدرجة تحقق القصد الخاص وخطورة الاستعمال المقصود، فقد نصت المادة المتعلقة بالتزوير في قانون العقوبات الجزائري، والمادة المكررة 51 من قانون09-04 ، على عقوبات تتراوح بين ثلاث إلى خمس سنوات حبساً وغرامة مالية قد تصل إلى 500.000 دينار جزائري في

---

[1] مي أحمد، محكمة **النقض توضح القصد الجنائي في جرائم التزوير**، موقع قاضي أنلاين، منشور منذ 3 سوات (2023)، تم الاطلاع عليه يوم 7 أفريل 2026، على الساعة 17:06، على الرابط: https://kadyonline.com

[2] **محكمة النقض توضح القصد الجنائي في جرائم التزوير**، نقابة المحامين المصرية، منشور بتاريخ 26 جويلية 2023، تم الاطلاع عليه يوم 7 أفريل 2026، على الساعة 17:10، على الرابط: https://egyls.com

[3] مصطفاوي اسامة، **المرجع السابق**، ص55.

حالات التزوير البسيط، بينما تصل العقوبة إلى عشر سنوات في حالات التزوير في محررات رسمية أو عند استخدام التوقيع الإلكتروني المزور[1].

وهذا التدرج في العقوبات يعكس تقدير المشرع لخطورة النية الخاصة، فكلما كان الاستعمال موجهاً نحو أغراض أكثر ضرراً بالنظام الاقتصادي أو الإداري أو القضائي، زادت العقوبة، كما يعاقب القانون على استعمال المزور بنفس عقوبة التزوير، مما يعكس استمرار الخطورة الجنائية للقصد الخاص حتى مرحلة التنفيذ الفعلي للجريمة[2].

نرى أن هذا التدرج العقابي يُعدّ تطبيقاً عملياً لمبدأ تناسب العقوبة مع خطورة الفعل والنية، ونلاحظ أن المشرع الجزائري قد أولى اهتماماً خاصاً بالتزوير في الوثائق الرسمية الإلكترونية نظراً لما يمثله من تهديد للثقة في المؤسسات العامة.

الفرع الثالث: وقت توافر الركن المعنوي من الجرائم العابرة للحدود

يشكل تحديد وقت توافر الركن المعنوي في الجرائم الإلكترونية العابرة للحدود إحدى أعقد المسائل القانونية التي تواجه الفقه الجنائي المعاصر، وذلك نظراً للطبيعة اللامادية للفضاء السيبراني التي تُفقد الجريمة رابطتها الجغرافية التقليدية بالإقليم الوطني، وفي سياق جريمة التزوير الرقمي، يكتسب هذا التحديد أهمية بالغة؛ إذ إن الفعل الجرمي قد يُخطط له من داخل الجزائر، بينما يُنفذ من خارجه، أو يمر عبر خوادم متعددة في دول مختلفة، مما يُعقد مهمة ربط الركن المعنوي بزمان ومكان محددين، وهنا نجد أنفسنا أمام إشكالية جوهرية تتمثل في كيفية تطبيق القواعد القانونية التقليدية على جرائم تتجاوز في طبيعتها الحدود الجغرافية المعروفة[3].

أولاً: مبدأ توافر الركن المعنوي في لحظة ارتكاب الفعل الجرمي

يستند القانون الجزائري في تحديد وقت توافر الركن المعنوي إلى القاعدة العامة القاضية بأن القصد الجنائي يتحقق في اللحظة التي يقوم فيها الجاني بارتكاب الفعل المادي للجريمة[4] ، وتطبيقاً لهذا المبدأ على جريمة التزوير الرقمي، يُعتبر الركن المعنوي متوافراً عند قيام الجاني بتعديل أو إدخال بيانات إلكترونية بقصد الغش، بغض النظر عن مكان ظهور النتيجة الإجرامية أو تحقق الضرر الفعلي، ونحن نرى أن هذا المبدأ

---

[1] مريم عيسات، **المرجع السابق**، ص57.

[2] مريم دوش، سميحة هلالي، **مدى مواجهة المشرع الجزائري للجرائم الالكترونية**، مذكرة ماستر تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة حمه لخضر – الوادي، سنة 2029، ص71.

[3] شيخ سناء، شيخ محمد زكرياء، **مكافحة الجرائم الالكترونية في القانون الجزائري**، موقع وميض الفكر، تم الاطلاع عليه يوم 7 أفريل 2026، على الساعة 17:47، على الرابط: https://wameedalfikr.com

[4] قانون رقم 09-04 المؤرخ في 5 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47، الصادر بتاريخ 16 أوت 2009.

يكتسب بعداً استثنائياً في الجرائم الإلكترونية حيث تختلف فيها المعايير الزمانية والمكانية عن الجرائم التقليدية، مما يستدعي مرونة في التفسير القانوني[1]، وقد عزز المشرع الجزائري هذا المبدأ من خلال نصوصه المتعلقة بالجرائم المعلوماتية، حيث يُشترط لقيام الجريمة توفر القصد الجنائي المتمثل في العلم والإرادة دون اشتراط اكتمال النتيجة الجرمية كعنصر لازم لتوافر الركن المعنوي[2].

ويتجلى ذلك جلياً في طبيعة التزوير الرقمي الذي يُشكل فعلاً إجرامياً خالصاً منذ لحظة التدخل في المستند الرقمي أو التوقيع الإلكتروني، ما دام هذا التدخل قد تم بعلم من الفاعل وبإرادة جنائية موجهة لإحداث التغيير المشروع فيه،[3] ومن ثم، فإن الركن المعنوي يُعتبر متوافراً بمجرد قيام الجاني بإنشاء أو تغيير بيانات رقمية من شأنها أن تؤدي إلى نتيجة مضللة أو ضارة، ولو لم يتم استعمال المستند المزور بعد أو تحقق الضرر المادي المترتب على ذلك، وهذا ما نؤكد عليه إذ أن التركيز على الفعل المادي يتيح للقضاء الجزائري مكافحة هذه الظاهرة قبل تفاقم آثارها[4].

ثانياً: خصوصية الجرائم الإلكترونية العابرة للحدود في تحديد وقت توافر الركن المعنوي

تكتسب جرائم التزوير الرقمي العابرة للحدود طابعاً استثنائاً يُفرض إعادة النظر في القواعد التقليدية لتحديد وقت توافر الركن المعنوي[5]، ففي ظل اللامركزية الجغرافية للإنترنت، قد يُخطط الجاني لجريمة التزوير الرقمي من داخل التراب الجزائري، بينما يتم تنفيذها فعلياً عبر خوادم موجودة في الخارج، أو يظهر أثرها النهائي في دولة أخرى[6] ، وفي هذا السياق، يُطبق القانون الجزائري مبدأ الاختصاص الإقليمي الموسع المنصوص عليه في المادة 5 من قانون04-09 ، والذي يُمكّن المحاكم الجزائرية من ممارسة اختصاصها القضائي في حال كان جزء من الفعل قد وقع داخل الجزائر، أو إذا كانت النتيجة قد ظهرت داخل التراب الوطني، أو حتى لو كان الجاني يحمل الجنسية الجزائرية[7].

---

[1] مسعود شهيرة، **المرجع السابق**، ص42.

[2] قانون رقم 09-04 المؤرخ في 5 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47، الصادر بتاريخ 16 أوت 2009.

[3] راضية مشري، **المرجع السابق**، ص60.

[4] راضية مشري، **المرجع السابق**، ص 61.

[5] محمد أمين زيان، **اشكالية الركن المعنوي في الجرائم الجمركية دراسة مقارنة**، مركز جيل البحث العلمي، منشور بتاريخ 28 ديسمبر 2017، تم الاطلاع عليه يوم 7 أفريل 2026، على الساعة: 18:04، على الرابط: https://jilrc.com

[6] محمد أمين زيان، **اشكالية الركن المعنوي في الجرائم الجمركية دراسة مقارنة**، مركز جيل البحث العلمي، منشور بتاريخ 28 ديسمبر 2017، تم الاطلاع عليه يوم 7 أفريل 2026، على الساعة: 18:10، على الرابط: https://jilrc.com

[7] قانون رقم 09-04 المؤرخ في 5 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47، الصادر بتاريخ 16 أوت 2009.

وبناءً عليه، يُعتبر الركن المعنوي متوافراً منذ لحظة بدء الفعل الجرمي في الجزائر، ولو كان التنفيذ الكامل للجريمة سيتم خارج الحدود، ونحن نعتبر أن هذا الاتجاه التشريعي يعكس حكمة المشرع في مواكبة التطور التكنولوجي، حيث إن انتظار ظهور النتيجة النهائية خارج التراب الوطني قد يُفوت الفرصة على العدالة الجنائية[1]، فالقصد الجنائي الموجه نحو ارتكاب التزوير الرقمي يتحقق بمجرد اتخاذ الجاني لخطوات فعلية نحو تنفيذ الجريمة، كالدخول إلى النظام المعلوماتي أو البدء في تعديل البيانات الرقمية، وذلك تطبيقاً لقاعدة" الفعل مكان "التي تستند إليها الاتفاقية الدولية لبودابست لمحاربة الجرائم الإلكترونية[2].

ثالثاً: دور الأدلة الرقمية في إثبات وقت توافر الركن المعنوي

تُشكل الأدلة الرقمية المحور الأساسي في إثبات توافر الركن المعنوي في جرائم التزوير الإلكتروني العابرة للحدود[3]، فقد أصبحت سجلات الدخول (logs) وعناوين بروتوكول الإنترنت (IP addresses) والبيانات الوصفية (metadata)أدوات حاسمة تُمكّن المحققين من تتبع مسارات الجريمة وتحديد اللحظة الزمنية الدقيقة لارتكاب الفعل الجرمي[4]، وقد عزز قانون 18-04 المتعلق بالجرائم المعلوماتية من آليات إثبات القصد الجنائي من خلال النصوص التي تُتيح تتبع الأنشطة الإلكترونية وتحليلها، مما يُسهم في تحديد الوقائع الإجرامية رغم عدم وضوح المكان الجغرافي التقليدي للجريمة[5].

وعلاوة على ذلك، فإن التعاون الدولي في مجال تبادل المعلومات وتنسيق التحقيقات يُعد عنصراً حيوياً لضمان إثبات الركن المعنوي في الجرائم العابرة للحدود[6]، ونحن نؤكد أن غياب هذا التعاون يُشكل العقبة الأكبر أمام القضاء الجزائري، إذ أن الجريمة الإلكترونية لا تعترف بالحدود السياسية بينما القانون الجنائي ما زال يحمل في طياته خصائصه الوطنية الضيقة[7]، فالقضايا التي تتجاوز الحدود الجغرافية التقليدية تستدعي استناداً إلى

[1] مريم دوش، سميحة هلالي، **المرجع السابق**، ص41.

[2] سيد طنطاوي محمد سيد، **الجريمة المعلوماتية: الصعوبات التي تواجه التعاون الوطني والدولي وكيفية مكافحتها**، المركز الديمقراطي العربي، منشور بتاريخ 17 جوان 2018، تم الاطلاع عليه يوم 7 أفريل 2026، على الساعة 18:11، على الرابط: https://democraticac.de

[3] بوحليط يزيد، **المرجع السابق**، ص79.

[4] بوحليط يزيد، **المرجع السابق**، ص80.

[5] مسعود شهيرة، **المرجع السابق**، ص 44.

[6] عمارة فتيحة، **المرجع السابق**، ص179.

[7] عمارة فتيحة، **المرجع السابق**، ص180.

اتفاقيات ثنائية ومتعددة الأطراف تُتيح تسليم المطلوبين وتبادل الأدلة الرقمية بما يضمن عدم الإفلات من العقاب[1].

رابعاً: التمييز بين التزوير الرقمي المحلي والعابر للحدود في وقت توافر الركن المعنوي

يفسر التحليل المقارن بين التزوير الرقمي المحلي والعابر للحدود عن اختلاف جوهري في درجة صعوبة تحديد وقت توافر الركن المعنوي[2]، ففي التزوير الرقمي التقليدي، يُعد تحديد مكان الفعل وإثبات الركن المعنوي نسبياً سهلاً، نظراً لتركز العناصر المادية للجريمة في إقليم واحد[3]، أما في التزوير الرقمي العابر للحدود، فإن الحاجة إلى التعاون الدولي تزداد بشكل كبير، بينما تقل سهولة إثبات الركن المعنوي وتحديد مكان الفعل، وذلك بسبب تعدد الجهات المشاركة في الجريمة وتشتت عناصرها المكانية والزمانية[4].

ومن ثم، يتعين على القاضي الجزائري، عند النظر في قضايا التزوير الرقمي العابر للحدود، أن يستند إلى قاعدة الارتباط الوظيفي بين عناصر الجريمة المختلفة؛ إذ يكفي لتوافر الركن المعنوي أن يكون هناك علم بالفعل الإجرامي وإرادة لتحقيق النتيجة المجرمة في لحظة ارتكاب أي جزء من أجزاء الفعل الجرمي، بغض النظر عن المكان الذي تظهر فيه النتيجة النهائية[5]، وهنا نستشعر أهمية الدور الذي يلعبه القاضي في سد الثغرات القانونية من خلال التفسير الموضوعي للنصوص الجنائية[6].

خامساً: التطور التشريعي وآفاق تحديد وقت توافر الركن المعنوي

يُظهر التطور التشريعي الجزائري حرصاً متزايداً على مواكبة التحديات المستجدة في مجال الجرائم الإلكترونية العابرة للحدود، فقد أدخل قانون 18-04 تعديلات جوهرية على الإطار القانوني لمحاربة الجرائم المعلوماتية، مُعززاً آليات إثبات القصد الجنائي في البيئات الرقمية المعقدة[7]، كما يُؤكد قانون 15-04 المتعلق بالتوقيع الإلكتروني والتصديق الإلكتروني على أهمية حماية الوثائق الرقمية ومعاقبة تزويرها بعقوبات صارمة

---

[1] سيد طنطاوي محمد سيد، **الجريمة المعلوماتية: الصعوبات التي تواجه التعاون الوطني والدولي وكيفية مكافحتها**، المركز الديمقراطي العربي، منشور بتاريخ 17 جوان 2018، تم الاطلاع عليه يوم 7 أفريل 2026، على الساعة 18:11، على الرابط: https://democraticac.de

[2] محمد أمين زيان، **اشكالية الركن المعنوي في الجرائم الجمركية دراسة مقارنة**، مركز جيل البحث العلمي، منشور بتاريخ 28 ديسمبر 2017، تم الاطلاع عليه يوم 7 أفريل 2026، على الساعة: 18:23، على الرابط: https://jilrc.com

[3] محمد أمين زيان، **اشكالية الركن المعنوي في الجرائم الجمركية دراسة مقارنة**، مركز جيل البحث العلمي، منشور بتاريخ 28 ديسمبر 2017، تم الاطلاع عليه يوم 7 أفريل 2026، على الساعة: 18:25، على الرابط: https://jilrc.com

[4] **تقسيم الجرائم من حيث ركنها المعنوي والشرعي**، المحاضرة الثامنة والعشرون، الجامعة المستنصرية، بغداد، تم الاطلاع عليه يوم 7 أفريل 2026، على الساعة: 18:28، على الرابط: https://uomustansiriyah.edu.iq

[5] بوحليط يزيد، **المرجع السابق**، ص 100.

[6] مريم دوش، سميحة هلالي، **المرجع السابق**، ص 44.

[7] مسعود شهيرة، **المرجع السابق**، ص 45.

تصل إلى خمس سنوات حبساً وغرامات مالية، مما يُشير إلى اعتبار الركن المعنوي متوافراً بمجرد قيام الفعل المادي للتزوير دون اشتراط نتيجة إضافية[1].

وعليه، يمكننا القول إن المشرع الجزائري قد اتجه نحو تبسيط قواعد إثبات الركن المعنوي في الجرائم الإلكترونية العابرة للحدود، من خلال الاكتفاء بالعلم والإرادة المصحوبتين بالفعل الإجرامي، مع مراعاة خصوصية الفضاء السيبراني الذي يُتيح للجريمة أن تكون في آن واحد محلية ودولية[2]، مما يستدعي منا كباحثين في المجال القانوني الدعوة إلى تطوير آليات التعاون الدولي وتعميق التنسيق بين الأجهزة القضائية والأمنية على المستويين الوطني والدولي[3].

المبحث الثالث: النظام العقابي لجرائم التزوير الرقمي

إنَّ فاعلية النصوص القانونية المجرمة للتزوير الرقمي تظل رهينة بالنظام العقابي المقرر لها؛ فالعقوبة هي الأداة التي تعيد التوازن القانوني الذي اختل بفعل الجريمة، وقد تبنى المشرع الجزائري في مواجهة هذه الجرائم سياسة جنائية تتسم بالشدة والنوعية، حيث زاوج بين العقوبات البدنية والمالية، وراعي في تقريرها طبيعة الجاني(سواء كان شخصاً طبيعياً أو معنوياً)وخطورة المحل المستهدف بالزوير، وهو ما سنفصله من خلال دراسة العقوبات الأصلية والتكميلية في هذا المبحث.

المطلب الأول: العقوبات الأصلية المقررة

تتمثل العقوبات الأصلية في الجزاءات التي نص عليها القانون كجزاء أساسي للجريمة، والتي تهدف إلى إيلام الجاني وردعه بصفة مباشرة، حيث نجد أنَّ المشرع قد وضع سلماً عقابياً يتدرج بحسب جسامة فعل التزوير الرقمي، مفرقاً بين العقوبات الموجهة للأشخاص الطبيعيين وتلك الموجهة للأشخاص المعنوية.

الفرع الأول: العقوبات المقررة للشخص الطبيعي

شكّل التزوير الرقمي جريمة اقتصادية واجتماعية خطيرة تُهدد أمن الدولة واستقرارها المالي، إذ إن انتشار التعاملات الرقمية في المعاملات المصرفية والإدارية جعل من هذه الظاهرة قضية تستوجب تدخلاً تشريعياً رادعاً يتناسب مع جسامتها، وقد عكف المشرع الجزائري على وضع إطار قانوني متكامل يجمع بين النصوص الجنائية العامة والخاصة، بهدف معاقبة الشخص الطبيعي المرتكب بعقوبات سالبة للحرية والمالية تتدرج بدقة

[1] راضية مشري، **المرجع السابق**، ص 62.

[2] راضية مشري، **المرجع السابق**، ص143.

[3] سيد طنطاوي محمد سيد، **الجريمة المعلوماتية: الصعوبات التي تواجه التعاون الوطني والدولي وكيفية مكافحتها**، المركز الديمقراطي العربي، منشور بتاريخ 17 جوان 2018، تم الاطلاع عليه يوم 7 أفريل 2026، على الساعة 19:11، على الرابط: https://democraticac.de

حسب نوع الوثيقة المزورة وخطورة الضرر المترتب على الفعل الجرمي، مما يستدعي الوقوف التحليلي على هذه العقوبات بأرقامها ومبالغها المالية المحددة.

أولاً: الإطار القانوني الشامل وقواعد المسؤولية الجنائية للشخص الطبيعي

يستند المشرع الجزائري في مكافحة جريمة التزوير الرقمي إلى مجموعة تشريعات متداخلة تشكل منظومة ردعية متكاملة، فقد صدر القانون رقم 24-02 المؤرخ في 26 فيفري 2024 المتعلق بمكافحة التزوير واستعمال المزور ليعالج كافة أشكال التزوير بما فيها الرقمية منها بشكل شامل[1]، حيث نصت المادة 219 مكرر من القانون العقوبات الجزائري على معاقبة كل من زور عمداً محررات رسمية أو إدارية إلكترونية بعقوبات سالبة للحرية، كما يكمل هذا الإطار القانون رقم 09-04 المؤرخ في 5 أوت 2009 المتعلق بالوقاية من الجرائم المرتبطة بالتكنولوجيات الإعلام والاتصال ومكافحتها، وهو النص الأساسي الذي يجرم الاعتداء على أنظمة المعالجة الآلية للمعطيات والتحريف فيها[2]، ونحن نرى أن هذا التكامل بين التشريعات يعكس حرصاً على سد الثغرات القانونية التي قد يستغلها المجرمون في الفضاء السيبراني، مما يشكل شبكة أمان تشريعية تحيط بالشخص الطبيعي المرتكب من كافة الجهات.

ثانياً: التدرج الدقيق في العقوبات السالبة للحرية والمالية حسب خطورة الجريمة

يتميز التشريع الجزائري بتدرج دقيق في العقوبات يرتبط بخطورة الفعل وطبيعة الوثيقة المزورة، ففي الحالات الأشد خطورة كتزوير النقود والسندات المالية والعملات الرقمية وتقليد أختام الدولة، يصل الحد الأقصى للعقوبة إلى السجن المؤبد[3]، أما في حالة تزوير المحررات الرسمية والإدارية الرقمية كالشهادات والرخص الإلكترونية، فتتراوح العقوبات الأساسية بين عشرة (10) إلى عشرين (20) سنة سجناً مع غرامات مالية تتراوح بين مليون (1.000.000) إلى مليوني (2.000.000) دينار جزائري، وتُشدد هذه العقوبات لتصل إلى السجن المؤبد أو ما بين عشرين (20) إلى ثلاثين (30) سنة سجناً إذا ارتكب الجريمة موظف عمومي أو ضابط أثناء أداء وظيفته[4]، كما يعاقب المشرع بصرامة تزوير وثائق المساعدات والإعانات الاجتماعية والصحية والجبائية

---

[1] قانون رقم 24-02 المؤرخ في 26 فيفري 2024، المتعلق بمكافحة التزوير واستعمال المزور، الجريدة الرسمية، العدد 15، الصادر بتاريخ 29 فيفري 2024.

[2] قانون رقم 09-04 المؤرخ في 5 أوت 2009، المتعلق بالوقاية من الجرائم المرتبطة بتكنولوجيات الاعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47، الصادر بتاريخ 16 أوت 2009.

[3] عبد الرؤوف حرشاوي، **صدور قانون جديد يسلط عقوبات ردعية على المزورين**، موقع أوراس ، منشور بتاريخ 13 مارس 2024، تم الاطلاع عليه يوم 9 أفريل 2026، على الساعة 23:07، على الرابط: https://awra.com

[4] عبد الرؤوف حرشاوي، **صدور قانون جديد يسلط عقوبات ردعية على المزورين**، موقع أوراس ، منشور بتاريخ 13 مارس 2024، تم الاطلاع عليه يوم 9 أفريل 2026، على الساعة 23:07، على الرابط: https://awra.com

بالسجن من خمس (5) إلى عشر (10) سنوات[1]، ونحن نؤكد أن هذا التفريق الدقيق في الأرقام والمبالغ يمثل مرونة تشريعية حكيمة تستجيب لمختلف درجات الخطورة، حيث يهدف التشديد في حالات الموظفين العموميين إلى حماية نزاهة الإدارة وضمان حسن سير المرفق الإداري.

ثالثاً: دور المحكمة العليا في توحيد الاجتهاد

تؤدي المحكمة العليا دوراً محورياً في توحيد الاجتهاد القضائي بشأن تطبيق العقوبات، حيث أصدرت قرارها رقم 1185414 بتاريخ 20 جويلية 2023 الذي حدد بدقة طبيعة المحرر الرقمي وتاريخ صدوره وطرق التحريف المشكلة للجريمة[2]، مما يوفر إرشادات قضائية ضرورية للمحاكم الابتدائية في تطبيق النصوص الجنائية المتعلقة بالتزوير الإلكتروني، وعليه يتضح أن العقوبات المقررة للشخص الطبيعي تشكل منظومة ردعية متكاملة تتدرج من السجن المؤبد في الحالات الأشد خطورة، مروراً بالعقوبات الثقيلة التي تصل إلى ثلاثين (30) سنة مع غرامات مالية كبيرة تصل إلى مليوني دينار جزائري، وصولاً إلى العقوبات الأقل كالحبس من خمس (5) إلى عشر (10) سنوات، إلا أننا ندعو إلى تعزيز آليات جمع الأدلة الرقمية وتطوير إجراءات التحقيق الوقائية لضمان فعالية هذه العقوبات، مع ضرورة مواكبة التطور التكنولوجي المستمر بمراجعة دورية للنصوص القانونية.

الفرع الثاني: المسؤولية الجزائية والعقوبات المقررة للشخص المعنوي

شهد الفقه الجنائي الجزائري تطوراً ملحوظاً في مجال مكافحة الجرائم المستحدثة، إذ امتد نطاق المسؤولية الجزائية ليشمل الكيانات الاعتبارية (الشركات، المؤسسات، الهيئات) في جرائم التزوير الرقمي، وذلك في سياق مواكبة التحولات الرقمية التي أصبحت تفرضها الحياة المعاصرة، وقد كان للمشرع الجزائري إسهامات قانونية جادة في هذا المجال، حيث أدرك أن الجرائم الإلكترونية المعقدة تستدعي محاسبة الشخص المعنوي بذاته، باعتباره كياناً مستقلاً ذا إرادة منظمة تمارس نشاطاً اقتصادياً أو إدارياً قد يُستخدم كواجهة لارتكاب أفعال إجرامية رقمية تُهدد الأمن الاقتصادي الوطني والثقة العامة في المعاملات الإلكترونية، وعليه يتعين التفحص الدقيق للإطار القانوني الذي يحدد شروط هذه المسؤولية وطبيعة العقوبات المقررة لها.

أولاً: الأساس القانوني والشروط الموضوعية لقيام المسؤولية الجزائية للشخص المعنوي

يستند توسيع دائرة المسؤولية الجزائية للشخص المعنوي في جرائم التزوير الرقمي إلى قانون رقم 24-02 المؤرخ في 26 فيفري 2024 المتعلق بمكافحة التزوير واستعمال المزور، والذي يُعدّ نقلة نوعية في التجريم

[1] عبد الرؤوف حرشاوي، **صدور قانون جديد يسلط عقوبات ردعية على المزورين**، موقع أوراس ، منشور بتاريخ 13 مارس 2024، تم الاطلاع عليه يوم 9 أفريل 2026، على الساعة 23:07، على الرابط: https://awra.com

[2] **قرار صادر عن المحكمة العليا: الغرفة الجزائية**، ملف رقم 1185414، المؤرخ في 20 جويلية 2023، قضية (ع،م) ومن معه ضد (د،م) والنيابة العامة، الموقع الالكتروني للمحكمة العليا، تم الاطلاع عليه يوم 9 أفريل 2026، على الساعة 23:17، على الرابط: https://coursupreme.dz

الجزائري لكونه يعالج جرائم التزوير الرقمي باعتبارها جرائم قد تُرتكب من قبل المؤسسات باسمها أو لحسابها، وليس فقط من قبل الأفراد[1]، وتتحقق هذه المسؤولية الجزائية بتوافر شروط موضوعية ثلاثة:

أ. أن يكون الفعل الإجرامي قد ارتكبه شخص طبيعي يتمتع بصفة ممثل أو موظف في الكيان المعنوي (كالمديرين التنفيذيين، الرؤساء، أو الموظفين التنفيذيين) ضمن إطار سلطات المؤسسة ومهامها.

ب. أن يكون الارتكاب لصالح الشخص المعنوي أو باسمه، سواء كان الهدف منه كسباً غير مشروع أو تجنب خسارة محتملة أو تحقيق أي منفعة مشروعة.

ج. توافر الأركان المادية والمعنوية للجريمة (القصد الجنائي المتمثل في العلم والإرادة) في الفعل المرتكب بالنسبة للممثل القانوني أو المسؤول التنفيذي[2].

ونحن نرى أن هذا التوسيع في نطاق المسؤولية يمثل تطوراً جوهرياً في الفلسفة الجنائية الجزائرية، حيث انتقلنا من نظام يقتصر على محاسبة الأفراد الطبيعيين إلى نظام يعترف بالشخصية الجرمية المستقلة للكيان الاعتباري، مما يعكس وعياً تشريعياً عميقاً بأن الجرائم الرقمية المعقدة تتطلب ردعاً مؤسساتياً يرتكز على محاسبة الذات القانونية للمؤسسة نفسها، لا مجرد محاسبة أفرادها.

ثانياً: طبيعة العقوبات المالية والإدارية المقررة للشخص المعنوي

نظراً للطبيعة الاعتبارية للشخص المعنوي التي تتعذر فيها العقوبات السالبة للحرية كالسجن، اعتمد المشرع الجزائري نظاماً عقابياً بديلاً صارماً يجمع بين العقوبات المالية والإدارية الرادعة، ففي مجال العقوبات المالية نص القانون على معاقبة الكيانات المعنوية بغرامات مالية باهظة تتراوح قيمتها بين خمسمائة ألف (500.000) دينار ومليوني (2.000.000) دينار جزائري، مع إمكانية تشديد هذه الغرامات وتضاعفها في حالات التعمد أو التكرار الجرمي[3]، أمّا على الصعيد الإداري، فقد منح القانون للمحكمة الجزائية سلطة الحكم بإغلاق المنشأة إغلاقاً مؤقتاً أو دائماً، وذلك بحسب خطورة الجريمة المرتكبة وتأثيرها على المصالح العامة والاقتصاد الوطني، كما نص على مصادرة الأدوات والوسائل الرقمية المستخدمة في ارتكاب الجريمة، والتي تشمل الخوادم والبرمجيات والأجهزة الإلكترونية المرتبطة بالفعل الإجرامي، بالإضافة إلى ذلك، يجوز للمحكمة

[1] قانون رقم 24-02 المؤرخ في 26 فيفري 2024، المتعلق بمكافحة التزوير واستعمال المزور، الجريدة الرسمية، العدد 15، الصادر بتاريخ 29 فيفري 2024.

[2] **المسؤولية الجزائية للشخص المعنوي في ظل قانون العقوبات الجزائري**، موقع أنامل الحقوق، منشور بتاريخ 19 جويلية 2013، تم الاطلاع عليه يوم 9 أفريل 2026، على الساعة 23:45، على الرابط: https://enamilsdroit.ahladalil.com

[3] **المسؤولية الجزائية للشخص المعنوي والشخص الطبيعي**، منشور على منتدى المحاكم والمجالس القضائية، بتاريخ 21 جوان 2018، تم الاطلاع عليه يوم 9 أفريل 2026ن على الساعة 23:49، على الرابط: https://www.tribunaldz.com

أن تحظر على الشخص المعنوي ممارسة نشاطه الاقتصادي لمدة تصل إلى خمس (5) سنوات[1]، ونحن نؤكد أن هذا المزيج من العقوبات المالية والإدارية يشكل رادعاً فعالاً وشاملاً، إذ يجعل من تكلفة الجريمة الرقمية أعلى بكثير من مكاسبها المحتملة، كما أنه يضرب الكيان الاعتباري في مصدر قوته الاقتصادية عبر الغرامات الباهظة والحظر عن النشاط، مما يحفز المؤسسات على وضع أنظمة رقابة داخلية صارمة ومكافحة شاملة للامتثال القانوني.

ثالثاً: التعويضات المدنية والمسؤولية المتوازية للأشخاص الطبيعيين

بالإضافة إلى العقوبات الجزائية المقررة للشخص المعنوي، يلتزم الكيان الاعتباري بدفع تعويضات مدنية للمتضررين من جريمة التزوير الرقمي، تستهدف تغطية الأضرار المادية والأدبية الناجمة عن الفعل الإجرامي[2]، ولا تقتصر المسؤولية على الشخص المعنوي وحده، بل يظل الأشخاص الطبيعيون المتورطون في الارتكاب (كالموظفين أو المديرين التنفيذيين أو الممثلين القانونيين) مسؤولين جنائياً بشكل شخصي وموازٍ للمسؤولية المعنوية، حيث تصل عقوباتهم السالبة للحرية إلى السجن لمدة تصل إلى ثلاثين (30) سنة أو السجن المؤبد في الحالات الخطيرة كتزوير التوقيعات الإلكترونية الحكومية أو الوثائق الرسمية الرقمية[3]، وهذا النهج المزدوج في المسؤولية يضمن عدم إفلات المسؤولين الفعليين عن الكيان الاعتباري من العقاب الجنائي الشخصي، ويحقق مبدأ المحاسبة الشاملة الذي يستهدف كل من الذات الاعتبارية والذات الطبيعية للجاني، وعليه نستخلص أن المشرع الجزائري قد نجح في وضع إطار قانوني متكامل يجمع بين ردع الكيان الاعتباري وتأديبه، ومحاسبة الأفراد المسؤولين بشكل شخصي، مما يشكل ضمانة قانونية قوية لحماية الاقتصاد الرقمي الوطني من جرائم التزوير المعقدة.

الفرع الثالث: عقوبة الشروع والمشاركة في التزوير الرقمي

تُمثّل مرحلتا الشروع والمشاركة في الجريمة من المفاهيم الجوهرية في النظرية الجنائية العامة، إذ تمتدان دائرة الحماية القانونية لتشمل الأفعال التمهيدية والمساعدة التي تسبق الجريمة التامة أو ترافقها، وذلك في سياق استراتيجية وقائية رامية إلى قطع دابر الجريمة قبل تحقق نتيجتها الإجرامية، وفي مجال التزوير الرقمي تكتسب

[1] **المسؤولية الجزائية للشخص المعنوي والشخص الطبيعي**، منشور على منتدى المحاكم والمجالس القضائية، بتاريخ 21 جوان 2018، تم الاطلاع عليه يوم 9 أفريل 2026ن على الساعة 23:49، على الرابط: https://www.tribunaldz.com

[2] **المسؤولية الجزائية للشخص المعنوي والشخص الطبيعي**، منشور على منتدى المحاكم والمجالس القضائية، بتاريخ 21 جوان 2018، تم الاطلاع عليه يوم 9 أفريل 2026ن على الساعة 23:49، على الرابط: https://www.tribunaldz.com

[3] **تحديد المسؤولية الجزائية للشخص الاعتباري في التشريع الجزائري والقانون المقارن**، موقع WordPress، منمنشور بتاريخ 6 أكتوبر 2013، تم الاطلاع عليه يوم 9 أفريل 2026، على الساعة 23:58، على الرابط: https://norbertnoland.wordpress.com

هاتان الظاهرتان أهمية بالغة نظراً للطبيعة التقنية المعقدة لهذه الجرائم، التي قد تتطلب مراحل إعداد وتخطيط مسبقة (كبرمجة أدوات الاختراق أو إعداد بيانات مزيفة)، أو مشاركة متعددة الأطراف (كتوزيع الأدوار بين مبرمج وممول ووسيط)، وقد أدرك المشرع الجزائري هذا الخصوصية، فنصّ صراحة في قانون رقم 24-02 المؤرخ في 26 فيفري 2024، بالإضافة إلى النصوص المكملة، على تجريم الشروع والمشاركة في التزوير الرقمي، معتبراً إياهما جرائم مستقلة تستوجب العقاب بذاتها، وذلك في إطار استراتيجية رادعة تهدف إلى حماية الثقة العامة في المعاملات الإلكترونية.

أولاً: مفهوم الشروع في التزوير الرقمي وشروطه وعقوبته

يُعرّف الشروع في الفقه الجنائي الجزائري بأنه "كل فعل ظاهري يشكل بداية لتنفيذ الجريمة المخطط لها، ولكنه يتوقف أو يقطع لسبب خارجي عن إرادة الجاني"، وهو تعريف يمتد ليشمل التزوير الرقمي باعتباره جريمة مادية يمكن أن يتوقف تنفيذها عند حد معين، وقد تكيّف المشرع هذا المفهوم ليشمل، في سياق التزوير الإلكتروني، أفعالاً كإعداد برمجيات خبيثة مخصصة لتزوير التوقيعات الإلكترونية، أو محاولة اختراق نظام معلومات بهدف تعديل بيانات حساسة، أو حتى البدء في تغيير بيانات رقمية دون اكتمال النتيجة المزيفة، وكلها أفعال تُعتبر شروعاً مجرماً يستوجب العقاب[1].

ووفقاً للمادة 33 من قانون رقم 24-02 المتعلق بمكافحة التزوير واستعمال المزور، يُعاقب الشارع في التزوير الرقمي بعقوبة سالبة للحرية تُماثل في حدها الأقصى تلك المقررة للجريمة التامة في بعض الحالات، حيث تصل مدة الحبس إلى خمس (5) سنوات، بالإضافة إلى غرامة مالية نقدية تتراوح بين خمسين ألف (50.000) وخمسمائة ألف (500.000) دينار جزائري[2]، وقد نص القانون على إمكانية تشديد هذه العقوبات في حالات معينة، خاصة عندما يتعلق الشروع بتزوير معاملات إلكترونية حساسة تُهدد الأمن القومي أو الاقتصاد العام.

ونحن نرى أن هذا التشديد في عقوبة الشروع يعكس وعياً تشريعياً عميقاً بخاصية الجرائم الإلكترونية التي تُعدّ في الخفاء، وقد لا يتم اكتشافها إلا بعد تحقق النتيجة، مما يجعل مرحلة الشروع هي الفرصة الأمثل للتدخل الوقائي، كما أن إعداد الأدوات الرقمية للتزوير (كبرمجيات التزييف أو اختراق الأنظمة) يُشكل بحد ذاته خطراً

[1] مهداوي حنان، **التنظيم القانوني للجريمة الالكترونية في التشريع الجزائري**، مجلة الفكر القانوني والسياسي، جامعة محمد لمين دباغين، سطيف 2، المجلد 06، العدد 02، منشور بتاريخ 02 نوفمبر 2022، ص 1068.

[2] **تفاصيل مشروع قانون مكافحة التزوير واستعمال المزور**، الاذاعة الجزائرية، منشور بتاريخ 21 نوفمبر 2023، تم الاطلاع عليه يوم 10 أفريل 2026، على الساعة 00:26، على الرابط: https://news.radioalgerie.dz

محدقاً على الأمن السيبراني، حتى ولو لم تتمكن الجريمة من التكامل، مما يستوجب ردعاً مبكراً يحول دون تحقيق النتيجة الإجرامية ويحمي النظام الرقمي من الاختراقات المستقبلية.

ثانياً: أركان وأشكال المشاركة في التزوير الرقمي وعقوباتها

تُعرّف المشاركة في الجريمة وفقاً للمشرع الجزائري بأنها "كل فعل يسهم في ارتكاب الجريمة، من اتفاق، أو مساعدة، أو تحريض، أو أي دور هامشي"، وهو نص عام تم تكييفه ليشمل التزوير الرقمي بكافة أشكاله ومراحله، فقد تشمل المشاركة في التزوير الرقمي تقديم الدعم اللوجستي (كإتاحة الخوادم أو الأجهزة الإلكترونية)، أو الدعم المالي (تمويل عمليات التزوير)، أو الدعم التقني (تصميم البرمجيات أو تقديم الخبرة التقنية)، أو حتى التحريض على ارتكاب الجريمة أو الترويج لخدمات تزوير رقمية عبر المنصات الإلكترونية، وكلها أفعال تُكتسب استقلالاً إجرامياً تستوجب العقاب حتى ولو لم يرتكب الفاعل الأصلي الجريمة بنفسه[1].

وقد نصت المادة 34 من قانون 24-02 على معاقبة المشاركين في التزوير الرقمي بعقوبة مماثلة لعقوبة الجريمة الأصلية، حيث تتراوح عقوبة الحبس بين سنة واحدة (1) وخمس (5) سنوات، بالإضافة إلى غرامة مالية قد تصل إلى خمسمائة ألف (500.000) دينار جزائري[2]، كما نص القانون صراحة على إمكانية تشديد العقوبات بشكل كبير في حالات معينة، وتحديداً عندما يتورط في المشاركة موظف عمومي أو ضابط يستغل منصبه، أو عندما تؤدي المشاركة إلى اختلال كبير بالثقة العامة أو الأمن القومي أو الاقتصاد الوطني، حيث تصل العقوبات في هذه الحالات الخطيرة إلى عشر (10) سنوات سجناً[3].

ونحن نؤكد أن هذا النهج في تجريم المشاركة يستهدف بشكل خاص طبيعة الجرائم الإلكترونية المنظمة، التي تتطلب عادةً تخصصات متعددة (مبرمجين، ممولين، وسطاء، مروجين)، مما يجعل معاقبة كل حلقة في سلسلة الجريمة ضرورة حتمية لتحقيق الردع العام، كما أن عقاب المشارك بعقوبة الجريمة الأصلية يعكس مبدأ المسؤولية الجنائية الشخصية، ويمنع اللجوء إلى "التقسيم الأدوار" كوسيلة للإفلات من العقاب، خاصة في ظل التعاملات الرقمية التي تسمح بإخفاء هوية المشاركين عبر الشبكات المشفرة.

---

[1] القانون رقم 24-02 المؤرخ في 26 فيفري 2024، المتعلق بمكافحة التزوير واستعمال المزور، الجريدة الرسمية، العدد 15، الصادر بتاريخ 29 فيفري 2024.

[2] القانون رقم 24-02 المؤرخ في 26 فيفري 2024، المتعلق بمكافحة التزوير واستعمال المزور، الجريدة الرسمية، العدد 15، الصادر بتاريخ 29 فيفري 2024.

[3] القانون رقم 24-02 المؤرخ في 26 فيفري 2024، المتعلق بمكافحة التزوير واستعمال المزور، الجريدة الرسمية، العدد 15، الصادر بتاريخ 29 فيفري 2024.

ثالثاً: العقوبات الإضافية والإجرائية المصاحبة للشروع والمشاركة

بالإضافة إلى العقوبات السالبة للحرية والمالية الأساسية، أقرّ المشرع الجزائري عقوبات إضافية وإجرائية رادعة تستهدف الأدوات المستخدمة في الجريمة والقدرة على العود إليها، ففي إطار قانون رقم 09-04 المؤرخ في 5 اوت 2009 المتعلق بالوقاية من الجرائم المرتبطة بالتكنولوجيات الإعلام والاتصال ومكافحتها، تُضاف عقوبات كمصادرة الأجهزة والوسائل الرقمية المستخدمة في ارتكاب جريمة الشروع أو المشاركة في التزوير الرقمي، والتي تشمل الحواسيب والخوادم والبرمجيات وأية أدوات تقنية أخرى مرتبطة بالفعل الإجرامي[1].

كما أدخلت التعديلات الحديثة لعام 2024، وتحديداً في إطار قانون 18-05، عقوبات إضافية تتمثل في الحظر من استخدام الإنترنت لمدة تصل إلى ثلاث (3) سنوات كعقوبة إضافية في حالات معينة[2]، مما يُشكل رادعاً فعالاً في بيئة الجريمة الرقمية التي تعتمد أساساً على الاتصال بالشبكة العنكبوتية، ونحن نعتبر أن هذه العقوبات الإضافية تكتسب أهمية استثنائية في مجال التزوير الرقمي، إذ إن مصادرة الأدوات التقنية تُفقد المجرم وسيلة الارتكاب، بينما يُشكل الحظر من الإنترنت عقوبة وقائية فعالة تمنع العود إلى الجريمة في بيئة رقمية أصبحت ضرورة للحياة العصرية.

يتضح مما تقدم أن المشرع الجزائري قد نجح في وضع إطار قانوني متكامل ومتطور يجمع بين تجريم الشروع والمشاركة في التزوير الرقمي، وتشديد العقوبات عليهما بما يتناسب مع خطورة الأفعال التمهيدية والمساعدة، مع إضافة عقوبات إجرائية تستهدف الوسائل المستخدمة، ونحن نرى أن هذا المنظومة القانونية تُمثّل قفزة نوعية في الفقه الجنائي الجزائري، تُحاكي التطورات الدولية في مكافحة الجرائم السيبرانية، وتضمن حماية شاملة للاقتصاد الرقمي الوطني من جرائم التزوير المعقدة، شريطة أن ترافقها آليات فعالة في جمع الأدلة الرقمية وتتبع الجناة عبر الحدود.

المطلب الثاني: الظروف المشددة والاعذار القانونية

لا يكتفي المشرع بوضع عقوبات ثابتة لكل الجرائم، بل يضع قواعد مرنة تسمح للقاضي بتشديد العقاب إذا اقترن الفعل بظروف تزيد من جسامته، أو تخفيفه إذا توافرت أعذار قانونية تبرر ذلك، وفي جريمة التزوير الرقمي، نجد أنَّ السياسة الجنائية الحديثة في الجزائر قد جعلت من "محل الجريمة" (المؤسسات الحساسة)

[1] **الأحكام الجديدة في قانون مكافحة التزوير واستعمال المزور محور يوم دراسي بالجزائر العاصمة**، وكالة الانباء الجزائرية، بتاريخ 30 جوان 2024، تم الاطلاع عليه يوم 10 أفريل 2026، على الساعة 00:42، على الرابط: https://www.aps.dz/ar/algerie/164434

[2] القانون رقم 18-05 المؤرخ في 10 ماي 2018، المتعلق بالتجارة الالكترونية، الجريدة الرسمية، العدد 28، الصادر بتاريخ 16 ماي 2018.

و"صفة الجاني" (الجماعة المنظمة) ركيزتين للتشديد، مقابل منح أعذار معفية أو مخففة لمن يساهم في كشف الحقيقة.

الفرع الأول: تشديد العقوبة في حال المساس بمؤسسات الدولة

مع التسارع المتزايد في التحول الرقمي على المستوى الوطني، أصبحت مؤسسات الدولة والقطاعات الحكومية هدفاً مباشراً واستراتيجياً للجرائم الإلكترونية المعقدة، مما يفرض على المشرع وضع ردع قانوني صارم يضمن حماية المصالح العليا للبلاد واستقرار مؤسساتها السيادية، وقد أدرك المشرع الجزائري خطورة المساس بالأمن السيبراني للدولة، فنصّ في التشريع الحديث – وتحديداً في قانون رقم 24-02 المؤرخ في 26 فيفري 2024 المتعلق بمكافحة التزوير واستعمال المزور – على اعتبار استهداف مؤسسات الدولة أو موظفيها العموميين ظرفاً مشدداً يستدعي تطبيق عقوبات استثنائية تفوق بكثير العقوبات العادية المقررة في الحالات المشابهة، وعليه يتعين التفحص الدقيق للأساس القانوني لهذا التشديد، وتحديد مدى العقوبات المقررة في هذه الحالات الخطيرة، وتقييم مدى فعالية هذا النهج في حماية المصلحة العامة.

أولاً: الإطار القانوني والمفهوم الجنائي لتشديد العقوبة عند المساس بالدولة

يستند تشديد العقوبة في جرائم التزوير الرقمي إلى النصوص الصريحة والواضحة لقانون رقم 24-02، الذي يُعدّ الإطار القانوني الأساسي والحديث لمكافحة هذه الظاهرة، حيث يتضمن أحكاماً خاصة تُطبق تلقائياً عندما يكون الهدف من الجريمة المساس بمؤسسات الدولة أو الأمن القومي أو الاستقرار الاقتصادي الوطني[1]، فقد نص القانون صراحة على أن جرائم التزوير الرقمي التي تطال الوثائق الرسمية الحكومية أو قواعد البيانات الإدارية أو العملات الرقمية والسندات المالية تُكتسب بعداً خطيراً يستدعي العقاب بأقصى درجات الشدة، وذلك حماية للسيادة الوطنية وسلطة القانون ونزاهة الإدارة العمومية[2]، ونحن نرى أن هذا التوجه التشريعي يعكس فلسفة رادعة جديدة تهدف إلى قطع الطريق على أي محاولة لاستهداف البنية التحتية الرقمية للدولة أو المساس بمصداقية مؤسساتها، مما يُشكل ضمانة قانونية جوهرية لاستقرار المؤسسات في مواجهة التهديدات السيبرانية المتطورة التي تتجاوز الحدود التقليدية للجريمة.

[1] قانون رقم 24-02 المؤرخ في 26 فيفري 2024، المتعلق بمكافحة التزوير واستعمال المزور، الجريدة الرسمية، العدد 15، الصادر بتاريخ 29 فيفري 2024.

[2] **صدور قانون مكافحة التزوير واستعمال المزور في الجريدة الرسمية**، موقع الجزائر الان، منشور بتاريخ 13 مارس 2024، تم الاطلاع عليه يوم 10 أفريل 2026، على الساعة 19:26، على الرابط: https://algeriemaintenant.dz

ثانياً: تدرج العقوبات المشددة حسب خطورة الجريمة وطبيعة المؤسسة المستهدفة

يتميز التشريع الجزائري بتدرج دقيق ومرن في العقوبات المقررة عندما يتعلق الأمر بالمساس بمؤسسات الدولة، حيث ترتفع سقف العقوبة بشكل كبير وجذري مقارنة بالجرائم الموجهة ضد الأفراد أو القطاع الخاص، ففي الحالات العادية من التزوير الرقمي، قد تتراوح العقوبة بين خمس (5) وعشر (10) سنوات سجناً، إلا أن هذا الحد الأدنى يتضاعف شدةً ليصل إلى خمس عشرة (15) أو عشرين (20) سنة سجناً عندما تستهدف الجريمة قواعد بيانات حكومية حساسة أو وثائق رسمية تخص الدولة ومؤسساتها السيادية[1]، أما في أشد الحالات خطورة، كتزوير النقود والسندات المالية الرقمية أو الأختام الرسمية للدولة أو التوقيعات الإلكترونية الحساسة التي تمس بالأمن الوطني المباشر، فإن العقوبة تصل إلى حد السجن المؤبد أو ثلاثين (30) سنة سجناً، مما يعكس إدراكاً عميقاً لخطورة هذه الأفعال على الاقتصاد الوطني والثقة العامة[2]، ونؤكد نحن أن هذا التفريق الدقيق في درجات العقوبات يُظهر حكمة المشرع في تكييف الرد القانوني بما يتناسب مع جسامة الضرر المحتمل على المصلحة العامة، حيث إن المساس بمؤسسات الدولة لا يقتصر على الضرر المادي المباشر، بل يمتد ليهدد الثقة الجماعية في النظام الإداري والمالي والسياسي للبلاد ككل.

ثالثاً: التشديد الإضافي عند تورط الموظف العام في استهداف مؤسسات الدولة

يُشدد القانون الجزائري العقوبة بشكل ملحوظ ومضاعف عندما يرتكب جريمة التزوير الرقمي موظف عمومي أو ضابط، خاصة إذا كان فعله يندرج في إطار استغلال منصبه الوظيفي للمساس بمؤسسة الدولة التي يعمل بها أو يتبع لها، وذلك اعتباراً لأن هذا التورط يُشكل خيانة صريحة للأمانة العامة واعتداءً مباشراً على الثقة التي يوليها المجتمع للموظفين العموميين القائمين على شؤون الدولة[3]، فقد نصّ القانون صراحة على أنه في حالة تورط موظف عمومي في التزوير الرقمي المستهدف للدولة، فإن العقوبة تُشدد لتصل إلى السجن المؤبد أو ما بين عشرين (20) وثلاثين (30) سنة سجناً، مع غرامات مالية ضخمة تتراوح بين مليون ومليوني دينار جزائري، بغض النظر عن العقوبات التأديبية الأخرى التي قد تُوقع عليه في إطار قواعد الوظيفة العمومية[4]، ونحن نعتبر أن هذا التشديد المزدوج – الجنائي والتأديبي – يعكس إدراكاً تشريعياً عميقاً لخطورة الفساد الرقمي

---

[1] رياض/خ، **قانون مكافحة جرائم التزوير في الجريدة الرسمية**، البلاد نت، منشور بتاريخ 13 مارس 2024، تم الاطلاع عليه يوم 10 أفريل 2026، على الساعة 19:30، على الرابط: https://elbilad.net

[2] رياض/خ، **قانون مكافحة جرائم التزوير في الجريدة الرسمية**، البلاد نت، منشور بتاريخ 13 مارس 2024، تم الاطلاع عليه يوم 10 أفريل 2026، على الساعة 19:30، على الرابط: https://elbilad.net

[3] **تفاصيل مشروع قانون مكافحة التزوير واستعمال المزور**، الاذاعة الجزائرية، منشور بتاريخ 21 نوفمبر 2023، تم الاطلاع عليه يوم 10 أفريل 2026، على الساعة 19:33، على الرابط: https://news.radioalgerie.dz

[4] **الأحكام الجديدة في قانون مكافحة التزوير واستعمال المزور محور يوم دراسي بالجزائر العاصمة**، وكالة الانباء الجزائرية، بتاريخ 30 جوان 2024، تم الاطلاع عليه يوم 10 أفريل 2026، على الساعة 19:40، على الرابط: https://www.aps.dz/ar/algerie/164434

المؤسساتي، ويؤكد أن الدولة لن تتسامح مع استغلال المنصب العام والسلطة المخولة للإضرار بالمصلحة العليا للبلاد، مما يعزز من نزاهة الإدارة ويضمن حسن سير المرفق العام ويحمي مؤسسات الدولة من الخيانة الداخلية.

يتضح مما تقدم أن المشرع الجزائري قد نجح في وضع إطار قانوني متكامل ومتطور يعتمد على تشديد العقوبات في حال المساس بمؤسسات الدولة، مستخدماً سلم عقابي تصاعدي يبدأ من السجن لسنوات طويلة ويصل إلى المؤبد في الحالات الأشد خطورة، ونحن نرى أن هذه المنظومة القانونية الصارمة تُمثّل قفزة نوعية في الفقه الجنائي الجزائري، تُحاكي التطورات الدولية في مكافحة الجرائم السيبرانية ضد الدول، وتضمن حماية شاملة للمصالح العليا والاقتصاد الرقمي الوطني، شريطة أن تترافق مع آليات رقابية فعالة داخل المؤسسات الحكومية لمنع وقوع هذه الجرائم قبل ارتكابها.

الفرع الثاني: صفة الفاعل (موظف عام أو متخصص في المعلوماتية)

تُعدّ صفة الفاعل في الجريمة من المعايير الجوهرية التي يعتمد عليها المشرع الجنائي في تقدير العقوبة وتشديدها، إذ إن ارتكاب الجريمة من قبل أشخاص يتمتعون بصفات خاصة (كالموظفين العموميين أو ذوي الخبرات التقنية) يُكتسب بموجبه الفعل الإجرامي بعداً خطيراً يستوجب ردعاً مضاعفاً، وفي مجال التزوير الرقمي، يكتسب هذا المعيار أهمية بالغة؛ فالموظف العام يستغل منصبه وسلطاته الوظيفية للإضرار بالمصلحة العامة، بينما يستغل المتخصص في المعلوماتية خبرته التقنية لإخفاء أثر الجريمة وتعقيد سبل اكتشافها، وقد أولى المشرع الجزائري في التشريع الحديث –وتحديداً في قانون رقم 24–02 المؤرخ في 26 فيفري 2024– اهتماماً بالغاً بهاتين الصفتين، معالجاً إياهما بشكل يضمن حماية مؤسسات الدولة والثقة العامة في الفضاء السيبراني.

أولاً: الموظف العام كظرف مشدد في جريمة التزوير الرقمي

يُعدّ الموظف العام في التشريع الجزائري ظرفاً مشدداً يستوجب تشديد العقاب عند ارتكابه لجريمة التزوير الرقمي، وذلك استناداً إلى قانون رقم 24–02 الذي ينص صراحة على أن ارتكاب الجريمة من قبل موظف عمومي يستغل منصبه يُعدّ خيانة للأمانة العامة واعتداءً على الثقة التي يوليها المجتمع للإدارة العمومية[1]، فقد نصت المادة المُعدّلة من القانون العقوبات على أن عقوبة التزوير الرقمي تتراوح بين سنتين (2) وعشر (10) سنوات سجناً عند ارتكابها من قبل موظف عمومي، مقارنة بعقوبة تتراوح بين سنة وخمس سنوات للفاعل

[1] رياض/خ، **قانون مكافحة جرائم التزوير في الجريدة الرسمية**، البلاد نت، منشور بتاريخ 13 مارس 2024، تم الاطلاع عليه يوم 10 أفريل 2026، على الساعة 19:55، على الرابط: https://elbilad.net

العادي، مع إمكانية تشديدها لتصل إلى عشرين (20) أو ثلاثين (30) سنة أو المؤبد في الحالات الخطيرة التي تستهدف مؤسسات الدولة[1].

ويرتكز هذا التشديد على اعتبار أن الموظف العام مكلف بحماية الوثائق الرسمية والبيانات الإدارية، فإذا انقلب إلى مرتكب للتزوير الرقمي باستغلال منصبه، فإنه يُعدّ فاعلاً خطيراً يستهدف النظام العام من الداخل، ونحن نرى أن هذا النهج التشريعي يعكس فلسفة رادعة تهدف إلى حماية نزاهة الإدارة العمومية وسلامة المؤسسات الحكومية من الخيانة الداخلية، حيث إن استغلال السلطة الوظيفية في ارتكاب الجرائم الرقمية يُفقد المواطنين الثقة في الحكومة الإلكترونية ويُهدد استقرار المرفق العام[2].

ثانياً: المتخصص في المعلوماتية وطبيعة معاملته القانونية

على النقيض من الموظف العام، لا يُعتبر المتخصص في المعلوماتية (المهندس أو الخبير السيبراني) صفة مستقلة في التشريع الجزائري تستوجب تشديداً خاصاً بالمعنى القانوني الصارم، إذ يُعامل كفاعل عادي من حيث الأصل، لكن المشرع أخذ بعين الاعتبار الخصوصية التقنية لهذه الفئة عند ارتكابها للتزوير الرقمي[3]، فالمتخصص في المعلوماتية يملك القدرة على استغلال برمجيات متقدمة أو اختراق أنظمة معقدة أو تزوير توقيعات إلكترونية بحرفية عالية، مما يجعل جريمته أكثر خطورة ويصعّب من اكتشافها وتحقيقها[4].

وقد نصت المادة 45 من قانون24-02 على إمكانية تشديد العقوبة عند استغلال خبرة تقنية متخصصة في ارتكاب التزوير الرقمي، حيث يُمكن للقاضي أن يرفع العقوبة من الحد الأدنى إلى الحد الأقصى المقرر قانوناً، وصولاً إلى ثماني (8) سنوات سجناً إذا تسبب الفعل في ضرر فادح لأنظمة معلوماتية حيوية[5]، ونحن نؤكد أن هذا التعامل المرن مع صفة المتخصص يكشف عن حكمة المشرع في مواكبة التطور التكنولوجي، إذ

---

[1] **تفاصيل مشروع قانون مكافحة التزوير واستعمال المزور**، الاذاعة الجزائرية، منشور بتاريخ 21 نوفمبر 2023، تم الاطلاع عليه يوم 10 أفريل 2026، على الساعة 19:58، على الرابط: https://news.radioalgerie.dz

[2] بن لعربي أسماء، الفحلة مديحة، **التزوير المعلوماتي في عصر الرقمنة: بين قابلية الخضوع للقواعد العامة وضرورة تبني نصوص خاصة**، مجلة الفكر القانوني والسياسي، جامعة عمار ثليجي الأغواط، المجلد 08، العدد 02، بتاريخ 20 نوفمبر 2024، ص 449.

[3] **الجزائر تتشدد في محاربة التزوير والاحتيال**، موقع الشرق الأوسط، منشور بتاريخ 22 نوفمبر 2023، تم الاطلاع عليه يوم 10 أفريل 2026، على الساعة 20:02، على الرابط: https://aawsat.com

[4] **مواجهة الجريمة المعلوماتية في التشريع الجزائري**، موقع جامع الكتب الاسلامية، تم الاطلاع عليه يوم 10 أفريل 2026، على الساعة 20:06، على الرابط: https://ketabonline.com

[5] **جريمة تزوير المحررات (التزوير الخطي) في القانون الجزائري**، مدونة الحقوق والعلوم السياسية (APP-ON)، منشور بتاريخ 22 أكتوبر 2013، تم الاطلاع عليه يوم 10 أفريل 2026، على الساعة 20:10، على الرابط: https://www.app-on.com/2013/10/blog-post9260.html

إن الخبرة التقنية –وإن لم تكن صفة مستقلة– تُشكل عامل خطورة موضوعية تبرر العقاب المشدد، خاصة أن المتخصص يستغل ثقة المؤسسات فيه لتضليل الأنظمة الأمنية.

ثالثاً: المقارنة بين الصفتين وأثرهما في المسؤولية الجنائية

تكشف المقارنة بين معاملة الموظف العام والمتخصص في المعلوماتية عن توجه تشريعي يستهدف حماية مزدوجة: الأولى حماية المؤسسات من الخيانة الداخلية (في حالة الموظف)، والثانية حماية الأنظمة الرقمية من الاستغلال التقني (في حالة المتخصص)، فبينما يُعدّ الموظف العام ظرفاً مشدداً شكلياً يُكتسب بمجرد توفر الصفة وارتكاب الجريمة في إطار الوظيفة، يظل تشديد العقاب في حق المتخصص مرهوناً بثبوت استغلاله الفعلي لخبرته التقنية في تنفيذ الجريمة[1].

وعليه، نستخلص أن المشرع الجزائري قد نجح في تكييف أحكام صفة الفاعل بما يتناسب مع طبيعة التزوير الرقمي، حيث جمع بين الردع الصارم للخونة الوظيفيين والتعامل المرن مع الخبرات التقنية المُسيئة استغلالها، ونحن ندعو إلى ضرورة إضفاء صفة قانونية أكثر وضوحاً للمتخصص في المعلوماتية في التعديلات المستقبلية، على غرار معاملة الموظف العام، وذلك لمواكبة الخطورة المتزايدة للجرائم السيبرانية المعقدة.

الفرع الثالث: الأعذار المعفية والمخففة للعقوبة

يعدّ استقراء الأعذار المعفية والمخففة للعقوبة في جرائم التزوير الرقمي من المسائل القانونية الدقيقة التي تقتضي الوقوف عند المنظومة التشريعية الجزائرية الحديثة، والتي حاولت الموازنة بين مقتضيات المصلحة الاجتماعية في مكافحة الجرائم الرقمية المتطورة، وبين مراعاة الظروف الفردية للمتهم التي قد تستدعي العطف القانوني، وإذا كان القانون رقم 24–02 المؤرخ في 26 فيفري 2024 المتعلق بمكافحة التزوير واستعمال المزور[2] قد شدد العقوبات في جرائم التزوير الرقمي، فإن المشرع الجزائري لم يغفل عن إمكانية تطبيق الأعذار العامة المنصوص عليها في قانون العقوبات، وتحديداً المادة 52 التي تحدد الأعذار المعفية والمخففة [3]، مما يعكس فلسفة تشريعية ترمي إلى تحقيق العدالة الجنائية في سياق الجرائم المعاصرة.

---

[1] **أركان جريمة التزوير في المحررات الرسمية أو العمومية في القانون الجزائري**، مدونة القانون والتعليم، منشور منذ 7 سنوات (سنة 2019)، تم الاطلاع عليه يوم 10 أفريل 2026، على الساعة 20:14، على الرابط: https://droit7.blogspot.com

[2] القانون رقم 24–02 المؤرخ في 26 فيفري 2024، المتعلق بمكافحة التزوير واستعمال المزور، الجريدة الرسمية، العدد 15، الصادر بتاريخ 29 فيفري2024.

[3] **الاعذار القانونية في قانون العقوبات الجزائري**، موقع المحاكم والمجالس القضائية، منشور بتاريخ 19 جانفي 2016، تم الاطلاع عليه يوم 10 أفريل 2026، على الساعة 20:47، على الرابط: https://tribunaldz.com

أولا: الأعذار المعفية للعقوبة في جرائم التزوير الرقمي

ينص قانون العقوبات الجزائري في المادة 52 على الأعذار المعفية للعقوبة بشكل عام، دون أن يخصص أعذاراً استثنائية لجرائم التزوير الرقمي، مما يعني أن الأعذار المنصوص عليها في هذه المادة تطبق على جرائم التزوير الرقمي متى توافرت شروطها[1]، وتجدر الإشارة إلى أن هذه الأعذار تتمحور حول ثلاثة محاور رئيسية:

أ. الخطأ في القانون أو الواقع، حيث ينص القانون صراحة على أنه إذا ارتكب المتهم فعل التزوير الرقمي بناءً على خطأ في الواقع أو جهالة بالقانون، فإنه يُعفى من العقوبة شريطة انتفاء النية الجنائية لديه.

ب. الإكراه أو الضرورة، إذ يسري الإعفاء من العقوبة إذا كان الجاني قد ارتكب الجريمة تحت تأثير إكراه مادي أو معنوي، أو في حالة الضرورة القصوى التي لا يتوفر فيها خيار آخر للجاني.

ج. الدفاع الشرعي، والذي يُعتبر عذراً معفياً إذا كان التعديل على الوثيقة الرقمية ضرورياً لدرء ضرر شيك عن المدافع أو الغير، بشرط ألا تتجاوز حدود الدفاع المشروع[2].

من خلال استقراء النصوص القانونية والواقع القضائي، يتبين أن تطبيق الأعذار المعفية في مجال التزوير الرقمي يواجه صعوبات تقنية وقانونية جوهرية، ففيما يخص الخطأ في الواقع، نلاحظ أن طبيعة الجرائم الرقمية التقنية المعقدة تجعل إثبات الجهل بمزية الوسائط الإلكترونية أمراً صعباً، إذ يفترض المشرع أن مستخدمي التكنولوجيا الرقمية يمتلكون وعياً كافياً بطبيعة الأدوات التي يستخدمونها، وعليه فإن التحقيقات التقنية تلعب دوراً محورياً في إثبات هذه الأعذار، حيث إن تحليل البيانات وفحص السجلات الإلكترونية يمكّن من الكشف عن مدى علم الجاني ونيته الجنائية[3].

ثانيا: الأعذار المخففة للعقوبة في جرائم التزوير الرقمي

ينص قانون العقوبات الجزائري في المادة 141 على مجموعة من الظروف المخففة للعقوبة التي تخول للقاضي تقديراً واسعاً في تكييف العقوبة بما يتناسب مع ظروف الجاني وملابسات الجريمة[4]، وتتجلى هذه الظروف في عدة عناصر: الظروف الشخصية للجاني كصغر السن وعدم وجود سوابق قضائية وطبيعة الشخصية؛ والتعاون مع سلطات التحقيق من خلال تقديم أدلة رقمية تسهل كشف ملابسات الجريمة والمتورطين

---

[1] المحامية مروة أبو العلا، **بحث ودراسة حول الأعذار القانونية في القانون الجنائي**، موقع محاماة نت، منشور بتاريخ 14 أكتوبر 2018، تم الاطلاع عليه يوم 10 أفريل 2026، على الساعة 20:49، على الرابط: https://mohamah.net

[2] معمري ايمان، فضيلة شعبان، **المرجع السابق**، ص20.

[3] بن صويلح سفيان، حريدي الياس، **مكافحة التزوير واستعمال المزور في ظل القانون 24-02**، مذكرة ماستر تخصص قانون الأعمال، كلية الحقوق والعلوم السياسية، جامعة 8 ماي 1945 قالمة، السنة الدراسية 2025/2024، ص 68.

[4] **الأعذار القانونية والظروف القضائية المخففة والمشددة**، مجلة المخبر القانوني ، تم الاطلاع عليه يوم 10 أفريل 2026، على الساعة 21:00، على الرابط: https://labodroit.com

في شبكات التزوير الإلكتروني؛ والندم والاعتراف الطوعي بالجريمة قبل افتضاح الأمر؛ فضلاً عن طفافة الضرر الناتج عن الجريمة[1]، وقد أكد المشرع في القانون 24-02 على أهمية الوقاية الرقمية والتعاون مع السلطات، مما يعكس توجهات تشريعية رامية إلى تشجيع الجناة على التراجع عن أفكارهم الإجرامية[2].

إن التحليل المقارن للأعذار المعفية والمخففة يكشف عن اختلاف جوهري في الآثار القانونية، فبينما تؤدي الأعذار المعفية إلى إزالة العقوبة كلياً مع بقاء الجريمة قائمة، فإن الأعذار المخففة تؤدي إلى تخفيض نوع العقوبة أو مدتها دون إلغائها [3]، ونرى أن الظروف المخففة تكتسي أهمية خاصة في جرائم التزوير الرقمي، حيث إن سرعة تطور التكنولوجيا قد تدفع بعض الأشخاص إلى ارتكاب تجاوزات دون وعي كامل بخطورة فعلهم، أو تحت تأثير الضغوط الاقتصادية والاجتماعية. كما أن التعاون مع التحقيقات يكتسي أهمية استراتيجية في مكافحة الجرائم المنظمة إلكترونياً، إذ يسهم في كشف الشبكات الإجرامية المعقدة[4].

المطلب الثالث: العقوبات التكميلية والتدابير الأمنية

لا يكتفي النظام العقابي الجزائري بالعقوبات الأصلية لمواجهة ظاهرة التزوير الرقمي، بل يعززها بمجموعة من العقوبات التكميلية والتدابير الأمنية التي تهدف إلى تجريد الجاني من الوسائل التي ساعدته على الإجرام، ومنعه من استغلال ثمار جريمته، وتكتسي هذه العقوبات أهمية خاصة في البيئة الرقمية؛ كونها تستهدف "الأدوات التقنية" و"الكيانات البرمجية" التي تُشكل خطراً مستمراً على أمن المعطيات.

الفرع الأول: المصادرة (الأجهزة والبرامج المستخدمة)

يُعد التزوير الرقمي من أخطر الظواهر الإجرامية المعاصرة التي تهدد الأمن المعلوماتي والثقة في المعاملات الإلكترونية، إذ يتجاوز مفهومه التقليدي المتمثل في تزوير المستندات الورقية ليشمل التلاعب بالبيانات الرقمية والتوقيعات الإلكترونية والشهادات الرقمية التصديقية[5]، ونظراً للطبيعة التقنية المعقدة لهذه الجريمة، فإن أدوات ارتكابها تتمثل في أجهزة إلكترونية متطورة وبرامج مضللة مصممة خصيصاً للتزوير

---

[1] عمار فتيحة، **المرجع السابق**، ص 176.

[2] **تفاصيل مشروع قانون مكافحة التزوير واستعمال المزور**، الاذاعة الجزائرية، منشور بتاريخ 21 نوفمبر 2023، تم الاطلاع عليه يوم 10 أفريل 2026، على الساعة 21:06، على الرابط: https://news.radioalgerie.dz

[3] **مجموعة القانون الجنائي**، موقع مجلة مغرب القانون، منشور بتاريخ 19 سبتمبر 2016، تم الاطلاع عليه يوم 10 أفريل 2026، على الساعة 21:08، على الرابط: https://maroclaw.com

[4] زعيون عبد الوهاب، بشكيط يوسف، **مكافحة جريمة تزوير المحررات الرسمية في ظل أحكام القانون رقم: 24-02**، مذكرة ماستر تخصص قانون جنائي، معهد الحقوق، المركز الجامعي عبد الحفيظ بوالصوف- ميلة، السنة الجامعية 2025/2024، ص 48.

[5] مشري راضية، السعيد زيدان، **جريمة تزوير التوقيع الالكتروني في التشريع الجزائري**، حوليات جامعة قالمة، جامعة 8 ماي 1945 قالمة، المجلد 2017، العدد 20، 30 جوان 2017، ص122.

والتلاعب، مما يفرض على المشرع الجزائري وضع آليات رادعة ليس فقط في مجال العقوبات، بل أيضاً في مجال إجراءات الضبط والتحقيق القضائي[1].

أولا: ماهية مصادرة الأجهزة والبرامج المستخدمة في التزوير الرقمي

سوف نتناول ذلك من خلال:

أ). المفهوم القانوني والنطاق الموضوعي

تُعد المصادرة في القانون الجزائري عقوبة أصلية أو تبعية تهدف إلى حرمان المجرم من ممتلكاته التي استخدمها في ارتكاب الجريمة أو كانت ناتجة عنها[2]، وفي سياق التزوير الرقمي، تتسع دائرة المصادرة لتشمل الأجهزة الإلكترونية والبرامج المستخدمة في ارتكاب هذه الجريمة، وذلك استناداً إلى نص المادة 24 مكرر من القانون 06-01 المتعلق بالوقاية من الفساد ومكافحته، والتي تتيح للديوان المركزي للقمع الفساد (OCRC) مصادرة أو حجز الأجهزة والبرامج المرتبطة بالجريمة[3]، كما ينص القانون 18-05 المتعلق بالوقاية من الجرائم المرتبطة بتكنولوجيا المعلومات والاتصالات على مصادرة الأدوات الرقمية المستخدمة في الجرائم الإلكترونية بما في ذلك التزوير[4].

من وجهة نظرنا نرى أن المشرع الجزائري قد اتبع نهجاً تكاملياً في تحديد نطاق المصادرة، إذ لم يقتصر على الأجهزة المادية بل شمل البرامج والتطبيقات الافتراضية، هذا التوسع يعكس وعياً تشريعياً بأن الجريمة الرقمية لا تقتصر على المادة المحسوسة، بل تمتد إلى البيانات والبرمجيات التي تشكل أداة الجريمة في عصر المعلوماتية.

ب). الأجهزة الإلكترونية المشمولة بالمصادرة

تشمل الأجهزة الإلكترونية الممكن مصادرتها في جرائم التزوير الرقمي مجموعة واسعة من المعدات التقنية، ومنها: أجهزة الكمبيوتر المكتبية والمحمولة، الهواتف الذكية، الأقراص الصلبة(Hard Disks) ، خوادم البيانات(Servers) ، وأي أجهزة تخزين بيانات أخرى، وقد أكدت المادة 24 مكرر من القانون06-01 على إمكانية مصادرة الأجهزة الإلكترونية المستخدمة في الجرائم المرتبطة بالفساد، وهو ما ينطبق بالتالي على جرائم التزوير الرقمي المرتبطة بالفساد الإلكتروني، كما تشمل هذه الأجهزة المعدات المستخدمة في إدخال أجهزة

---

[1] راضية مشري، **المرجع السابق**، ص 133.

[2] أحمد محمد محروس عبد العال، **المرجع السابق**، ص 54.

[3] المادة 24 مكرر من القانون رقم 06-01 المؤرخ في 20 فيفري 2006، المتعلق بالوقاية من الفساد ومكافحته، موقع الديوان المركزي لقمع الفساد، تم الاطلاع عليه يوم 14 أفريل 2026، على الساعة 14:24، على الرابط: https://ocrc.gov.dz

[4] القانون رقم 18-05 المؤرخ في 10 ماي 2018، المتعلق بالتجارة الالكترونية، الجريدة الرسمية، العدد 28، الصادر بتاريخ 16 ماي 2018.

محظورة إلى الجزائر عبر المنافذ الجمركية، حيث تقوم الجمارك بمصادرتها فوراً إذا كانت مرتبطة بأنشطة غير قانونية[1].

من وجهة نظرنا نلاحظ أن المشرع الجزائري قد أدرك ضرورة مواكبة التطور التكنولوجي في تحديد الأجهزة المشمولة بالمصادرة، غير أننا نرى أن النصوص القانونية تفتقر إلى تحديد دقيق لبعض الأجهزة الحديثة مثل الأجهزة القابلة للارتداء (Wearable Devices) وإنترنت الأشياء (IoT) ، مما قد يخلق ثغرات قانونية في التطبيق العملي.

ج). البرامج والتطبيقات المشمولة بالمصادرة

لا تقتصر المصادرة على الأجهزة المادية فحسب، بل تمتد لتشمل البرامج والتطبيقات المستخدمة في التزوير الرقمي. ومن بين هذه البرامج: البرمجيات الضارة (Malwares) المستخدمة في التزوير والتلاعب، والبرامج المضللة التي تستهدف التلاعب بالبيانات الرقمية أو التوقيعات الإلكترونية[2]، كما تشمل المصادرة الأدوات الرقمية والمنصات الإلكترونية المستخدمة في إنشاء مستندات أو سجلات غير صحيحة[3]، وقد نص القانون 18-05 صراحة على مصادرة الأدوات المستخدمة في الجرائم الإلكترونية، وهو ما يشمل البرامج والتطبيقات المستخدمة في التزوير الرقمي[4].

من وجهة نظرنا نعتبر أن إدراج البرامج ضمن نطاق المصادرة يمثل إنجازاً تشريعياً هاماً، إذ أن البرنامج في الجريمة الرقمية يعادل السلاح في الجريمة المادية، لكننا نستحسن أن يكون التحديد أكثر تفصيلاً في النصوص القانونية، مع تحديد أنواع البرمجيات المستخدمة في التزوير الرقمي بشكل استنباطي لضمان قابلية التطبيق القضائي.

---

[1] **خمسة اجهزة محظورة عند دخول الجزائر**، منشور على منصة اخر الأخبار، بتاريخ 17 ديسمبر 2024، تم الاطلاع عليه يوم 14 أفريل 2026، على الساعة 14:32، على الرابط: https://elikhbaria.dz

[2] نور اليقين، **شرح برنامج DSploit لاختراق الأجهزة المتصلة بنفس الشبكة**، موقع لوك ويب، بتاريخ 06 مارس 2021، تم الاطلاع عليه يوم 14 أفريل 2026، على الساعة 14:36، على الرابط: https://loqweb.com

[3] الفالح نافل، عبد الكريم العقلة، **جريمة التزوير الالكتروني: دراسة تحليلية مقارنة**، مذكرة ماجستير، كلية الحقوق، جامعة الاسراء بالأردن، سنة 2014، ص51.

[4] القانون رقم 18-05 المؤرخ في 10 ماي 2018، المتعلق بالتجارة الالكترونية، الجريدة الرسمية، العدد 28، الصادر بتاريخ 16 ماي 2018.

ثانيا: الأساس القانوني والإجرائي للمصادرة

ويظهر من خلال:

أ). الأساس القانوني المتكامل

يرتكز الأساس القانوني لمصادرة الأجهزة والبرامج المستخدمة في التزوير الرقمي على مجموعة من النصوص القانونية المتكاملة، في مقدمتها يأتي القانون 18-05 المتعلق بالوقاية من الجرائم المرتبطة بتكنولوجيا المعلومات والاتصالات، والذي حدد بشكل عام الأطر العامة لمكافحة الجرائم الإلكترونية، كما يلعب القانون رقم 15-04 المتعلق بالتوقيع الإلكتروني والشهادات الرقمية دوراً محورياً في تحديد جريمة التزوير الرقمي وآليات مكافحتها[1]، إلى جانب ذلك، يأتي القانون 06-01 المتعلق بالوقاية من الفساد ومكافحته، والذي خصص نصوصاً خاصة بمصادرة الأجهزة والبرامج المستخدمة في الجرائم المرتبطة بالفساد[2]، وأخيراً، يكمل القانون العقوبات الجزائري، وخاصة المادة 374 مكرر، الصورة القانونية بتجريم التزوير المكرر وارتباطه بجرائم أخرى مثل النصب الإلكتروني.

من وجهة نظرنا نرى أن هذا التكامل التشريعي يعكس رؤية استراتيجية في مواجهة الجريمة الرقمية، لكننا نلاحظ وجود تداخل في بعض الأحكام بين النصوص المختلفة، نستحسن أن يتم توحيد النصوص المتعلقة بالمصادرة في نص قانوني واحد متخصص، يجمع بين دقة التحديد وشمولية التغطية، لتفادي أي لبس في التطبيق.

ب) الإجراءات القضائية للمصادرة

تنطلق إجراءات المصادرة في قضايا التزوير الرقمي من لحظة معاينة الموقع الرقمي من قبل قاضي التحقيق، حيث يتم بواسطة الضبط القضائي جمع الأدلة الرقمية الأولية[3]، وتكون المصادرة إلزامية إذا كانت الأجهزة أو البرامج أدوات للجريمة أو أدلة عليها، ويتم حفظها لدى الجهات المختصة حتى صدور الحكم القضائي.

من وجهة نظرنا نعتبر أن الإلزامية في المصادرة تُعد ضمانة ناجعة لعدم تكرار الجريمة، لكننا نرى ضرورة تدعيم الإجراءات بآليات تقنية متخصصة لضمان سلامة الأدلة الرقمية من التلاعب، كما نستحسن

---

[1] القانون رقم 15-04 المؤرخ في 01 فيفري 2015، المتعلق بتحديد القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، الجريدة الرسمية، العدد 06، الصادر بتاريخ 10 فيفري 2015.

[2] المادة 24 مكرر من القانون رقم 06-01 المؤرخ في 20 فيفري 2006، المتعلق بالوقاية من الفساد ومكافحته، موقع الديوان المركزي لقمع الفساد، تم الاطلاع عليه يوم 14 أفريل 2026، على الساعة 14:24، على الرابط: https://ocrc.gov.dz

[3] مريم عيسات، **المرجع السابق**، ص 64.

إنشاء وحدات خاصة ضمن الضبط القضائي تتولى التعامل مع الجرائم الرقمية، نظراً للتخصص العالي الذي تتطلبه هذه الجرائم.

ج). المصادرة كإجراء إثباتي

تُعد المصادرة إجراءً حاسماً في جمع الأدلة الرقمية، إذ تتيح للمحققين الحصول على معلومات قيمة تساعد في كشف تفاصيل الجريمة وتحديد المتورطين[1]، وتكتسب المصادرة أهمية بالغة في ظل الطبيعة الافتراضية للجرائم الرقمية، حيث تُشكل تحدياً كبيراً للجهات التحقيقية والقضائية في إثباتها، إن الأدلة الرقمية التي يتم مصادرتها تتمثل في سجلات النشاط الإلكتروني، الملفات المزورة، البيانات المخزنة على الأجهزة، وحتى التوقيعات الرقمية المشوهة[2].

من وجهة نظرنا نرى أن المصادرة في الجرائم الرقمية تكتسب بعداً إثباتياً يفوق أهميتها كعقوبة، إذ أن الأدلة الرقمية الموجودة في الأجهزة المصادرة تُشكل غالباً الدليل الوحيد على الجريمة، لذا نستحسن أن يصاحب إجراء المصادرة إجراءات تقنية محددة لضمان سلامة البيانات وعدم تلفها، مع مراعاة خصوصية البيانات الشخصية للأطراف غير المتورطين.

ثالثا: العقوبات المترتبة والتحديات التطبيقية

وهي:

أ). العقوبات السالبة للحرية والمالية

تفرض التشريعات الجزائرية عقوبات صارمة على مرتكبي جرائم التزوير الرقمي تهدف إلى تحقيق الردع، فقد تصل عقوبة السجن إلى 5 سنوات في جرائم التزوير الرقمي، وتزداد شدتها إذا ارتبطت الجريمة بالمصادرة، كما تصل الغرامات المالية إلى مبالغ كبيرة تصل إلى ملايين الدنانير الجزائرية، خاصة عند التعامل مع جرائم أخرى مثل الفساد الرقمي أو النصب الإلكتروني[3].

من وجهة نظرنا نعتبر أن العقوبات المقررة تتماشى مع خطورة الجريمة الرقمية في ظل التحول الرقمي الذي تشهده الجزائر، غير أننا نرى أن الغرامات المالية يجب أن تكون متناسبة مع حجم الضرر المادي أو المعنوي الناتج عن الجريمة، مع إمكانية تطبيق عقوبات إضافية مثل الإغلاق الإداري للمنصات الإلكترونية المستخدمة في التزوير.

---

[1] مريم عيسات، **المرجع السابق**، ص 65.

[2] أحمد محمد محروس عبد العال، **المرجع السابق**، ص 55.

[3] القانون رقم 18-05 المؤرخ في 10 ماي 2018، المتعلق بالتجارة الالكترونية، الجريدة الرسمية، العدد 28، الصادر بتاريخ 16 ماي 2018.

ب). البعد الوقائي والعقابي للمصادرة

تُعد المصادرة عقوبة تكميلية ذات أبعاد وقائية وعقابية في آن واحد، فهي تمنع الجناة من استخدام الأدوات ذاتها مرة أخرى في ارتكاب مماثلة، كما تساهم في ردع الآخرين من التفكير في ارتكاب مثل هذه الأفعال[1]، ويسهم تطبيق المصادرة في بناء بيئة رقمية أكثر أماناً وثقة، مما يعزز الرقابة على المستهلكين والتجارة الإلكترونية[2].

من وجهة نظرنا نرى أن البعد الوقائي للمصادرة يكتسب أهمية استراتيجية في الجرائم الرقمية، حيث أن إزالة أدوات الجريمة قد تكون أكثر فعالية من العقوبات السالبة للحرية في بعض الحالات، نستحسن أن تُدرج المصادرة ضمن السياسة الجنائية العامة للدولة في مجال الأمن السيبراني، وأن تُرفق ببرامج توعوية للمستخدمين.

ج). التحديات الرقمية والتشريعية

تواجه المصادرة في جرائم التزوير الرقمي تحديات تقنية وتشريعية متعددة، من بينها التطور المستمر للتكنولوجيا الذي يتطلب مراجعة مستمرة للتشريعات لضمان فعاليتها وديناميكيتها، كما تبرز إشكالية عدم وجود نصوص محددة بالكامل في بعض القوانين، مما يجعل القضاء يعتمد أحياناً على القانون العام للعقوبات لتغطية هذه الجرائمة، إضافة إلى ذلك، تواجه عملية المصادرة تحديات تقنية تتمثل في تشفير البيانات، التخزين السحابي، والحدود الجغرافية الافتراضية[3].

من وجهة نظرنا نعتبر أن أخطر التحديات التي تواجه المصادرة في الجرائم الرقمية هو التخزين السحابي والخوادم الأجنبية، حيث تفقد الدولة السيادة المباشرة على البيانات، نرى ضرورة إبرام اتفاقيات دولية في مجال التعاون القضائي الإلكتروني، مع تطوير القدرات الوطنية في مجال الجرائم الرقمية، كما نستحسن إنشاء سجل وطني للأجهزة والبرامج المصادرة لدراسة أنماط الجريمة الرقمية وتطوير الاستجابة التشريعية.

الفرع الثاني: المنع من الإقامة أو ممارسة النشاط المهني

يُعد التزوير الرقمي من أخطر الجرائم المعاصرة التي تهدد الأمن المعلوماتي والثقة في المعاملات الإلكترونية، إذ يتجاوز مفهومه التقليدي المتمثل في تزوير المستندات الورقية ليشمل التلاعب بالبيانات الرقمية والتوقيعات الإلكترونية والشهادات الرقمية التصديقية[4]، ونظراً للطبيعة التقنية المعقدة لهذه الجريمة، فإن المشرع

---

[1] **عقوبة التصوير في الدوائر الحكومية**، موقع محامي النخبة، تم الاطلاع عليه يوم 14 أفريل 2026، على الساعة 14:55، على الرابط: https://arablawfirm.org

[2] راضية مشري، **المرجع السابق**، ص 60.

[3] غلاب عبد الحق، **المرجع السابق**، ص 497.

[4] معمري ايمان، فضيلة شعبان، **المرجع السابق**، ص20.

الجزائري لم يكتفِ بالعقوبات السالبة للحرية والمالية، بل استحدث عقوبات أصلية متمثلة في "المنع من الإقامة" و"المحكومية" و"المنع من ممارسة النشاط المهني"، وذلك استناداً إلى نص المادة 51 من قانون العقوبات المعدلة بالقانون 09-04[1]، هذه العقوبات تكتسب أهمية بالغة في سياق مكافحة الجرائم الرقمية، إذ تستهدف تجريد المجرم من القدرة على تكرار الجريمة وتحقيق الردع الوقائي بشكل فعال[2].

أولا: ماهية عقوبتي المنع من الإقامة والمنع من ممارسة النشاط المهني

سوف نتطرق لهذا من خلال:

أ). المفهوم القانوني والأساس التشريعي

تنص المادة 51 من قانون العقوبات الجزائري المعدلة بالقانون 09-04 على إمكانية فرض عقوبة "المنع من الإقامة" أو "المحكومية" و"المنع من ممارسة النشاط المهني" كعقوبات أصلية في جرائم التزوير الرقمي، وذلك عندما تكون الجريمة مرتبطة بالمساس بالأمن الوطني أو الاقتصاد الوطني[3]، وتتراوح مدة المنع من الإقامة بين 5 و10 سنوات، وذلك وفقاً للمادة 52 من قانون العقوبات المستندة إلى القانون 09-04[4]، أما المنع من ممارسة النشاط المهني فيُطبق في الحالات التي يرتبط فيها التزوير الرقمي بنشاط تجاري أو مهني، حيث يمكن للمحكمة أن تمنع المدان من ممارسة هذا النشاط لمدة تصل إلى 5 سنوات، ويشمل هذا المنع إغلاق النشاط وإلزامية سحب التراخيص[5].

من وجهة نظرنا نرى أن المشرع الجزائري قد اتبع نهجاً تكاملياً في مواجهة جرائم التزوير الرقمي، إذ لم يقتصر على العقوبات التقليدية بل استحدث عقوبات أصلية تستهدف الجذور الاقتصادية والاجتماعية للجريمة، نعتبر أن هذه العقوبات تكتسب طابعاً وقائياً استباقياً يتجاوز الوظيفة العقابية التقليدية، حيث تمنع المجرم من الاستفادة من البيئة التي مكنته من ارتكاب الجريمة، غير أننا نستحسن أن يكون التحديد أكثر دقة في النصوص

---

[1] **الأحكام الجديدة في قانون مكافحة التزوير واستعمال المزور**، موقع هوريزونز، منشور بتاريخ 30 جوان 2024، تم الاطلاع عليه يوم 14 أفريل 2026، على الساعة: 15:28، على الرابط: https://horizons.dz

[2] **كل الوثائق الادارية قابلة للتزوير في الجزائر**، موقع الشروق أنلاين، منشور بتاريخ 25 سبتمبر 2012، تم الاطلاع عليه يوم 14 أفريل 2026، على الساعة: 15:30، على الرابط: https://echoroukonline.com

[3] **التزوير واستعمال المزور..القوانين المحينة والعقوبات في القانون الجزائري**، منصة اليوتيوب على قناة الشروق نيوز، منشور بتاريخ 10 جويلية 2023، تم الاطلاع عليه يوم 14 أفريل 2026، على الساعة 15:38، على الرابط: https://youtu.be/SW0Wu00MIiY?si=f-wUNMsiAp5yoOxm

[4] **المستشار القانوني يكشف عن الحالات التي يتم فيها تطبيق قانون التزوير التي تصل عقوبته ل30 سنة سجن**، منصة اليوتيوب على قناة الشروق نيوز، منشور بتاريخ 3 جوان 2025، تم الاطلاع عليه يوم 14 أفريل 2026، على الساعة 15:42، على الرابط: https://youtu.be/U7mjzYzo1Pw?si=Hd3soooE-krl12-f

[5] **معلومة قانونية: عقوبة التزوير أو التحريف في وثائق الحالة المدنية**، منصة اليوتيوب على قناة النهار tv ، منشور بتاريخ 16 جوان 2025، تم الاطلاع عليه يوم 14 أفريل 2026، على الساعة 15:48، على الرابط: https://youtu.be/uAlPN5_sBwA?si=m89ts0tLgvel8uWK

القانونية، مع تحديد معايير واضحة لتحديد متى تكون الجريمة "مرتبطة بالأمن الوطني أو الاقتصاد الوطني" لتفادي التوسع التفسيري.

ب). شروط تطبيق العقوبات الأصلية

تتطلب تطبيق عقوبتي المنع من الإقامة والمنع من ممارسة النشاط المهني شروطاً محددة يجب توفرها، ففيما يخص المنع من الإقامة، يشترط أن يكون المدان أجنبياً أو أن تكون الجريمة مرتبطة بالمساس بالأمن الوطني، كما هو الحال في تزوير وثائق الهجرة أو المصارف ذات الأهمية القومية[1]، أما فيما يخص المنع من ممارسة النشاط المهني، فيشترط أن يرتبط التزوير الرقمي بنشاط تجاري أو مهني، كتزوير البيانات الإلكترونية في العقود التجارية أو السجلات التجارية الرقمية[2]، وقد نصت المادة 10 من القانون 08-04 المتعلق بالشروط التي يمارس فيها التجار نشاطهم على إمكانية وصول العقوبة إلى 5 سنوات حبس في حالة التزوير في السجلات التجارية الرقمية[3].

من وجهة نظرنا نلاحظ أن المشرع الجزائري قد أدرك ضرورة ربط العقوبة بالسياق الاقتصادي والاجتماعي للجريمة، نرى أن هذه الشروط تضمن عدم التوسع في تطبيق العقوبات، لكننا نعتقد أنها قد تكون محدودة في ظل التحول الرقمي المتسارع. فالعديد من جرائم التزوير الرقمي تتم عبر المنصات الإلكترونية دون امتلاك "نشاط مهني" تقليدي، مما قد يخلق ثغرة قانونية، نستحسن توسيع نطاق التطبيق ليشمل الأنشطة الإلكترونية غير التقليدية، مثل التجارة الإلكترونية والعمل عبر المنصات الرقمية.

ج). الآثار القانونية والاجتماعية للعقوبات

تترتب على عقوبتي المنع من الإقامة والمنع من ممارسة النشاط المهني آثار قانونية واجتماعية عميقة، فالمنع من الإقامة يؤدي إلى طرد المدان الأجنبي من التراب الجزائري ومنعه من العودة إليه، مما يحقق وظيفة الردع الخاص والعام في آن واحد[4]، أما المنع من ممارسة النشاط المهني فيؤدي إلى إغلاق المنشأة التجارية

---

[1] **تساؤلات: قانون مكافحة التزوير واستعمال المزور.. هذه هي التفاصيل**، منصة اليوتيوب على قناة النهار tv ، منشور بتاريخ 20 ماي 2024، تم الاطلاع عليه يوم 14 أفريل 2026، على الساعة 15:50، على الرابط: https://youtu.be/Y5kjKn9r1ys?si=Is0LiqFMMu4oysT6

[2] ديابي زينب، **جرائم التزوير واستعمال المزور في التشريع الجزائري**، مذكرة ماستر تخصص قانون خاص، معهد الحقوق، المركز الجامعي مغنية، السنة الجامعية 2024/2023، ص 32.

[3] هشام بن سليمان، **تزوير المحررات الرسمية في القانون الجزائري**، مذكرة ماستر تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس مستغانم، السنة الجامعية 2024/2023، ص 50.

[4] زعيون عبد الوهاب، بشكيط يوسف، **المرجع السابق**، ص 56.

وإلزامية سحب التراخيص، مما يؤثر على المستوى الاقتصادي للمدان ويمنعه من الاستفادة من البنية التحتية التي استخدمها في ارتكاب الجريمة[1].

من وجهة نظرنا نعتبر أن هذه العقوبات تكتسب أهمية استراتيجية في السياسة الجنائية الجزائرية، إذ أنها لا تستهدف فقط الفرد المجرم بل البيئة المحيطة به، نرى أن إغلاق النشاط وإلزامية سحب التراخيص يمثلان إجراءً وقائياً فعالاً في مواجهة الجرائم الاقتصادية المنظمة، لكننا نستحسن أن يصاحب هذه العقوبات إجراءات تأهيلية وإعادة إدماج، خاصة في الحالات التي لا تكون فيها الجريمة مرتبطة بالأمن القومي، لضمان عدم إقصاء المدان بشكل دائم من المجتمع.

الفرع الثالث: غلق المواقع الإلكترونية أو المنصات الرقمية محل الجريمة.

إن مكافحة الجريمة الإلكترونية في التشريع الجزائري الحديث قد اقتضت إقرار آليات استباقية ورادعة تستهدف الوسيلة التي تمارس من خلالها الجريمة، لا سيما في ظل تنامي استخدام المواقع الإلكترونية والمنصات الرقمية كأدوات للتزوير والنصب والاحتيال، وقد أولى المشرع اهتماماً خاصاً بمسألة غلق هذه المواقع اعتباراً من كونها تمثل حالة استمرارية للجرم الإلكتروني، مما يتطلب تدخلاً سريعاً وفعالاً لوقف آثارها الضارة، وفي هذا الإطار، يقتضي التحليل المنهجي لهذا الموضوع الوقوف على الأسس القانونية التي يستند إليها الغلق، والشروط والإجراءات المقررة، وذلك في أفق تقييم مدى فعالية هذه الآلية في تحقيق الأمن السيبراني.

أولاً: الإطار القانوني وطبيعة غلق المواقع الإلكترونية محل الجريمة

يستند غلق المواقع الإلكترونية أو المنصات الرقمية محل الجريمة إلى نصوص قانون24-02 المتعلق بمكافحة الجرائم الإلكترونية، والذي يخول للقاضي أو المحكمة المختصة إصدار أمر بإغلاق فوري لأي موقع إلكتروني أو منصة رقمية تُستخدم في ارتكاب جريمة التزوير الرقمي، وذلك بالتعاون مع هيئة البريد والمواصلات الإلكترونية (ARPCE) وهيئة تنظيم الإنترنت في الجزائر[2]، وقد جاء هذا النص تأكيداً لأهمية التدخل القضائي السريع لوقف الجريمة الإلكترونية في حال استمراريتها، حيث يُعتبر الغلق تدبيراً احتياطياً أو عقابياً يهدف إلى قطع الطريق على مرتكبي الجرائم الرقمية.

كما يتضح من وثائق التشريع الجزائري أن المشرع قد ميّز بين نوعين من العقوبات المترتبة على جرائم التزوير الرقمي: العقوبات السالبة للحرية والعقوبات المالية، إلا أنه أضاف عقوبة مغلقة تتمثل في "حظر

[1] عمارة فتيحة، **المرجع السابق**، ص 181.

[2] القانون رقم 24-02 المؤرخ في 26 فيفري 2024، المتعلق بمكافحة التزوير واستعمال المزور، الجريدة الرسمية، العدد 15، الصادر بتاريخ 29 فيفري 2024.

الوصول إلى المنصات الرقمية" أو إغلاقها نهائياً في حالات معينة [1]، وقد عزز قانون 24-02 هذا التوجه من خلال إقرار آليات تقنية وقانونية تتيح للسلطات المختصة إصدار أوامر إغلاق فورية للمواقع والمنصات المتورطة في أنشطة التزوير الرقمي [2].

يمكن القول إن الغلق المقرر في إطار مكافحة التزوير الرقمي يكتسب طابعاً قضائياً فورياً، يختلف عن الغلق الإداري الذي قد تقوم به السلطات الإدارية بناءً على تعليمات أو قرارات وزارية، فالغلق القضائي يستند إلى أمر قضائي صادر عن قاضي التحقيق أو قاضي الأمور المستعجلة، ويتم تنفيذه عبر الـ ARPCE التي تتولى التنسيق مع مزودي خدمات الإنترنت لحجب الموقع المخالف [3]، وقد نصت المادة 381 من قانون الإجراءات الجزائية على وجوب إصدار الأمر بإغلاق المنصات الرقمية التي تُستخدم في ارتكاب جرائم التزوير، مع تحديد الآليات الفنية للتنفيذ.

ثانياً: شروط وإجراءات غلق المواقع الإلكترونية

يُشترط لصحة أمر الغلق القضائي للمواقع الإلكترونية أن تتوافر مجموعة من العناصر الموضوعية والشكلية. من الناحية الموضوعية، يجب أن يثبت استخدام الموقع أو المنصة في ارتكاب جريمة التزوير الرقمي، سواء كان ذلك بإنشاء مواقع ويب وهمية أو توزيع وثائق إلكترونية مزيفة أو بيانات إلكترونية مزيفة تستهدف الضرر بالغير[4]، أما من الناحية الشكلية، فيجب أن يصدر الأمر من السلطة القضائية المختصة، وأن يكون مسبباً ومحدداً في ذاته، مع تحديد هوية الموقع وعنوانه الإلكتروني (URL) بوضوح تام، وذلك احتراماً لمبدأ الشرعية الجنائية والاختصاص القضائي.

تتولى هيئة البريد والمواصلات الإلكترونية (ARPCE) تنفيذ قرارات الغلق القضائية بالتنسيق مع مزودي خدمات الإنترنت(ISP) ، حيث يتم حجب الوصول إلى الموقع على مستوى الخوادم الوطنيةDNS Blocking))، وقد نصت التشريعات الجزائرية على أن الغلاق يطال المواقع المتورطة في التزوير الرقمي والمنصات

[1] أبو بكر التيتاوي، الياس مالك قرادي، **جرائم النصب والاحتيال الالكتروني في التشريع الجزائري**، مذكرة ماستر تخصص القانون الجنائي والعلوم الجنائية، معهد الحقوق، المركز الجامعي المقاوم الشيخ امود بن مختار ايليزي، السنة الجامعية 2025/2024، ص 36.

[2] عزة خولة ، ربيع شيماء، **المرجع السابق**، ص 33.

[3] عيمور راضية، **الجريمة الالكترونية واليات مكافحتها في التشريع الجزائري**، المجلة الأكاديمية للبحوث القانونية والسياسية، جامعة عمار ثليجي الأغواط، المجلد 06، العدد 01، منشور بتاريخ 31 مارس 2022، ص 95.

[4] سلاوي مارية، يوسفي عفاف، **أحكام الجرائم السيبرانية في التشريع الجزائري**، مذكرة ماستر تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة 1، السنة الجامعية 2025/2024، ص 46.

المستخدمة لنشر محتوى مزور أو احتيالي [1]، وفي حالات التهديد الخطير للأمن السيبراني، يمكن أن يتم إغلاق المواقع الحساسة التي تتجاوز حدود 500 ألف دينار جزائري في حالات الغش التجاري عبر الإنترنت، وذلك لمدة تتراوح بين 12 شهراً إلى 3 سنوات في حالات تزوير الشهادات أو تزوير النقود أو الأختام الرسمية الرقمية [2].

من خلال استقراء النصوص القانونية والممارسات القضائية، يتبين أن آلية غلق المواقع الإلكترونية محل الجريمة تُعدّ إجراءً رادعاً واستباقياً يسهم في قطع الطريق على استمرار الجريمة الإلكترونية، إلا أن هذا الإجراء يطرح إشكاليات عملية تتعلق بمدى فعاليته في ظل وجود تقنيات الـ VPN والبروكسي التي تمكن المخالفين من تجاوز الحجب [3]، كما أن سرعة تطور التقنيات الرقمية تجعل من الصعب على المشرع مواكبة أشكال التزوير الجديدة، مما يقتضي مراجعة مستمرة للإطار القانوني.

يقتضي الأمر، في ظل هذه الإشكاليات، ضرورة تطوير الإطار القانوني لغلق المواقع بما يضمن سرعة التنفيذ وشمولية الحماية، فالغلق يجب ألا يقتصر على المستوى الوطني فحسب، بل يتطلب التعاون الدولي في مجال مكافحة الجرائم السيبرانية، خاصة وأن الجرائم الإلكترونية تتجاوز الحدود الإقليمية ، كما يُقترح إنشاء وحدات خاصة داخل الـ ARPCE مكلفة بمراقبة المنصات الرقمية بشكل استباقي، وليس فقط رد الفعل بعد وقوع الجريمة، مع تعزيز التعاون الدولي لتبادل المعلومات والخبرات مع الدول الأخرى في مجال مكافحة الجرائم الإلكترونية [4].

ختاماً، يمكن القول إن غلق المواقع الإلكترونية محل الجريمة يُمثّل آلية قانونية ضرورية لكنها غير كافية وحدها، ويجب أن ترافقها تدابير وقائية وتربوية تهدف إلى الحد من ظاهرة التزوير الرقمي من جذورها، مع ضمان احترام الحريات الأساسية وحقوق الإنسان في الفضاء الرقمي، وعدم استخدام هذه الآلية كوسيلة للتضييق على حرية التعبير.

---

[1] **حظر العملات الرقمية وتجميد الاصول..الجزائر تشدد قبضتها على المال غير المشروع**، موقع تدامسا نيوز، منشور بتاريخ 28 جويلية 2025، تم الاطلاع عليه يوم 14 أفريل 2026، على الساعة 17:02، على الرابط: https://tadamsanews.dz

[2] **الجزائر تراهن على الأقمار الصناعية لضمان استمرارية الانترنت**، موقع العربي الجديد، منشور بتاريخ 10 فريل 2026، تم الاطلاع عليه يوم 14 أفريل 2026، على الساعة 17:05، على الرابط: https://www.aajae.co/entertainment_media

[3] **The legality of accessing blocked websites and using web proxy servers**, Site web Masaar, Publié le 7 mars 2021, Consulté le 14 avril 2026, à 17:12, Sur le lien: https://masaar.net

[4] ايمان مكري، **الجريمة الالكترونية في التشريع الجزائري**، مذكرة ماجستير تخصص تشريعات اعلامية، كلية الاعلام والاتصال، جامعة الجزائر 3، السنة الجامعية 2015/2014، ص 224.

خلاصة الفصل الأول

يتضح من دراسة هذا الفصل أن التزوير الرقمي يمثل استحداثاً إجرامياً خطيراً يستهدف النزاهة والثقة في النظام المعلوماتي، ويختلف جوهرياً عن نظيره التقليدي في المحررات الورقية، سواء من حيث الوسيلة المستخدمة أو سرعة الانتشار أو خفاء الفاعل، وقد استطاع المشرع الجزائري – من خلال القانون رقم 09-08 المتعلق بالجريمة المعلوماتية والقانون رقم 15-04 المنظم للمحرر الإلكتروني – أن يؤسس لنظام قانوني يعترف بالقيمة القانونية للمعطيات الرقمية والتوقيع الإلكتروني، ويوفر الحماية الجنائية اللازمة لها ضد أشكال التلاعب والتزييف.

وفيما يخص المبحث الأول، تبين أن محل جريمة التزوير الرقمي يتمثل في المحرر الإلكتروني بما يحمله من بيانات ومعطيات ذات حجية قانونية، وأن التوقيع الإلكتروني يشكل هدفاً رئيسياً لعمليات التزوير نظراً لدوره في إثبات هوية صاحب المحرر واعترافه بمضمونه، كما تنوعت صور هذه الجريمة في الواقع العملي بين تزوير البيانات المخزنة، والتلاعب بالمواقع والبريد الإلكتروني، واستنساخ أو تزييف البطاقات البنكية ووسائل الدفع الإلكتروني.

أما المبحث الثاني، فقد أوضح أن جريمة التزوير الرقمي تتركب – كسائر الجرائم – من أركان ثلاثة: ركن مفترض يتمثل في النظام المعلوماتي والبيانات الرقمية ذات القيمة القانونية والمصلحة المحمية؛ وركن مادي يتجسد في السلوك الإجرامي القائم على تغيير الحقيقة بالوسيلة الرقمية مع تحقق النتيجة الإجرامية المتمثلة في احتمال وقوع الضرر، وتربط بينهما علاقة سببية تتسم بخصوصية تفرضها طبيعة الوسيلة الإلكترونية؛ وركن معنوي يقتضي توافر القصد الجنائي العام (العلم والإرادة) إلى جانب قصد خاص يتمثل في نية استعمال المحرر المزور، مع ما يطره الأمر من إشكالية في تحديد وقت توافر هذا الركن في الجرائم العابرة للحدود.

وفي المبحث الثالث، اتضح أن المشرع الجزائري أقر نظاماً عقابياً متدرجاً يتناسب مع خطورة الجريمة وصفة فاعلها، حيث نص على عقوبات أصلية مشددة تطبق على الشخص الطبيعي والمعنوي على السواء، مع مراعاة حالات الشروع والمشاركة، كما أجاز تشديد العقوبة في حالات خاصة كالمساس بمؤسسات الدولة أو ارتكاب الجريمة من قبل موظف عمومي أو متخصص في المعلوماتية، دون إغفال الأعذار المعفية أو المخففة، فضلاً عن ذلك أقر تدابير تكميلية وأمنية – كمصادرة الأدوات المستخدمة ومنع ممارسة النشاط وغلق المواقع الإلكترونية – تهدف إلى تجفيف منابع الجريمة وحماية النظام الرقمي من الاستغلال الإجرامي.

ويمكن الاستنتاج من هذا الفصل بأجمعه أن النجاعة في مكافحة التزوير الرقمي تقتضي فهماً دقيقاً للبنية القانونية لهذه الجريمة وتمييزها عن الجرائم الإلكترونية المجاورة، وأن التطور التكنولوجي المستمر يفرض على

المشرع مواكبة دائمة لتجاوز الثغرات النصية وضمان حماية فعالة للمحرر الإلكتروني كبديل شرعي للمحرر الورقي في التعاملات القانونية.

الفصل الثاني

مظاهر الحماية القانونية من جرائم التزوير الرقمي في التشريع الجزائري

إذا كان الفصل الأول قد خصص لدراسة البنية القانونية لجريمة التزوير الرقمي وعناصرها العقابية، فإن معرفة هذه الأركان وحدها لا تكفي لضمان فعالية المكافحة، إذ إن النص الجنائي – مهما بلغت دقته – يظل حبراً على ورق ما لم تتوفر الآليات الإجرائية والمؤسساتية القادرة على تفعيله على أرض الواقع. فالخصوصية التي تكتسيها الجريمة المعلوماتية، من حيث خفاء الفاعل، وسرعة ارتكابها، وانتقالها عبر الحدود الجغرافية، وطبيعة الأدلة الرقمية القابلة للتلف أو التغيير، تجعل من إجراءات البحث والتحري والإثبات فيها تحدياً غير مسبوق للأنظمة القانونية التقليدية.

وفي هذا السياق، يكتسي الفصل الثاني أهمية حاسمة، إذ ينتقل بالبحث من المستوى النظري إلى المستوى التطبيقي، ليركز على كيفية كشف هذه الجريمة وإثباتها وملاحقة مرتكبيها في ظل النظام القانوني الجزائري، فالتحقيق في جرائم التزوير الرقمي يتطلب أساليب تقنية خاصة تختلف جوهرياً عن تلك المستخدمة في الجرائم التقليدية، بدءاً من المعاينة والتفتيش الإلكتروني، مروراً بضبط البيانات الرقمية وحفظها وفق قواعد فنية دقيقة تضمن سلامتها وعدم تلاعبها، وانتهاءً بالاستعانة بالخبرة المعلوماتية التي أضحت ضرورة حتمية لفك شفرات الأدلة الرقمية وكشف آثار التزوير.

كما أن الإثبات في هذه الجرائم يطرح إشكاليات جوهرية تتعلق بحجية الدليل الرقمي وموثوقيته خاصة وأن المحرر الإلكتروني ذاته قد يكون محلاً للتزوير، مما يستدعي تطوير معايير قانونية وفنية تضمن نزاهة المستخرجات الرقمية وقابليتها للاعتماد أمام القضاء، ولا يقتصر الأمر على الجانب الإجرائي المحلي بل يمتد ليشمل الاختصاص القضائي في جرائم ترتكب عبر الشبكات العنكبوتية، حيث تبرز صعوبات في تحديد مكان الوقائع وتنازع الاختصاص بين المحاكم فضلاً عن ضرورة التعاون الدولي في ظل طبيعة هذه الجرائم العابرة للحدود.

من جهة أخرى، لم يعد بمقدور الدولة وحدها مواجهة هذا النوع من الجريمة، إذ أضحى القطاع الخاص – وخاصة مقدمو خدمات الإنترنت والمؤسسات المالية – شريكاً لا غنى عنه في الكشف عن التزوير وحماية البيانات. وفي المقابل، تبرز الحاجة إلى هيئات وطنية متخصصة تمتلك الكفاءة التقنية والقانونية اللازمة لمكافحة الجرائم المعلوماتية، وتنسيق الجهود بين الأجهزة الأمنية والقضائية والهيئات الرقابية.

من هذا المنطلق، يهدف هذا الفصل إلى دراسة الآليات الإجرائية والمؤسساتية التي يعتمد عليها النظام القانوني الجزائري في مكافحة التزوير الرقمي، من خلال تفحص إجراءات البحث والتحري الخاصة، وقواعد إثبات الجريمة أمام القضاء، والهيئات المكلفة بمكافحتها على المستوى الوطني والدولي.

المبحث الأول: اجراءات البحث والتحري في جرائم التزوير الرقمي

لقد شهد العقدان الأخيران تحولًا جذريًا في طبيعة الجريمة وأساليب ارتكابها، إذ أصبح الفضاء الرقمي مسرحًا جديدًا للنشاط الإجرامي يتجاوز في خطورته الحدود التقليدية للجريمة المادية، وفي هذا السياق، برزت جرائم التزوير الرقمي كإحدى أخطر صور الاعتداء على النظام المعلوماتي، ذلك أنها تمسُّ جوهر الثقة في المعاملات الإلكترونية والوثائق الرقمية التي أصبحت تمثل الشريان الحيوي للاقتصاد الرقمي والإدارة الإلكترونية الحديثة[1]، وقد تم التعبير عن طبيعة هذه الجريمة بكونها "من أخطر صور الغش المعلوماتي في المجال التكنولوجي، نظرًا للدور الهام الذي أصبح يقوم به جهاز الحاسوب كونه اقتحم كافة المجالات"[2].

وإدراكًا من المشرع الجزائري لخطورة هذا النوع الجديد من الإجرام، سعى إلى وضع إطار قانوني متكامل يُجسِّد التوازن المطلوب بين ضرورة مكافحة الجريمة الرقمية وحماية الحقوق والحريات الفردية[3]، وفي هذا الإطار، انتهج المشرع سياسة جنائية مزدوجة تتمثل في تعديل النصوص الجنائية العامة من جهة واستحداث قواعد إجرائية خاصة من جهة أخرى، فقد أدخل تعديلات جوهرية على قانون العقوبات بموجب القانون رقم 24-06 المؤرخ في 28 أفريل 2024 المتضمن قانون العقوبات الجزائري، ثم قانون الإجراءات الجزائية بموجب القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المتضمن قانون الاجراءات الجزائية، قبل أن يستكمل هذا المسعى بإصدار القانون رقم 09-04 المؤرخ في 14 شعبان 1430 الموافق 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[4].

ويمثل القانون 09-04 نقلة نوعية في المنظومة القانونية الجزائرية، إذ أرسى قواعد إجرائية جديدة تضمن تحكمًا رشيدًا في أساليب مكافحة الجريمة المعلوماتية بما يتوافق وخصائصها الفريدة[5]، وقد أجمع الباحثون على أن هذا القانون "قام بإرساء قواعد إجرائية جديدة تضمن تحكمًا جيدًا في أساليب مكافحة هذا النوع الجديد من الإجرام"[6]، غير أن هذه الأساليب الحديثة للتحري، كالمراقبة الإلكترونية وتفتيش الأنظمة المعلوماتية، أثارت

---

[1] عمار فتيحة، **المرجع السابق**، ص 166.

[2] عمار فتيحة، **المرجع السابق**، ص 167.

[3] أحمد مسعود مريم، قريشي محمد، **اليات مكافحة جرائم تكنولوجيات الاعلام والاتصال في ضوء القانون رقم 04/09**، مذكرة ماجستير تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح ورقلة، السنة الجامعية 2013/2012، ص 11.

[4] القانون رقم 09-04 المؤرخ في 5 أوت 2009، المتعلق بالوقاية من الجرائم المرتبطة بتكنولوجيات الاعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47، الصادر بتاريخ 16 أوت 2009.

[5] حشمان عمار، **المرجع السابق**، ص45.

[6] أحمد مسعود مريم، قريشي محمد، **المرجع السابق**، ص 12.

إشكالية جوهرية تتمثل في مدى مشروعيتها ومدى توافقها مع الحقوق والحريات الأساسية للفرد، خاصة وأنها "تمس بالحقوق والحريات الأساسية للفرد والمعترف بها في الاتفاقيات الدولية"[1].

ولعل من أبرز المستجدات التي جاء بها القانون 09-04 إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بموجب المادة 13، والتي تُعدُّ "أهم الآليات المستحدثة" في مجال مكافحة الجريمة الإلكترونية[2]، وقد كُلِّفت هذه الهيئة بمهام وقائية وقمعية متعددة، تتجاوز مجرد المساعدة التقنية للسلطات القضائية لتشمل "تجميع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية"[3].

ومع ذلك، يظل التحدي الأكبر يتمثل في كيفية تكييف الإجراءات الجنائية التقليدية – التي نشأت في عصر المحررات الورقية والمادية – مع خصوصية الأدلة الرقمية التي تتسم بالطابع غير المادي، والقابلية للتغيير، والانتشار عبر الحدود الإقليمية[4]، فالأدلة الرقمية في جرائم التزوير "تطرح العديد من المشاكل من ناحية القانون الإجرائي، إذ يصعب على المحققين إجراء تحقيق وجمع الأدلة الرقمية بإتباع الإجراءات التقليدية للتحقيق: كالمعاينة، التفتيش، الضبط"[5].

ومن هنا تبرز أهمية هذا المبحث الذي يتناول بالدراسة والتحليل إجراءات البحث والتحري في جرائم التزوير الرقمي على النحو الذي رتبه المشرع الجزائري في القانون 09-04 وما تضمنته من آليات استحداثية، وقد قسّمنا هذا المبحث إلى ثلاثة مطالب رئيسة:

المطلب الأول يتناول التفتيش الإلكتروني، ويبحث في خصوصية تفتيش الأنظمة المعلوماتية وشروطه وضوابطه القانونية، فضلًا عن حماية الخصوصية أثناء إجراءات البحث، المطلب الثاني يركِّز على ضبط البيانات الرقمية وحفظها، من خلال استعراض طرق ضبط الوسائط الإلكترونية وتأمينها، والقواعد الفنية لضمان عدم تغيير البيانات المضبوطة، فضلًا عن إجراءات التحريز الرقمي (Hash Value) التي تُعدُّ الضمانة التقنية الأساسية لسلامة الأدلة الرقمية، وأخيرا المطلب الثالث يُخصَّص للأساليب التحقيقية الخاصة، ويتناول اعتراض

[1] حشمان عمار، **المرجع السابق**، ص48.

[2] أحمد مسعود مريم، قريشي محمد، **المرجع السابق**، ص 15.

[3] حشمان عمار، **المرجع السابق**، ص50.

[4] حشمان عمار، **المرجع السابق**، ص 52.

[5] القانون رقم 09-04 المؤرخ في 5 أوت 2009، المتعلق بالوقاية من الجرائم المرتبطة بتكنولوجيات الاعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47، الصادر بتاريخ 16 أوت 2009.

المراسلات الإلكترونية وتسجيلها، والمراقبة الإلكترونية والولوج إلى الأنظمة، فضلًا عن التسرب الإلكتروني كآلية حديثة لكشف المزورين.

المطلب الأول: التفتيش الالكتروني

بعد التفتيش الإلكتروني من أولى وأهم إجراءات البحث والتحري في جرائم التزوير الرقمي، إذ تمسُّ مباشرةً جوهر الأدلة الرقمية التي تختلف جوهريًا عن الأدلة المادية التقليدية، وقد اقتضت طبيعة الجريمة المعلوماتية – التي تُرتَكَب في فضاء افتراضي غير محسوس – استحداث قواعد إجرائية خاصة تُجيب على إشكالية كيفية تفتيش الأنظمة المعلوماتية والولوج إليها، سواء كان ذلك بشكل مباشر أو عن بُعد[1].

ولقد نصَّ القانون رقم 09-04 في المادة 5 على إمكانية "الدخول، بغرض التفتيش، ولو عن بعد، إلى منظومة معلوماتية أو جزء منها"[2]، مما يُجسِّد إقرار المشرع الجزائري بخصوصية هذا النوع من التفتيش الذي يتجاوز حدود المكان المادي التقليدي، غير أن هذا التوسع في سلطات التفتيش يستدعي ضرورة التوفيق بين فعالية التحري وحماية الحقوق الدستورية، خاصةً حق الخصوصية وحماية المعطيات الشخصية[3].

الفرع الأول: خصوصية تفتيش الأنظمة المعلوماتية

يُعدّ تفتيش الأنظمة المعلوماتية إجراءً تحقيقيًا استثنائيًا يتجاوز حدود التفتيش التقليدي، إذ يمتد إلى فضاء افتراضي غير مرئي، ولقد نصّ القانون رقم 09-04 في المادة 5 على إمكانية "الدخول، بغرض التفتيش، ولو عن بعد، إلى منظومة معلوماتية"[4]، ويتطلب هذا التوسع دراسة دقيقة لطبيعته وضوابطه.

أولاً: ماهية التفتيش الإلكتروني

يُعرّف التفتيش الإلكتروني في المادة 5 من القانون 09-04 بأنه "الدخول، بغرض التفتيش، ولو عن بعد، إلى منظومة معلوماتية أو جزء منها"[5]، وهذا التعريف يتضمن عنصرين جوهريين يُميّزانه عن التفتيش التقليدي، أما العنصر الأول فيتمثل في عنصر المسافة، إذ يتيح التفتيش الإلكتروني للسلطات المكلفة بالتفتيش الولوج إلى النظام المعلوماتي دون الحاجة إلى الحضور المادي إلى مكان الجريمة، فقد نصّت المادة 5 صراحةً على جواز

---

[1] عمار حشمان، **المرجع السابق**، ص52.

[2] المادة 5 من القانون رقم 09-04 المؤرخ في 5 أوت 2009، المتعلق بالوقاية من الجرائم المرتبطة بتكنولوجيات الاعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47، الصادر بتاريخ 16 أوت 2009.

[3] أحمد مسعود مريم، قريشي محمد، **المرجع السابق**، ص 18.

[4] المادة 5 من القانون رقم 09-04 المؤرخ في 5 أوت 2009، المتعلق بالوقاية من الجرائم المرتبطة بتكنولوجيات الاعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47، الصادر بتاريخ 16 أوت 2009.

[5] المادة 5 من القانون رقم 09-04 المؤرخ في 5 أوت 2009، المتعلق بالوقاية من الجرائم المرتبطة بتكنولوجيات الاعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47، الصادر بتاريخ 16 أوت 2009.

التفتيش "عن بعد"[1]، مما يُمكّن من تفتيش أنظمة موجودة في أقاليم جغرافية بعيدة أو حتى خارج التراب الوطني، وهذا التوسع يُشكّل تحولاً نوعيًا في فلسفة التفتيش الجنائي التي كانت تقتصر تقليديًا على المكان المادي للجريمة، غير أن هذا العنصر يثير إشكالية قانونية تتعلق بتحديد الاختصاص القضائي والأمني، فالتفتيش عن بُعد قد يمسّ بأنظمة معلوماتية موجودة في دول أخرى، مما يستدعي "أهمية التعاون الدولي" و"اتفاقية بودابست" للتعاون في مجال الجرائم الإلكترونية[2].

أما العنصر الثاني فيتمثل في عنصر الجزئية، إذ يمكن الاقتصار في التفتيش الإلكتروني على "جزء من" المنظومة المعلوماتية لا النظام بأكمله، وهذا يعني إمكانية تفتيش ملف معين أو قاعدة بيانات محددة أو حساب بريد إلكتروني واحد، دون الولوج إلى بقية البيانات المخزنة في النظام، وتكتسب هذه الجزئية أهمية بالغة في حماية الخصوصية، إذ تضمن عدم تجاوز التفتيش الحدود الضرورية لجمع الأدلة، فالمادة 5 تُشترط أن يكون التفتيش "مبررًا وضروريًا لجمع الأدلة"[3]، وهو ما يُجسّد مبدأ الضرورة والتناسب.

ثانياً: التمييز بين التفتيش الإلكتروني والتفتيش التقليدي

يمكن التمييز بين النوعين من التفتيش من خلال جملة من المحاور: فمن حيث الموضوع، يكمن التمييز الجوهري في طبيعة موضوع التفتيش، ففي حين يقتصر التفتيش التقليدي على "الأشياء المادية المحسوسة" كالأوراق والمحررات والأدوات المادية، يمتد التفتيش الإلكتروني ليشمل البيانات والمعلومات الرقمية المخزنة أو المعالجة أو المرسلة[4]، وهذه البيانات غير مادية بطبيعتها، قابلة للتكرار والنقل الفوري، ويمكن تعديلها أو حذفها بسهولة. ولقد نصّت المادة 9 من القانون 09-04 على إمكانية "حجز أو نسخ البيانات والمعلومات الرقمية"[5]، مما يكشف عن طبيعة مزدوجة للموضوع: الوسيط المادي (الحاسوب، الهاتف، الخادم) والمحتوى غير المادي (البيانات، الملفات، الرسائل).

---

[1] المادة 5 من القانون رقم 09-04 المؤرخ في 5 أوت 2009، المتعلق بالوقاية من الجرائم المرتبطة بتكنولوجيات الاعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47، الصادر بتاريخ 16 أوت 2009.

[2] **قانون مكافحة التزوير واستعمال المزور يصدر في الجريدة الرسمية**، موقع الشروق أونلاين، منشور بتاريخ 12 مارس 2024، تم الاطلاع عليه يوم 17 أفريل 2026، على الساعة 15:14، على الرابط: https://www.echoroukonline.com

[3] عمار حشمان، **المرجع السابق**، ص51.

[4] شعباني نوال، **مظاهر تفعيل قواعد مكافحة جرائم التزوير المقررة بموجب القانون رقم 24-02 المتعلق بمكافحة التزوير واستعمال المزور**، المجلة النقدية للقانون والعلوم السياسية، جامعة مولود معمري تيزي وزو، المجلد 20، العدد 01، منشور بتاريخ 30 جوان 2025، ص 597.

[5] زعيون عبد الوهاب، بشكيط يوسف، **المرجع السابق**، ص 38.

ومن حيث المكان، يظل التفتيش التقليدي مقرونًا بمكان محدد يُحدّد في أمر التفتيش، ويُمنع تجاوزه، أما التفتيش الإلكتروني فيتجاوز هذا القيد، إذ يمكن الولوج عن بُعد إلى أنظمة في أماكن متفرقة جغرافيًا، وقد لاحظ الباحثون أن "التحقيق في الجرائم الإلكترونية يصعب إجراؤه باتباع الإجراءات التقليدية"[1] نظرًا لهذه الخصوصية. ومن حيث الزمان، يتيح التفتيش الإلكتروني التفتيش الفوري والمستمر، فالمادة 4 من القانون 09-04 تجيز "إجراء عمليات مراقبة للاتصالات الإلكترونية وجمع وتسجيل محتواها بشكل فوري"[2]، وهذا يعني إمكانية التسجيل الآني للبيانات أثناء إرسالها أو استقبالها، وهو ما يختلف عن التفتيش التقليدي الذي يتم في لحظة محددة.

أما من حيث الضمانات، فيتطلب التفتيش الإلكتروني ضمانات تقنية إضافية لا تتوفر في التفتيش التقليدي، فضبط الأدلة الرقمية يقتضي "إجراءات تحقيقية خاصة" تضمن سلامتها[3]، كما يجب "الحفاظ على سرية البيانات غير المتعلقة بالجريمة"[4]، وهو ما يستدعي تقنيات فلترة وتصنيف للبيانات.

الفرع الثاني: شروط وضوابط التفتيش الالكتروني في القانون الجزائري

إذا كان التفتيش الإلكتروني يمثل إجراءً تحقيقيًا استثنائيًا يتجاوز حدود التفتيش التقليدي، فإن هذا التجاوز يستوجب بالضرورة إقرار ضمانات قانونية رصينة تضمن عدم الإخلال بالحقوق الدستورية للأفراد، ولقد سعى المشرع الجزائري إلى تحقيق هذا التوازن من خلال نصوص موزعة بين القانون 09-04 المتخصص والقانون 06-22 المعدل والمتمم لقانون الإجراءات الجزائية، مما يشكل منظومة متكاملة من الشروط والضوابط التي نتناولها في هذا الفرع.

أولا: الشروط الموضوعية والشكلية للتفتيش الإلكتروني

وهي:

أ). الشروط الموضوعية

يستند التفتيش الإلكتروني في قانونه الجزائري إلى مجموعة من الشروط الموضوعية التي تضمن شرعيته وفعاليته معاً، فأولاً، وجود قرائن كافية ودلائل قوية تُشير إلى ارتكاب جريمة رقمية، إذ "يجب أن تتوفر لدى

---

[1] **الزام المؤسسات والادارات والهيئات العمومية باستحداث هيكل مكلف بأمن أنظمتها المعلوماتية وحماية معطياتها**، موقع الحراك الاخباري، منشور بتاريخ 21 جانفي 2026، تم الاطلاع عليه يوم 17 أفريل 2026، على الساعة 15:36، على الرابط: https://alhirak-alikhbari.dz

[2] المادة 4 من القانون رقم 09-04 المؤرخ في 5 أوت 2009، المتعلق بالوقاية من الجرائم المرتبطة بتكنولوجيات الاعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47، الصادر بتاريخ 16 أوت 2009.

[3] غلاب عبد الحق، **المرجع السابق**، ص 501.

[4] عز الدين العثماني، **اجرائات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلوماتية**، مجلة دائرة البحوث والدراسات القانونية والسياسية، جامعة تبسة، العدد الرابع، جانفي 2018، ص 51.

جهات التحقيق دلائل كافية على وجود أجهزة أو أدوات استُخدمت في جريمة تزوير رقمي"[1]، وهذا الشرط يُجسد مبدأ الاشتباه المعقول الذي يمنع تحويل التفتيش إلى إجراء روتيني أو استكشافي عام يمسّ بالحريات دون مبرر.

ثانياً، يُشترط أن تكون القرائن "قوية" بما يكفي لتبرير الولوج إلى النظام المعلوماتي، فلا يكفي الاشتباه المجرد بل يجب أن تستند عملية التفتيش إلى "أولية أدلة تُشير بوضوح إلى تورط النظام في ارتكاب الجريمة المعلوماتية أو أشياء متحصلة منها أو مستندات إلكترونية ذات صلة بكشف الحقيقة"[2]، ونحن نرى أن هذا الشرط يُمثل ضمانةً جوهريةً تمنع التوسع غير المبرر في التفتيش، خاصةً وأن الأنظمة المعلوماتية تحتوي على بيانات شخصية وحساسة قد لا تكون ذات صلة بالجريمة محل التحقيق.

ثالثاً، يتطلب التفتيش الإلكتروني "مهارات تقنية للتعامل مع الأدلة الرقمية"[3]، وهو ما يُشكل شرطاً موضوعياً ضمنياً يتعلق بكفاءة المحققين وليس بموضوع التفتيش ذاته، فالتفتيش الإلكتروني يختلف عن التفتيش التقليدي في أنه يتطلب "تدريب المحققين المتخصصين واستخدام الأدوات الرقمية المناسبة"[4]، ونحن نعتقد أن غياب هذا الشرط قد يُفضي إلى إجراء تفتيشي غير فعّال أو حتى مُخلّ بسلامة الأدلة الرقمية.

ب). الشروط الشكلية

أما الشروط الشكلية فتتمثل في المبادئ الإجرائية التي تحكم سير التفتيش الإلكتروني، وفي مقدمتها "الحصول مسبقاً على إذن قضائي"[5]، فقد نصّ القانون 06-22 على أن التفتيش يجب أن يكون بناءً على "أمر قضائي مسبق من وكيل الجمهورية أو قاضي التحقيق"[6]، ونحن نلاحظ أن المشرع الجزائري قد شدد على هذا الشرط بشكلٍ يُجسّد التزامه بحماية الحقوق الفردية، إذ "يُعد عدم الحصول مسبقاً على إذن قضائي إجراءً قانونياً يضمناً حقوق الأفراد ويحميها من التعدي"[7].

---

[1] كيحول عبد القادر، **التفتيش الالكتروني كاجراء للتحقيق في الجرائم المعلوماتية**، مذكرة ماستر تخصص قانون جنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة زيان عاشورالجلفة، السنة الجامعية 2020/2019، ص 38.

[2] اية الوصيف، **بحث ودراسة قانونية حول التفتيش الالكتروني**، موقع محاماة نت، منشور بتاريخ 4 أكتوبر 2019، تم الاطلاع عليه يوم 17 أفريل 2026، على الساعة 16:05، على الرابط: https://www.mohamah.net

[3] مجدوب لامية، **اجراء التفتيش في التزوير الالكتروني**، مجلة التواصل في العلوم الانسانة والاجتماعية، جامعة باجي مختار عناية، المجلد 25، العدد 03، 30 سبتمبر 2019، ص 110.

[4] بن صويلح سفيان، حريدي الياس، **المرجع السابق**، ص 81.

[5] علمي مخلوف، بومحراث ليندة، **ضوابط التفتيش في الجرائم الالكترونية**، مجلة المعيار، جامعة الأمير عبد القادر للعلوم الاسلامية قسنطينة، المجلد 28، العدد 01، 15 جانفي 2024، ص 340.

[6] القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006، المتضمن قانون الاجراءات الجزائية، الجريدة الرسمية، العدد 84، الصادر بتاريخ 24 ديسمبر 2006.

[7] أحمد محمد محروس عبد العال، **المرجع السابق**، ص 54.

كما يُشترط أن يكون الإذن القضائي "مكتوباً ويحدد بوضوح نطاق التفتيش"[1]، فلا يجوز للمحققين تجاوز النطاق المحدد في الأمر القضائي تحت طائلة البطلان. وقد "يُسمح بتأجيل الحصول على الإذن على مدة لا تتجاوز 24 ساعة في حالات الطوارئ القصوى"[2]، وهو استثناءٌ ضيقٌ يُبرز القصد التشريعي في عدم الإخلال بالشرط الأساسي.

ثالثاً، يجب أن يكون التفتيش "ضرورياً ومتناسباً مع خطورة الجريمة"[3]، وهو ما يُجسّد مبدأ الضرورة والتناسب الذي يُقيّد السلطة التقديرية للمحققين، فالتفتيش الإلكتروني لا يجوز أن يكون إجراءً روتينياً بل يجب أن يقتصر على "الأدلة عن للكشف متناسباً ومتناسباً مع صالحيات التفتيش"[4]، ونحن نرى أن هذا الشرط يُشكل رادعاً قانونياً ضد الإفراط في استخدام سلطات التفتيش.

ثانيا: الضوابط التقنية والإجرائية للتفتيش الإلكتروني

وهي:

أ). الضوابط التقنية

يتطلب التفتيش الإلكتروني "تعامله مع الجوانب الفنية للأجهزة والأنظمة المعلوماتية"، وهو ما يستوجب ضوابط تقنية دقيقة تضمن سلامة الأدلة الرقمية، فأولاً، يجب "استخدام برامج متخصصة لعمل نسخ رقمية أصلية "(forensic imaging) تضمن عدم تلف البيانات أو تغييرها، وهو ما يُعرف في المصطلحات التقنية بـ"سلسلة الحيازة" (Chain of Custody)[5].

ثانياً، يُشترط "الحفاظ على المكونات المادية للحاسوب والبيانات الرقمية بحذر شديد"، فالتفتيش الإلكتروني يتطلب "ضمان عدم تلف الأدلة أو تغييرها"[6] أثناء عملية الضبط والحجز، ونحن نعتقد أن هذا الضابط يكتسب أهميةً بالغةً في جرائم التزوير الرقمي، حيث يمكن أن يُؤدي أي تغيير طفيف في البيانات إلى إبطال صلاحيتها كدليل قضائي.

---

[1] بن داني راضية، **الرقابة والاشراف على الأعمال الضبطية القضائية في التشريع الجزائري**، مذكرة ماستر تخصص قانون جنائي، كلية الحقوق والعلوم الساسية، جامعة عبد الحميد بن باديس مستغانم، السنة الجامعية 2020/2019، ص 86.

[2] كيحول عبد القادر، **التفتيش الالكتروني كاجراء للتحقيق في الجرائم المعلوماتية**، مذكرة ماستر تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور الجلفة، السنة الجامعية 2020/2019، ص 47.

[3] **التفتيش والانابة القضائية في القانون الجزائري**، موقع قانون تك، منشور بتاريخ 12 أفريل 2023، تم الاطلاع عليه يوم 17 أفريل 2026، على الساعة 16:32، على الرابط: https://www.9anon4dz.com

[4] بن لعربي أسماء، الفحلة مديحة، **المرجع السابق**، ص 448.

[5] لمصارة أنفال، محلول منال، **اجراءات التفتيش الالكتروني في التشريع الجزائري**، مذكرة ماستر تخصص قانون جنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة باتنة1 الحاج لخضر، السنة الجامعية 2024-2025، ص 38.

[6] معمري ايمان، فضيلة شعبان، **المرجع السابق**، ص 56.

ثالثاً، يتطلب التفتيش "تقديم كلمة المرور من المشتبه به"[1] في حال وجود تشفير، وهو ما يُشكل ضابطاً تقنياً يتقاطع مع الحق في عدم الإدلاء على النفس، وقد لاحظنا أن المشرع الجزائري لم يُقرّر صراحةً كيفية التعامل مع رفض المشتبه به تقديم كلمة المرور، مما يُثير إشكاليةً قانونيةً تستوجه التوضيح التشريعي.

ب). الضوابط الإجرائية

أما الضوابط الإجرائية فتتمثل في الإجراءات الشكلية التي يجب اتباعها أثناء التفتيش، فأولاً، "يجب حضور ضابط الشرطة القضائية المتخصص" أثناء التفتيش[2]، وهو ما يضمن احترافية الإجراء وخضوعه للإشراف القضائي، ثانياً، يجب "توثيق جميع الإجراءات في محضر رسمي يتضمن التاريخ والوقت"، وهو ما يضمن الشفافية والنزاهة في العملية التحقيقية.

ثالثاً، يُشترط "حضور ممثل النظام أو صاحبه" أثناء التفتيش، وهو ما يُجسّد مبدأ المُحاكمة العادلة وحق الدفاع، كما يجب "إضافة شاهدين محايدين" لتعزيز مصداقية الإجراءات[3]، ونحن نرى أن هذه الضوابط مجتمعةً تُشكل ضماناتٍ إجرائيةٍ رصينةٍ تمنع أي إساءة استخدام لسلطة التفتيش.

الفرع الثالث: حماية الخصوصية أثناء اجراءات البحث والتحري

إذا كانت إجراءات البحث والتحري في جرائم التزوير الرقمي تستوجب توسعاً في سلطات التفتيش والمراقبة، فإن هذا التوسع يقتضي بالضرورة إقرار ضمانات رصينة لحماية الخصوصية الفردية، فالخصوصية في العصر الرقمي لم تعد مجرد حق ثانوي، بل أصبحت "قدسية" يؤكد عليها المشرع الجزائري في ظل التطورات التكنولوجية المتسارعة، ولقد سعى المشرع إلى تحقيق التوازن الدقيق بين مصلحة مكافحة الجريمة وحماية الحقوق الأساسية للأفراد، من خلال منظومة تشريعية متكاملة نتناولها في هذا الفرع.

أولا: الأساس القانوني لحماية الخصوصية في التشريع الجزائري

يظهر من خلال:

أ). التأسيس الدستوري للحق في الخصوصية

يستند الحق في الخصوصية في التشريع الجزائري إلى تأسيس دستوري رصين، إذ نصّت المادة 47 من الدستور على أن "الحياة الخاصة سرية" وأن "الحماية الشخصية حق مكفول"، وهذا النص الدستوري يُشكّل السقف الأعلى لجميع الإجراءات التحقيقية، ويُلزم المشرع بإقرار ضمانات قانونية تضمن عدم المساس

[1] بومدين رحال، **محل التفتيش في مجال جرائم التجارة الالكترونية وفق القانون الجزائري**، المجلة الجزائرية للحقوق والعلوم السياسية، جامعة أحمد بن يحي الونشريسي تيسمسيلت، المجلد 03، العدد 02، 01 ديسمبر 2018، ص 166.

[2] عزالدين العثماني، **المرجع السابق**، ص 53.

[3] علمي مخلوف، بومحراث ليندة، **المرجع السابق**، ص 401.

بالخصوصية إلا في الحالات الاستثنائية المبررة، غير أن التحدي يكمن في كيفية تفعيل هذا الحق في سياق الجرائم الرقمية، حيث "يصبح الأفراد عرضة للاستغلال عندما لا يكونون على دراية بحقوقهم"[1]، ولقد لاحظنا أن المشرع الجزائري قد أدرك هذه الإشكالية فأقرّ في القانون 09-04 ضمانات إجرائية تضمن "حماية البيانات الشخصية" أثناء إجراءات البحث والتحري[2].

ب). الضمانات القانونية في القانون 09-04 والقوانين المكملة

يُجسّد القانون 09-04 التزام المشرع الجزائري بحماية الخصوصية من خلال مجموعة من الضمانات؛ فأولاً، اشتراط "الحصول مسبقاً على أمر قضائي" للتفتيش الإلكتروني، وهو ما يضمن إشراف القضاء على الإجراءات ومنع أي تدخل عشوائي؛ ثانياً، نصّ القانون على أن يكون التفتيش "مبرراً وضرورياً لجمع الأدلة"[3]، وهو ما يُجسّد مبدأ الضرورة والتناسب، كما نصّ القانون 18-07 المتعلق بحماية البيانات الشخصية على "تدابير تقنية وقانونية لحماية البيانات الشخصية"[4]، وهو ما يُكمل المنظومة القانونية لحماية الخصوصية، ونحن نرى أن هذا التكامل بين القوانين يُشكّل إطاراً قانونياً متيناً يحمي الخصوصية في سياق التحقيق الجنائي.

ثانيا: معايير حماية الخصوصية في سياق التحقيق الرقمي

وهي:

أ). مبدأ الضرورة والتناسب

يُعدّ مبدأ الضرورة والتناسب الركيزة الأساسية لحماية الخصوصية أثناء إجراءات البحث والتحري، فقد نصّ القانون الجزائري على أن "يجب أن يقتصر البحث على البيانات المتعلقة بالجريمة"، وهو ما يمنع التوسع غير المبرر في التفتيش، كما يُحظر استخدام البيانات الشخصية "لأغراض أخرى" غير التحقيق في الجريمة محل الاشتباه[5]، ونحن نعتقد أن هذا المبدأ يكتسب أهميةً بالغةً في جرائم التزوير الرقمي، حيث يمكن أن تكون

[1] المادة 47، دستور الجمهورية الجزائرية الديمقراطية الشعبية لسنة 1996 المعدل والمتمم، الجريدة الرسمية، العدد 82، الصادر بتاريخ 30 ديسمبر 2020.

[2] القانون رقم 09-04 المؤرخ في 5 أوت 2009، المتعلق بالوقاية من الجرائم المرتبطة بتكنولوجيات الاعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47، الصادر بتاريخ 16 أوت 2009.

[3] راضية مشري، **المرجع السابق**، ص 135.

[4] القانون رقم 18-07 المؤرخ في 10 جوان 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية، العدد 34، الصادر بتاريخ 10 جوان 2018.

[5] شعباني نوال، **المرجع السابق**، ص 601.

الأنظمة المعلوماتية تحتوي على بيانات شخصية وحساسة لا علاقة لها بالجريمة، فـ"الحماية الشخصية حق مكفول" يقتضي عدم المساس بهذه البيانات أو استغلالها[1].

ب). التدابير التقنية لحماية البيانات

تتجاوز حماية الخصوصية المجرد النصوص القانونية لتشمل تدابير تقنية دقيقة، فقد نصّت الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية 2025-2029 على "وضع توجيهات واضحة لحماية المعطيات" أثناء التعامل مع الأنظمة الرقمية[2]، كما تتطلب إجراءات التحقيق "استخدام آليات تشفير" تضمن عدم وصول غير المصرح لهم إلى البيانات[3]، وقد لاحظنا أن "وكالة أمن الأنظمة المعلوماتية" تلعب دوراً محورياً في هذا الإطار، إذ تتولى نشر الاستراتيجية الوطنية لأمن الأنظمة وتضمن تطبيق المعايير التقنية لحماية الخصوصية.

ج). الرقابة القضائية والمراجعة

تتجلى حماية الخصوصية أيضاً في الرقابة القضائية المستمرة على إجراءات التحقيق، فقد نصّ القانون على "دور المراجعة القضائية" في ضمان شرعية الإجراءات المتخذة، كما أن "المحكمة العليا" تتولى مراقبة تطبيق الضوابط القانونية وضمان عدم تجاوزها[4]، ونحن نرى أن هذه الرقابة تكتسب أهميةً استثنائيةً في الجرائم الرقمية، حيث يجب على الدول حماية الخصوصية في العصر الرقمي وفقاً لمعايير حقوق الإنسان الدولية.

ثالثا: التحديات والآفاق المستقبلية

أ). التحديات الراهنة

تواجه حماية الخصوصية في الجزائر تحدياتٍ جوهريةٍ تتطلب معالجة تشريعية وتقنية؛ فأولاً، "التزوير المعلوماتي في عصر الرقمنة" يطرح إشكاليات جديدة تتعلق بتحديد نطاق الخصوصية في الفضاء الرقمي؛ ثانياً، "السلامة السيبرانية والأمن الرقمي" تتطلب توازناً دقيقاً بين الحماية والمراقبة[5]، كما نلاحظ أن "الشركات تحتاج إلى حماية نفسها من خروقات البيانات"، وهو ما يُشير إلى ضرورة تطوير الإطار القانوني لمواكبة التهديدات الرقمية المتجددة.

---

[1] **كيف تحمي خصوصيتك؟**، موقع الجزيرة، منشور بتاريخ 5 أكتوبر 2025، تم الاطلاع عليه يوم 17 أفريل 2016، على الساعة 17:28، على الرابط: https://www.aljazeera.net

[2] **الكشف عن مضمون الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية للفترة 2025-2029**، وكالة الأنباء الجزائرية، منشور بتاريخ 3 مارس 2026، تم الاطلاع عليه يوم 17 أفريل 2016، على الساعة 17:36، على الرابط: https://www.aps.dz

[3] غلاب عبد الحق، **المرجع السابق**، ص 502.

[4] عمارة فتيحة، **المرجع السابق**، ص 182.

[5] بن لعربي أسماء، الفحلة مديحة، **المرجع السابق**، ص 450.

ب). الآفاق المستقبلية

تتجه الجهود المستقبلية نحو "تعزيز القدرات المؤسسية" لحماية الخصوصية، فقد أطلقت الجزائر "استراتيجية وطنية لأمن الأنظمة المعلوماتية" تتضمن "تأمين سيادة رقمية وحماية رقمية"، كما تسعى إلى "بناء بيئة رقمية آمنة" تحترم حقوق الأفراد[1]، ونحن نعتقد أن هذه الجهود تستدعي "وضع ضوابط الحضور الرقمي" وأخلاقيات استخدام التكنولوجيا، بما يضمن حماية الخصوصية في سياق التحقيق الجنائي وخارجه.

المطلب الثاني: ضبط البيانات الرقمية وحفظها

يُشكِّل ضبط البيانات الرقمية وحفظها ركيزة أساسية في إجراءات البحث والتحري بجرائم التزوير الرقمي، إذ تتسم الأدلة الرقمية بطبيعةٍ غير ماديةٍ وقابليةٍ عاليةٍ للتغيير أو الحذف أو التلف، مما يستوجب استحداث قواعد فنية وقانونية خاصة تضمن سلامتها وصحتها[2]، ولقد نصَّ القانون رقم 09-04 في المادة 9 على إمكانية "حجز أو نسخ البيانات والمعلومات الرقمية المخزنة أو المعالجة أو المرسلة من خلال نظام معلوماتي"[3]، مُقرِّراً بذلك ضرورة التمييز بين الوسائط الإلكترونية ذاتها والبيانات المخزنة فيها.

وتكتسب عملية الضبط الرقمي أهميةً بالغةً في جرائم التزوير، حيث يتعيَّن على المحققين اتخاذ إجراءات تقنية دقيقة تضمن عدم تغيُّر البيانات المضبوطة أثناء نقلها أو تحليلها، وذلك من خلال ما يُعرف بإجراءات التحريز الرقمي (Hash Value) التي تُمثِّل بصمةً إلكترونيةً فريدةً للبيانات[4]، غير أن هذا الضبط يثير إشكاليةً تتعلق بمدى كفاية القواعد القانونية الجزائرية في ضمان سلسلة الحفظ الرقمي وعدم انقطاعها، خاصةً في ظل غياب نصوص تفصيليةٍ تنظم الإجراءات الفنية للحجز الرقمي[5].

الفرع الأول: طرق ضبط الوسائط الالكترونية وتأمينها

يشكل التزوير الرقمي في العصر الراهن من أخطر الظواهر الإجرامية التي تهدد الأمن المعلوماتي والثقة في المعاملات الإلكترونية، إذ يتجاوز مفهومه التقليدي المتمثل في تزوير المستندات الورقية ليشمل التلاعب بالبيانات الرقمية والتوقيعات الإلكترونية والشهادات الرقمية التصديقية[6]، ونظراً للطبيعة التقنية المعقدة لهذه

---

[1] شعباني نوال، **المرجع السابق**، ص 602.

[2] حشمان عمار، **المرجع السابق**، ص54.

[3] المادة 9 من القانون رقم 09-04 المؤرخ في 5 أوت 2009، المتعلق بالوقاية من الجرائم المرتبطة بتكنولوجيات الاعلام والاتصال، الجريدة الرسمية، العدد 47، الصادر بتاريخ 16 أوت 2009.

[4] حشمان عمار، **المرجع السابق**، ص 56.

[5] أحمد مسعود مريم، قريشي محمد، **المرجع السابق**، ص 22.

[6] **حل سؤال عملية ايصال محتوى الوسائط الرقمية التي تم شراؤها عبر التجارة الالكترونية** ، موقع المتوفر، منشور بتاريخ 23 أكتوبر 2021، تم الاطلاع عليه يوم 19 أفريل 2026، على الساعة 07:41، على الرابط: https://ask.tanfis.com/28661

الجريمة، فإن المشرع الجزائري قد اتجه نحو بناء إطار قانوني وتنظيمي متكامل يهدف إلى ضبط الوسائط الإلكترونية وتأمينها من أخطار التزوير، وذلك عبر مجموعة من التشريعات المتخصصة والهيئات الرقابية والآليات التقنية الحديثة[1].

أولاً: الإطار القانوني والتنظيمي لضبط الوسائط الإلكترونية

سوف نتناول هذا من خلال:

أ). الأساس القانوني للضبط

يستند إطار ضبط الوسائط الإلكترونية في التشريع الجزائري إلى مجموعة من النصوص القانونية المتكاملة؛ في مقدمتها يأتي القانون 23-14 المتعلق بالأعمال العضوي المؤرخ في 27 أوت 2023، والذي يعد حجر الزاوية في تنظيم الإعلام الجزائري، إذ وسع نطاقه ليشمل النشاط العالمي عبر الإنترنت، ونص صراحة على حظر نشر المعلومات الكاذبة والمزورة عبر الإلكترونيات[2]، كما يكمل هذا القانون المرسوم التنفيذي 20-332 المؤرخ في 22 نوفمبر 2020، والذي يحدد كيفية ممارسة النشاط العالمي عبر الإنترنت ويتيح آلية للأفراد والجهات المتضررة من معلومات خاطئة للمطالبة بتصحيحها ونشر الردود[3]، إلى جانب ذلك، يأتي القانون 24-02 المتعلق بمكافحة التزوير واستعمال المزور، والذي يعد أداة رئيسية في مكافحة التزوير بكل أشكاله، حيث وسع نطاقه ليشمل المحررات الإلكترونية والوثائق الرقمية، ويفرض عقوبات صارمة بالحبس والغرامات تهدف إلى الردع والحماية[4]، كما لا يمكن إغفال دور المادة 394 مكرر من القانون رقم 24-06 المتضمن قانون العقوبات الجزائري، والتي تتناول المساس بأنظمة معالجة المعطيات القانونية، حيث تفرض عقوبات بالحبس والغرامة على كل من يدخل أو يبقى عن طريق غش في هذه الأنظمة[5].

من وجهة نظرنا نرى أن المشرع الجزائري قد اتبع نهجاً تكاملياً في وضع الإطار القانوني لضبط الوسائط الإلكترونية، إذ جمع بين القوانين العامة المتعلقة بالتزوير والقوانين الخاصة بالجرائم الإلكترونية، نعتبر أن هذا

---

[1] راغب ملي، **قانون الاعلام الجديد في الجزائر: ضبط المحتوى حتى على الانترنت**، منصة سمكس، منشور بتاريخ 02 أكتوبر 2023، تم الاطلاع عليه يوم 19 أفريل 2026، على الساعة 07:44، على الرابط: https://smex.org

[2] القانون رقم 23-14 المؤرخ في 27 أوت 2023، المتعلق بالاعلام، الجريدة الرسمية، العدد 56، الصادر بتاريخ 29 أوت 2023.

[3] المرسوم التنفيذي رقم 20-332 المؤرخ في 22 نوفمبر 2020، المتعلق بتحديد كيفيات ممارسة نشاط الاعلام عبر الانترنت ونشر الرد أو التصحيح عبر الموقع الالكتروني، الجريدة الرسمية، العدد 70، الصادر بتاريخ 25 نوفمبر 2020.

[4] القانون رقم 24-02 المؤرخ في 26 فيفري 2024، المتعلق بمكافحة التزوير واستعمال المزور، الجريدة الرسمية، العدد 15، الصادر بتاريخ 29 فيفري 2024.

[5] المادة 394 مكرر من القانون 24-06 المؤرخ في 28 أفريل 2024 المعدل والمتمم للأمر رقم 66-156 المؤرخ في 8 جوان 1966، المتضمن قانون العقوبات، الجريدة الرسمية، العدد 30، الصادر بتاريخ 30 أفريل 2024.

التكامل ضروري لمواكبة طبيعة الجريمة الرقمية المتعددة الأوجه، لكننا نستحسن أن يتم توحيد هذه النصوص في مدونة خاصة بالجرائم الرقمية تضمن وضوح الأحكام وتجنب الازدواجية في التطبيق.

ب). الهيئات التنظيمية والرقابية

يلعب الهيكل التنظيمي دوراً محورياً في ضبط الوسائط الإلكترونية وتأمينها من التزوير، فالهيئة العليا المستقلة للسمعي البصري تشرف على تنظيم النشاط العالمي، بما في ذلك المنصات والمواقع الإلكترونية، وتلعب دوراً حيوياً في تطبيق القوانين ومراقبة الأنشطة المرتبطة بهذا المجال[1]، كما تبرز أهمية سلطة ضبط البريد والاتصالات الإلكترونية (ARPCE)، والتي ترتب نشاطات البريد والاتصالات وتراقب تطبيق القوانين المتعلقة بهذا المجال[2].

من وجهة نظرنا نعتقد أن تواجد هيئات متعددة قد يؤدي أحياناً إلى تداخل في الاختصاصات أو غياب التنسيق الفعال، نرى ضرورة إنشاء هيئة وطنية موحدة للأمن السيبراني تتولى تنسيق الجهود بين مختلف المتدخلين، مع إعطائها صلاحيات استباقية في مجال الرقابة والتفتيش على المنصات الإلكترونية المشتبه في استخدامها في أعمال التزوير الرقمي.

ثانياً: آليات الضبط التقني والتقنيات الرقمية لتأمين الوسائط

أ). ضبط المحتوى الرقمي والرقابة على المنصات

تتنوع آليات ضبط الوسائط الإلكترونية وتأمينها بين جوانب تنظيمية وتقنية وقضائية؛ فعلى المستوى التنظيمي، يشترط القانون على جميع المنصات والمواقع الإلكترونية التسجيل لدى السلطات التنظيمية، وعدم الالتزام بهذا الشرط يترتب عليه عقوبات تصل إلى الحبس والغرامات[3]، كما يتضمن ضبط المحتوى الرقمي رقابة واسعة النطاق على ما يتم نشره عبر الإنترنت، مع حظر واضح لنشر الأخبار الكاذبة والمزورة، حيث تطالب

[1] القانون رقم 23-14 المؤرخ في 27 أوت 2023، المتعلق بالاعلام، الجريدة الرسمية، العدد 56، الصادر بتاريخ 29 أوت 2023.

[2] **سلطة ضبط البريد والاتصالات الالكترونية**، الصفحة الرئيسية، تم الاطلاع عليه بتاريخ 19 أفريل 2026، عللى الساعة 08:04، على الرابط: https://www.arpce.dz

[3] زعموش فوزية، خوادجية سميحة حنان، **النظام القانوني للاعلام الالكتروني في الجزائر بين الضمانات والضوابط: دراسة مقارنة**، موقع اليف، منشور بتاريخ 22 نوفمبر 2024، تم الاطلاع عليه يوم 19 أفريل 2026، على الساعة 08:13، على الرابط: https://aleph.edinum.org/13306

القانونية الإلكترونية المنصات بوضع آليات للتحقق من مصداقية المحتوى ومصادره[1]، ويشجع النهج المتبع على نشر التصحيحات فورية عند وجود معلومات خاطئة، مما يعزز الشفافية ويحد من انتشار المعلومات المضللة[2].

نلاحظ أن المشرع الجزائري قد أدرك ضرورة مواكبة سرعة انتشار المعلومات الرقمية، ونرى أن إلزامية التسجيل تُعد خطوة استباقية جيدة، لكنها قد تواجه صعوبة في التطبيق العملي على المنصات الأجنبية، لذلك نستحسن تطوير آليات التعاون الدولي لضمان فعالية هذا الضبط، مع ضمان عدم المساس بالحريات الأساسية للتعبير في إطار القانون.

ب). التقنيات الأمنية للحماية والتأمين

على المستوى التقني، تشجع الجزائر على استخدام التقنيات الحديثة لتأمين الوثائق والبيانات، فالتوقيع الإلكتروني يعتبر أساسية وسيلة لضمان صحة الوثائق الرقمية، إذ يعد أي تعديل على وثيقة موقعة إلكترونياً تزويراً إلكترونياً[3]، كما يستخدم التشفير لحماية البيانات أثناء نقلها وتخزينها، مما يقلل من مخاطر الوصول غير المصرح به والتلاعب، وتلزم المؤسسات المالية وخاصة البنوك بتطبيق آليات كشف متطورة عن البطاقات والحسابات المزورة، بهدف حماية المعاملات المالية الإلكترونية[4]، وقد أظهر الرسم البياني أسفله أهمية هذه التقنيات في الحماية من التزوير الرقمي، حيث حصل التوقيع الإلكتروني على أعلى درجة أهمية (5/5)، تلاه الكشف عن التلاعب بالبيانات والمصادقة متعددة العوامل.

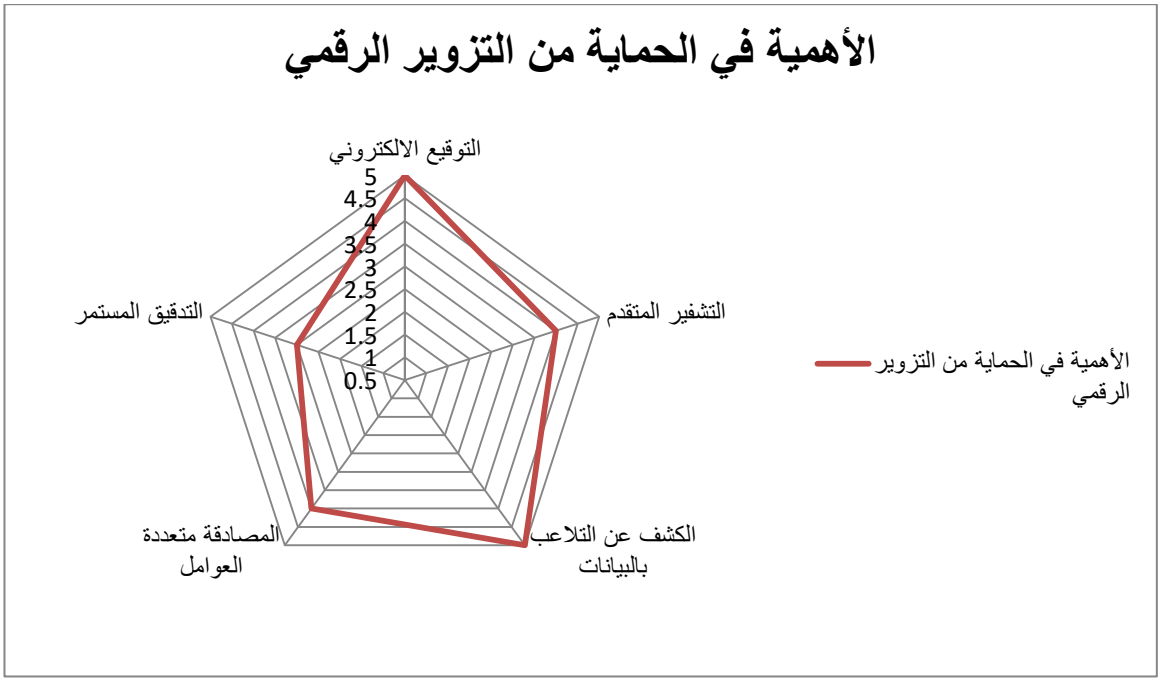
---

[1] راغب ملي، **قانون الاعلام الجديد في الجزائر: ضبط المحتوى حتى على الانترنت**، منصة سمكس، منشور بتاريخ 02 أكتوبر 2023، تم الاطلاع عليه يوم 19 أفريل 2026، على الساعة 08:15، على الرابط: https://smex.org

[2] زعموش فوزية، خوادجية سميحة حنان، **النظام القانوني للاعلام الالكتروني في الجزائر بين الضمانات والضوابط: دراسة مقارنة**، موقع اليف، منشور بتاريخ 22 نوفمبر 2024، تم الاطلاع عليه يوم 19 أفريل 2026، على الساعة 08:16، على الرابط: https://aleph.edinum.org/13306

[3] **ما هي العقوبة التي حددها القانون الجزائري للجريمة الالكترونية؟**، موقع تخصصات بيت.كوم، منشور عام 2015، تم الاطلاع عليه يوم 19 أفريل 2026، على الساعة 08:18، على الرابط: https://www.bayt.com

[4] عمارة فتيحة، **المرجع السابق**، ص 173.



المصدر: من اعداد الطالبتين بالاعتماد على مخرجات الدراسة، 2026.

من وجهة نظرنا نعتبر أن الاعتماد على التقنيات الأمنية يمثل ركيزة أساسية في الوقاية من التزوير الرقمي، غير أننا نرى أن هذه التقنيات تبقى قاصرة إذا لم تصاحبها برامج توعوية مكثفة للمواطنين والمؤسسات حول مخاطر التزوير وكيفية الحماية منه، كما نستحسن إلزام المؤسسات الحكومية والخاصة الكبرى بتطبيق معايير دولية في مجال الأمن السيبراني.

الفرع الثاني: القواعد الفنية لضمان عدم تغيير البيانات المضبوطة

تكتسب القواعد الفنية لضمان عدم تغيير البيانات المضبوطة أهمية استثنائية في سياق جرائم التزوير الرقمي، إذ أن طبيعة الأدلة الرقمية الافتراضية تجعلها عرضة بشكل فريد للتلاعب والتغيير دون ترك آثار مادية ظاهرة[1]، وقد أدرك المشرع الجزائري هذا التحدي التقني المحدق، فأرسى مجموعة من المبادئ الفنية والقانونية المتكاملة تهدف إلى الحفاظ على سلامة البيانات المضبوطة من لحظة جمعها وحتى تقديمها أمام المحكمة[2]، إن هذا الفرع يكتسب أهمية بالغة في سياق البحث العلمي، لأنه يتناول الجانب التقني الدقيق للإجراءات القضائية في مجال الجرائم الإلكترونية، وهو ما يتطلب تحليلاً متخصصاً للآليات التقنية والضمانات القانونية المرتبطة بها، بعيداً عن التكرار مع الفروع السابقة التي تناولت الإطار العام للضبط والتأمين.

[1] جليلة بلعلمي، صالح مزري، **الدليل الرقمي والاثبات الجنائي**، مذكرة ماستر تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح ورقلة، السنة الجامعية 2022/2021، ص 57.

[2] أحمد محمد محروس عبدالعال، **المرجع السابق**، ص53.

أولا: المبادئ الأساسية للقواعد الفنية لضمان عدم التغيير

وهي:

أ). مبدأ السلامة والنزاهة (Integrity)

يُعد مبدأ السلامة والنزاهة (Integrity) ركيزة أساسية في القواعد الفنية لضمان عدم تغيير البيانات المضبوطة، إذ يتطلب التأكد من أن الدليل الرقمي لم يتعرض لأي تعديل أو تغيير منذ لحظة ضبطه، ويلزم القانون 18-07 المتعلق بحماية البيانات الشخصية باستخدام تقنيات التشفير (Encryption) والتجزئة (Hashing) لضمان سلامة البيانات، حيث يجب تسجيل البيانات بأي شكل من أشكال التعديل وإتلافها[1]، ويطبق هذا المبدأ باستخدام خوارزميات هاش قوية مثل SHA-256 لإنشاء بصمة رقمية فريدة تكشف أي تغيير تطرأه الحق، مما يضمن أن الأدلة تبقى غير معدلة منذ الضبط من قبل السلطات القضائية والشرطة الإلكترونية[2].

من وجهة نظرنا نرى أن المشرع الجزائري قد أدرك بحداثة أن الأدلة الرقمية تختلف جوهرياً عن الأدلة المادية التقليدية في قابليتها للتغيير السريع والخفي، نعتبر أن اعتماد خوارزميات التجزئة يمثل ضمانة تقنية ناجعة، لكننا نستحسن أن يُحدد في النصوص القانونية نوع الخوارزميات المستخدمة ودرجة أمانها، مع مراعاة التطور السريع في مجال التشفير والحوسبة الكمومية التي قد تهدد فعالية هذه الخوارزميات في المستقبل القريب.

ب). مبدأ سلسلة الحراسة (Chain of Custody)

يشكل مبدأ سلسلة الحراسة (Chain of Custody) ضمانة حاسمة للمساءلة والشفافية الكاملة في التعامل مع الدليل الرقمي، إذ يجب توثيق جميع خطوات التعامل مع الدليل منذ لحظة جمعه وضبطه، مروراً بنقله وتخزينه وفحصه، وصولاً إلى تقديمه للمحكمة[3]، ويؤكد هذا النهج التسلسلي على توثيق كل خطوة بما في ذلك التواريخ والأماكن والأشخاص المخولين، ليثبت أن الدليل لم يتعرض لتعديل غير مصرح به[4]، وتتطلب هذه العملية إجراءات دقيقة موثقة في الأمر 09-04 المتعلق بالوقاية من الجرائم الإلكترونية، والتي تضمن عدم المساس بالبيانات المضبوطة[5].

---

[1] معزوز راضية، **الحماية الجزائية للبيانات الرقمية في التشريع الجزائري**، مذكرة ماستر تخصص القانون القضائي، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس مستغانم، السنة الجامعية 2024/2023، ص 63.

[2] معمري ايمان، فضيلة شعبان، **المرجع السابق**، ص 20.

[3] قسمية نجاة، **الحماية الجزائية للخصوصية الرقمية في التشريع الجزائري**، مذكرة ماستر تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة باتنة 1 الحاج لخضر، السنة الجامعية 2025/2024، ص 74.

[4] عمارة فتيحة، **المرجع السابق**، ص177.

[5] القانون رقم 09-04 المؤرخ في 5 أوت 2009، المتعلق بالوقاية من الجرائم المرتبطة بتكنولوجيات الاعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47، الصادر بتاريخ 16 أوت 2009.

نعتبر أن سلسلة الحراسة تمثل الضمانة الإجرائية التي تكمل الضمانة التقنية لمبدأ السلامة، غير أننا نلاحظ أن التطبيق العملي لهذا المبدأ في الجزائر قد يواجه صعوبات لوجستية، خاصة في ظل غيور نظم رقمية موحدة لتوثيق هذه السلسلة، نستحسن تطوير منظومة إلكترونية وطنية لإدارة سلسلة الحراسة، تربط بين مختلف الجهات المعنية وتضمن تتبعاً آلياً دقيقاً للأدلة الرقمية.

ج). مبدأ الأمن والحماية (Security)

يُعد مبدأ الأمن والحماية (Security) ركيزة أساسية لضمان سرية الدليل وحمايته من الوصول غير المصرح به، حيث يجب حفظ البيانات في وسائط تخزين آمنة ومحمية، وتتضمن هذه الحماية استخدام تقنيات التشفير القوي، وتحديد صلاحيات الوصول، واستخدام شبكات VPN وHTTPS لضمان سلامة البيانات أثناء نقلها، كما يلعب التوقيع الإلكتروني دوراً أساسياً في ضمان أصالة المحررات الرقمية ومنع تزوير التوقيعات، حيث يُفرض استخدام الشهادات الرقمية الصادرة عن هيئات معتمدة مثل الهيئة الوطنية للأمن الإلكتروني، والتحقق من صحة التوقيع عبر بروتوكول PKI(Public Key Infrastructure)[1].

من وجهة نظرنا نرى أن المبدأ الأمني يكتسب بعداً مزدوجاً: حماية البيانات من التغيير الخارجي، وحمايتها من التسرب والوصول غير المشروع، نعتقد أن التشريع الجزائري قد أرسى قاعدة جيدة في هذا المجال، لكننا نستحسن تطوير معايير وطنية إلزامية لأمن البيانات المضبوطة، تضع تصنيفات دقيقة لمستويات الحماية المطلوبة حسب حساسية البيانات وخطورة الجريمة المرتبطة بها.

ثانيا: الإجراءات التقنية والتحقيقية لتطبيق القواعد الفنية

وهي:

أ). إجراءات النسخ الاحتياطي الجنائي (Forensic Imaging)

تتطلب ضبط وحفظ البيانات الرقمية في قضايا التزوير الإلكتروني إتباع بروتوكولات فنية دقيقة، من بينها إنشاء نسخة مطابقة رقمية من الأصل باستخدام أدوات جنائية رقمية متخصصة مثل EnCase وFTK، حيث يجب أن تتم العملية على نسخة طبق الأصل دون المساس بالبيانات الأصلية، ويسمح هذا الإجراء بالعمل على نسخة الاحتياطي دون تغيير الأصل، مما يضمن سلامة الدليل الأصلي، كما يمكن في الحالات المتقدمة استخدام تقنيات البلوكتشين (Blockchain) لتوفير سجل غير قابل للتعديل يؤكد عدم التلاعب[2].

---

[1] حايطي فاطيمة، هروال نبيلة هبة، **الحماية الاجرائية للحق في الخصوصية الرقمية في مواجهة الجريمة المعلوماتية**، مجلة الدراسات القانونية، جامعة يحيى فارس بالمدية، المجلد 07، العدد 02، منشور بتاريخ 24 جوان 2021، ص 130.

[2] سويسي فتيحة، **التكييف القانوني لجرائم المعلوماتية والاشكالات العلمية المترتبة عنها**، مداخلة مقدمة خلال الندوة البحثية المنظمة من طرف مركز البحوث القانونية والقضائية، المنعقد بتاريخ 18 جانفي 2022، ص 18.

نعتبر أن النسخ الجنائي يمثل خطوة تقنية حاسمة تفصل بين "الأدلة العملية" و"الأدلة القانونية، غير أننا نلاحظ أن توفر الأدوات المتخصصة في الجزائر قد يكون محدوداً في بعض الهياكل القضائية والأمنية، نستحسن إنشاء مراكز وطنية للخبرة الجنائية الرقمية مجهزة بأحدث التقنيات، مع تكوين مستمر للقضاة والمحامين في فهم هذه الإجراءات التقنية.

ب). التحقق الفني والخبرة الرقمية

يلزم قانونياً فحص الأدلة أمام متخصصين تقنيين بخبرة أصيلة، مع إمكانية الاستعانة بخبراء رقميين جنائيين، ويتضمن هذا التحقيق تحليل البيانات الوصفية (Metadata) والآثار الرقمية والتأييد للكشف عن محاولات التغيير، حيث تلعب التقارير الفنية والخبرات التقنية دوراً حاسماً في إثبات صحة الدليل الرقمي[1].

من وجهة نظرنا نرى أن الخبرة الرقمية تمثل العنصر البشري الذي يضمن صحة التطبيق التقني للقواعد الفنية، لكننا نعتقد أن هناك فجوة في الجزائر بين التطور التقني للأدلة الرقمية والقدرة التحليلية للخبراء المحليين، نستحسن إنشاء برامج تأهيل وطنية للخبراء الرقميين، مع إمكانية الاستعانة بالخبرة الدولية في القضايا المعقدة، ووضع معايير مهنية وقانونية لاعتماد الخبراء في هذا المجال.

الفرع الثالث: اجراءات التحرير الرقمي (Hash Value)

إن الانتقال من الإطار النظري العام لمفهوم التزوير الرقمي إلى الدخول في تفاصيل الإجراءات العملية لإثبات هذه الجريمة، يقتضي منا الوقوف عند آليات التحرير الرقمي التي أضحت تشكل ركيزة أساسية في العمل الجنائي المعاصر، إذ لم يعد الاعتماد على الأدلة المادية التقليدية كافياً في مواجهة جرائم تستند إلى بنية تقنية معقدة، ومن ثم يتعين علينا أن نستحضر المفهوم الحديث للتحرير الرقمي الذي يتجاوز مجرد حفظ البيانات إلى ضمان سلامتها وعدم تعرضها للتلاعب، وهو ما يقودنا بشكل طبيعي إلى الاهتمام بقيمة الهاش (Hash Value) بوصفها البصمة الرقمية الفريدة التي تمكن من تحديد هوية الملف الإلكتروني وكشف أي تغيير قد يطال محتواه، ومن هنا تبرز أهمية هذا الفرع في محاولة تفكيك المراحل الإجرائية التي يتعين على الضابط القضائي والخبير التقني اتباعها ضمن المنظومة القانونية الجزائرية، والتساؤل عن مدى كفاية التشريع الجزائري في تأطير هذه الإجراءات بما يضمن قبولها الإثباتي أمام القضاء.

[1] عبيزة منيرة، **الحماية القانونية للبيانات الشخصية من الجرائم المعلوماتية في ضوء التشريع الجزائري**، مجلة الاجتهاد القضائي، جامعة محمد خيضر بسكرة، المجلد 15، العدد 02، منشور بتاريخ 30 نوفمبر 2023، ص 178.

أولا: المرتكز التقني لمفهوم قيمة الهاش ودورها في كشف التزوير الرقمي

يُعد مفهوم قيمة الهاش (Hash Value) من المفاهيم التقنية الأساسية في مجال الجرائم الرقمية، إذ يتم إنشاؤها باستخدام خوارزميات تشفيرية معقدة تنتج قيمة رقمية فريدة لكل ملف أو مستند إلكتروني، وتتميز هذه القيمة بكونها ثابتة وقصيرة بغض النظر عن حجم الملف الأصلي أو تعقيده، وتشبه في ذلك البصمة الوراثية للإنسان التي لا تتطابق بين فردين، وقد أكدت المعطيات التقنية على أن أي تغيير طفيف في المحتوى الأصلي للملف، ولو كان حرفاً واحداً أو مسافة فارغة، سيؤدي إلى تغيير جذري وغير متوقع في القيمة الناتجة، وهو ما يجعل من هذه التقنية أداة قوية للتحقق من سلامة البيانات وعدم تعرضها للتلاعب، كما أنها تُستخدم في توثيق الأدلة الرقمية وحمايتها من التزوير، إذ يتم حساب قيمة الهاش عند إنشاء المستند الرقمي، وعند الاشتباه في تزويره يتم إعادة حسابها ومقارنتها بالقيمة الأصلية الموثقة، فإذا تطابقت القيمتان تأكدت سلامة المستند، وإذا اختلفتا يُعد ذلك دليلاً قاطعاً على وقوع تلاعب[1].

نرى أن هذا المرتكز التقني يمثل نقلة نوعية في مجال الإثبات الجنائي، إذ يتيح للقضاء الجزائري الاعتماد على معايير علمية دقيقة بدلاً من الاجتهادات الذاتية في تقييم الأدلة الرقمية، ونلاحظ أن قيمة الهاش تُعالج إحدى أبرز مشكلات التزوير الرقمي المتمثلة في سهولة تعديل الملفات الإلكترونية دون ترك آثار مادية ظاهرة، كما نستخلص أن هذا المفهوم، رغم تعقيده التقني، يحمل في طياته بساطة في التطبيق العملي، حيث يمكن للخبير إثبات وقوع التزوير من خلال مجرد مقارنة رقمية، مما يعزز من موثوقية الإجراءات القضائية ويضمن تحقيق العدالة الرقمية في ظل التحديات التقنية المتسارعة.

ثانيا: الإطار التشريعي الجزائري المؤطر لإجراءات التحرير الرقمي

لم يأتِ الاعتراف بإجراءات التحرير الرقمي وقيمة الهاش من فراغ، بل استند إلى منظومة تشريعية متكاملة سعى المشرع الجزائري من خلالها إلى مواكبة التطورات التكنولوجية، حيث نجد أن قانون 09-04 المتعلق بالوقاية من الجرائم المرتبطة بتكنولوجيا المعلومات والاتصالات قد وضع الإطار العام لتصنيف الجرائم المعلوماتية ومنها جريمة التزوير الإلكتروني، في حين أن قانون 18-07 المتعلق بالتوقيع الإلكتروني والشهادة الإلكترونية قد فتح الباب أمام استخدام تقنيات التجزئة (الهاش) كدليل إثباتي معترف به قانونياً، وأضفى الشرعية على استخدام التوقيعات الرقمية والشهادات الإلكترونية، وأخيراً جاء مشروع قانون 24-02 (الصادر/المشروع) المتعلق بمكافحة التزوير واستعمال المزور ليعزز هذا الإطار بشكل خاص من خلال تضمينه لجرائم التزوير

[1] هاجر طبا، صبرينة مقالتي، **الأدلة الرقمية ودورها في الإثبات الجنائي**، مذكرة ماجستير في الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي – برج بوعريريج، السنة الجامعية 2020-2021، ص 59.

التي تستعمل الأدوات الرقمية، وتحديد العقوبات المقررة لها، وتجديد التدابير المتعلقة بتأمين الوثائق رقمياً[1]، كما أشارت وكالة الأنباء الجزائرية إلى الأحكام الجديدة التي تفرضها هذه التشريعات في مجال مكافحة التزوير[2].

نعتقد أن هذا الإطار التشريعي يعكس وعياً لدى المشرع الجزائري بخطورة جريمة التزوير الرقمي وتأثيرها على الثقة في المعاملات الإلكترونية والاقتصاد الرقمي، غير أننا نلاحظ أن التفرقة بين التزوير التقليدي والتزوير الرقمي لا تزال تحتاج إلى مزيد من التوضيح في النصوص التطبيقية، إذ أن الاعتماد على أدوات تقنية متطورة يقتضي إثباتها ببراعة فائقة، ونرى أن التشريع الجزائري، رغم تطوره، يظل بحاجة إلى تفاعل أكبر بين الجانب القانوني والجانب التقني، خاصة فيما يتعلق بتفاصيل إجراءات حساب قيمة الهاش وتوثيقها ضمن محاضر رسمية تلقى القبول لدى المحاكم، ونستخلص أن التكامل بين هذه القوانين يشكل خطوة متقدمة، لكنه يظل رهيناً بتطوير البنية التحتية الرقمية وتكوين الكفاءات المتخصصة.

ثالثا: المراحل العملية لإجراءات التحرير الرقمي في ضوء التشريع الجزائري

تمر إجراءات التحرير الرقمي في جريمة التزوير الرقمي بمراحل متتالية تبدأ بالاستيلاء الآمن على الأدلة الرقمية من مصادرها المختلفة، سواء كانت أجهزة حواسيب أو هواتف ذكية أو خوادم، حيث يتعين على الضابط القضائي والخبير التقني تأمين الموقع الإلكتروني واستخدام برمجيات متخصصة مثل FTK أو EnCase لاستنساخ البيانات مع المحافظة على سلامتها دون إحداث أي تعديل، وقد نصت المادة 63 مكرر من قانون الإجراءات الجزائية على ضرورة أن يتم استخراج البيانات وفقاً للإجراءات القانونية المقررة، وتلي هذه المرحلة خطوة حساب قيمة الهاش فوراً عند الاستيلاء على كل ملف أو مستند رقمي، إذ تعتبر هذه الخطوة أساسية لإثبات سلامة الملف، حيث تسجل هذه القيمة الفريدة بدقة وتعمل كـ"بصمة" للمستند، ثم تأتي مرحلة توثيق سلسلة الحيازة (Chain of Custody) التي تعد أمراً جوهرياً لضمان قبول الدليل الرقمي أمام المحكمة، إذ يجب توثيق جميع الإجراءات التي تمت على الدليل الرقمي منذ جمعه وحتى عرضه في محضر رسمي، ومقارنة قيمة الهاش الحالية بالقيمة الأصلية الموثقة عند الاشتباه في وقوع تزوير، وأخيراً يتم التخزين الآمن للأدلة في وسائط محمية بتقنيات تشفير مضادة للتزوير، مع حساب قيمة هاش جديدة للدليل المخزن بعد فترة لضمان عدم تعرضه للتغيير[3].

---

[1] **تفاصيل مشروع قانون مكافحة التزوير واستعمال المزور**، موقع الاذاعة الجزائرية، منشور بتاريخ 21 نوفمبر 2023، تم الاطلاع عليه يوم 24 أفريل 2026، على الساعة 21:06، على الرابط: https://news.radioalgerie.dz/ar/node/35842

[2] عبد القادر دارم، جلال حدوش، **السياسة الجنائية في ظل القانون 24-02 يتعلق بمكافحة التزوير واستعمال المزور**، مذكرة ماستر تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة غرداية، السنة الجامعية 2025/2024، ص 58.

[3] مجدوب لامية، **المرجع السابق**، ص 115.

نستخلص من هذه المراحل أن الإجراءات الجزائرية تسعى إلى استلهام أفضل الممارسات الدولية في مجال الجرائم الرقمية، غير أننا نرى أن سلسلة الحيازة تظل نقطة ضعف محتملة إذا لم يتم توثيقها بشكل آلي وليس يدوياً فقط، إذ أن التلاعب قد يطال المحضر نفسه، ونلاحظ أن أهمية حساب الهاش تكمن في كونها الخطوة الأكثر موضوعية وعلمية في هذه السلسلة، حيث تخرجنا من دائرة الشك إلى دائقة اليقين التقني، كما نعتقد أن التشريع الجزائري، من خلال إقراره بضرورة استخدام برمجيات متخصصة، يعترف ضمناً بأن الأدلة الرقمية تحتاج إلى معاملة خاصة تختلف كلياً عن الأدلة المادية التقليدية، ونرى أن التحدي الأكبر يبقى في ضمان أن يتمتع القضاة والمحامون بأدنى مستوى من الوعي التقني لفهم دلالات قيمة الهاش ووزنها الإثباتي.

رابعا: القيمة الإثباتية لإجراءات التحرير الرقمي أمام القضاء الجزائري

إن الاعتراف القانوني بالأدلة الرقمية في التشريع الجزائري قد توطد بشكل خاص مع صدور قانون 18-07 المتعلق بالتوقيع الإلكتروني والشهادة الإلكترونية، والذي يضفي الشرعية على استخدام التوقيعات الرقمية والشهادات الإلكترونية، ومن ثم فإن قيمة الهاش تكتسب قوة إثباتية خاصة عند مقارنتها بالقيمة الأصلية للمستند، فإذا تطابقت القيمتان يؤكد ذلك سلامة المستند وعدم تعرضه للتلاعب، وإذا اختلفتا يكون دليلاً قاطعاً على وقوع تزوير، كما أن المحكمة الجزائرية أصبحت بإمكانها الاعتماد على هذه التقنيات في إدانة المتورطين في جرائم التزوير الرقمي، شريطة أن تتم الإجراءات وفقاً للضوابط القانونية والتقنية المعمول بها، وأن يتم تقديم شهادات الخبراء المختصين أمام القاضي لتوضيح آلية العمل، وقد تناولت الدراسات القانونية التحديات التي تواجه العقود الإلكترونية والإثبات الرقمي في القانون الجزائري[1]، كما أشارت الدراسات إلى أن السياسة الجنائية في ظل قانون 24-02 المتعلق بمكافحة التزوير قد أكدت على ضرورة مواكبة التطورات التكنولوجية في مجال الإثبات[2].

نرى أن القيمة الإثباتية لقيمة الهاش لا تنحصر في كونها دليلاً مادياً على وقوع التزوير، بل تمتد لتشكل ضمانة لحقوق المتعاملين في الفضاء الإلكتروني، ونلاحظ أن المحكمة الجزائرية، حين تقبل بهذا النوع من الأدلة، إنما تؤسس لعصر جديد من العدالة الرقمية، غير أننا نعتقد أن هذا القبول يظل مشروطاً بمدى استقلالية الخبير التقني ونزاهته، إذ أن أي خطأ في حساب القيمة أو في توثيقها قد يؤدي إلى إبطال الدليل برمته، ونستخلص أن التحدي المستقبلي للمشرع الجزائري يكمن في وضع معايير دقيقة لاعتماد الخبراء الرقميين وتوحيد

[1] بن زيدان زوينة، **التأسيس النظري لعقود الأعمال الرقمية**، ندوة تكوينية لصالح الطلبة تحت عنوان: التحديات القانونية لعقود الأعمال الرقمية ، جامعة الجزائر 1، ص 117.

[2] دارم عبد القادر، حدوش جلال، **المرجع السابق**، ص59.

إجراءات التحقيق الإلكتروني، حتى تظل قيمة الهاش حصناً منيعاً ضد التزوير الإلكتروني، وليست مجرد رقم عابر في ملف قضائي معقد.

المطلب الثالث: الأساليب التحقيقية الخاصة

تستوجب طبيعة جرائم التزوير الرقمي – التي تُرتكب في فضاء افتراضي عابر للحدود وغير مرئي – اللجوء إلى أساليب تحقيقية خاصة تتجاوز الإجراءات التقليدية، تتمثل في اعتراض المراسلات الإلكترونية والمراقبة التقنية للأنظمة والتسرب الإلكتروني المُوجَّه[1]، ولقد أجاز القانون رقم 09-04 في المادة 4 "إجراء عمليات مراقبة للاتصالات الإلكترونية وجمع وتسجيل محتواها بشكل فوري"[2]، مُقرِّراً بذلك صفة الشرعية القانونية لهذه الأساليب التي تمسُّ جوهر الحقوق والحريات الأساسية.

غير أن هذا التوسع في سلطات التحري يُثير إشكاليةً جوهريةً تتعلق بمدى توافقها مع الحق في الخصوصية وحماية المعطيات الشخصية المكفولة دستورياً[3]، خاصةً وأن المراقبة الإلكترونية تُتيح الولوج إلى الأنظمة المعلوماتية "ولو عن بعد" دون علم صاحبها[4]، وقد اقتضى التوفيق بين فعالية المكافحة وحماية الحقوق إقرار ضمانات إجرائية رصينة، تتمثل في اشتراط أمر كتابي مسبق من النيابة العامة أو قاضي التحقيق، مع تقييد مدة المراقبة[5].

الفرع الأول: اعتراض المراسلات الالكترونية وتسجيلها

إننا وإذ نتناول إجراءات اعتراض المراسلات الإلكترونية وتسجيلها في إطار مكافحة جريمة التزوير الرقمي، نجد أنفسنا أمام إشكالية قانونية وتقنية معقدة تتجاذبها مطلبان متساويان في الأهمية: الأول يتمثل في ضرورة تفعيل آليات الكشف عن الجريمة الرقمية وإدانة مرتكبيها، والثاني يتمثل في ضرورة حماية الحقوق الدستورية للأفراد وعلى رأسها حرمة المراسلات وسرية الاتصالات، ومن ثم يتعين علينا أن نستحضر التوازن الدقيق الذي يسعى إليه المشرع الجزائري بين هذين المطلبين، خاصة مع التطور المتسارع للجرائم الإلكترونية التي باتت تستغل الفضاء الرقمي في تزوير المستندات والتوقيعات الإلكترونية، مما يجعل من اعتراض المراسلات الإلكترونية وتسجيلها أداة تحقيقية حاسمة لا غنى عنها، ومن هنا تبرز أهمية هذا الفرع في محاولة

---

[1] حشمان عمار، **المرجع السابق**، ص 48.

[2] المادة 4 من القانون رقم 09-04 المؤرخ في 5 اوت 2009، المتعلق بالوقاية من الجرائم المرتبطة بتكنولوجيات الاعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47، الصادر بتاريخ 16 أوت 2009.

[3] حشمان عمار، **المرجع السابق**، ص50.

[4] المادة 5 من القانون رقم 09-04 المؤرخ في 5 اوت 2009، المتعلق بالوقاية من الجرائم المرتبطة بتكنولوجيات الاعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47، الصادر بتاريخ 16 أوت 2009.

[5] أحمد مسعود مريم، قريشي محمد، **المرجع السابق**، ص20.

تفكيك الإطار القانوني والدستوري والإجرائي لهذه الآلية، والتساؤل عن مدى كفاية التشريع الجزائري في تأطيرها بما يضمن فعالية المكافحة دون المساس بالحريات الأساسية.

أولا: الإطار القانوني والدستوري لاعتراض المراسلات الإلكترونية في التشريع الجزائري

يستند الإطار القانوني لاعتراض المراسلات الإلكترونية في الجزائر إلى مبادئ دستورية راسخة تضمن حرمة المراسلات وسرية الاتصالات، إذ نصت المادة 46 من الدستور الجزائري على هذا المبدأ الأساسي بوصفه أحد مقومات الحياة الخاصة للأفراد التي لا يجوز المساس بها إلا في حالات استثنائية محددة[1]، غير أن المشرع أدرك أن سرية هذه المراسلات قد تستغل في ارتكاب جرائم إلكترونية خطيرة تستهدف أمن الدولة والاقتصاد الوطني، ومن ثم سمح بخروج استثنائي عن هذا المبدأ في ظروف معينة تقتضيها المصلحة العامة، شريطة أن تتم الإجراءات بأمر قضائي صريح وتحت رقابة صارمة تضمن عدم التعسف[2]، وقد أكدت الدراسات القانونية المتخصصة أن هذا التوازن يمثل تحدياً حقيقياً للمشرع الجزائري، إذ يتعين عليه أن يوفق بين متطلبات مكافحة الجريمة وحماية الحقوق الدستورية للأفراد[3]، وفي سياق متصل، يعد قانون 04-09 المتعلق بالوقاية من الجرائم المرتبطة بتكنولوجيا المعلومات والاتصالات الصادر عام 2009 حجر الزاوية في التصدي للجرائم الإلكترونية بما فيها التزوير الرقمي، حيث وسع التعريف بالتزوير ليشمل البيئة الرقمية ونص على عقوبات مشددة تصل إلى عشر سنوات حبساً وغرامات مالية كبيرة[4]، أما قانون 02/24 المتعلق بمكافحة التزوير واستعمال المزور فقد جاء ليعزز هذا الإطار بتوفير آليات جديدة وعقوبات وتدابير مشددة تستهدف على وجه الخصوص تزوير التوقيعات الإلكترونية والمحررات الرقمية[5].

نرى أن المشرع الجزائري قد نجح في رسم توازن دستوري دقيق بين حماية الخصوصية وضرورة مكافحة الجريمة، غير أننا نلاحظ أن التحدي يكمن في التطبيق العملي لهذه الضوابط، إذ أن سرعة التطور التكنولوجي قد تجاوزت في بعض الأحيان القدرة التشريعية على المواكبة، ونستخلص أن الاعتراض الإلكتروني، رغم ما يثيره من مخاوف على الحريات الفردية، يظل ضرورة قصوى في عالم يعتمد بشكل متزايد على الاتصالات

[1] مقلاتي مونة، بوخميس سهيلة، **الحق في اعتراض سرية الاتصالات والمراسلات في التشريع الجزائري**، المجلة الأكاديمية للبحوث القانونية والسياسية، جامعة عمار ثليجي الأغواط، المجلد 03، العدد 02، منشور بتاريخ 24 أكتوبر 2019، ص 122.

[2] مقلاتي مونة، بوخميس سهيلة، **المرجع نفسه**، ص123.

[3] أحمد غلاب، زهرة كيسي، **اجراءات اعتراض المكالمات السلكية واللاسلكية كالية لمتابعة جرائم المخدرات**، مجلة تحولات، جامعة قاصدي مرباح ورقلة، المجلد 02، العدد 01، منشور بتاريخ 01 جانفي 2019، ص 264.

[4] القانون رقم 09-04 المؤرخ في 5 اوت 2009، المتعلق بالوقاية من الجرائم المرتبطة بتكنولوجيات الاعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47، الصادر بتاريخ 16 أوت 2009.

[5] القانون رقم 24-02 المؤرخ في 26 فيفري 2024، المتعلق بمكافحة التزوير واستعمال المزور، الجريدة الرسمية، العدد 15، الصادر بتاريخ 29 فيفري 2024.

الرقمية في ارتكاب الجرائم، ونعتقد أن التشريع الجزائري، من خلال إقراره بالأمر القضائي كشرط أساسي للاعتراض، يضع ضمانة قانونية تحول دون التعسف في استخدام هذه الآلية، لكنه يظل بحاجة إلى مزيد من التوضيح فيما يتعلق بتطبيقات التواصل الحديثة كالمراسلة الفورية المشفرة والمنصات الرقمية المتطورة.

ثانيا: جريمة التزوير الرقمي وعلاقتها باعتراض المراسلات الإلكترونية

يُعرّف التزوير الرقمي في التشريع الجزائري بأنه تعديل أو إدخال غير مشروع للمعلومات باستخدام وسائل إلكترونية أو نظام معلومات، بقصد الإضرار بالغير أو تحقيق منفعة غير مشروعة، ويشمل ذلك تزوير المستندات الرقمية والتوقيعات الإلكترونية والتلاعب بالبيانات المحفوظة[1]، ويُعتبر هذا الشكل من التزوير ركيزة أساسية في الجرائم الإلكترونية، إذ يتم استخدام التوقيع الإلكتروني أو نسخه أو تقليده لإبرام عقود أو معاملات غير مشروعة دون علم صاحبه[2]، وفي سياق مكافحة هذه الجريمة، يُعد اعتراض المراسلات الإلكترونية أداة تحقيقية حاسمة، إذ يمكن من خلالها تتبع مسار الجناة وتحديد هويات المتورطين وكشف كيفية تنفيذ الجريمة، خاصة أن الجناة يستخدمون غالباً بريداً إلكترونياً أو تطبيقات مراسلة تحتوي على مستندات مزورة أو توقيعات إلكترونية مزيفة[3]، وقد تناولت الدراسات المقارنة مدى مواجهة المشرع الجزائري لهذه التحديات، مؤكدة أن التزوير الإلكتروني يتطلب أدوات تحقيقية خاصة تختلف عن الجرائم التقليدية[4].

نستخلص أن العلاقة بين جريمة التزوير الرقمي واعتراض المراسلات الإلكترونية علاقة تكاملية لا تقتصر على مجرد جمع الأدلة، بل تمتد إلى فهم آليات ارتكاب الجريمة منذ مراحلها الأولى، ونلاحظ أن التزوير الإلكتروني، بخلاف التزوير التقليدي، يترك آثاراً رقمية قابلة للتتبع إذا ما تم الاعتراض في الوقت المناسب، ونرى أن المشرع الجزائري، حين أدرج التزوير الرقمي ضمن جرائم المعلوماتية، إنما أقر بأن هذه الجرائم تتطلب أدوات تحقيقية خاصة تختلف عن الجرائم التقليدية، ونعتقد أن اعتراض المراسلات يمثل الخطوة الأولى في سلسلة الإثبات، لكنه يظل رهيناً بوجود خبراء تقنيين قادرين على تحليل البيانات المحصلة وفقاً للمعايير القانونية المعمول بها.

ثالثا: تسجيل المراسلات الإلكترونية كآلية لتوثيق الأدلة الرقمية في قضايا التزوير

إن تسجيل المراسلات الإلكترونية يُعد أداة قيمة لإنشاء سجل زمني ملموس للأحداث وتقديم دليل على مسار الجريمة نفسها، حيث يتضمن حفظ وتوثيق الرسائل الرقمية سواء كانت لأغراض تحقيقية أو كجزء من

[1] هاجر طبا، صبرينة مقالتي، **المرجع السابق**، ص60.

[2] معمري ايمان، فضيلة شعبان، **المرجع السابق**، ص 32.

[3] هاجر طبا، صبرينة مقالتي، **المرجع السابق**، ص61.

[4] معمري ايمان، فضيلة شعبان، **المرجع السابق**، ص 33.

إجراءات التقاضي[1]، وقد سمح القانون الجزائري بتسجيل المراسلات الإلكترونية في إطار التحقيقات الجنائية شريطة أن تتم بأمر قضائي ووفقاً للإجراءات القانونية المقررة، ويهدف هذا الشرط إلى ضمان جمع الأدلة بطريقة قانونية وعادلة مع الحفاظ على حقوق المتهمين[2]، وفي سياق متصل، تؤكد الدراسات القانونية أن تسجيل المراسلات يلعب دوراً محورياً في قضايا تزوير التوقيع الإلكتروني، إذ يمكن من خلاله تسجيل عمليات الدخول والخروج وتعديل المستندات وتبادل البيانات التي تكشف عن الوصول غير المشروع إلى المحتوى، كما أن هذه السجلات تساعد في توفير أدلة قوية تساعد القضاء على اتخاذ قراراته المستنيرة[3]، وقد تناولت دراسة متخصصة إجراءات التسريب والتقاط الصور كإجراءات تحقيق قضائي مكملة للتسجيل[4].

نرى أن تسجيل المراسلات الإلكترونية يمثل ضمانة مزدوجة: الأولى للمجتمع من خلال توفير أدلة قوية تساعد القضاء على اتخاذ قراراته المستنيرة، والثانية للعدالة الجنائية من خلال ضمان عدم تعرض المتهم للظلم، ونلاحظ أن القيمة الإثباتية للتسجيل الرقمي تفوق في دقتها التسجيلات التقليدية، إذ أن البيانات الرقمية تحمل بصمات زمنية ومعرفات تقنية يصعب التلاعب بها إذا ما تم توثيقها بشكل سليم، ونستخلص أن التحدي الأكبر يكمن في ضمان سلامة هذه السجلات من التلف أو التعديل خلال فترة التخزين، مما يقتضي استخدام تقنيات حماية متقدمة تضمن بقاء الدليل الرقمي صالحاً للعرض أمام المحكمة.

رابعا: الضوابط القانونية والقضائية لاعتراض وتسجيل المراسلات وعلاقتها بمكافحة التزوير الرقمي

تخضع إجراءات اعتراض وتسجيل المراسلات الإلكترونية في الجزائر لضوابط قانونية صارمة تهدف إلى ضمان مشروعيتها وعدم تعسف استخدامها في انتهاك حقوق الأفراد، حيث نصت المادة 340 مكرر من قانون العقوبات على تجريم اعتراض المراسلات دون ترخيص قضائي، مما يؤكد على التوازن الدقيق بين مكافحة الجريمة وحماية الخصوصية[5]، وقد تناولت الدراسات المستقبلية التحديات التي تواجه التشريعات الجزائرية في

---

[1] جميلة محلق، **اعتراض المراسلات، تسجيل الأصوات والتقاط الصور في قانون الاجراءات الجزائية الجزائري**، مجلة التواصل في الاقتصاد والادارة والقانون، جامعة باجي مختار عنابة، العدد 42، جوان 2015، ص 25.

[2] جميلة محلق، **المرجع نفسه**، ص 26.

[3] عمارة فوزي، **اعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كاجراءات تحقيق قضائي في المواد الجنائية**، مركز المعرفة الرقمي، منشور سنة 2010، تم الاطلاع عليه يوم 25 أفريل 2026، على الساعة 13:46، على الرابط: https://ddl.ae/book/5180436

[4] عمارة فوزي، **اعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كاجراءات تحقيق قضائي في المواد الجنائية**، مركز المعرفة الرقمي، منشور سنة 2010، تم الاطلاع عليه يوم 25 أفريل 2026، على الساعة 13:46، على الرابط: https://ddl.ae/book/5180436

[5] مقلاتي مونة، بوخميس سهيلة، **المرجع السابق**، ص124.

مواكبة التطورات التكنولوجية المستمرة في أساليب الجريمة السيبرانية[1]، وفي إطار مكافحة التزوير الرقمي تحديداً، نجد أن المحكمة العليا قد أصدرت أحكاماً متعلقة بجرائم التزوير في المحررات الإلكترونية[2]، كما تناولت دراسة بعنوان "جريمة تزوير التوقيع الإلكتروني في التشريع الجزائري" العقوبات المقررة لهذه الجرائم[3]، وأشارت دراسة أخرى إلى ضرورة مواكبة التطورات التكنولوجية في التشريعات الجزائرية لضمان فعالية المكافحة[4]، وقد تطرقت دراسة متخصصة إلى التحديات التشريعية المستجدة بين الطابع الشخصي ورهانات التطبيق[5].

نعتقد أن الضوابط القانونية الواردة في المادة 340 مكرر من قانون العقوبات تمثل حجر الزاوية في ضمان مشروعية اعتراض المراسلات، إذ أن تجريم الاعتراض غير المشروع يخلق رادعاً قانونياً يحول دون استخدام هذه الآلية بشكل عشوائي، ونلاحظ أن التشريع الجزائري، رغم تطوره، يظل بحاجة إلى مزيد من التفصيل فيما يتعلق بإجراءات اعتراض المراسلات عبر التطبيقات المشفرة والشبكات الافتراضية الخاصة، ونستخلص أن فعالية مكافحة التزوير الرقمي مرهونة بمدى قدرة القضاء الجزائري على تطوير آليات الرقابة القضائية على عمليات الاعتراض والتسجيل، وضمان أن تتم هذه العمليات بما يتوافق مع المعايير الدولية لحقوق الإنسان، وأن يتم تكوين القضاة والمحامين بما يكفي لفهم التعقيدات التقنية المرتبطة بالأدلة الرقمية.

الفرع الثاني: المراقبة الالكترونية والولوج الى الأنظمة

إننا وإذ نتناول موضوع المراقبة الإلكترونية والولوج إلى الأنظمة في إطار مكافحة جريمة التزوير الرقمي، نجد أنفسنا أمام منظومة قانونية وتقنية مترابطة، إذ لم يعد التزوير مقتصراً على المحررات الورقية التقليدية، بل امتد ليشمل الفضاء الرقمي بكامله مستغلاً نقاط الضعف في الأنظمة المعلوماتية والمنصات الإلكترونية، ومن ثم يتعين علينا أن نستحضر الآليات المزدوجة التي اعتمدها المشرع الجزائري: آلية وقائية تقوم على المراقبة الإلكترونية كبديل عقابي وتقنية رقابية، وآلية قمعية تستهدف الولوج غير المشروع إلى الأنظمة بوصفه جريمة مستقلة ووسيلة أساسية للتزوير الرقمي، ومن هنا تبرز أهمية هذا الفرع في محاولة تفكيك الإطار التشريعي

---

[1] **مخاطر الجريمة الالكترونية في عام 2026: قراءة قانونية– تقنية في التهديدات المستجدة وسبل الوقاية**، منصة مكتب النشاشيبي للمحاماة، منشور سنة 2026، تم الاطلاع عليه يوم 25 أفريل 2026، على الساعة 14:22، على الرابط: https://nashashibilaw.weebly.com/magazine/-20257338351

[2] ايهاب فوزي السقا، **جريمة التزوير في المحررات الالكترونية**، منصة المحكمة العليا، منشور سنة 2008، تم الاطلاع عليه يوم 25 أفريل 2026، على الساعة 14:25، على الرابط: https://coursupreme.dz

[3] راضية مشري، **المرجع السابق**، ص 98.

[4] سعيدة بوزنون، **المرجع السابق**، ص 59.

[5] **مخاطر الجريمة الالكترونية في عام 2026: قراءة قانونية– تقنية في التهديدات المستجدة وسبل الوقاية**، منصة مكتب النشاشيبي للمحاماة، منشور سنة 2026، تم الاطلاع عليه يوم 25 أفريل 2026، على الساعة 14:22، على الرابط: https://nashashibilaw.weebly.com/magazine/-20257338351

المتكامل الذي يؤطر هاتين الآليتين، والتساؤل عن مدى فعالية هذا الإطار في تحقيق التوازن بين حماية الأنظمة الرقمية وضمان حقوق الأفراد.

أولا: المراقبة الإلكترونية كآلية وقائية وعقابية في مواجهة التزوير الرقمي

يعد نظام المراقبة الإلكترونية، المعروف بـ"السوار الإلكتروني"، من التطورات المهمة في السياسة العقابية الجزائرية، إذ أقره المشرع بموجب القانون المتمم والمعدل لقانون تنظيم السجون رقم 18-01، ويهدف هذا النظام إلى تحقيق أهداف ثلاثة رئيسية: أولها التفريد العقابي بتكييف العقوبة بما يتناسب مع حالة المحكوم عليه، وثانيها إعادة الإدماج الاجتماعي للمحكوم عليه مع الحفاظ على روابطه الأسرية والمهنية، وثالثها تخفيف الاكتظاظ داخل المؤسسات العقابية[1]، ويصدر قرار الوضع تحت المراقبة الإلكترونية من قبل قاضي تطبيق العقوبات شريطة أن لا تتجاوز العقوبة الأصلية ثلاث سنوات[2]، وفي سياق مكافحة التزوير الرقمي تلعب هذه الآلية دوراً حاسماً إلى جانب التشريعات الجنائية، إذ تمكن السلطات من مراقبة الأنشطة الإلكترونية للمحكوم عليهم وكشف محاولات الاختراق والتلاعب بالبيانات، كما تتطلب التحقيقات المتعلقة بهذه الجرائم استخدام تقنيات متطورة في التحليل الجنائي الرقمي مع التركيز على جمع الأدلة بطرق قانونية وموثوقة[3].

نستخلص أن إدخال السوار الإلكترونية كبديل عن العقوبات السالبة للحرية يمثل نهجاً عقلانياً يراعي التطورات العقابية الحديثة، غير أن فعاليته في مكافحة التزوير الرقمي تبقى محدودة إذا لم ترافقه آليات تقنية متطورة لمراقبة الأنشطة الإلكترونية وليس مجرد تحديد الموقع الجغرافي، ونرى أن المشرع الجزائري، من خلال هذا النظام، يعترف ضمناً بأن العقوبة السجنية التقليدية غير كافية في مواجهة الجرائم الرقمية المعقدة، ونعتقد أن المراقبة الإلكترونية يجب أن تشمل مراقبة الاتصالات الرقمية والولوج إلى الشبكات بشكل خاص حين يتعلق الأمر بمرتكبي التزوير الإلكتروني.

ثانيا: الولوج غير المشروع إلى الأنظمة كجريمة مستقلة ووسيلة للتزوير الرقمي

يُعد الولوج غير المشروع إلى الأنظمة الإلكترونية جريمة إلكترونية مستقلة بذاتها في التشريع الجزائري، إذ يقوم المتسلل بالولوج إلى نظام بنكي مثلاً لتغيير أرصدة أو إصدار أوامر دفع مزورة، ويرتبط هذا الفعل ارتباطاً وثيقاً بجريمة التزوير الرقمي حيث يمثل الولوج غير المشروع أداة يستخدمها الجاني لارتكاب تزوير رقمي

[1] معمري ايمان، فضيلة شعبان، **المرجع السابق**، ص 19.

[2] القانون 24-02 المؤرخ في 26 فيفري 2024، المتعلق بمكافحة التزوير واستعمال المزور، الجريدة الرسمية، العدد 15، الصادر بتاريخ 29 فيفري 2024.

[3] معمري ايمان، فضيلة شعبان، **المرجع السابق**، ص22.

ناجح[1]، وقد شدد قانون 24-02 على معاقبة أفعال الولوج غير المشروع بشدة، خاصة إذا كانت مرتبطة بأغراض إجرامية كالتزوير، مع التأكيد على أهمية استخدام تقنيات التشفير ومراقبة الشبكات للكشف عن هذه الأفعال ومنعها[2]، كما تعزز التشريعات من دور الجهات الأمنية في رصد الاختراقات وحماية الأنظمة من التلاعب بالبيانات[3].

نلاحظ أن المشرع الجزائري قد نجح في تجريم الولوج غير المشروع كجريمة مستقلة، لكنه يظل بحاجة إلى مزيد من التوضيح فيما يتعلق بالتمييز بين الولوج البسيط والولوج المؤدي إلى تزوير البيانات، ونستخلص أن العلاقة بين الولوج والتزوير علاقة سببية مباشرة في معظم الحالات، إذ لا يمكن تصور تزوير رقمي ناجح دون اختراق مسبق للنظام المستهدف، ونعتقد أن تشديد العقوبات في قانون 24-02 يرسل رسالة واضحة بأن الفضاء الرقمي ليس منفصلاً عن السيادة القانونية للدولة، وأن فعالية هذا التجريم مرهونة بقدرة الأجهزة الأمنية على رصد الاختراقات في وقتها الفعلي.

ثالثا: الإطار التشريعي المتكامل واستراتيجية التحول الرقمي

لم يأتِ الاعتراف بالمراقبة الإلكترونية والولوج إلى الأنظمة من فراغ، بل استند إلى منظومة تشريعية متكاملة تتضمن قانون 24-02 المتعلق بمكافحة التزوير واستعمال المزور، وقانون 09-04 المتعلق بالوقاية من الجرائم المرتبطة بتكنولوجيا المعلومات والاتصالات الذي وفر إطاراً وقائياً للمراقبة الإلكترونية، وقانون 06-22 المتعلق بالبحث والتحري الذي يشمل أساليب تقنية لجمع الأدلة الرقمية وتتبع المجرمين الإلكترونيين، بالإضافة إلى قانون 18-01 المتمم والمعدل لقانون تنظيم السجون[4]، كما تسعى الجزائر من خلال استراتيجية "جزائر رقمية 2030" إلى تحقيق تحول رقمي شامل نحو حكومة أقل بيروقراطية وأكثر رقمية، تتضمن اعتماد تقنيات حديثة للتشفير ومصادقة البيانات لتأمين المعاملات الحكومية، مما يجعل اختراق الأنظمة وتزوير الوثائق الرقمية أكثر صعوبة، ويدعم جهود الأجهزة الأمنية والقضائية في كشف الجرائم الرقمية والتحقيق فيها[5]، بالإضافة إلى مصادقة الجزائر على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

نرى أن استراتيجية التحول الرقمي تمثل سيفاً ذو حدين، فهي من ناحية تسهل الخدمات وتقلص الفساد، ومن ناحية أخرى تخلق فرصاً جديدة للمتلاعبين إذا لم يتم تأمين الأنظمة بشكل كافٍ، ونلاحظ أن المراقبة

[1] بن صويلح سفيان، حريدي الياس، **المرجع السابق**، ص 99.

[2] أحمد محمد محروس عبد العال، **المرجع السابق**، ص 54.

[3] بن صويلح سفيان، حريدي الياس، **المرجع السابق**، ص 100.

[4] شعباني نوال، **المرجع السابق**، ص 595.

[5] **الاستراتيجية الوطنية للتحول الرقمي في الجزائر**، المندوبية العليا للرقمنة، منشور في أوت 2024، تم الاطلاع عليه يوم 25 أفريل 2026، على الساعة 16:04، على الرابط: https://hcn.dz/SNTN-Ar.pdf

الإلكترونية والولوج المشروع إلى الأنظمة يصبحان أكثر أهمية في ظل هذه الاستراتيجية، إذ أن كل نظام رقمي يصبح عرضة للتزوير كلما كان غير موثق بالتقنيات الأمنية اللازمة، ونستخلص أن نجاح مكافحة التزوير الرقمي في الجزائر مرهون بمدى قدرة هذه الاستراتيجية على دمج البعد الأمني السيبراني في جميع مراحل التحول الرقمي، وليس فقط في مرحلة التشريع، وأن يتم تكوين الموارد البشرية وتزويدها بالكفاءات اللازمة لمواجهة الأساليب المستمرة التطور للجريمة.

الفرع الثالث: التسرب الالكتروني كالية لكشف المزورين

إننا وإذ نتناول موضوع التسرب الإلكتروني في إطار مكافحة جريمة التزوير الرقمي، نجد أنفسنا أمام آلية تحقيقية حديثة تكتسب أهمية متزايدة في ظل التحول الرقمي المتسارع، إذ لم يعد التزوير مقتصراً على التلاعب بالمحررات الورقية التقليدية، بل امتد ليشمل الفضاء الإلكتروني بكامله مستغلاً نقاط الضعف في الأنظمة المعلوماتية والشبكات الرقمية، ومن ثم يتعين علينا أن نستحضر مفهوم التسرب الإلكتروني بوصفه أداة تحقيقية فعالة تستخدمها السلطات القضائية والشرطة في كشف الجرائم الرقمية وجمع الأدلة المرتبطة بالتزوير الإلكتروني، وهو ما يقودنا بشكل طبيعي إلى التساؤل عن الإطار القانوني والشروط الموضوعية والشكلية التي تؤطر هذه الآلية، ومدى كفاية التشريع الجزائري في ضمان فعاليتها دون المساس بالحريات الفردية والخصوصية.

أولا: مفهوم التسرب الإلكتروني وشروطه الموضوعية والشكلية في التشريع الجزائري

يُعرّف التسرب الإلكتروني في التشريع الجزائري بأنه إجراء يقوم به ضابط أو عون من الشرطة القضائية بتنسيق وإشراف قضائي، بهدف جمع معلومات وأدلة حاسمة في تحقيق دقيق، وذلك من خلال التظاهر بكونه شريكاً أو متواطئاً مع المشتبه به في جناية أو جنحة إلكترونية[1]، ويُعتبر هذا الأسلوب ضرورياً في التعمق في الشبكات الإجرامية الرقمية وفهم آليات عمل المزورين، إذ يصعب على السلطات القضائية الحصول على الأدلة المتعلقة بالتزوير الرقمي بالطرق التقليدية نظراً لتطور أساليب الجريمة[2]، وتفرض التشريعات الجزائرية شروطاً صارمة لتطبيق التسرب الإلكتروني تهدف إلى تحقيق التوازن بين فعاليته وحماية الحريات الفردية، منها: الحصول على إذن مسبق من النيابة العامة أو قاضي التحقيق، وضرورة التناسب بين جسامة الجريمة المراد

[1] **الشروط الشكلية والموضوعية لعملية التسرب في القانون الجزائري**، مدونة القانون والتعليم، منشور سنة 2020، تم الاطلاع عليه يوم 25 أفريل 2026، على الساعة 16:20، على الرابط: http://droit7.blogspot.com/2019/09/blog-post_91.html

[2] **التسرب الالكتروني: دوافع نفسية وامكانات ضئيلة**، موقع الرأي، منشور بتاريخ 28 نوفمبر 2020، تم الاطلاع عليه يوم 25 أفريل 2026، على الساعة 16:22، على الرابط: https://alrai.com/article/10564648

كشفها والتسرب الإلكتروني، وإشراف قضائي صارم على العملية، بالإضافة إلى التنسيق بين الضابط القضائي وعون الشرطة القضائية لضمان التزام الإجراءات القانونية وجمع الأدلة بشكل مشروع[1].

نرى أن التسرب الإلكتروني يمثل نقلة نوعية في أساليب التحقيق الجنائي، إذ يتيح للسلطات اختراق الجدار الافتراضي الذي يحيط بالمجرمين الرقميين، غير أننا نلاحظ أن هذه الآلية تحمل في طياتها مخاطر جسيمة على الحقوق الفردية إذا لم يتم احترام الشروط القانونية المحددة، ونستخلص أن المشرع الجزائري، من خلال إقراره بالإذن القضائي المسبق كشرط أساسي، يضع ضمانة قانونية تحول دون تحول التسرب إلى أداة للتجسس العشوائي، ونعتقد أن فعالية هذه الآلية تبقى مرهونة بمدى قدرة الضباط القضائيين على التكيف مع التقنيات الرقمية المتطورة.

ثانيا: دور التسرب الإلكتروني في كشف التزوير الرقمي وجمع الأدلة

يُعتبر التسرب الإلكتروني أداة فعالة في كشف جرائم التزوير الرقمي، إذ يساهم في التتبع الرقمي عبر التعديات التي تطرأ على المستندات الإلكترونية، ويساعد في تحديد مصدر التزوير من خلال سجلات الدخول والخروج، كما يسهل الحصول على أدلة رقمية يصعب اكتشافها بالوسائل التقليدية كرسائل البريد الإلكتروني والمحادثات المشفرة وسجلات المعاملات الرقمية[2]، ويساعد التسرب الإلكتروني أيضاً في تحديد هوية الجناة من خلال تتبع الآثار الرقمية وعناوين IP التي تربط الجناة بالجريمة، بالإضافة إلى دوره في كشف العمليات المشبوهة في المستندات الإلكترونية[3]، وتعتمد آليات الكشف الحديثة على تحديد عناوين IP والآثار الرقمية، وتحليل البيانات التي تمثل سجلات الوصول إلى الخوادم، والتعاون مع الجهات السيبرانية في التحقيقات الرقمية، وهو ما يبرز الحاجة إلى الخبرة الفنية في تحليل الأدلة الرقمية المرتبطة بالتزوير[4].

نرى أن دور التسرب الإلكتروني يتجاوز مجرد جمع الأدلة إلى فهم البنية التحتية للشبكات الإجرامية الرقمية، ونلاحظ أن هذه الآلية تمكن المحققين من رصد الجريمة في طور ارتكابها وليس بعد وقوعها، مما يعزز من فرص الوقاية والحماية، ونستخلص أن فعالية التسرب الإلكتروني في كشف التزوير تبقى مرتبطة بجودة

---

[1] **الشروط الشكلية والموضوعية لعملية التسرب في القانون الجزائري**، مدونة القانون والتعليم، منشور سنة 2020، تم الاطلاع عليه يوم 25 أفريل 2026، على الساعة 16:23، على الرابط: http://droit7.blogspot.com/2019/09/blog-post_91.html

[2] لشخب عبد الحق، جبايلي عبد الرحيم، **جريمة التزوير في التشريع الجزائري**، مذكرة ماستر تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة عباس لغرور خنشلة، السنة الجامعية 2025/2024، ص 17.

[3] القينعي بن يوسف، **اليات الكشف عن جرائم التزوير ومعرفة مرتكبيها على ضوء القانون رقم 24-02**، المجلة الجزائرية للحقوق والعلوم السياسية، جامعة أحمد بن يحي الونشريسي تيسيمسيلت، المجلد 09، العدد 02، منشور بتاريخ 01 جانفي 2024، ص57.

[4] لشخب عبد الحق، جبايلي عبد الرحيم، **المرجع السابق**، ص 18.

التنسيق بين الأجهزة الأمنية والقضائية والخبراء التقنيين، ونعتقد أن غياب هذا التنسيق قد يؤدي إلى فقدان الأدلة الرقمية أو تلويثها، مما يجعلها غير صالحة للعرض أمام المحكمة.

ثالثا: الإطار القانوني المتكامل والتحديات المستقبلية

لم يأتِ الاعتراف بالتسرب الإلكتروني من فراغ، بل استند إلى منظومة تشريعية متكاملة تتضمن قانون 24-02 المتعلق بمكافحة التزوير واستعمال المزور الذي يُعد تحديثاً جوهرياً يدمج جرائم التزوير الرقمي ضمن نصوصه ويعزز القدرة على ملاحقة مرتكبيها[1]، وقد أظهرت الدراسات المقارنة أن مستوى التغطية القانونية لآليات مكافحة التزوير قد تطور بشكل ملحوظ بعد صدور هذا القانون، خاصة فيما يتعلق بأدوات الكشف والضمانات القانونية وخبرة فنية التحقيق[2]، وتتطلع التشريعات المستقبلية إلى الاستفادة من التقنيات الحديثة كالذكاء الاصطناعي في تحليل التسربات ودعم التحقيقات، مما يعزز القدرة على كشف الجرائم الرقمية المعقدة[3]، ويواجه هذا الإطار تحديات تتمثل في ضرورة موازنة فعالية التحقيق مع حماية الحقوق الأساسية للأفراد وخاصة الحق في الخصوصية، بالإضافة إلى الحاجة المستمرة إلى الخبرة الفنية والتعاون الدولي في مواجهة الجرائم الإلكترونية التي تتطور باستمرار[4].

نعتقد أن الإطار القانوني المتكامل الذي وفره قانون 24-02 يمثل خطوة متقدمة في مواجهة التزوير الرقمي، غير أننا نلاحظ أن التحدي الأكبر يكمن في التطبيق العملي لهذه النصوص، إذ أن التحقيقات الرقمية تتطلب بنية تحتية تقنية متطورة قد لا تتوفر في جميع وحدات الشرطة القضائية والنيابات، ونستخلص أن التسرب الإلكتروني، رغم فعاليته، يظل أداة حساسة تتطلب رقابة قضائية مستمرة ودقيقة، ونعتقد أن مستقبل مكافحة التزوير الرقمي في الجزائر مرهون بقدرة المشرع على مواكبة التطورات التقنية بشكل مستمر، وبقدرة الأجهزة القضائية والأمنية على تكوين كوادر متخصصة في المجال السيبراني.

المبحث الثاني: اثبات جريمة التزوير الرقمي والملاحقة القضائية

يشهد العصر الحالي تحولاً رقمياً عميقاً غيّر بشكل جذري من طبيعة العلاقات الإنسانية والمعاملات الاقتصادية والإدارية، إذ أصبح الفضاء الإلكتروني مساحة جديدة للتفاعل الاجتماعي والنشاط التجاري، بل

---

[1] القانون رقم 24-02 المؤرخ في 26 فيفري 2024، المتعلق بمكافحة التزوير واستعمال المزور، الجريدة الرسمية، العدد 15، الصادر بتاريخ 29 فيفري 2024.

[2] وفاء صدراتي، **اليات الحماية القانونية للتوقيع الالكتروني من جرائم التزوير الالكتروني في التشريع الجزائري**، مجلة العلوم القانونية والسياسية، جامعة الشهيد حمه لخضر بالوادي ، المجلد 11، العدد 01، منشور بتاريخ 28 أفريل 2020، ص 580.

[3] سعيدة بوزنون، **المرجع السابق**، ص 110.

[4] القينعي بن يوسف، **المرجع السابق**، ص 58.

وحتى للنشاط الإجرامي، وفي هذا السياق، برزت الجرائم المعلوماتية كظاهرة عالمية تستوجب اهتماماً تشريعياً وقضائياً متزايداً، نظراً لما تمثله من تهديد حقيقي للأمن الاقتصادي والاجتماعي للدول.[1]

إن التزوير الرقمي يعد من أخطر أنواع الجرائم المعلوماتية، إذ أنه يمسّ بأحد الركائز الأساسية لاستقرار المعاملات، ألا وهو صحة الوثائق والبيانات، ففي ظل الاعتماد المتزايد على الوثائق الإلكترونية والتوقيعات الرقمية في مختلف المجالات، أصبح التلاعب بالبيانات الرقمية وسيلة فعّالة لارتكاب جرائم اقتصادية وإدارية ومالية، مما يستدعي وقفة تأملية جدية حول الآليات القانونية المتاحة لمواجهة هذا الخطر.[2]

ومن الملاحظ أن المشرّع الجزائري قد سعى إلى مواكبة هذا التطور من خلال إصدار القانون رقم 09-04 المؤرخ في 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والذي يعتبر الإطار القانوني الأساسي لمعالجة هذه الجرائم في التشريع الجزائري، غير أن هذا النص التشريعي، رغم أهميته، يظل محدوداً في جانبه الإجرائي والإثباتي، مما يطرح إشكاليات جوهرية تتعلق بكيفية إثبات هذه الجرائم أمام المحاكم الجزائية.[3]

إن الإثبات في المادة الجزائية يظل ركيزة أساسية لتحقيق العدالة، إذ لا يكفي أن يكون الفعل مجرّماً قانونياً، بل يجب أن يثبت ارتكابه وفقاً للقواعد الإجرائية المعمول بها، وفي مجال الجرائم المعلوماتية، تتعقد مسألة الإثبات بسبب الطبيعة غير المادية للأدلة الرقمية، وقابليتها للتلف أو التغيير، وصعوبة ربطها بشخص مرتكب محدد.[4]

كما أن الملاحقة القضائية للجرائم الرقمية تواجه تحديات إضافية تتجاوز الإطار الوطني، نظراً للطبيعة العابرة للحدود للإنترنت، التي تجعل من الجريمة المعلوماتية ظاهرة دولية بامتياز، فالجاني قد يرتكب فعله من دولة، مستخدماً خادماً إلكترونياً موجوداً في دولة أخرى، ليؤثر في ضحية تقع في دولة ثالثة، مما يخلق تعقيدات قانونية وقضائية تستوجب تطوير آليات التعاون الدولي.[5]

---

[1] اية بن ميسية، **المرجع السابق**، ص23 .

[2] أوساسي فؤاد، **دور الدليل الرقمي في الاثبات الجنائي**، مذكرة ماستر تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور بالجلفة، الموسم الجامعي 2020/2019، ص 58.

[3] القانون رقم 09-04 المؤرخ في 5 أوت 2009، المتعلق بالوقاية من الجرائم المرتبطة بتكنولوجيات الاعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47، الصادر بتاريخ 16 أوت 2009.

[4] درابلة العمري سليم، **حجية الدليل الرقمي في الاثبات الجنائي**، أطروحة دكتوراه علوم تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر 01، السنة الجامعية 2025/2024، ص 252.

[5] الكثيري سعيد مسعود، **الجريمة الالكترونية في ضوء اتفاقية بودابست: الاطار المفاهيمي والتصنيفي**، مجلة البحوث القانونية والاقتصادية، المركز الجامعي أفلو، المجلد 09، العدد 01، منشور بتاريخ 01 جانفي 2026، ص 944.

وبناءً على ما تقدم، يتبين أن موضوع إثبات جريمة التزوير الرقمي والملاحقة القضائية يشكل قضية مركزية في دراسة الجرائم المعلوماتية، تستوجب النظر الشامل إلى مختلف الأبعاد القانونية والقضائية والتقنية المتعلقة بها، ومن هذا المنطلق، سنعمل في هذا المبحث على تناول ثلاثة محاور رئيسية: المحور الأول يخصص لدراسة حجية الدليل الرقمي في القضاء الجزائري وشروط قبوله، والمحور الثاني يتناول دور الخبرة القضائية والمعلوماتية في كشف التزوير الرقمي، أما المحور الثالث فيركز على تحليل الاختصاص القضائي في جرائم التزوير الرقمي وتحديات الملاحقة القضائية.

المطلب الأول: حجية الدليل الرقمي في القضاء الجزائري

يُعدّ الدليل الرقمي من أبرز التحديات التي تواجه منظومة الإثبات في المادة الجزائية المعاصرة، إذ أن انتشار تكنولوجيات الإعلام والاتصال جعل من الفضاء الإلكتروني مسرحاً جديداً للجرائم، بما فيها جريمة التزوير الرقمي، وفي ظل هذا التطور برزت إشكالية أساسية تتمثل في مدى قبول الدليل الرقمي أمام القضاء الجزائي وتحقيقه لحجيته في الإثبات.[1]

إن المشرّع الجزائري، وإن كان قد أقرّ بضرورة مواكبة هذا التحول عبر إصدار القانون رقم 09-04 المؤرخ في 5 أوت 2009، إلا أن النصوص الإجرائية والقانونية لا تزال تفتقر إلى تنظيم دقيق لحجية هذا النوع من الأدلة، مما يجعل قضاء الموضوع يواجه صعوبات جمة في تقييمه والاعتماد عليه.[2]

ومن هذا المنطلق، سيتم في هذا المطلب تناول مفهوم الدليل الرقمي وشروطه من حيث الموثوقية والنزاهة، ثم بيان القيمة القانونية للمستخرجات الرقمية في الإثبات، وذلك قبل الوقوف على تحديات تزوير الأدلة الرقمية ذاتها.

الفرع الأول: مفهوم الدليل الرقمي وشروطه (الموثوقية والنزاهة)

إننا وإذ نتناول موضوع الدليل الرقمي وشروط قبوله في إطار مكافحة جريمة التزوير الرقمي، نجد أنفسنا أمام تحول جوهري في ميدان الإثبات الجنائي، إذ لم يعد الاعتماد على الأدلة المادية التقليدية كافياً في مواجهة جرائم تستند إلى بنية تقنية معقدة، ومن ثم يتعين علينا أن نستحضر المفهوم الحديث للدليل الرقمي الذي يشمل أي بيانات أو معلومات إلكترونية يتم إنشاؤها أو إصدارها أو تسليمها أو حفظها أو إبلاغها عبر وسائط رقمية، وهو ما يجعل من دراسة شروط قبوله وخاصة الموثوقية والنزاهة أمراً محورياً في فهم كيفية مواجهة التشريع

[1] أوساسي فؤاد، **المرجع السابق**، ص 59.

[2] القانون رقم 09-04 المؤرخ في 5 أوت 2009، المتعلق بالوقاية من الجرائم المرتبطة بتكنولوجيات الاعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47، الصادر بتاريخ 16 أوت 2009.

الجزائري لهذه التحديات، ومن هنا تبرز أهمية هذا الفرع في محاولة تفكيك المفهوم القانوني والتقني للدليل الرقمي والتساؤل عن مدى كفاية الإطار التشريعي الجزائري في ضمان قبوله كحجة أمام المحكمة.

أولا: مفهوم الدليل الرقمي وطبيعته القانونية في التشريع الجزائري

يُعرّف الدليل الرقمي في التشريع الجزائري بأنه أي بيانات أو معلومات إلكترونية يتم إنشاؤها أو إصدارها أو تسليمها أو حفظها أو إبلاغها عبر وسائط رقمية، وتكون هذه البيانات قابلة للاسترجاع والفهم، ويتسع هذا التعريف ليشمل طيفاً واسعاً من البيانات كالرسائل الإلكترونية والسجلات الرقمية (Log files) والملفات المشفرة وبيانات الشبكات والصور والفيديوهات والتسجيلات الصوتية[1]، ويبرز مفهوم الدليل الرقمي أهمية التحول الرقمي في الحياة المعاصرة وتأثيره على الأنظمة القانونية، إذ لم تعد الأدلة المادية التقليدية كافية بمفردها لإثبات وقائع الجريمة في الفضاء السيبراني الذي تتنشأ فيه الجرائم المعقدة[2]، وقد عكست التشريعات الجزائرية هذا التحول من خلال اعترافها بالدليل الرقمي كوسيلة إثبات جنائية، حيث نص قانون 09-04 المتعلق بالوقاية من الجرائم المرتبطة بتكنولوجيا المعلومات والاتصالات الصادر عام 2009 على مبادئ عامة في هذا المجال، وأكد قانون 18-07 المتعلق بالتوقيع الجنائي المعدل الصادر عام 2018 في المادة 61 على حجية الدليل الرقمي في الإجراءات القضائية، كما تناولت المواد 302 ومكرر 303 من قانون الإجراءات الجزائية والقانون المعدل لقانون العقوبات جوانب تتعلق بتزوير التوقيع الجنائي والمستندات الإلكترونية[3].

نرى أن هذا التعريف الشامل للدليل الرقمي يعكس إدراكاً متقدماً لدى المشرع الجزائري بطبيعة الجرائم الرقمية، غير أننا نلاحظ أن التحدي يكمن في تحديد المعايير الدقيقة التي تميز الدليل الرقمي الصالح للقبول عن مجرد بيانات إلكترونية عشوائية، ونستخلص أن التشريع الجزائري، رغم تطوره، يظل بحاجة إلى مزيد من التفصيل فيما يتعلق بتصنيف الأدلة الرقمية حسب درجة قوتها الإثباتية، ونعتقد أن الدليل الرقمي، حين يتم جمعه وتوثيقه بشكل سليم، يمكن أن يكون أكثر دقة وموثوقية من الأدلة التقليدية، لكنه يظل يواجه تحدياً في إقناع القضاء التقليدي بقيمته الإثباتية.

---

[1] رحموني محمد، بن الطيبي امبارك، **شروط قبول الدليل الرقمي كدليل اثبات في الجريمة الالكترونية**، مجلة القانون والعلوم السياسية، المركز الجامعي صالحي أحمد – النعامة، المجلد 05، العدد 02، منشور بتاريخ 31 أكتوبر 2019، ص 21.

[2] رحموني محمد، بن الطيبي امبارك، **المرجع نفسه**، ص 22.

[3] أومدور رجاء، **مفهوم الدليل الرقمي**، مداخلة في الملتقى الدولي حول: أدلة الاثبات الجنائية الحديثة في التشريعات المقارنة، جامعة طاهري محمد – بشار، المنعقد يومي 25 و 26 أفريل 2018، ص 08.

ثانيا: شروط قبول الدليل الرقمي في التشريع الجزائري

تفرض التشريعات الجزائرية شروطاً صارمة لقبول الدليل الرقمي أمام المحكمة تهدف إلى ضمان عدالة الإثبات وموثوقية الأدلة المقدمة، وتتجلى هذه الشروط في معيارين أساسيين هما الموثوقية والنزاهة، بالإضافة إلى شروط تكميلية أخرى تساهم في تعزيز حجيته أمام القضاء[1].

أ). شرط الموثوقية

تُعد الموثوقية شرطاً أساسياً لقبول الدليل الرقمي أمام المحكمة، إذ يجب أن يكون الدليل جديراً بالثقة من حيث مصدره وطريقة جمعه واستخلاصه، ويتطلب هذا الشرط عدة جوانب حيوية منها: الحصول على الدليل بشكل شرعي دون انتهاك حقوق الأفراد أو الخصوصية، واستخدام تقنيات متخصصة وبرمجيات آمنة في استخراج البيانات، وإنشاء بصمة فريدة للدليل (Hashing) باستخدام تقنيات التجزئة التي تضمن عدم تعديله أو تغييره، فضلاً عن ضرورة تدخل خبراء تقنيين معتمدين من الجهات القضائية لشرح الجوانب الفنية للدليل وتحليله وتوثيقه وتقديم تقارير فنية تثبت صحة وسلامة الدليل[2]، وتُعتبر سجلات الوصول (Log files) أدلة قيمة في جرائم التزوير الرقمي، إذ تسجل جميع الأنشطة على الأنظمة الرقمية من هوية المستخدمين وأنماط الوصول والتعديلات، مما يمكن من كشف التلاعب بالمستندات الإلكترونية ويعزز مصداقية الدليل المقدم[3].

ب). شرط النزاهة

تُعني النزاهة بضمان عدم تعرض الدليل الرقمي للتلاعب أو التحريف أو التغيير منذ لحظة جمعه وحتى تقديمه أمام المحكمة، وهو شرط حيوي بشكل خاص في قضايا التزوير الرقمي حيث يكون التلاعب بالبيانات هو هدف الجريمة نفسها[4]، وتتطلب النزاهة عدة ضمانات منها: توثيق سلسلة الحراسة (Chain of Custody) بشكل دقيق وموثق، حيث يجب تحديد كل شخص تعامل مع الدليل منذ لحظة اكتشافه وتحليله ونقله وتخزينه وصولاً إلى تقديمه للمحكمة، واستخدام تقنيات التوقيع الإلكتروني والتشفير لحماية الدليل من الوصول غير المصرح به أو التغيير، بالإضافة إلى الالتزام بالمعايير الدولية للأدلة الرقمية الصادرة عن المنظمة الدولية للتوحيد القياسي (ISO) التي تعزز نزاهة الدليل على نطاق واسع وتضمن قبوله[5].

---

[1] محمد الشريف بوالعراس، أسامة طلحي، **جريمة التزوير المعلوماتية**، مذكرة ماستر تخصص قانون اعلام الي وانترنت، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الابراهيمي– برج بوعريريج، السنة الجامعية 2022/2021، ص 41.

[2] محمد الشريف بوالعراس، أسامة طلحي، **المرجع نفسه**، ص42.

[3] محمد الشريف بوالعراس، أسامة طلحي، **المرجع نفسه**، ص42.

[4] رحموني محمد، بن الطيبي امبارك، **المرجع السابق**، ص 23.

[5] رحموني محمد، بن الطيبي امبارك، **المرجع السابق**، ص 24.

ج). الشروط الأخرى

إلى جانب الموثوقية والنزاهة، تتطلب شروط قبول الدليل الرقمي في التشريع الجزائري عدة معايير أخرى تساهم في تعزيز حجيته أمام القضاء، منها: شرط اليقين الذي يقتضي أن يقدم الدليل معلومات واضحة ومحددة تساهم في بناء قناعة راسخة لدى القاضي حول وقائع الجريمة وتجنب الغموض في ربط التزوير بالجريمة، وشرط المناقشة الحضورية الذي يتيح فحص الدليل ومناقشته أمام القاضي بشكل حضوري مع الاستعانة بالخبراء التقنيين وتقديم فرص الدفاع، وشرط الاسترجاع والفهم الذي يعني أن تكون البيانات الرقمية قابلة للاسترجاع والتحليل والفهم من قبل الجميع لضمان سهولة التعامل مع الدليل وشرحه للمحكمة[1].

نستخلص أن هذه الشروط مجتمعة تمثل منظومة متكاملة تهدف إلى ضمان قبول الدليل الرقمي كحجة قانونية صالحة، ونلاحظ أن الموثوقية والنزاهة يشكلان عموداً فقرياً لا يمكن الاستغناء عنه، بينما الشروط الأخرى تكتسب أهمية تكميلية في ضمان المحاكمة العادلة، ونرى أن التشريع الجزائري قد نجح في وضع إطار قانوني متوازن، غير أن التحدي يكمن في التطبيق العملي لهذه الشروط، إذ أن جمع الدليل الرقمي بما يستوفي جميع هذه المعايير يتطلب تنسيقاً دقيقاً بين الأجهزة الأمنية والقضائية والخبراء التقنيين، ونعتقد أن أي خلل في أحد هذه الشروط قد يؤدي إلى إبطال الدليل برمته، مما يعزز أهمية التوثيق الدقيق في جميع مراحل التحقيق.

الفرع الثاني: القيمة القانونية للمستخرجات الرقمية في الاثبات

إننا وإذ نتناول موضوع القيمة القانونية للمستخرجات الرقمية في إطار مكافحة جريمة التزوير الرقمي، نجد أنفسنا أمام تحول جوهري في ميدان الإثبات الجنائي، إذ لم يعد الاعتماد على الأدلة المادية التقليدية كافياً في مواجهة جرائم تستند إلى بنية تقنية معقدة، ومن ثم يتعين علينا أن نستحضر المفهوم الحديث للمستخرجات الرقمية بوصفها أدلة إلكترونية تكتسب حجية قانونية في التشريع الجزائري، وهو ما يجعل من دراسة شروط قبولها وقيمتها الإثباتية أمراً محورياً في فهم كيفية مواجهة التشريع الجزائري لهذه التحديات، ومن هنا تبرز أهمية هذا الفرع في محاولة تفكيك المفهوم القانوني والتقني للمستخرجات الرقمية والتساؤل عن مدى كفاية الإطار التشريعي الجزائري في ضمان قبولها كحجة أمام المحكمة.

أولا: مفهوم المستخرجات الرقمية وأهميتها في التشريع الجزائري

يشمل الدليل الرقمي في التشريع الجزائري أي معلومات يتم إنشاؤها أو تخزينها أو نقلها إلكترونياً، وتشمل هذه العناصر التي تستخدَم في إثبات حقيقة أو نفيها في الإجراءات القانونية، ويمكن أن تكون أدلة تقدم بصرية

[1] مليكة سعيدان، **تتبع الدليل الرقمي في جرائم المعلوماتية في التشريع الجزائري**، مذكرة ماستر تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر – بسكرة، الموسم الجامعي 2017/2016، ص 83.

وسمعية قد تكون حاسمة في تحديد وقائع الجريمة وسلامتها وأصالتها[1]، وتشمل فئة المستخرجات الرقمية رسائل البريد الإلكتروني والمحادثات الفورية ووسائط التواصل الاجتماعي، كما يمكن أن تشمل الصور والفيديوهات والتسجيلات الصوتية المخزنة رقمياً، وقد أدرك المشرع الجزائري أهمية هذه الأدلة مع تزايد الاعتماد على التكنولوجيا في جميع مناحي الحياة، فسعى إلى تطوير قوانين تضمن قبولها كأدلة في الإجراءات القضائية وتزيد من مرونة المحاكم في التعامل معها، خاصة في سياق جرائم التزوير الرقمي[2].

نرى أن هذا التعريف الشامل للمستخرجات الرقمية يعكس إدراكاً متقدماً لدى المشرع الجزائري بطبيعة الجرائم الرقمية، غير أننا نلاحظ أن التحدي يكمن في تحديد المعايير الدقيقة التي تميز المستخرج الرقمي الصالح للقبول عن مجرد بيانات إلكترونية عشوائية، ونستخلص أن التشريع الجزائري، رغم تطوره، يظل بحاجة إلى مزيد من التفصيل فيما يتعلق بتصنيف المستخرجات الرقمية حسب درجة قوتها الإثباتية، ونعتقد أن المستخرجات الرقمية، حين يتم جمعها وتوثيقها بشكل سليم، يمكن أن تكون أكثر دقة وموثوقية من الأدلة التقليدية، لكنها تظل تواجه تحدياً في إقناع القضاء التقليدي بقيمتها الإثباتية.

ثانيا: الشروط القانونية لقبول المستخرجات الرقمية كأدلة

تفرض التشريعات الجزائرية شروطاً صارمة لقبول المستخرجات الرقمية كأدلة أمام المحكمة تهدف إلى ضمان عدالة الإثبات وموثوقية الأدلة المقدمة، وتتجلى هذه الشروط في عدة معايير أساسية[3].

أ). شرط الأصالة والسلامة: يجب أن تكون المستخرجات الرقمية أصيلة وموثقة منذ إنشائها وأن يكون مصدرها موثوقاً به، ويتم التحقق من ذلك عادةً من خلال تقنيات عبر التشفير والشهادات الرقمية، بالإضافة إلى التحقق من سلسلة الحفظ (Chain of Custody) التي تضمن عدم التلاعب بالمحتوى، وعندما يقع عبء إثبات التزوير على أحد الأطراف يجب التحقق من عدم التلاعب بالبيانات[4].

ب). شرط الحصول المشروع على الدليل: يُشترط أن يتم الحصول على الدليل الرقمي بشكل مشروع ووفقاً للإجراءات القانونية المحددة، فمثلاً إذا تم جمعه في إطار التحقيق في جرائم التزوير الإلكترونية يجب أن

[1] أومدور رجاء، **مفهوم الدليل الرقمي**، مداخلة في الملتقى الدولي حول: أدلة الاثبات الجنائية الحديثة في التشريعات المقارنة، جامعة طاهري محمد – بشار، المنعقد يومي 25 و 26 أفريل 2018، ص 09.

[2] أومدور رجاء، **مفهوم الدليل الرقمي**، مداخلة في الملتقى الدولي حول: أدلة الاثبات الجنائية الحديثة في التشريعات المقارنة، جامعة طاهري محمد – بشار، المنعقد يومي 25 و 26 أفريل 2018، ص 10.

[3] بن لعربي أسماء، الفحلة مديحة، **المرجع السابق**، ص 449.

[4] بن لعربي أسماء، الفحلة مديحة، **المرجع السابق**، ص 450.

يتوافق مع قانون 24-02 المتعلق بمكافحة التزوير المعدل في 2024، وقد تتبنى المحاكم الجزائرية آليات جديدة للتعامل مع الأدلة الرقمية المعللة[1].

ج). شرط الاختصاص القضائي وعدم التلاعب: تتطلب الشروط القانونية للحجية ضمان الاختصاص القضائي الصحيح وعدم التلاعب بالمستخرجات، حيث يجب أن تكون المستخرجات قابلة للخضوع للقواعد العامة للإثبات الجنائي وفقاً للمادة 60 من قانون الإجراءات الجزائية، وغالباً ما يتطلب ذلك الاستعانة بالخبراء التقنيين في الطب الشرعي الرقمي لتوضيح الجوانب التقنية للدليل وضمان فهمه الشامل للقضاة[2].

نستخلص أن هذه الشروط مجتمعة تمثل منظومة متكاملة تهدف إلى ضمان قبول المستخرجات الرقمية كحجة قانونية صالحة، ونلاحظ أن شرط الأصالة والسلامة يشكل عموداً فقرياً لا يمكن الاستغناء عنه، بينما الشروط الأخرى تكتسب أهمية تكميلية في ضمان المحاكمة العادلة، ونرى أن التشريع الجزائري قد نجح في وضع إطار قانوني متوازن، غير أن التحدي يكمن في التطبيق العملي لهذه الشروط، إذ أن جمع المستخرجات الرقمية بما يستوفي جميع هذه المعايير يتطلب تنسيقاً دقيقاً بين الأجهزة الأمنية والقضائية والخبراء التقنيين، ونعتقد أن أي خلل في أحد هذه الشروط قد يؤدي إلى إبطال الدليل برمته.

الفرع الثالث: تحديات تزوير الأدلة الرقمية ذاتها

يشهد العالم المعاصر تحولاً رقمياً متسارعاً، لم تستثن منه الجزائر، إذ أصبح الاعتماد على المعاملات الإلكترونية والوثائق الرقمية في تزايد مستمر، مما خلق بيئة خصبة لنشاط جرائم التزوير الرقمي، وقد برزت معضلة تزوير الأدلة الرقمية ذاتها كإحدى أبرز التحديات التي تواجه المنظومة القانونية الجزائرية المعاصرة، خاصة وأن الطبيعة غير المستقرة لهذه الأدلة تجعلها عرضة للتلاعب والحذف بسهولة، مما يؤثر على حجيتها القانونية أمام المحاكم، وفي هذا السياق، يتطلب التصدي لجرائم التزوير الرقمي تفعيل التعاون بين الكفاءات القانونية والتقنية المتخصصة في الأدلة الجنائية الرقمية، ومواجهة الجرائم العابرة للحدود المحلية والدولية.[3]

أولا: القصور التشريعي وتكييف القوانين

إن المشكلة التي تواجه المنظومة القانونية الجزائرية في مجال مكافحة التزوير الرقمي لا تقتصر على إمكانية تزوير المستندات الرقمية فحسب، بل إن هذا التعقيد يضع عبئاً إضافياً على النظام القانوني والقضائي

[1] عمارة فتيحة، **المرجع السابق**، ص 182.

[2] عمارة فتيحة، **المرجع السابق**، ص 183.

[3] نورهان محمد الربيعي، **اليات الحصول على الأدلة الرقمية واستخدامها كوسائل اثبات في الجرائم الالكترونية**، مجلة الباحث في العلوم القانونية، كلية القانون جامعة اوروك- بغداد، المجلد 05، العدد 2، منشور بتاريخ ديسمبر 2024، ص 159.

في إثبات هذا التزوير[1]، وعلى الرغم من الجهود التشريعية المبذولة، إلا أن التشريعات الجزائرية تزال غير كافية في مواكبة التطورات السريعة، خاصة فيما يتعلق بتقنيات التزوير الرقمي والتوقيع الإلكتروني[2].

وقد شهدت الجزائر خطوة مهمة في هذا الاتجاه بإصدار القانون رقم 09-04 المتعلق بالوقاية من الجرائم المرتبطة بأنظمة المعلومات، المعدل والمتمم عام 2009، والذي يهدف إلى مكافحة التزوير واستعمال المزور من خلال توسيع نطاق القانون ليشمل الأفعال المجرمة المتعلقة بتزوير الوثائق والمحررات التقليدية والسندات والنقود، وصولاً إلى تزوير المعاملات المالية والخدمات الرقمية، بل وحتى الانتحال والألقاب الوظيفية[3]، غير أن هذا القانون، على أهميته، يواجه تحديات تشريعية جوهرية تتمثل في عدم مواكبته للتطورات التكنولوجية المتسارعة، خاصة فيما يتعلق بأساليب التزوير الرقمي المتقدمة والتوقيع الإلكتروني والذكاء الاصطناعي.

كما أن القانون 04/15 المتعلق بالتوقيع الإلكتروني، والذي يحدد القواعد المتعلقة بالتصديق الإلكتروني، يثير تساؤلات عدة حول مدى كفايته في تغطية جريمة تزوير التوقيع الإلكتروني بشكل مباشر، حيث إن النقص في هذا النص يترك ثغرات قد يستغلها المجرمون، مما يصعّب على المحاكم التعامل مع الحالات المعقدة[4]، وفي هذا الإطار، يتطلب الأمر تحديثاً تشريعياً مستمراً يرقى إلى مستوى التحديات التقنية المتطورة التي تواجه الأدلة الرقمية في الجزائر.

نرى أن القصور التشريعي الحالي يمثل العقبة الأساسية التي تحول دون فعالية المنظومة القانونية في مواجهة جرائم التزوير الرقمي، إذ يتبين لنا أن القانون 09-04 رغم كونه خطوة إيجابية، إلا أنه يفتقر إلى المرونة اللازمة لمواكبة التطورات التقنية المتسارعة. نحن نعتقد أن التشريع الجزائري بحاجة ماسة إلى مراجعة شاملة تضع في اعتبارها الخصوصيات التقنية للأدلة الرقمية، وتتجاوز النصوص العقابية التقليدية إلى إقرار آليات تقنية للتحقق والتدقيق، نلاحظ أن غياب نص صريح يجرم تزوير التوقيع الإلكتروني بشكل مستقل يترك ثغرة قانونية خطيرة، مما يستدعي إصدار نصوص تشريعية خاصة تتناول بالتفصيل جرائم التزوير الرقمي بمختلف صورها، مع مراعاة التطورات المستقبلية في مجال الذكاء الاصطناعي والتعلم الآلي.

---

[1] مشري راضية ، **المرجع السابق**، ص 79.

[2] درايلة العمري سليم، **المرجع السابق**، ص249.

[3] **تفاصيل مشروع قانون مكافحة التزوير واستعمال المزور**، الاذاعة الجزائرية، منشور بتاريخ 21 نوفمبر 2023، تم الاطلاع عليه يوم 1 ماي 2026، على الساعة 15:04، على الرابط: https://news.radioalgerie.dz/ar/node/35842

[4] زروقي خديجة، **المرجع السابق**، ص55.

ثانيا: التهديدات التقنية المتطورة وانعكاساتها على الأدلة الرقمية

إن ظهور تقنيات متقدمة مثل "Deepfakes" والتشفير المعقد وأساليب إخفاء البيانات، يجعل تزوير الأدلة الرقمية أكثر إتقاناً وأصعب اكتشافاً، مما يضاعف من صعوبة تحديد أصالتها، وعلى الرغم من أن القانون الجزائري الحالي يعاقب على التزوير الإلكتروني بعقوبات قد تصل إلى 5 سنوات حبساً وغرامات كبيرة، إلا أن القدرة على مواجهة هذه التحديات التكنولوجية تتطلب استثمارات ضخمة في التكنولوجيا الحديثة وتطوير آليات فنية متقدمة للتحقق[1].

إن التشفير المعقد والذكاء الاصطناعي يؤثران بشكل مباشر على قدرة الأجهزة القضائية والتحقيقية على تتبع البيانات وتحليلها، حيث يصبح من شبه المستحيل في بعض الحالات فك التشفير أو التعرف على المحتوى المزور[2]، وفي هذا السياق، يتطلب الأمر تطوير آليات فنية موحدة للتحقق من أصالة الوثائق والتوقيعات الرقمية، مع استخدام تقنيات متقدمة مثل البلوك تشين والبصمات الرقمية لضمان سلامة البيانات ومنع التلاعب بها.

نحن نعتقد أن التهديدات التقنية المتطورة تمثل التحدي الأكبر أمام الأجهزة القضائية الجزائرية، إذ يتبين لنا أن تقنيات "Deepfakes" والتشفير المعقد قد تجعل من الأدلة الرقمية أدوات مزدوجة الاستخدام، فهي في الوقت الذي تخدم فيه سير العدالة، قد تكون وسيلة لتزييف الحقائق وإعاقة سيرها، نرى أن الجزائر مطالبة بالاستثمار العاجل في التكنولوجيا الحديثة وإنشاء مختبرات متخصصة في التحليل الرقمي، تكون مجهزة بأحدث البرمجيات والأدوات التقنية لكشف التزوير الرقمي، نحن نلاحظ أن استخدام تقنية البلوك تشين يمكن أن يكون حلاً مبتكراً لضمان سلامة الأدلة الرقمية، حيث توفر هذه التقنية سجلاً غير قابل للتعديل يضمن أصالة البيانات منذ لحظة إنشائها.

ثالثا: إشكالية الإثبات والحجية القانونية وسلسلة الحفظ

تُعد الطبيعة غير المستقرة للأدلة الرقمية تحدياً رئيسياً من الناحية القانونية، إذ يمكن تعديلها أو حذف البيانات بسهولة وسرعة، مما يجعل إثبات سلامتها وأصالتها أمراً معقداً[3]، وقد نصت المادة 58 من قانون

[1] **الجزائر تتجه الى اصدار قانون جديد للحد من جرائم التزوير**، منصة العربي الجديد، منشور بتاريخ 29 ماي 2023، تم الاطلاع عليه يوم 1 ماي 2026، على الساعة 15:09، على الرابط: https://www.alaraby.co.uk/society

[2] راضية مشري، **المرجع السابق**، ص 130.

[3] خليفي فتيحة، مهداوي محمد صالح، **المرجع السابق**، ص 257.

الإجراءات الجزائية الجزائرية على أن الأدلة الرقمية تكون موثوقة، ولكن غياب آليات فنية موحدة للتحقق يتطلب إجراءات جزائية وقضائية صارمة[1].

إن ضمان حجية الدليل الرقمي يقتضي الحفاظ على سلامته من لحظة جمعه وحتى تقديمه للمحكمة، وهو ما يُعرف بـ"سلسلة الحفظ" (Chain of Custody)، حيث يجب توثيق جميع الخطوات المتخذة لضمان عدم تعرض الأدلة للتلاعب، فأي خلل في هذه السلسلة قد يؤدي إلى فقدان القوة الإثباتية للدليل[2]، وقد ترفض بعض المحاكم هذه الأدلة في القضايا الجزائية لعدم ضمان سلامة سلسلة الحفظ، مما يضعف من فعالية المنظومة القضائية في مواجهة جرائم التزوير الرقمي.

وفي هذا الإطار، يتطلب الأمر تطوير بروتوكولات دقيقة لجمع الأدلة الرقمية وتحليلها وتقديمها أمام المحاكم، مع ضمان توثيق كل مرحلة من مراحل التعامل مع الدليل الرقمي، كما يجب على القضاة والمحامين والخبراء التعرف على كيفية تقييم حجية الأدلة الرقمية بشكل صحيح، وهو ما يستدعي برامج تكوين مستمرة في هذا المجال[3].

نحن نرى أن إشكالية الإثبات تمثل جوهر المشكلة في مجال الأدلة الرقمية، إذ يتبين لنا أن المادة 58 من قانون الإجراءات الجزائية، رغم اعترافها بحجية الأدلة الرقمية، إلا أنها تفتقر إلى تحديد الآليات التقنية التي تضمن هذه الحجية، نحن نعتقد أن مفهوم "سلسلة الحفظ" يجب أن يكون محور اهتمام المشرع الجزائري، فهو الضامن الأساسي لعدم تلاعب الأدلة طوال مسار الدعوى الجزائية، نحن نلاحظ أن رفض بعض المحاكم للأدلة الرقمية لعدم ضمان سلامة سلسلة الحفظ يعكس حالة من عدم الثقة في هذه الأدلة، مما يستدعي وضع بروتوكولات وطنية موحدة لجمع وتحليل وحفظ الأدلة الرقمية، تضمن لها القبول أمام جميع درجات التقاضي.

رابعا: التوازن بين الخصوصية والرقابة ونقص الكفاءات التقنية

إن مسألة حماية الخصوصية تُعد من أبرز التحديات في مجال الأدلة الرقمية، حيث يتطلب جمع هذه الأدلة في كثير من الأحيان الوصول إلى بيانات شخصية حساسة، مما يفرض على النظام القانوني تحقيق توازن دقيق بين حماية حقوق الأفراد في الخصوصية وضرورة جمع الأدلة لإثبات الجرائم، ووفقاً للقانون 18-07 المتعلق بحماية الأفراد وحقوق الخصوصية، يجب وضع آليات صارمة لضمان أن جمع الأدلة لا يقتصر

[1] أبو بكر التيتاوي، الياس مالك قرادي، **جرائم النصب والاحتيال الالكتروني في التشريع الجزائري**، مذكرة ماستر تخصص القانون الجنائي والعلوم الجنائية، معهد الحقوق، المركز الجامعي المقاوم الشيخ امود بن مختار – اليزي، السنة الجامعية 2025/2024، ص 38.

[2] الدكتور محمود، **التوازن بين حماية الحق في الخصوصية ومشروعية الدليل الجنائي الرقمي**، المجلة الافريقية للدراسات القانونية والسياسية، جامعة أحمد دراية– أدرار، المجلد 07، العدد 02، منشور بتاريخ 04 جانفي 2024، ص 103.

[3] أحمد محمد محروس عبدالعال، **المرجع السابق**، ص 52.

على البيانات الحساسة غير ذات الصلة بالجريمة، مع اتخاذ كافة الاحتياطات اللازمة لحماية البيانات الشخصية[1].

ومن جهة أخرى، تفتقر الجهات القضائية في الجزائر إلى خبرات فنية متقدمة في مجال التحقيق في جرائم التزوير الرقمي، وهو ما يعيق التعامل الفعال مع الأدلة الجنائية الرقمية، وكما هو الحال في العديد من البلدان الأخرى، يتطلب التحقيق في هذه الجرائم كفاءات متخصصة في مجالات التشفير وفكه، والطب الشرعي الرقمي، واستعادة البيانات، وتحليلها وفقاً للمعايير الدولية، وقد أوضحت الصورة المرفقة في الوثيقة أهمية المختبرات المتخصصة في تحليل الأدلة الجنائية الرقمية، مما يؤكد على ضرورة تطوير هذه القدرات في الجزائر[2].

وفي هذا السياق، يتطلب الأمر تكويناً مستمراً للقضاة والمحققين على أحدث التقنيات، ليكونوا قادرين على فهم كيفية عمل التزوير الرقمي وكيفية جمع الأدلة الرقمية بشكل صحيح وتحليلها وتقييم حجيتها أمام المحاكم، كما يستدعي الأمر إنشاء هيئة وطنية متخصصة للأمن السيبراني تتولى مسؤولية وضع المعايير وتقديم الدعم التقني وتدريب الكفاءات، وتنسيق الجهود للاستجابة لجرائم التزوير الرقمي[3].

نحن نعتقد أن تحقيق التوازن بين حماية الخصوصية وجمع الأدلة الرقمية يمثل تحدياً أخلاقياً وقانونياً في آن واحد، إذ يتبين لنا أن القانون 18-07، رغم كونه خطوة في الاتجاه الصحيح، إلا أنه يحتاج إلى تفعيل أكبر على أرض الواقعن نحن نرى أن نقص الكفاءات التقنية المتخصصة يمثل عائقاً خطيراً أمام تطوير المنظومة القضائية الجزائرية، فلا يمكن لقاضٍ أو محقق غير مطلع على التقنيات الرقمية أن يتعامل بفعالية مع أدلة معقدة تتطلب خبرة تقنية عالية، نلاحظ أن الجزائر بحاجة ماسة إلى إنشاء هيئة وطنية للأمن السيبراني تكون مسؤولة عن تنسيق الجهود الوطنية، وتقديم الدعم التقني للجهات القضائية، وتنظيم برامج التكوين المستمر للقضاة والمحامين والخبراء في مجال الأدلة الجنائية الرقمية.

المطلب الثاني: دور الخبرة القضائية والمعلوماتية

تُعدّ الخبرة القضائية ركيزة أساسية في منظومة الإثبات الجنائي، إذ أن القاضي الجزائي غالباً ما يعجز عن فهم الآليات التقنية المعقدة التي تحيط بالجرائم المعلوماتية، ومنها جريمة التزوير الرقمي، وفي ظل هذا

---

[1] ليلى بن برغوث، **الأمن السيبراني وحماية خصوصية البيانات الرقمية في الجزائر في عصر التحول الرقمي والذكاء الاصطناعي**، المجلة الدولية للاتصال الاجتماعي ، جامعة عبد الحميد بن باديس– مستغانم، المجلد 10، العدد 01، منشور بتاريخ 31 مارس 2023، ص 445.

[2] والي أمير، بلعلمي اسحاق، **مكافحة جريمة التزوير الالكتروني في الجزائر**، مذكرة ماستر تخصص قانون اعلام الي، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الابراهيمي،– برج بوعريريج، السنة الجامعية 2023/2022، ص 67.

[3] عمارة فتيحة، المرجع السابق ، ص 188.

العجز يصبح الاستعانة بالخبير المعلوماتي ضرورة ملحّة لكشف آثار التلاعب الرقمي وتقديم تفسيرات تقنية دقيقة أمام قاضي الموضوع.[1]

إن قانون الإجراءات الجزائية الجزائري الصادر بالأمر رقم 66-155 المؤرخ في 8 جوان 1966، قد نظّم الخبرة القضائية في مواده المتعلقة بالتحقيق الجنائي، غير أن هذه النصوص ظلت عامة ولم تُخصّص بما يكفي للخبرة المعلوماتية، مما يطرح إشكالية تكييف هذه الأحكام على الجرائم الرقمية.[2]

ومن هذا المنطلق، سيتم في هذا المطلب تناول استعانة القضاء بالخبراء في المعلوماتية، ثم بيان مهام الخبير الرقمي في كشف التزوير، وذلك قبل الوقوف على حجية تقرير الخبير أمام قاضي الموضوع.

الفرع الأول: استعانة القضاء بالخبراء في المعلوماتية

إنّ التطور المتسارع للتقنيات الرقمية وانتشار المعاملات الإلكترونية قد أفرز ظاهرة جديدة في ميدان الجريمة تتمثل في التزوير الرقمي، وهو ما يفرض على منظومة العدالة الجزائرية ضرورة ملحة للاستعانة بخبراء متخصصين في المعلوماتية، ونظراً لطبيعة الأدلة الرقمية المعقدة، والتي تختلف جوهرياً عن الأدلة المادية التقليدية، فإن القاضي الجزائي يصبح بحاجة ماسة إلى وسيط تقني يمتلك الاختصاص اللازم لكشف زيف المحررات الإلكترونية وتتبع البيانات المزورة.

أولاً: الإطار القانوني لاستعانة القضاء بخبراء المعلوماتية

يستند التشريع الجزائري في مجال مكافحة التزوير الرقمي إلى مجموعة من النصوص القانونية العامة والخاصة، أبرزها قانون 24-02 المتعلق بمكافحة التزوير واستعمال المزور، وتحديداً المواد من 219 فما فوق من قانون العقوبات، والذي يتناول التزوير في المحررات الرسمية والعرفية[3]، كما يدخل في هذا الإطار قانون 09-04 المتعلق بالوقاية من الجرائم المرتبطة بأنظمة المعلومات والاتصال، والذي يعالج بالتفصيل الجرائم الإلكترونية المرتبطة بالاعتداء على الأنظمة والبيانات[4]، غير أننا نلاحظ أن هذه النصوص، رغم أهميتها، لم

[1] عمور زهير، الخبرة القضائية في المواد الجنائية، مذكرة ماستر تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس- مستغانم، السنة الجامعية 2021/2020، ص 72.

[2] الأمر رقم 66-156 المؤرخ في 08 جوان 1966، المتضمن قانون العقوبات، الجريدة الرسمية، العدد 32، الصادر بتاريخ 11 جوان 1966.

[3] القانون رقم 24-02 المؤرخ في 26 فيفري 2024، المتعلق بمكافحة التزوير واستعمال المزور، الجريدة الرسمية، العدد 15، الصادر بتاريخ 29 فيفري 2024.

[4] القانون رقم 09-04 المؤرخ في 05 أوت 2009، المتعلق بالوقاية من الجرائم المرتبطة بتكنولوجيات الاعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47، الصادر بتاريخ 16 أوت 2009.

تخصص بشكل صريح فصلاً مستقلاً للتزوير الإلكتروني، مما يجعل القضاء يعتمد في تكييف هذه الجرائم على نصوص التزوير التقليدية، وفيما يخص إجراءات الاستعانة بالخبراء، قد أكدت المحكمة العليا الجزائرية في قرارها رقم 1168028 المؤرخ في 09 فيفري 2023 على ضرورة توثيق صحة المستندات الرقمية غير الرسمية عن طريق الخبرة قبل تطبيق أحكام التزوير عليها، مما يعكس إدراكاً قضائياً متقدماً لأهمية الخبرة التقنية في هذا المجال[1].

نرى أن الإطار القانوني الجزائري، وإن كان قد وفر قاعدة قانونية عامة تمكن القضاء من الاستعانة بالخبراء، إلا أنه يظل ناقصاً ومبهماً فيما يتعلق بالتزوير الرقمي بعينه، فنحن نعتقد أن غياب تعريف تشريعي صريح للتزوير الإلكتروني في قانون العقوبات يخلق لبساً قانونياً قد يؤثر سلباً على وحدة التطبيق القضائي، كما نستخلص أن صلاحية القاضي في تعيين الخبير المعلوماتي رغم كونها سلطة تقديرية واسعة تبقى مرتبطة بمدى وعي القاضي نفسه بأهمية الخبرة التقنية، وهو ما قد يتفاوت من قاضٍ إلى آخر، ومن ثم نرى أنه كان من الأجدى أن يُدرج المشرع الجزائري نصاً صريحاً يُلزم القضاء بالاستعانة بخبير معلوماتي في كل قضية تتعلق بالتزوير الرقمي، وذلك لضمان دقة التحقيق وعدالة الأحكام، بدلاً من ترك الأمر للتقدير القضائي المطلق.

الفرع الثاني: مهام الخبير الرقمي في كشف التزوير

إنّ خبراء المعلوماتية يضطلعون دوراً محورياً في سياق جرائم التزوير الرقمي، حيث إنهم يقومون بمجموعة من المهام الفنية الدقيقة التي تفوق إمكانيات القاضي أو المحقق العادي، فهم يستخدمون تقنيات التحليل الجنائي الرقمي (Digital Forensics) لفحص وتحليل الملفات والسجلات الرقمية والشبكات الإلكترونية[2]، وتشمل مهامهم تحليل البيانات الوصفية (Metadata) المتعلقة بالوثائق الرقمية، واستعادة البيانات المحذوفة، والتحقق من صحة التوقيعات الرقمية، وتوثيق المسارات الرقمية التي أُنشئت فيها الوثائق المزورة، كما يقوم الخبير بتقييم أصالة المحررات الإلكترونية ونسبتها إلى أصحابها من خلال فحص خوادم الشبكات وتحليل بروتوكولات الاتصال، ويقدم في النهاية تقريراً فنياً مفصلاً يدعم الإثبات القضائي أمام المحكمة، وقد تناولت

[1] **قرار صادر عن المحكمة العليا**، الغرفة الجزائية، ملف رقم 1168028، المؤرخ في 09 فيفري 2023، قضية (ب.ب) ضد (ب.ع) والنيابة العامة، موقع المحكمة العليا، تم الاطلاع عليه يوم 05 ماي 2026، على الساعة 00:28، على الرابط: https://coursupreme.dz/

[2] أحمد محمد محروس عبد العال، **المرجع السابق**، ص 55.

الدراسات المتخصصة أهمية تبادل الخبرات في هذا المجال، وضرورة أن يكون الخبير على دراية عميقة بأنظمة الحاسوب وهياكل البيانات وتقنيات التشفير والتزوير الرقمي[1].

نستخلص من هذا العرض أن دور خبير المعلوماتية لم يعد مجرد مساعدة فنية للقضاء، بل أصبح ركيزة أساسية في بناء الإثبات الجنائي في قضايا التزوير الرقمي، فنحن نرى أن القاضي مهما بلغت درايته القانونية، يظل عاجزاً عن فهم لغة البيانات الثنائية (Binary) أو كشف التلاعب في البيانات الوصفية دون الاستعانة بهذا الخبير، ونعتقد أن أهمية الخبير تتجلى بشكل خاص في ظل ظهور تقنيات التزييف العميق (Deepfake) والذكاء الاصطناعي، حيث أصبح التمييز بين الأصل والمزور يتطلب أدوات تقنية متخصصة لا يمتلكها إلا الخبراء، ومن ثم نرى أن أي ضعف في تقرير الخبير أو أي قصور في منهجيته قد يؤدي إلى انهيار الدعوى الجزائية برمتها، مما يفرض على المشرع والقضاء على حد سواء ضرورة وضع معايير دقيقة لاختيار هؤلاء الخبراء وضبط إجراءات عملهم.

الفرع الثالث: حجية تقرير الخبير أمام قاضي الموضوع

يشهد الفضاء الرقمي المعاصر تطوراً متسارعاً في المعاملات الإلكترونية، مما أفرز ظاهرة جديدة تمثلت في جريمة التزوير الرقمي التي باتت تشكل تحدياً جسيماً أمام منظومة العدالة الجزائرية، ونظراً لطبيعة الأدلة الرقمية المعقدة وافتراضيتها فإن قاضي الموضوع يصبح بحاجة ماسة إلى تقرير الخبير المعلوماتي لفك رموزها التقنية، غير أن هذا التقرير رغم أهميته الفنية يثير إشكالية جوهرية تتمثل في مدى حجيته أمام قاضي الموضوع، وهل هو ملزم له أم مجرد عنصر من عناصر الإثبات يخضع لسلطته التقديرية.

أولا: مكانة تقرير الخبير في الإثبات الجنائي أمام قاضي الموضوع

إنّ المبدأ الأساسي الذي يحكم العلاقة بين تقرير الخبير وقاضي الموضوع في النظام القانوني الجزائري، هو أن التقرير الخبري لا يُعتبر ملزماً للقاضي، بل هو مجرد عنصر من عناصر الإثبات يخضع لسلطته التقديرية الكاملة، فالقاضي حر في أخذ التقرير كله أو جزء منه، أو رفضه مع بيان الأسباب المستندة إلى أوراق الدعوى، غير أننا نلاحظ أنه في قضايا التزوير الرقمي، حيث تكون الأدلة غالباً معقدة وغير مادية، يصبح تقرير الخبير بمثابة ترجمة تقنية للوقائع يساعد القاضي على تكوين قناعته، دون أن يكون ذلك ملزماً له، وقد أكدت المادة 288 المكرر من قانون الإجراءات الجزائية المعدل على أهمية موثوقية الدليل الرقمي في مجال

[1] بن صويلح سفيان، حريدي الياس، **المرجع السابق**، ص64.

الأمن السيبراني والطب الشرعي، مما يرفع من مستوى الاعتراف القانوني بالأدلة الرقمية[1]، كما تظهر الممارسة القضائية أن المحاكم الجزائرية باتت تعتمد بشكل متزايد على تقارير الخبراء في القضايا الجنائية المرتبطة بالجرائم الإلكترونية[2].

نستخلص من هذا العرض أن مبدأ عدم إلزامية تقرير الخبير، وإن كان يضمن استقلالية القاضي ويمنع تأثير الخارج على قراراته، إلا أنه في مجال التزوير الرقمي يثير إشكالية عملية، فنحن نرى أن القاضي مهما بلغت درايته القانونية يظل عاجزاً عن فهم لغة البيانات الثنائية أو كشف التلاعب في البيانات الوصفية دون الاستعانة بالخبير، ونعتقد أن رفض القاضي لتقرير الخبير في هذه القضايا دون تبرير سائغ قد يؤدي إلى انهيار الإثبات برمته، نظراً لطبيعة الأدلة الرقمية التي لا يمكن للقاضي تقييمها بمفرده، ومن ثم نرى أنه يجب التمييز بين السلطة التقديرية للقاضي في الجوانب القانونية، وبين الجوانب التقنية الصرفة التي يجب أن يخضع فيها رأي القاضي لرأي الخبير المختص.

ثانيا: شروط ومعايير موثوقية تقرير الخبير في قضايا التزوير الرقمي

لكي يحظى تقرير الخبير بثقة القاضي ويؤخذ به كدليل قوي، يجب أن يستوفي مجموعة من الشروط والمعايير القانونية والفنية، فعلى الصعيد الفني يجب أن يوضح الخبير في تقريره المنهجية المستخدمة في الفحص بدقة، مثل صحة البيانات الوصفية (Metadata) والتوقيع الرقمي وسلسلة زمنية دقيقة للأحداث، كما يجب ضمان "سلسلة حراسة الدليل" (Chain of Custody) منذ لحظة جمعه وحتى تقديمه للمحكمة، لضمان عدم التلاعب به[3]، وعلى الصعيد القانوني، يجب أن تتوفر في الخبير أهليته واختصاصه التقني في مجال الطب الشرعي الرقمي أو الأمن السيبراني، كما يجب أن يتسم التقرير بالوضوح والموضوعية والحياد، وأن يتضمن تفاصيل دقيقة عن طرق الفحص والتحليل المستعملة، وقد أوضحت الدراسات المتخصصة أن جودة تقرير الخبير تتأثر بعدة معايير أبرزها الخبرة الفنية والالتزام الإجرائي والقدرة على الدفاع عن التقرير أمام المحكمة[4].

---

[1] فلاك مراد، **اليات الحصول على الأدلة الرقمية كوسائل اثبات في الجرائم الالكترونية**، مجلة الفكر القانوني والسياسي، جامعة عمار ثليجي– الاغواط، المجلد 03، العدد 01، منشور بتاريخ 23 سبتمبر 2019، ص 206.

[2] بورطل أمينة، **اثبات الجريمة الالكترونية بالدليل الرقمي وفق التشريع الجزائري**، المجلة الجزائرية للعلوم القانونية والسياسية، جامعة عين تمونشت، المجلد 61، العدد 01، منشور سنة 2024، ص 55.

[3] بيكة باكة، موساوي لمياء، **اليات مكافحة الجريمة الالكترونية في التشريع الجزائري**، مذكرة ماستر تخصص قانون جنائي وعلوم جنائية، معهد الحقوق، المركز الجامعي الشيخ أمود بن مختار اليزي، السنة الجامعية 2023/2022، ص 20.

[4] بن صويلح سفيان، حريدي الياس، **المرجع السابق**، ص 80.

نرى أن هذه الشروط ليست مجرد شكليات إجرائية، بل تمثل ضمانات جوهرية لصدقية التقرير الخبري، فنحن نعتقد أن أي خلل في سلسلة حراسة الدليل الرقمي، ولو كان طفيفاً، قد يؤدي إلى بطلان التقرير برمته، نظراً لسهولة تعديل البيانات الرقمية، كما نستخلص أن أهلية الخبير في المجال الرقمي يجب أن تكون محددة بدقة، وألا تقتصر على مجال عام، إذ إن التزوير الرقمي يتطلب معرفة متخصصة بتقنيات التشفير وتحليل البيانات الوصفية، ونعتقد أن القاضي يجب أن يكون له سلطة تقديرية غير ملزمة في تقييم هذه الشروط، ولكن ضمن إطار يضمن عدم قبول تقارير تفتقر إلى المعايير العلمية المعترف بها دولياً.

ثالثا: تطبيقات عملية لدور الخبير وحدود سلطة القاضي التقديرية

إنّ تقرير الخبير في قضايا التزوير الرقمي يساعد في تفكيك المعلومات التقنية المعقدة وتحويلها إلى حقائق ملموسة يمكن للقاضي استيعابها، فالخبير يقوم بتوضيح كيفية تزييف التوقيعات الرقمية، أو تغيير السجلات الإلكترونية، أو اختراق الأنظمة للحصول على بيانات مزورة، كما يساهم في تكوين القناعة القضائية من خلال تقديم تفسيرات فنية دقيقة للوقائع المعروضة عليه[1]، وقد تناولت تقارير إعلامية متخصصة خطورة ظاهرة التزوير الإلكتروني والاحتيال الرقمي في الجزائر، مؤكدة على أهمية تقارير الخبراء في كشف هذه الجرائم وإدانة المتورطين[2].

نستخلص مما تقدم أن تقرير الخبير في قضايا التزوير الرقمي يمثل حلقة وصل حاسمة بين العالم التقني والعالم القضائي، فنحن نرى أن الخبير لا يقدم مجرد رأي فني، بل يترجم لغة البيانات إلى لغة قانونية يفهمها القاضي.

ومع ذلك، نعتقد أن سلطة القاضي التقديرية يجب أن تمارس بحرص شديد في هذا المجال، إذ إن تجاهل تقرير خبير معلوماتي دون مبرر تقني مقبول قد يؤدي إلى قرار قضائي غير عادل، ونرى أن المستقبل يقتضي تطوير قضاء متخصص في الجرائم السيبرانية، يجمع بين الفهم القانوني والخلفية التقنية، مما يقلل من الاعتماد المطلق على الخبراء ويضمن تكامل الإثبات في هذه القضايا المعقدة.

[1] بوجلال كواشي، بوريو فيصل، جريمة التزوير واستعمال المزور وفق القانون رقم 24-02، مذكرة ماستر تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة باتنة 1 الحاج لخضر، السنة الجامعية 2025/2024، ص 73.

[2] بورطل أمينة، المرجع السابق، ص 56.

المطلب الثالث: الاختصاص القضائي في جرائم التزوير الرقمي

تُعدّ مسألة الاختصاص القضائي من أبرز الإشكاليات التي تواجه الملاحقة القضائية للجرائم المعلوماتية، ومنها جريمة التزوير الرقمي نظراً للطبيعة العابرة للحدود التي تتميز بها هذه الجرائم، ففي ظل انتشار الإنترنت والشبكات الدولية قد يقع الفعل الجرمي في دولة مستخدماً خادماً إلكترونياً في دولة أخرى ليؤثر في ضحية تقع في دولة ثالثة مما يخلق تعقيدات قانونية وقضائية جوهرية تتجاوز الإطار الوطني.

إن المشرّع الجزائري، وإن كان قد حدد في المادة 05 من قانون 09-04 المؤرخ في 5 أوت 2009 اختصاص المحكمة العليا بالنسبة للجرائم المعلوماتية إلا أن هذا التنظيم ظل محدوداً في مواجهة التحديات الدولية، خاصة فيما يتعلق بالاختصاص المحلي للجرائم المرتكبة عبر الإنترنت وتنازع الاختصاص في الجرائم الدولية.[1]

ومن هذا المنطلق، سيتم في هذا المطلب تناول الاختصاص النوعي والأقطاب القضائية المتخصصة، ثم بيان الاختصاص المحلي في الجرائم المرتكبة عبر الإنترنت، وذلك قبل الوقوف على مشكلة تنازع الاختصاص في الجرائم الدولية.

الفرع الأول: الاختصاص النوعي (الأقطاب القضائية المختصة)

يشهد الفضاء الرقمي المعاصر تطوراً متسارعاً في المعاملات الإلكترونية مما أفرز ظاهرة جديدة تمثلت في جريمة التزوير الرقمي التي باتت تشكل تحدياً جسيماً أمام منظومة العدالة الجزائرية، ونظراً لطبيعة هذه الجريمة المعقدة تقنياً وقانونياً فإن تحديد الاختصاص النوعي للجهات القضائية المختصة بمكافحتها يكتسب أهمية بالغة في ضمان فعالية التحقيق وسرعة العدالة.

أولاً: القطب الجزائي الاقتصادي والمالي

يُعتبر القطب الجزائي الاقتصادي والمالي من الأقطاب القضائية المتخصصة التي تتداخل اختصاصاتها مع قضايا التزوير الرقمي، خاصة عندما تكون الجريمة مرتبطة بالنصب المالي أو تزوير العقود الرقمية[2]، فقد

[1] المادة 05 من القانون رقم 09-04 المؤرخ في 05 أوت 2009، المتعلق بالوقاية من الجرائم المرتبطة بتكنولوجيات الاعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47، الصادر بتاريخ 16 أوت 2009.

[2] أبوبكر تيتاوي، الياس مالك قرادي، **جرائم النصب والاحتيال الالكتروني في التشريع الجزائري**، مذكرة ماستر تخصص القانون الجنائي والعلوم الجنائية، معهد الحقوق، المركز الجامعي المقاوم الشيخ امود بن مختار- ايليزي ، السنة الجامعية 2025/2024، ص 51.

جاء قانون 24-02 المتعلق بمكافحة التزوير واستعمال المزور، الصادر في 26 فيفري 2024 ليعزز الرقابة على الوثائق الرقمية المصدرة من الجهات الإدارية والاقتصادية، ويغطي التزوير في المعاملات الإدارية والاقتصادية والرقمية ويحدد عقوبات مشددة تصل إلى السجن والغرامات[1]، وفي هذا السياق يبرز دور هذا القطب في متابعة التحقيقات المالية التي تتطلب خبرة متخصصة في الاحتيال الإلكتروني مع اختصاص موسع للتحقيقات المالية[2].

نرى أن القطب الجزائي الاقتصادي والمالي يكتسب أهمية خاصة في قضايا التزوير الرقمي ذات البعد المالي إذ إن تزوير العقود الرقمية والسندات المالية يمثل شكلاً متطوراً من أشكال الجريمة الاقتصادية، فنحن نعتقد أن هذا القطب رغم عدم تخصصه الحصري في الجرائم الرقمية، إلا أنه يوفر إطاراً قضائياً مناسباً للتعامل مع الجرائم التي تتداخل فيها الجوانب التقنية والمالية، ومن ثم نستخلص أن نجاح هذا القطب في مكافحة التزوير الرقمي الاقتصادي مرهون بتوفير كوادر قضائية مدربة على التحليل المالي الرقمي وذلك لضمان دقة التحقيق وسرعة الفصل في هذه القضايا المعقدة.

ثانياً: القطب الجزائي للاتصال والتكنولوجيات

يُعتبر القطب الجزائي للاتصال والتكنولوجيات أولاً وأكثر الأقطاب تخصصاً في التعامل مع جرائم التزوير الرقمي إذ يقع مقره في مجلس قضاء الجزائر، ويشمل اختصاص وكيل الجمهورية وقاضي التحقيق في متابعة التحقيق في الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال[3]، ويتم تمديد اختصاص هذا القطب ليشمل التزوير الإلكتروني والاحتيال الإلكتروني عبر الإنترنت مع التركيز على تزوير المستندات الإلكترونية[4]، ويشمل اختصاصه محلياً موسعاً أربع جهات قضائية رئيسية (الجزائر، عنابة، قسنطينة، وغيرها) لضمان تغطية واسعة،

[1] القانون رقم 24-02 المؤرخ في 26 فيفري 2024، المتعلق بمكافحة التزوير واستعمال المزور، الجريدة الرسمية، العدد 15، الصادر بتاريخ 29 فيفري 2024.

[2] زيداني جمال الدين، **مهام الأقطاب الجزائية المتخصصة في القضاء الجزائري**، مذكرة ماستر تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف- المسيلة، السنة الجامعية 2022/2021، ص 47.

[3] جنيدي محمد الصغير، منصوري محمد عبد الوهاب، **الأقطاب الجزائية المستحدثة في التشريع الجزائري**، مذكرة ماستر تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح- ورقلة، السنة الجامعية 2022/2021، ص 47.

[4] بومحراث ليندة، **الأقطاب الجزائية المتخصصة كالية لمكافحة الجرائم الالكترونية**، مداخلة في ملتقى دولي بعنوان: التكنولوجيات الحديثة والجريمة، جامعة الأمير عبد القادر للعلوم الاسلامية- قسنطينة، المنعقد يوم 23 نوفمبر 2022، ص 13.

وقد أكد قانون 09-04 المتعلق بالجرائم الإلكترونية على أهمية هذا القطب في توفير إطار قانوني للتحقيقات الرقمية وتحديد اختصاصات وكيل الجمهورية وقاضي التحقيق في هذا المجال[1].

نستخلص من هذا العرض أن القطب الجزائي للاتصال والتكنولوجيات يمثل الركيزة الأساسية في مكافحة التزوير الرقمي في الجزائر، فنحن نرى أن مقره في مجلس قضاء الجزائر واختصاصه المحلي الموسع على أربع جهات قضائية رئيسية يضمان تغطية جغرافية واسعة تلائم طبيعة الجرائم الإلكترونية العابرة للحدود، ونعتقد أن تخصص هذا القطب في جرائم الإعلام والاتصال يجعله الأكثر كفاءة في التعامل مع التزوير الإلكتروني والاحتيال عبر الإنترنت، إذ إن القضاة والمحققين في هذا القطب يمتلكون الخبرة اللازمة لفهم التعقيدات التقنية لهذه الجرائم، ومن ثم نرى أن تعزيز قدرات هذا القطب تقنياً وبشرياً يمثل أولوية قصوى لضمان فعالية العدالة في مواجهة التزوير الرقمي.

ثالثاً: الاختصاص النوعي (الأقطاب القضائية) وتحقيق العدالة

إنّ إنشاء الأقطاب الجزائية المتخصصة يمثل استراتيجية تحوّلية في التشريع الجزائري الحديث، خاصة في ظل قانوني 24-02 ، تسعى من خلالها الجزائر إلى تعزيز قدراتها على التحقيق في الجرائم المعقدة ومحاكمة مرتكبيها بفعالية أكبر، فهذه الأقطاب باختصاصها النوعي الدقيق تضمن متابعة دقيقة وشاملة للجرائم المنظمة وتساهم في بناء بيئة رقمية أكثر أماناً وموثوقية[2]، وقد أوضحت الدراسات أن الأقطاب المتخصصة توفر تخصصاً دقيقاً في التعامل مع التعقيدات الرقمية وتغطي محلياً موسعاً عبر مجالس قضائية عدة مما يعزز فرص تحقيق العدالة.

نرى أن الاختصاص النوعي للأقطاب القضائية المتخصصة يمثل حجر الزاوية في تحقيق العدالة الفعالة في قضايا التزوير الرقمي، فنحن نعتقد أن تجزئة الاختصاص بين القطب الاقتصادي والمالي والقطب التقني للاتصالات يضمن تخصيصاً أمثل للموارد القضائية وفق طبيعة كل جريمة، ونستخلص أن هذا النموذج القضائي المتخصص، وإن كان يمثل تقدماً ملحوظاً إلا أنه يحتاج إلى مزيد من التطوير من حيث تكوين القضاة وتوفير البنية التحتية التقنية، ومن ثم نرى أن تحقيق العدالة في ظل التزوير الرقمي لا يقتصر على

[1] القانون رقم 09-04 المؤرخ في 05 أوت 2009، المتعلق بالوقاية من الجرائم المرتبطة بتكنولوجيات الاعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47، الصادر بتاريخ 16 أوت 2009.

[2] بلحاج أسامة، خليفي سمير، **خصوصيات مكافحة الجريمة الالكترونية في الجزائر على ضوء التشريع والممارسة القضائية**، مجلة القانون والمجتمع، جامعة البويرة، المجلد 13، العدد 02، منشور سنة 2025، ص 245.

وجود نصوص قانونية متقدمة بل يتطلب أيضاً قضاة متخصصين يجمعون بين الفهم القانوني والخلفية التقنية مما يضمن تكامل الإجراءات وسرعة الفصل في هذه القضايا المعقدة.

الفرع الثاني: الاختصاص المحلي في الجرائم المرتكبة عبر الانترنت

يشهد الفضاء الرقمي المعاصر تطوراً متسارعاً في المعاملات الإلكترونية، مما أفرز ظاهرة جديدة تمثلت في جريمة التزوير الرقمي التي باتت تشكل تحدياً جسيماً أمام منظومة العدالة الجزائرية، ونظراً لطبيعة هذه الجريمة المرتكبة عبر الإنترنت، فإن تحديد الاختصاص المحلي للجهات القضائية المختصة بمكافحتها يكتسب أهمية بالغة، نظراً للطبيعة الافتراضية للفضاء السيبراني التي تتجاوز الحدود الإقليمية التقليدية.

أولا: الإطار التشريعي المنظم للاختصاص المحلي

إنّ تحديد الاختصاص المحلي في قضايا التزوير الرقمي في الجزائر يعتمد على مبادئ تقليدية تستند إلى قانون الإجراءات الجزائية المتمم (القانون 66-156)، حيث تتحدد هذه المبادئ بشكل عام على: مكان وقوع الجريمة، ومكان إقامة المتهم، ومكان إلقاء القبض على المتهم، غير أن طبيعة الجرائم الإلكترونية الافتراضية تتطلب تكييفاً لهذه المبادئ التقليدية، إذ يمكن اعتبار مكان ظهور آثار الجريمة أو مكان حدوث الضرر أو مكان وقوع الجريمة الافتراضية كأساس للاختصاص المحلي[1]، وقد وفر قانون 09-04 إطاراً شاملاً لتنظيم الجرائم الإلكترونية وتحديد الإجراءات الوقائية والعقابية، مع معالجة كيفية تحديد الاختصاص المحلي في قضايا التزوير الرقمي، كما يُعاقب التزوير الرقمي بموجب المادة 340 مكرر من قانون العقوبات بعقوبات مشددة تتراوح بين سنتين وخمس سنوات سجناً وغرامة تصل إلى 500,000 دينار جزائري[2].

نستخلص من هذا العرض أن المشرع الجزائري قد حاول تكييف المبادئ التقليدية للاختصاص المحلي مع طبيعة الجرائم الإلكترونية، إلا أن هذا التكييف يبقى غير كافٍ في مواجهة تعقيدات الفضاء السيبراني، فنحن نرى أن اعتبار مكان ظهور آثار الجريمة أو مكان حدوث الضرر كأساس للاختصاص يخلق إشكالية عملية إذ إن التزوير الرقمي المرتكب عبر الإنترنت قد يظهر آثاره في عدة أماكن في آن واحد، ونعتقد أن غياب نص صريح يحدد معايير دقيقة لتحديد الاختصاص المحلي في الجرائم الإلكترونية يضع القضاء في مأزق قانوني،

[1] لموسخ محمد، **تنازع الاختصاص في الجرائم الالكترونية**، دفاتر السياسة والقانون، جامعة قاصدي مرباح– ورقلة، المجلد 09، العدد 02، منشور بتاريخ 31 ديسمبر 2009، ص 149.

[2] أسامة بلحاج، خليفي سمير، **خصوصيات مكافحة الجريمة الالكترونية في الجزائر على ضوء التشريع والممارسة القضائية**، مجلة القانون والمجتمع، جامعة أدرار، المجلد 13، العدد 02، منشور بتاريخ 01 ديسمبر 2025، ص 233.

خاصة عندما يتعلق الأمر بالجرائم العابرة للحدود، ومن ثم نرى أنه يجب على المشرع الجزائري أن يستلهم التجارب الدولية في هذا المجال وأن يضع معايير واضحة تضمن تحديداً دقيقاً للاختصاص المحلي دون الإخلال بمبدأ المساواة أمام القانون.

ثانيا: الجهات المتخصصة ودور القطب الجزائي للجرائم الإلكترونية

إنّ استحداث "القطب الجزائي للجرائم الإلكترونية" في الجزائر يمثل إدراكاً متخصصاً لطبيعة الجرائم المعقدة، حيث يتمتع هذا القطب بصالحيات واسعة إلكترونية تحقيق، ويتمتع بتفرد في التعاون مع الجهات الأمنية المتخصصة[1]، وقد تم إنشاء هذا القطب بموجب القانون 21-11 المتمم لقانون الإجراءات الجزائية (صادر في 2021)، ويتولى التحقيق والمحاكمة في الجرائم السيبرانية بما فيها التزوير الرقمي[2]، ويمنح هذا القطب اختصاصاً محلياً في المحاكم الجهازية الرئيسية مع إمكانية نقل القضايا إلى المحكمة العليا إذا تجاوزت الولايات الإقليمية الحدود[3]، كما تسجل مصالح الشرطة المتخصصة في مكافحة الجرائم الإلكترونية شكاوى متزايدة حيث تم مؤخرا تسجيل حوالي 567 قضية تتعلق بجرائم الانترنت(الوثيقة أسفله)[4]، مما يؤكد على الحاجة إلى آليات تحقيق ومحاكمة سريعة وفعالة.

نوع الجريمة	القضايا المسجلة	القضايا المعالجة	عدد المتورطين	النسبة المئوية للقضايا المعالجة
جرائم المساس بالأشخاص عبر الأنترنت	430	289	365	%68
جرائم الإعتداء على سلامة الأنظمة المعلوماتية	57	31	39	%55
جرائم الإحتيال عبر الأنترنت	25	17	32	%68
جرائم التحريض والتطرف عبر الأنترنت	14	14	31	%100
الجرائم المخلة بالحياء	12	08	22	%67
جرائم بيع السلع المحظورة عبر الأنترنت	06	05	15	%84
جرائم مختلفة (نسخ البرامج دون حق، القرصنة)	23	21	39	%92
المجموع	**567**	**385**	**543**	**%68**

[1] زعيطي امنة، **مكافحة الجرائم الالكترونية في ضوء قانون العقوبات الجزائري**، مجلة حقوق الانسان والحريات العامة، جامعة عبد الحميد بن باديس- مستغانم، المجلد 20، العدد 07، منشور بتاريخ جوان 2019، ص 220.

[2] الأمر رقم 21-11 المؤرخ في 25 أوت 2021 المعدل والمتمم للأمر رقم 66-153 المؤرخ في 08 جوان 1966، المتضمن قانون الاجراءات الجزائية، الجريدة الرسمية، العدد 65، الصادر بتاريخ 26 أوت 2021.

[3] لموسخ محمد، **المرجع السابق**، ص 150.

[4] **مصالح شرطة مكافحة الجرائم الالكترونية تسجل 567 قضية تتعلق بجرائم الانترنت**، منشور على موقع الشرطة الجزائرية، تم الاطلاع عليه يوم 07 ماي 2026، على الساعة 19:22، على الرابط: https://www.algeriepolice.dz

نرى أن إنشاء القطب الجزائي للجرائم الإلكترونية يمثل خطوة إيجابية نحو تخصيص العدالة الجنائية في الجزائر، فنحن نعتقد أن هذا القطب باختصاصه المحلي الموسع وإمكانية نقل القضايا إلى المحكمة العليا يضمن مرونة فعالة في التعامل مع الجرائم العابرة للحدود، ومع ذلك نستخلص أن التحدي الرئيسي يكمن في قدرة هذا القطب على مواكبة السرعة التكنولوجية لتطور الجرائم الإلكترونية، إذ إن التزوير الرقمي يتطور بوتيرة أسرع من استجابة المنظومة القضائية، ونعتقد أن نجاح هذا القطب مرهون بتوفير البنية التحتية التقنية اللازمة وتكوين القضاة والمحققين بشكل مستمر في مجال الجرائم السيبرانية، ومن ثم نرى أن الاستثمار في الكادر البشري والتقني لهذا القطب ليس رفاهية، بل هو شرط ضروري لضمان فعالية العدالة في مواجهة التزوير الرقمي.

ثالثا: معايير تحديد الاختصاص المحلي في التزوير الرقمي

إنّ تحديد الاختصاص المحلي في قضايا التزوير الرقمي يعتمد على مجموعة من المعايير القانونية والتقنية التي تضمن دقة التحقيق وسرعة العدالة، فمن المعايير الأساسية: مكان القبض على المتهم، ومكان وقوع الجريمة، ومكان إقامة المتهم، ومكان ظهور آثار الجريمة أو الضرر[1]، فالاختصاص المحلي في التزوير الرقمي بالجزائر يتكامل مع عدة عناصر، أبرزها: الأطر التشريعية (قانون مكافحة التزوير واستعمال المزور، قانون 09-04، قانون الإجراءات الجزائية)، والجهات المتخصصة (القطب الجزائي للجرائم الإلكترونية، النيابة العامة، قاضي التحقيق)، وقد أوضحت الدراسات أن مستوى التطور في الجزائر يظهر تقدماً كبيراً في التشريع والتخصص القضائي، بينما يحتاج التحقيق الرقمي والبنية التحتية إلى مزيد من التطوير[2].

نستخلص من هذا العرض أن تحديد الاختصاص المحلي في قضايا التزوير الرقمي يمثل تحدياً قانونياً وتقنياً في آن واحد، فنحن نرى أن المعايير التقليدية (مكان وقوع الجريمة، مكان إقامة المتهم) تفقد فعاليتها في الفضاء السيبراني، إذ إن الجريمة الإلكترونية لا تعترف بالحدود الجغرافية، ونعتقد أن اعتماد معايير بديلة، مثل مكان ظهور آثار الجريمة أو مكان حدوث الضرر، يمثل حلاً جزئياً ولكنه غير كافٍ في ظل تعقيدات الإنترنت، ومن ثم نعتقد أن الجزائر مطالبة بتطوير إطار قانوني متكامل يجمع بين المبادئ التقليدية والمعايير الدولية الحديثة وذلك لضمان تحديد دقيق للاختصاص المحلي دون الإخلال بحقوق المتهمين.

---

[1] بوحليط يزيد، **المرجع السابق**، ص89.

[2] دبابي زينب، **جرائم التزوير واستعمال المزور في التشريع الجزائري**، مذكرة ماستر تخصص قانون خاص، معهد الحقوق، المركز الجامعي مغنية، السنة الجامعية 2024/2023، ص 35.

الفرع الثالث: مشكلة تنازع الاختصاص في الجرائم الدولية

يشهد الفضاء الرقمي المعاصر تطوراً متسارعاً في المعاملات الإلكترونية، مما أفرز ظاهرة جديدة تمثلت في جريمة التزوير الرقمي التي باتت تشكل تحدياً جسيماً أمام منظومة العدالة الجزائرية، ونظراً لطبيعة هذه الجريمة العابرة للحدود فإن مشكلة تنازع الاختصاص القضائي الدولي تكتسب أهمية بالغة، إذ إن الفاعل قد يرتكب جريمته في بلد واحد بينما يقع الضرر في بلد آخر وتنتشر آثارها في بلد ثالث.

أولاً- طبيعة الجرائم الرقمية وتحديات الاختصاص القضائي

إنّ الجرائم الرقمية وخاصة التزوير الرقمي تتميز بطبيعة عابرة للحدود تجعل تحديد مكان وقوع الجريمة أمراً معقداً، مما يؤدي إلى تنازع بين الولايات القضائية المختلفة[1]، فقد يتم ارتكاب الفعل الإجرامي في دولة واحدة بينما ينتج الضرر عنه في دولة أخرى وتقع الضحية في دولة ثالثة مما يخلق "تنازع اختصاص" بين عدة ولايات قضائية تتنافس على الحق في محاكمة الجاني[2]، ويُعرّف التزوير الرقمي في القانون الجزائري بأنه تزييف المحررات أو البيانات الإلكترونية أو التوقيعات الإلكترونية، وتندرج هذه الجريمة ضمن إطار الجرائم المعلوماتية التي تتولى مواد قانون العقوبات معاقبتها، وقد شددت التشريعات الجزائرية عقوباتها وحددت تجريمها[3]، كما أن صعوبة تحديد "محل الجريمة" في الفضاء السيبراني تتداخل فيه المواقع الافتراضية مع الجغرافية، مما يجعل تطبيق المبادئ التقليدية للاختصاص أمراً صعباً[4].

نرى أن طبيعة الجرائم الرقمية العابرة للحدود تمثل تحدياً جوهرياً للنظام القانوني الجزائري، إذ إن المبادئ التقليدية للاختصاص القضائي التي تعتمد على مكان وقوع الجريمة أو مكان إقامة المتهم تفقد فعاليتها في الفضاء الافتراضي، فنحن نعتقد أن التزوير الرقمي المرتكب عبر الإنترنت لا يعترف بالحدود الجغرافية، مما يجعل تحديد الاختصاص القضائي الدولي مسألة معقدة تتطلب تكييفاً قانونياً جديداً، ونستخلص أن غياب معايير دولية موحدة لتحديد الاختصاص في الجرائم الإلكترونية يضع القضاء الجزائري في مأزق عندما يتعلق

[1] موسى لسود، **معايير الاختصاص القضائي في جرائم قانون التجارة الالكترونية الجزائري 18/05**، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة العربي التبسي- تبسة، المجلد 04، العدد 02، منشور بتاريخ 08 جانفي 2020، ص 369.

[2] لموسخ محمد، **المرجع السابق**، ص 151.

[3] عمارة فتيحة، **المرجع السابق**، ص 185.

[4] خميس جمعة الشهواني، **اشكالية تحديد الاختصاص القضائي في الجرائم الالكترونية**، مجلة الشرق الأوسط للدراسات القانونية والفقهية، جامعة صفاقس، المجلد 06، العدد 01، منشور بتاريخ 13 فيفري 2026، ص 160.

الأمر بالجرائم العابرة للحدود، ومن ثم نرى أنه يجب على المشرع الجزائري أن يتبنى معايير مرنة تجمع بين المبادئ التقليدية والمعايير الدولية الحديثة، وذلك لضمان فعالية العدالة دون الإخلال بحقوق المتهمين.

ثانياً– الاستجابة التشريعية والمؤسسية في القانون الجزائري

إنّ المشرع الجزائري قد أدرك خطورة التحديات القانونية والمؤسسية في مواجهة تنازع الاختصاص في الجرائم الإلكترونية وعمل على تطوير آلياته القانونية لمواجهة التزوير الرقمي، فقد صدر مؤخراً قانون 02/24 المتعلق بمكافحة التزوير واستعمال المزور، والذي شدد قدرته على تعزيز مكافحة التزوير بصفة عامة والرقمي خاصة، ويشمل نطاق هذا القانون تطبيقه على تزوير الوثائق والمحررات والمساعدات على الحصول والإعانات العمومية وتزوير النقود وتقليدها، وانتحال الوظائف، وشهادة الزور[1]، كما اعتمد المشرع الجزائري أسلوب التخصص من خلال إنشاء أقطاب وطنية جزائرية متخصصة، يقع القطب الوطني الجزائري في العاصمة ويهدف إلى توحيد الاختصاص وتسهيل التحقيق في الجرائم الإلكترونية بما فيها التزوير الرقمي مع التعاون الدولي عبر منظمة الشرطة الجنائية الدولية (الإنتربول)[2] ، وقد شهدت الجزائر تحديثات تقنية كبيرة في القانون الجزائي، بينما يظل التعاون الدولي في مستوى أقل نسبياً مقارنة بالتحديات القانونية والتشريعية[3].

نستخلص من هذا العرض أن الاستجابة التشريعية الجزائرية تمثل خطوة إيجابية نحو مواجهة تنازع الاختصاص في الجرائم الدولية، فنحن نرى أن قانون 02/24 قد وفر إطاراً قانونياً متقدماً لمكافحة التزوير الرقمي، إلا أنه يظل ناقصاً فيما يتعلق بالنصوص الخاصة بتنازع الاختصاص الدولي، ونعتقد أن إنشاء الأقطاب الجزائية المتخصصة يمثل حلاً جزئياً للمشكلة، إذ إن تمركز الاختصاص في قطب واحد يقلل من احتمالات التنازع بين المحاكم الجزائرية، غير أننا نلاحظ أن التعاون الدولي يظل مجالاً ضعيفاً في الجزائر، نظراً لغياب اتفاقيات دولية شاملة تضع معايير واضحة لتحديد الاختصاص في الجرائم الإلكترونية، ومن ثم نرى أنه يجب على الجزائر الانضمام الكامل إلى اتفاقية بودابست بشأن الجريمة الإلكترونية، وتفعيل آليات التعاون القضائي الدولي، وذلك لضمان فعالية العدالة في مواجهة الجرائم العابرة للحدود.

---

[1] **الأحكام الجديدة في قانون مكافحة التزوير واستعمال المزور محور دراسي بالجزائر العاصمة**، موقع الان، منشور منذ 2024، تم الاطلاع عليه يوم 07 ماي 2026، على الساعة 20:27، على الرابط: https://elaane.dz

[2] بومحراث ليندة، **المرجع السابق**، ص 14.

[3] سعيدة بوزنون، **المرجع السابق**، ص 50.

ثالثاً– معايير تحديد الاختصاص وحلول التنازع

إنّ تحديد الاختصاص في قضايا التزوير الرقمي يعتمد على مجموعة من المعايير القانونية التي تجمع بين المبادئ التقليدية والمعايير الحديثة، فعلى الصعيد التقليدي يعتمد القانون الجزائري على مبدأ الإقليمية (المادة 5 من قانون الإجراءات الجزائية)، حيث يطبق القانون الجزائري إذا ارتكبت الجريمة جزئياً في التراب الجزائري أو إذا كان الجاني جزائرياً[1]، وفيما يتعلق بالمعايير المقترحة لمعالجة تنازع الاختصاص في الجرائم الرقمية تعتمد الجزائر على عدة معايير: مكان الفعل الإجرامي (أين حدث التزوير)، ومكان النتيجة/الضرر (أين وقع الضرر الناتج عن الجريمة)، وجنسية الجاني أو الضحية في بعض الحالات[2].

نرى أن المعايير المقترحة لتحديد الاختصاص في قضايا التزوير الرقمي تمثل حلاً توفيقياً بين المبادئ التقليدية ومتطلبات العصر الرقمي، فنحن نعتقد أن اعتماد مكان الفعل الإجرامي ومكان النتيجة كمعايير أساسية للاختصاص يضمن تغطية شاملة للجرائم الإلكترونية، إلا أنه قد يخلق تنازعاً عندما يتباعد هذان المكانان، ونستخلص أن مبدأ الاختصاص العالمي وإن كان يمثل حلاً فعالاً للجرائم الخطيرة إلا أن تطبيقه في جرائم التزوير الرقمي يثير إشكاليات تتعلق بسيادة الدول وحقوق المتهمين، ونعتقد أن التدريب والتأهيل يمثلان حجر الزاوية في حل مشكلة التنازع، إذ إن قضاة متخصصين في الجرائم الرقمية قادرون على تطبيق المعايير بشكل دقيق وموحد، ومن ثم نرى أن الجزائر مطالبة بتطوير قوانينها لتشمل "الاختصاص العالمي" للجرائم الرقمية الخطيرة، مع ضمانات قانونية تحمي حقوق المتهمين.

المبحث الثالث: الاليات المؤسساتية والتعاون الدولي لمكافحة التزوير الرقمي

لم يعد الاكتفاء بالتجريم القانوني كافياً لمواجهة تحديات الجرائم المعلوماتية، ومنها التزوير الرقمي في ظل التطور المتسارع لتكنولوجيات الإعلام والاتصال، فالنصوص التشريعية وإن كانت ضرورية إلا أنها تبقى حبراً على ورق ما لم تترافق مع آليات مؤسساتية فعالة تضمن تطبيقها على أرض الواقع، وفي هذا السياق نرى أن المشرّع الجزائري قد أدرك هذه الحاجة من خلال إصدار القانون رقم 09-04 المؤرخ في 5 أوت 2009، والذي

[1] أسامة بلحاج، خليفي سمير، **المرجع السابق**، ص 247.

[2] مريم عراب، **الاختصاص القضائي في الجرائم المعلوماتية**، حوليات كلية الحقوق والعلوم الساسية، جامعة وهران 2 محمد بن أحمد، المجلد 07، العدد 03، منشور بتاريخ 22 ديسمبر 2015، ص 270.

لم يقتصر على التجريم بل نصّ على إحداث هيئات وطنية متخصصة ومكلفة بالوقاية من هذه الجرائم ومكافحتها مما يعكس إدراكاً عميقاً بأن مواجهة الجريمة المعلوماتية تتطلب بنية تحتية مؤسساتية متكاملة.[1]

غير أن هذه الآليات المؤسساتية الوطنية رغم أهميتها تواجه تحديات جسيمة تتعلق بمدى فعاليتها وتنسيقها فيما بينها خاصة في مجال الكشف عن جرائم التزوير الرقمي التي تتطلب خبرات تقنية عالية ووسائل تحقيق متخصصة فالجرائم المعلوماتية لا تُكتشف بالطرق التقليدية المعتمدة في الجرائم العادية بل تستوجب وجود هياكل تقنية ولوجستية متطورة تتمتع بالكفاءة والسرعة في التدخل، وهو ما يطرح إشكالية تنسيقية بين مختلف الأجهزة الأمنية والقضائية المعنية.[2]

كما أننا نلاحظ أن مكافحة التزوير الرقمي لا يمكن أن تتحقق بمعزل عن القطاع الخاص، وخاصة مقدمي خدمات الإنترنت والمؤسسات المالية التي تشكل خط الدفاع الأول في حماية المعطيات الرقمية والمحررات الإلكترونية، فهذه الجهات الخاصة تمتلك البنى التحتية التقنية والقدرة على رصد الشبهات والتبليغ عنها مما يجعلها شريكاً لا غنى عنه للسلطات العمومية في هذا المجال، وقد نص القانون 09-04 في المادتين 11 و12 على التزامات محددة لهؤلاء المقدمين، مما يؤكد الدور المحوري الذي يؤدونه في المنظومة الوقائية.[3]

وفي المقابل، تبرز إشكالية جوهرية تتمثل في الطبيعة العابرة للحدود للإنترنت التي تجعل من جريمة التزوير الرقمي ظاهرة دولية بامتياز، فالجاني قد يرتكب فعله من دولة مستخدماً خادماً إلكترونياً في دولة أخرى ليؤثر في ضحية تقع في دولة ثالثة مما يجعل الملاحقة القضائية الوطنية وحدها عاجزة عن مواجهة هذا النوع من الجرائم، ومن ثم يصبح التعاون الدولي سواء على مستوى تسليم المجرمين أو المساعدة القضائية المتبادلة أو التنسيق عبر المنظمات الدولية كالإنتربول ضرورة قصوى لا محيد عنها.[4]

---

[1] القانون رقم 09-04 المؤرخ في 5 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47، الصادر بتاريخ 16 أوت 2009.

[2] اية بن ميسية، **المرجع السابق**، ص 52.

[3] المواد 11 و 12 من القانون رقم 09-04 المؤرخ في 5 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47، الصادر بتاريخ 16 أوت 2009.

[4] الكثيري سعيد مسعود، **الجريمة الالكترونية: في ضوء اتفاقية بودابست: الاطار المفاهيمي والتصنيفي**، مجلة البحوث القانونية والاقتصادية، المركز الجامعي-افلو، المجلد 09، العدد 01، منشور بتاريخ 01 جانفي 2026،ص 947.

وبناءً على ما تقدم، يتبين أن موضوع الآليات المؤسساتية والتعاون الدولي لمكافحة التزوير الرقمي يشكل محوراً حاسماً في دراسة الجرائم المعلوماتية تستوجب النظر الشامل إلى مختلف الأبعاد المؤسساتية والوطنية والدولية المتعلقة بها، ومن هذا المنطلق سنعمل في هذا المبحث على تناول ثلاثة محاور رئيسية: المحور الأول يخصص لدراسة الهيئات الوطنية المتخصصة في الجزائر، والمحور الثاني يتناول دور مقدمي الخدمات والقطاع الخاص، أما المحور الثالث فيركز على التعاون الدولي في مكافحة التزوير الرقمي.

المطلب الاول: الهيئات الوطنية المتخصصة في الجزائر

إن مكافحة التزوير الرقمي تستلزم وجود هياكل مؤسساتية وطنية متخصصة تضطلع بمهام الوقاية والرصد والتدخل نظراً للطبيعة التقنية المعقدة لهذه الجرائم التي تفوق قدرات الأجهزة الأمنية التقليدية وقد أدرك المشرّع الجزائري هذه الضرورة من خلال نصوص القانون رقم 09-04 المؤرخ في 5 أوت 2009، الذي أرسى إطاراً مؤسساتياً يهدف إلى تنسيق الجهود الوطنية في مجال مكافحة الجرائم المعلوماتية.[1]

الفرع الاول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال

يشهد الفضاء الرقمي المعاصر تطوراً متسارعاً في المعاملات الإلكترونية، مما أفرز ظاهرة جديدة تمثلت في جريمة التزوير الرقمي التي باتت تشكل تهديداً جسيماً للأمن السيبراني وللموثوقية الرقمية في الجزائر، ونظراً لطبيعة هذه الجريمة المعقدة تقنياً وقانونياً، فإن إنشاء هيئات وطنية متخصصة يكتسب أهمية بالغة في ضمان فعالية الوقاية والمكافحة.

أولاً- الإطار التشريعي لإنشاء الهيئة الوطنية ومكافحة التزوير الرقمي

يستند التشريع الجزائري في مجال مكافحة التزوير الرقمي إلى مجموعة من النصوص القانونية، أبرزها القانون 09-04 المتعلق بالوقاية من الجرائم المرتبطة بأنظمة المعلومات والاتصال، الصادر في 5 أوت 2009، والذي يُعد حجر الزاوية في التشريع الجزائري الخاص بالجرائم السيبرانية، إذ يحدد القواعد الخاصة بالوقاية والعقاب ويؤسس للهيئة الوطنية للوقاية من هذه الجرائم[2]، كما شهد التشريع الجزائري مؤخراً إصدار قانون 24-02 المتعلق بمكافحة التزوير واستعمال المزور، والذي يقدم تدابير جديدة لتأمين حماية الوثائق والمحررات

[1] القانون رقم 09-04 المؤرخ في 5 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47، الصادر بتاريخ 16 أوت 2009.

[2] القانون رقم 09-04 المؤرخ في 5 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47، الصادر بتاريخ 16 أوت 2009.

الورقية والمالية، ويفرض ضوابط صارمة للولوج إلى البيانات الحساسة عبر مواصفات تقنية يصعب معها تزوير الوثائق، مما يعزز الحصانة ضد التلاعب الرقمي[1]، وقد عكست هذه التحديثات التشريعية اهتماماً متزايداً بالتكيف مع المشهد الرقمي المتغير، حيث دعت الجهات الرسمية إلى تحديث المنظومة التشريعية لتعزيز السياسة الجنائية في مجال حماية البيانات الشخصية والوقاية التقنية[2].

نرى أن الإطار التشريعي الجزائري وإن كان قد وفر قاعدة قانونية متينة لإنشاء الهيئة الوطنية وتنظيم مكافحة التزوير الرقمي إلا أنه يظل ناقصاً في بعض جوانبه، فنحن نعتقد أن القانون 09-04 رغم أهميته التأسيسية لم يخصص بشكل صريح فصلاً مستقلاً مفصلاً لمهام الهيئة في مجال التزوير الرقمي بعينه، مما يجعل اختصاصاتها تستمد من النصوص العامة المتعلقة بالجرائم الإلكترونية، كما نستخلص أن قانون 24-02 وإن كان قد شدد العقوبات إلا أنه يقتصر في مجال التقنية على مواصفات وقائية عامة دون تفصيل آليات التدخل الفعلي للهيئة، ومن ثم نرى أنه كان من الأجدى أن يُدرج المشرع نصوصاً صريحة تلزم الهيئة الوطنية بالتنسيق المباشر مع الأجهزة القضائية المتخصصة في قضايا التزوير الرقمي وذلك لضمان تكامل الإجراءات بين الوقاية والمكافحة.

ثانياً- الدور المحوري للهيئة الوطنية في مكافحة التزوير الرقمي

إنّ الهيئة الوطنية للوقاية من الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال والتي أُنشئت بموجب القانون 09-04، تُشكل الركيزة الأساسية في الاستراتيجية الجزائرية لمكافحة التزوير الرقمي حيث تعمل كجهاز حكومي مستقل تتولى مهام متعددة تسهم في التحقيق السيبراني[3]، فمن أهم أدوارها التنسيق بين مختلف الجهات الفاعلة في مجال الأمن السيبراني، ومراقبة الفضاء السيبراني، والكشف عن الجوانب التقنية والأمنية المتعلقة بالتلاعب بالوثائق الإلكترونية والمصرفية والإدارية[4]، كما تلتزم الهيئة بتنظيم حملات توعوية مكثفة حول مخاطر

---

[1] رياض/خ ، **قانون مكافحة جرائم التزوير في الجريدة الرسمية**، منصة البلاد نت، منشور بتاريخ 13 مارس 2024، تم الاطلاع عليه يوم 08 ماي 2026، على الساعة 19:05، على الرابط: https://www.elbilad.net

[2] **مكافحة الجريمة الالكترونية: بوغالي يبرز ضرورة تحديث المنظومة التشريعية الوطنية**، منصة الاذاعة الجزائرية، منشور بتاريخ 30 جوان 2025، تم الاطلاع عليه يوم 08 ماي 2026، على الساعة 19:09، على الرابط: http://news.radioalgerie.dz/ar/node/67139

[3] عبدالنبي مصطفى، **قراءة في النصوص القانونية المنظمة للهيئة الوطنية للوقاية من جرائم تكنولوجيات الاعلام والاتصال ومكافحتها**، دفاتر السياسة والقانون، جامعة قاصدي مرباح-ورقلة، المجلد 13، العدد 03، منشور بتاريخ 21 جوان 2021، ص 409.

[4] عبد النبي سلمى، **دور القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال في مواجهة الاعتداءات الواقعة على المعطيات المعلوماتية**، مجلة الحقوق والعلوم السياسية، جامعة عباس لغرور- خنشلة، المجلد 11، العدد 02، منشور بتاريخ 26 جوان 2024، ص 19.

التزوير الرقمي وكيفية حماية الأفراد والمؤسسات وتشجع على استخدام التقنيات الأمنية الحديثة مثل التشفير والتوقيعات الرقمية التي تعتبر أدوات حيوية لمنع التعديل غير المشروع للبيانات والوثائق[1]، وتتعاون الهيئة بشكل وثيق مع الشرطة القضائية في التحقيقات الجنائية خاصة فيما يتعلق بجمع الأدلة الرقمية التي تتطلب خبرة متخصصة، كما تلعب دوراً استشارياً في اقتراح تعديلات قانونية لمواكبة التطورات التكنولوجية السريعة[2].

نستخلص من هذا العرض أن دور الهيئة الوطنية يتجاوز مجرد التنسيق الإداري ليصل إلى جوهر الاستجابة التقنية والقضائية ضد التزوير الرقمي، فنحن نرى أن مراقبة الفضاء السيبراني والكشف عن التلاعب بالوثائق الإلكترونية يمثلان وظيفة استباقية ضرورية في عصر تتسارع فيه الجرائم الرقمية، ومع ذلك نعتقد أن الحملات التوعوية وإن كانت مهمة تبقى غير كافية ما لم ترافقها استثمارات حقيقية في البنية التحتية التقنية للكشف عن التزوير، كما نستخلص أن التعاون مع الشرطة القضائية يظل مجالاً يحتاج إلى مزيد من الترسيخ المؤسسي إذ إن جمع الأدلة الرقمية يتطلب بروتوكولات دقيقة تضمن سلامة سلسلة الحراسة (Chain of Custody). ومن ثم نرى أن تمكين الهيئة من صلاحيات تقنية وتنفيذية أوسع بما في ذلك القدرة على التدخل المباشر في الأنظمة المعرضة للخطر يمثل شرطاً ضرورياً لفعاليتها.

ثالثاً– الآليات القضائية والمؤسساتية المتخصصة

إنّ مكافحة التزوير الرقمي في الجزائر لا تقتصر على دور الهيئة الوطنية بل تتكامل مع آليات قضائية ومؤسساتية متخصصة تضمن استجابة فعالة ومتكاملة، فقد تم إنشاء القطب الجزائي الوطني المتخصص في مكافحة الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال كآلية قضائية جديدة ضمن الجهاز القضائي المتخصص، والذي يعزز القدرة على تتبع الجرائم الرقمية في بيئة افتراضية غالباً ما تتطلب خبرات وأدوات متخصصة[3]، كما تتضمن الجهود المؤسسية إنشاء مصالح مركزية متخصصة تابعة للمديرية الوطنية للأمن الجنائي ومعهد الدرك الوطني والتي تعمل على تعزيز القدرات البشرية والتقنية في مجال التحقيق الجنائي

[1] أجعود سعاد، **الحماية الجزائية لتكنولوجيات الاعلام والاتصال في التشريع الجزائري "دراسة على ضوء النصوص المستحدثة"**، مجلة الرسالة للدراسات والبحوث الانسانية، جامعة العربي التبسي– تبسة، المجلد 07، العدد 04، منشور بتاريخ 14 جوان 2022، ص 220.

[2] زكريا بوعون، **دور الهيئة الوطنية للوقاية من الجرائم الالكترونية في حماية المستهلك**، مجلة العلوم الانسانية، جامعة منتوري قسنطينة، المجلد 29، العدد 01، منشور بتاريخ 30 جوان 2018، ص 420.

[3] بن زهرة السعيد، بلعربي بلقاسم، **القطب الجزائي الوطني المتخصص في مكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال: دراسة في المفهوم والاختصاص**، مجلة الدراسات القانونية والاقتصادية، المركز الجامعي سي الحواس– بريكة، المجلد 08، العدد 02، منشور بتاريخ 20 ديسمبر 2025، ص 560.

الرقمي، وتتكامل هذه الآليات مع التدابير الوقائية التي يفرضها القانون، مثل استخدام التشفير والتوقيع الإلكتروني قبل وقوع الجريمة مما يشكل حماية استباقية للبيانات والوثائق الرقمية[1].

نرى أن إنشاء القطب الجزائي الوطني المتخصص والمصالح المركزية يمثل خطوة استراتيجية نحو تخصيص العدالة الجنائية في مواجهة التزوير الرقمي، فنحن نعتقد أن التحقيق في الجرائم السيبرانية يتطلب قضاة ومحققين يجمعون بين الفهم القانوني والخلفية التقنية، وهو ما يوفره هذا القطب المتخصص، ومع ذلك نلاحظ أن الفجوة بين التشريع والتطبيق تظل واضحة إذ إن توفر الأدوات التقنية المتخصصة للكشف عن التزوير لا يزال محدوداً مقارنة بالتطور السريع للتقنيات المستخدمة في ارتكاب الجريمة، ونستخلص أن التدابير الوقائية كالتشفير والتوقيع الإلكتروني وإن كانت فعالة إلا أن انتشارها بين المؤسسات والأفراد يظل دون المستوى المطلوب، ومن ثم نرى أنه يجب تعميم استخدام هذه التقنيات الوقائية بشكل إلزامي في المعاملات الإدارية والمصرفية مع تطوير قدرات المصالح الأمنية على التحقيق الرقمي بشكل مستمر.

الفرع الثاني: دور مركز مكافحة الجرائم المعلوماتية (الدرك والأمن الوطني)

يشهد العالم اليوم تحولاً رقمياً متسارعاً أفرز ظواهر إجرامية جديدة تمثلت في جريمة التزوير الرقمي التي باتت تهدد الأمن الاقتصادي والاجتماعي للدولة الجزائرية، ونظراً لتعقيد هذه الجريمة وتطور أساليب ارتكابها عبر الفضاء السيبراني برزت ضرورة ملحة لإنشاء مراكز متخصصة ضمن جهازي الدرك والأمن الوطني لمكافحتها بفعالية.

أولا– دور الدرك الوطني والأمن الوطني في التحقيق الجنائي الرقمي

إنّ الدرك الوطني والأمن الوطني يضطلعان بدور حيوي ومحوري في حماية الفضاء الرقمي ومكافحة التزوير، حيث تتولى المديرية العامة للأمن الوطني والدرك الوطني مهام الدفاع الأول ضد الجرائم المعلوماتية من خلال مراكز متخصصة[2]، ويعتبر المعهد الوطني للأدلة الجنائية التابع للدرك الوطني ركيزة أساسية في جمع وتحليل الأدلة الرقمية، إذ يطور آليات متخصصة لمعالجة السجلات الإلكترونية والآثار الرقمية والروابط

[1] بيكة باكة، موساوي لمياء، **المرجع السابق**، ص 37.

[2] **مهام الدرك الوطني**، منشور على موقع الدرك الوطني، تم الاطلاع عليه يوم 08 ماي 2026، على الساعة 20:05، على الرابط: https://www.gendarmerie.mr/ar/missions

المزيفة[1]، كما سجلت مصالح شرطة مكافحة الجرائم الإلكترونية التابعة للأمن الوطني قضية 567 المتعلقة بجرائم عبر الإنترنت، مما يعكس النشاط الكبير لهذه المصالح في رصد ومتابعة قضايا التزوير الرقمي[2].

نستخلص من هذا العرض أن التخصص بين الدرك والأمن الوطني يمثل نموذجاً فعالاً في مكافحة التزوير الرقمي، فنحن نرى أن تركيز الدرك على المناطق الريفية والحدودية والأمن على المناطق الحضرية يضمن تغطية جغرافية شاملة للفضاء السيبراني، ومع ذلك نعتقد أن جمع الأدلة الرقمية يظل يواجه صعوبات تقنية نظراً لطبيعة الجرائم السيبرانية التي لا تترك آثاراً مادية واضحة، ونرى أن المعهد الوطني للأدلة الجنائية يجب أن يزود بأحدث التقنيات لتحليل البيانات الضخمة والتعرف على الأنماط الإجرامية، ومن ثم نعتقد أن التكامل المؤسسي بين هذين الجهازين يجب أن يرتقي إلى مستوى تبادل المعلومات اللحظي لضمان فعالية الردع.

ثانيا– أساليب التزوير الرقمي وآليات الوقاية والتوعية

إنّ التزوير الرقمي يتخذ أشكالاً متعددة يستغل فيها المجرمون الثغرات التكنولوجية والسلوكية، منها التصيد الاحتيالي (Phishing) عبر إرسال رسائل إلكترونية مزيفة تهدف إلى سرقة البيانات المصرفية وكلمات المرور، وتزوير الوثائق والمحررات الإلكترونية وتزييف التوقيعات الإلكترونية، والوصول غير المشروع إلى البيانات المالية، وتزوير العلامات التجارية واستخدام شعارات مزيفة لخداع المستهلكين[3] ، وتعمل المراكز المتخصصة على وضع استراتيجيات وقائية تشمل مراقبة الشبكات وتحديد الثغرات الأمنية وتنظيم حملات توعية للجمهور بمخاطر التزوير الرقمي[4]، كما يلعب المركز الوطني للتوقيع الإلكتروني دوراً حيوياً في تأمين الوثائق الرقمية عبر تقنيات التشفير والتصديق التي تعتبر أدوات وقائية حاسمة[5].

نرى أن أساليب التزوير الرقمي تتطور بوتيرة أسرع من آليات المكافحة، مما يفرض على الأجهزة الأمنية مواكبة مستمرة، فنحن نعتقد أن التوعية المجتمعية وإن كانت مهمة تبقى غير كافية ما لم ترافقها حماية تقنية

---

[1] **الفرقة الخاصة للتدخل**، منشور على موقع الدرك الوطني، تم الاطلاع عليه يوم 08 ماي 2026، على الساعة 20:07، على الرابط: https://www.mdn.dz/site_cgn/sommaire/presentation/unit_spe/dsi/dsi_ar.php

[2] **مصالح شرطة مكافحة الجرائم الالكترونية تسجل 567 قضية تتعلق بجرائم الانترنت**، منشور على موقع الشرطة الجزائرية، تم الاطلاع عليه يوم 08 ماي 2026، على الساعة 20:11، على الرابط: https://www.algeriepolice.dz

[3] عمار حشمان، **المرجع السابق**، ص41.

[4] سعيدة بوزنون، **المرجع السابق**، ص51.

[5] **دور المركز الوطني للتصديق الرقمي في تعزيز المعاملات الرقمية الامنة**، منشور على موقع Signit، تم الاطلاع عليه يوم 08 ماي 2026، على الساعة 20:16، على الرابط:https://signit.sa/ar/blogs

مدمجة في الأنظمة المعلوماتية، ونستخلص أن التوقيع الإلكتروني والتشفير يمثلان خط دفاع أولى فعالاً، إلا أن انتشارهما بين المؤسسات والأفراد لا يزال دون المستوى المطلوب، ومن ثم نرى أنه يجب إلزام المؤسسات العمومية والمصرفية باعتماد معايير أمنية رقمية صارمة مع تطوير برامج توعية مستهدفة تصل إلى جميع فئات المجتمع.

الفرع الثالث: دور السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي

يشهد العالم اليوم تحولاً رقمياً متسارعاً أفرز ظواهر إجرامية جديدة تمثلت في جريمة التزوير الرقمي التي باتت تهدد خصوصية الأفراد وسلامة بياناتهم الشخصية، ونظراً لخطورة هذه الجريمة وتداعياتها على الحقوق الدستورية برزت ضرورة ملحة لإنشاء هيئة وطنية مستقلة تضمن حماية المعطيات ذات الطابع الشخصي في مواجهة التلاعب الرقمي.

أولاً- الإطار التشريعي لحماية المعطيات الشخصية ومكافحة التزوير الرقمي

يستند التشريع الجزائري في مجال حماية المعطيات ذات الطابع الشخصي ومكافحة التزوير الرقمي إلى مجموعة من النصوص القانونية المتكاملة. فقد صدر القانون 18-07 المؤرخ في 10 جوان 2018 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، والذي يُعد حجر الزاوية في التشريع الجزائري لحماية البيانات، إذ يهدف إلى تحديد القواعد التي تحكم جمع ومعالجة وتخزين واستخدام البيانات الشخصية، ويضمن مبادئ الشرعية والشفافية وحماية الحقوق الفردية، كما تم تعديله وتتميمه بموجب القانون 25-11 المؤرخ في 24 جويلية 2025 ليتوافق مع المعايير الدولية ويضمن أن تكون عمليات المعالجة متوافقة مع الحقوق الدستورية[1]، وفي سياق مكافحة التزوير الرقمي، يدخل في هذا الإطار قانون 24-02 المتعلق بمكافحة التزوير واستعمال المزور، الذي يفرض عقوبات مشددة على المتورطين في تزوير الوثائق الإلكترونية ويحدد مواصفات تقنية متقدمة تجعل تزويرها أكثر صعوبة[2]، كما يُكمل هذا الإطار قانون 09-04

[1] القانون رقم 25-11 المؤرخ في 24 جويلية 2025، المعدل والمتمم للقانون رقم 18-07 المؤرخ في 10 جوان 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية، العدد 48، الصادر بتاريخ 24 جويلية 2025.

[2] القانون رقم 24-02 المؤرخ في 26 فيفري 2024، المتعلق بمكافحة التزوير واستعمال المزور، الجريدة الرسمية، العدد 15، الصادر بتاريخ 29 فيفري 2024.

المتعلق بالوقاية من الجرائم المرتبطة بأنظمة المعلومات والاتصال[1]، وقانون 15-04 المتعلق بالقواعد الخاصة بالتوقيع الإلكتروني والتصديق[2].

نرى أن الإطار التشريعي الجزائري قد وفّر قاعدة قانونية شاملة تجمع بين حماية البيانات الشخصية ومكافحة التزوير الرقمي، فنحن نعتقد أن القانون 18-07 يمثل خطوة نوعية في الاعتراف الدستوري بالحق في حماية البيانات إلا أن سرعة التطور التقني تجعل تعديله بموجب القانون 25-11 ضرورة ملحة، كما نستخلص أن قانون 24-02، رغم تركيزه على العقوبات قد أدرك أهمية الحماية التقنية للبيانات الحساسة مما يعكس إدراكاً متقدماً لطبيعة الجريمة الرقمية، ومن ثم نرى أن التكامل بين هذه النصوص يشكل درعاً قانونياً متيناً ولكنه يحتاج إلى آليات تنفيذية فعالة تضمن الانتقال من النص إلى الفعل.

ثانياً- دور السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي (ANPDP)

إنّ السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي (ANPDP) تُعد هيئة إدارية مستقلة تتبع رئاسة الجمهورية وتتمتع بالاستقلال المادي والمعنوي، وتضطلع بدور محوري في حماية الأفراد من إساءة استعمال معلوماتهم الشخصية[3]، فمن أهم مهامها الرقابة والتفتيش، حيث تضطلع بدور العين الساهرة على احترام القانون إذ يحق لها إجراء تحقيقات وتفتيشات في حال وجود شكوك حول انتهاكات قانون حماية البيانات، مثل ممارسات إساءة الاستخدام التي قد تؤدي إلى تزوير الهويات الرقمية، كما تشرف السلطة على منح التراخيص والاعتمادات للجهات التي تعالج البيانات سواء كانت مؤسسات عامة أو شركات خاصة مما يضمن عدم وجود ثغرات أمنية تسمح بالتلاعب الرقمي[4]، وتساهم السلطة في تعزيز الحماية الجنائية بالتنسيق مع الجهات القضائية حيث تقوم بإبلاغ السلطات المختصة لاتخاذ الإجراءات الجزائية اللازمة ضد المخالفين، وتشمل العقوبات

[1] القانون رقم 09-04 المؤرخ في 05 أوت 2009، المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47، الصادر بتاريخ 16 أوت 2009.

[2] القانون رقم 15-04 المؤرخ في 01 فيفري 2015، المتعلق بالتوقيع والتصديق الالكترونيين، الجريدة الرسمية، العدد 06، الصادر بتاريخ 10 فيفري 2015.

[3] عواشرة ياسر، **دور السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي**، مذكرة ماستر تخصص قانون الأعمال، كلية الحقوق والعلوم السياسية، جامعة محمد الصديق بن يحي- جيجل، السنة الجامعية 2022/2021، ص62.

[4] قرانة عادل، بوحديد فارس، **مهام السلطة الوطنية لحماية المعطيات الشخصية في التشريع الجزائري**، مجلة العلوم القانونية والاجتماعية، جامعة زيان عاشور بالجلفة، المجلد 06، العدد 02، منشور بتاريخ 01 جوان 2021، ص 1066.

صارمة السجن والغرامات التي تصل إلى خمس سنوات[1]، كما تتعاون السلطة مع جهات دولية وإقليمية في تبادل الخبرات والمعلومات مما يعزز قدرة الجزائر على مواجهة التحديات العالمية الرقمية[2].

نستخلص من هذا العرض أن دور السلطة الوطنية يتجاوز مجرد الرقابة الإدارية ليصل إلى صلب الاستجابة الجنائية ضد التزوير الرقمي، فنحن نرى أن استقلاليتها المؤسسية تمنحها مصداقية في تطبيق القانون، إلا أننا نعتقد أن صلاحياتها التفتيشية يجب أن تكون مدعومة بأدوات تقنية متطورة تمكنها من الكشف المبكر عن الانتهاكات، ونلاحظ أن منح التراخيص والاعتمادات يمثل آلية وقائية فعالة، ولكنه يتطلب تسريع الإجراءات لمواكبة سرعة التحول الرقمي، كما نرى أن التعاون الدولي يظل مجالاً يحتاج إلى مزيد من التفعيل، إذ إن الجرائم العابرة للحدود تستدعي تنسيقاً دولياً ملزماً، ومن ثم نعتقد أن تمكين السلطة من صلاحيات تنفيذية أوسع بما في ذلك القدرة على إصدار أوامر فورية بوقف معالجة البيانات المشبوهة يمثل شرطاً ضرورياً لفعاليتها.

المطلب الثاني: دور مقدمي الخدمات والقطاع الخاص

إن مكافحة التزوير الرقمي لا يمكن أن تتحقق بجهود السلطات العمومية وحدها، بل تستلزم مشاركة فاعلة من القطاع الخاص وخاصة مقدمي خدمات الإنترنت والمؤسسات المالية التي تشكل خط الدفاع الأول في حماية البنية التحتية الرقمية، فهذه الجهات تمتلك القدرة التقنية على رصد الشبهات والتبليغ عنها مما يجعلها شريكاً استراتيجياً لا غنى عنه في المنظومة الوقائية، وقد أقرّ المشرّع الجزائري بهذا الدور من خلال نصوص القانون رقم 09-04 المؤرخ في 5 أوت 2009 التي فرضت التزامات محددة على مقدمي الخدمات في مجال الكشف عن الجرائم المعلوماتية وحماية المعطيات.

الفرع الأول: التزامات مقدمي خدمات الانترنت في الكشف عن التزوير

يُعدّ القانون رقم 24-02 المتعلق بمكافحة التزوير واستعمال المزور الصادر بتاريخ 26 فيفري 2024، من أهم النصوص التشريعية الجزائرية التي استجابت للتحديات الرقمية المستجدة ، إذ وسّع المشرع من خلاله نطاق مفهوم التزوير ليشمل المحررات الرقمية والإلكترونية والتوقيعات الرقمية بما يتجاوز الأطر التقليدية

[1] محمد العيداني، يوسف زروق، **حماية المعطيات الشخصية في الجزائر على ضوء القانون رقم 18-07**، معالم للدراسات القانونية والسياسية، المركز الجامعي تندوف، المجلد 02، العدد 03، منشور بتاريخ 20 ديسمبر 2018، ص 118.

[2] معزوزي نادية، زنير ريان، **النظام القانوني للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي**، مذكرة ماستر تخصص دولة ومؤسسات، كلية الحقوق والعلوم السياسية، جامعة 20 أوت 1955-سكيكدة، دورة جوان 2025، ص52.

المقتصرة على الوثائق المادية، كما ألقى هذا القانون على عاتق مقدمي خدمات الإنترنت مجموعة من الالتزامات المحددة في إطار الكشف عن هذه الجريمة والتعاون في مكافحتها[1].

أولا- التزام الرصد والإبلاغ الفوري

يُلزم القانون 24-02 مقدمي خدمات الإنترنت بمراقبة الأنشطة الرقمية للكشف عن أي تغييرات مشبوهة في البيانات قد تشير إلى ارتكاب جريمة تزوير رقمي، كما يفرض عليهم وجوب الإبلاغ الفوري عن هذه الحالات إلى الجهات المختصة كهيئة حماية البيانات أو الشرطة الإلكترونية أو السلطات القضائية، ويعاقب القانون عدم الإبلاغ بعقوبات جزائية إضافية نظراً لاحتمال تواطؤ مقدم الخدمة في الجريمة[2].

نرى نحن أن هذا الالتزام يكتسي حيوية بالغة في الكشف المبكر عن الجريمة ومنع انتشارها، غير أننا نعتقد أنه يطرح إشكاليات قانونية تتعلق بتحديد درجة العلم المطلوبة من مقدم الخدمة، كما نلاحظ أن مراقبة المحتوى الرقمي والإبلاغ الإلزامي قد تؤدي إلى نوع من الرقابة الاستباقية على الاتصالات، مما يتعارض مع مبدأ حرية الاتصال وحقوق المستخدمين في الخصوصية، وندرك أن الفقرة الجزائية المتعلقة بعقوبة عدم الإبلاغ تظل غامضة في تحديد المعايير الدقيقة للتقصير الموجب للعقاب.

ثانيا- التزام حفظ السجلات والأدلة الرقمية

يُطلب من مقدمي خدمات الإنترنت الاحتفاظ بسجلات النشاط الرقمي لمدة محددة تتراوح بين ستة أشهر وسنة ، كما يتعين عليهم تخزين البيانات الرقمية غير المعدلة كدليل قضائي يمكن استخدامه في التحقيقات المتعلقة بحالات التزوير، ويشترط القانون ضمان سرية هذه المعلومات وعدم الولوج إليها إلا بأمر قضائي.[3]

ندرك أن هذا الالتزام ضروري لتمكين السلطات من تتبع الجرائم الرقمية وجمع الأدلة اللازمة لمحاكمة الجناة ، غير أننا نرى أن التزام حفظ السجلات لمدة طويلة يُثقل كاهل مقدمي الخدمات مادياً وتقنياً، كما نعتقد أنه قد يتعارض مع مبدأ حماية البيانات الشخصية إذا لم تُضمن ضمانات صارمة للولوج إلى هذه البيانات وتخزينها، ونؤكد أن هذه السجلات تشمل البيانات الوصفية والمعلومات المتعلقة بالهوية الرقمية وهي عناصر تقنية ضرورية لإثبات واقعة التزوير الرقمي أمام القضاء.

---

[1] القانون رقم 24-02 المؤرخ في 26 فيفري 2024، المتعلق بمكافحة التزوير واستعمال المزور، الجريدة الرسمية، العدد 15، الصادر بتاريخ 29 فيفري 2024.

[2] بوجلال كواشي، بوريو فيصل، **المرجع السابق**، ص 72.

[3] بن لعربي أسماء، الفحلة مديحة، **المرجع السابق**، ص 450

ثالثا– التزام التعاون مع السلطات الأمنية والقضائية

يشدد القانون على وجوب تقديم مقدمي الخدمات للوصول إلى البيانات عند الطلب الرسمي من السلطات المختصة، كما يُلزمهم بتطبيق تقنيات التشفير والتحقق من البيانات بشكل فعال في إطار التعاون المستمر مع الجهات الأمنية والقضائية، ويعرض القانون مقدم الخدمة الذي يمتنع عن هذا التعاون إلى عقوبات جزائية إضافية.[1]

نرى أن هذا التعاون يعد ركيزة أساسية في محاربة التزوير الرقمي، خاصة وأن الشرطة الإلكترونية في الجزائر تلعب دوراً محورياً في التحقيق في الجرائم الرقمية، غير أننا نعتقد أن التعاون يجب أن يكون مؤطّراً بإجراءات قضائية واضحة لمنع أي استخدام تعسفي للسلطة من قبل الأجهزة الأمنية، كما نلاحظ أن المشرع كان بإمكانه تحديد آلية زمنية دقيقة لتقديم البيانات المطلوبة لضمان الفعالية دون الإخلال بالحقوق الدستورية للمستخدمين.

رابعا– التزام تطبيق معايير الوقاية التقنية

يشجع القانون مقدمي خدمات الإنترنت على تبني معايير أمنية متقدمة وتطبيق بروتوكولات التحقق من الهوية الرقمية، كما يشمل هذا الالتزام استخدام أنظمة الكاميرات الرقمية والبرمجيات المتقدمة للكشف عن التزوير باعتباره خطوة وقائية استباقية، ويُعدّ هذا التعزيز الأمني ركيزة لتعزيز الثقة في البيئة الرقمية وحماية المستخدمين من المخاطر الرقمية.[2]

نرى أن هذا الالتزام يمثل توجيهاً إيجابياً نحو الوقاية قبل العلاج، غير أننا نعتقد أن المشرع أخطأ بعدم جعله التزاماً قانونياً ملزماً بصياغة صريحة، كما نلاحظ أن التشجيع دون الإلزام يُضعف من فعالية هذه المعايير ويترك المجال أمام مقدمي الخدمات للتملص من المسؤولية التقنية، ونؤكد أننا كنا نفضّل أن يكون التبني إلزامياً مع تحديد معايير دقيقة تضمن جودة الأنظمة الأمنية المطبقة بما يتوافق مع المستوى العالمي.

[1] شعباني نوال، **المرجع السابق**، ص 597.

[2] بوجلال كواشي، بوريو فيصل، **المرجع السابق**، ص 73.

الفرع الثاني: مسؤولية البنوك في حماية المحررات المالية الرقمية

يُعدّ القانون رقم 24-02 المتعلق بمكافحة التزوير واستعمال المزور الصادر بتاريخ 26 فيفري 2024، من أهم النصوص التشريعية الجزائرية التي استجابت للتحديات الرقمية المستجدة في مجال المحررات المالية[1]، إذ وسّع المشرع من خلاله نطاق مفهوم التزوير ليشمل المحررات الرقمية والإلكترونية والتوقيعات الرقمية بما يتجاوز الأطر التقليدية المقتصرة على الوثائق المادية[2]، كما شدد هذا القانون من العقوبات المقررة بشكل استثنائي إذ بلغت العقوبة السجنية عشر سنوات في حالة التزوير في المحررات الإدارية، وتراوحت بين ثلاث وخمس سنوات في حالة الحصول على إعانات أو وثائق مالية بالتزوير، وبين خمس وعشر سنوات في حالة تزوير وثائق مالية أو مساعدات عبر التزوير، وفي سياق متصل، أصدر بنك الجزائر النظام رقم 24-02 المؤرخ في 13 أكتوبر 2024، والمتعلق بتنظيم تقديم الخدمات والمنتجات المصرفية عبر القنوات الرقمية، والذي يفرض على البنوك تبني متطلبات أمنية صارمة لحماية المحررات المالية الرقمية[3]، وقد تضمنت هذه الإطارات التشريعية والتنظيمية مسؤوليات مزدوجة للبنوك تجاه العملاء والسلطات، تتجاوز المجرد الالتزام بالقوانين لتشمل جوانب وقائية وتقنية وتعاونية[4].

أولا- الإطار القانوني والتنظيمي لمسؤولية البنوك

يفرض القانون 24-02 المتعلق بمكافحة التزوير واستعمال المزور، الصادر في 26 فيفري 2024، إطاراً قانونياً صارماً يهدف إلى حماية المحررات المالية الرقمية من جريمة التزوير[5]، وقد جاء هذا القانون ليمثل نقلة نوعية في المقاربة القانونية للتصدي لجرائم التزوير الرقمية، إذ يعالج الاختلالات الناجمة عن ظاهرة التزوير الرقمي المتنامية وما يرتبط بها من تقنيات رقمية ، كما يهدف النظام رقم 24-02 الصادر عن بنك الجزائر بتاريخ 13 أكتوبر 2024 إلى تنظيم تقديم الخدمات والمنتجات المصرفية عبر القنوات الرقمية، مع

---

[1] القانون رقم 24-02 المؤرخ في 26 فيفري 2024، المتعلق بمكافحة التزوير واستعمال المزور، الجريدة الرسمية، العدد 15، الصادر بتاريخ 29 فيفري 2024.

[2] **القانون الجديد: مكافحة التزوير واستعمال المزور في الجريدة الرسمية**، موقع ديزاد news، منشور بتاريخ 13 مارس 2024، تم الاطلاع عليه يوم 13 ماي 2026، على الساعة 13:51، على الرابط: https://dznews.dz

[3] **هذه أهم الشروط الخاصة بانشاء بنك رقمي في الجزائر**، موقع ايكو ألجيريا، منشور بتاريخ 22 نوفمبر 2024، تم الاطلاع عليه يوم 13 ماي 2026، على الساعة 13:57، على الرابط: https://www.eco-algeria.dz/content

[4] كعوان محمد، بلعزام مبروك، **مسؤولية البنك المحسوب عليه عند الوفاء للشيك المتقن التزوير عبر المقاصة الالكترونية**، مجلة العلوم القانونية والاجتماعية، جامعة زيان عاشور- الجلفة، المجلد 08، العدد 03، منشور بتاريخ 01 سبتمبر 2023، ص 1005.

[5] القانون رقم 24-02 المؤرخ في 26 فيفري 2024، المتعلق بمكافحة التزوير واستعمال المزور، الجريدة الرسمية، العدد 15، الصادر بتاريخ 29 فيفري 2024.

التركيز على الإدارة عن بعد وحصر آلية الإدارة عبر الإنترنت، ويشترط هذا النظام على مؤسسي البنوك امتلاك الخبرة الرقمية اللازمة لتأسيس وممارسة نشاط البنوك الرقمية، ويفرض على البنوك تطبيق أنظمة صارمة لضمان أمن المعاملات المصرفية الإلكترونية، وذلك من خلال بنية تحتية قوية للحماية تشمل أنظمة المقاصة الإلكترونية وأنظمة الدفع الإلكتروني[1].

ثانيا– التدابير الوقائية والتقنية للحماية

تتجاوز مسؤولية البنوك المجرد الالتزام بالقوانين لتشمل جوانب وقائية وتقنية تضمن أقصى درجات الحماية للمحررات المالية الرقمية، وتشمل هذه التدابير تبني البنوك لآليات أمنية متطورة للحماية من التزوير الإلكتروني، كالتشفير القوي، وأنظمة التحقق الثنائي (Two-Factor Authentication)، والرصد المستمر للمعاملات المشبوهة[2]، كما يُشدد على ضرورة امتثال البنوك للمعاملات باستخدام تقنيات حديثة مثل "تشين البلوك" (Blockchain) لتعزيز الأمان والشفافية وحماية البيانات الشخصية والمالية للمواطنين[3].

ثالثا– المسؤولية المدنية والجزائية للبنوك

تتحمل البنوك مسؤولية قانونية مزدوجة في إطار حماية المحررات المالية الرقمية تتجلى في مسؤولية وقائية ومدنية وجنائية [4]، وفي مجال تزوير بطاقات الدفع الإلكترونية يعالج المشرع الجزائري هذه الجريمة بالاعتماد على النصوص العامة في قانون العقوبات الجزائري، سيما المواد المتعلقة بالتزوير في الفصول 280 وما يليها، دون وجود نصوص صريحة خاصة بالبطاقات الإلكترونية، ويتحمل المرتكبون العقوبات الجنائية المباشرة، كما قد تتحمل البنوك مسؤولية مدنية تعويضية بموجب قانون المعاملات البنكية إذا أثبت العميل إهمال البنك في تطبيق أنظمة الحماية الرقمية[5]، ويُبرز مبدأ العناية الواجبة ضرورة اتخاذ البنوك إجراءات وقائية دقيقة

---

[1] **هذه أهم الشروط الخاصة بانشاء بنك رقمي في الجزائر**، موقع ايكو ألجيريا، منشور بتاريخ 22 نوفمبر 2024، تم الاطلاع عليه يوم 13 ماي 2026، على الساعة 14:05، على الرابط: https://www.eco-algeria.dz/content

[2] كعوان محمد، بلعزام مبروك، **المرجع السابق**، ص 1006.

[3] منير ركاب، **توظيف الذكاء الاصطناعي و"البلوك تشين" والدينار الرقمي لحماية السيادة المالية بالجزائر**، موقع الشروق أونلاين، منشور بتاريخ 27 أفريل 2026، تم الاطلاع عليه يوم 13 ماي 2026، على الساعة 14:09، على الرابط: https://www.echoroukonline.com

[4] كعوان محمد، بلعزام مبروك، **المرجع السابق**، ص 1007.

[5] حسونة عبد الغني، **المعالجة القانونية لتزوير بطاقات الدفع الالكترونية**، مجلة الحقوق والحريات، جامعة محمد خيضر– بسكرة، المجلد 12، العدد 01، منشور بتاريخ 05 أفريل 2024، ص 285.

داخلية تتطلب مطابقة النموذج مع الإضاءة، بالإضافة إلى تضافر الأنظمة التقنية الخارجية قبل الاعتماد على الاستثمار[1].

رابعا- التعاون مع السلطات والامتثال التنظيمي

تفرض التشريعات الجزائرية على البنوك التعاون الفعال مع السلطات الرقابية والأمنية في مجال مكافحة التزوير الرقمي، ويضع حظر تداول العملات الافتراضية والأصول الرقمية بموجب المادة 6 مكرر من قانون مكافحة غسل الأموال وتمويل الإرهاب تحدياً أمام البنوك لضمان عدم استخدام منصاتها في أنشطة محظورة، كما يعكس هذا الحظر التزام الجزائر بتعزيز الشفافية في النظام المصرفي وبمكافحة الجرائم المالية، وتسعى البنوك الجزائرية، كبنك الخارجي الجزائري (BEA)، إلى التطور نحو الالتزام بمعايير الأمن السيبراني وتعزيز خدماتها الرقمية[2].

الفرع الثالث: التبليغ عن الجرائم الرقمية وحماية المبلغين

يُعتبر القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتعلق بالوقاية من الجرائم المرتبطة بالتكنولوجيات الإعلامية والاتصال بمثابة الحجر الزاوي في المنظومة القانونية الجزائرية لمكافحة الجرائم الرقمية، وقد جاء هذا القانون ليضع إطاراً للعقوبات ويوفر الآليات اللاحقة العامة القضائية لمكافحة الجرائم الإلكترونية بما في ذلك التزوير الرقمي[3]، كما يتناول القانون رقم 24-02 الصادر في 26 فيفري 2024 المتعلق بمكافحة التزوير واستعمال المزور، بشكل خاص جريمة التزوير الإلكتروني والتوقيعات الرقمية والسجلات الإلكترونية وشهادات التصديق التي أصبحت جزءاً لا يتجزأ من الحياة اليومية والاقتصادية[4]، وفي هذا السياق، تكتسي آليات التبليغ عن هذه الجرائم وحماية المبلغين أهمية حيوية لضمان فعالية المكافحة، حيث

[1] كعوان محمد، بلعزام مبروك، **المرجع السابق**، ص 1007.

[2] **تعليمات صارمة لمنع العملات المشفرة في الجزائر**، موقع العربي الجديد، منشور بتاريخ 01 ديسمبر 2025، تم الاطلاع عليه يوم 13 ماي 2026، على الساعة 14:17، على الرابط: https://www.aajsa.com/economy

[3] القانون رقم 09-04 المؤرخ في 05 أوت 2009، المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47، الصادر بتاريخ 16 أوت 2009.

[4] القانون رقم 24-02 المؤرخ في 26 فيفري 2024، المتعلق بمكافحة التزوير واستعمال المزور، الجريدة الرسمية، العدد 15، الصادر بتاريخ 29 فيفري 2024.

تتطلب الجرائم الرقمية استجابة قانونية شاملة تسلط الضوء على الأنظمة القانونية وآليات الكشف وحماية الشهود والمبلغين[1].

أولا- آليات التبليغ الإلزامي والطوعي عن جريمة التزوير الرقمي

تدرك الجزائر أن فعالية مكافحة الجرائم الرقمية تعتمد بشكل كبير على قدرة الأفراد والمؤسسات على الإبلاغ عن هذه الجرائم، ولذلك وضعت آليات متعددة لتسهيل عملية التبليغ، ويفرض القانون 09-04 بموجب المادة 6 منه، على مقدمي خدمات الاتصال والهاتف والإنترنت التبليغ الإلزامي الفوري عن أي جريمة رقمية يتم اكتشافها، مما يعزز دور هذه المؤسسات كخط دفاع أول في مكافحة الجرائم الإلكترونية[2]، كما يشجع القانون الأفراد على التبليغ الطوعي عن الجرائم الرقمية إلى الجهات المختصة كالشرطة الجزائرية والدرك الوطني والوحدات المتخصصة في الجرائم الإلكترونية التابعة لوزارة العدل، بالإضافة إلى السلطات القضائية، وأصبحت متاحة منصات إلكترونية رسمية مثل موقع الشرطة الجزائرية وتطبيقات الإبلاغ الرقمية لتسهيل عملية التبليغ على الأفراد والمؤسسات الأمنية والقضائية، كما يتطلب التبليغ عن الجرائم الرقمية تقديم أدلة رقمية تمثل سجلات الوصول والبرمجيات المصابة، ويجري التحقيق فيها من قبل السلطات القضائية المتخصصة، وهناك تعاون دولي محتمل عبر اتفاقيات مثل اتفاقية بودابست التي انضمت إليها الجزائر لتعزيز قدرتها على معالجة الجرائم العابرة للحدود[3].

ثانيا- حماية المبلغين في التشريع الجزائري

تُعد حماية المبلغين عن الجرائم الرقمية أمراً حيوياً لضمان فعالية جهود المكافحة، حيث يتردد الأفراد في الإبلاغ عن المخالفات خوفاً من الانتقام في ظل غياب حماية كافية[4]، ويتضمن القانون 09-04 أحكاماً لحماية المبلغين من الانتقام، حيث تطبق قواعد الحماية العامة للشهود المنصوص عليها في قانون الإجراءات الجزائية، خاصة المواد 25 و127 المتعلقة بسرية الهوية ومنع التعرض للمبلغين والشهود ، وتشمل الحماية القانونية

---

[1] **الدعوة الى التعجيل باصدار التنظيم المتعلق بتدابير حماية المبلغين عن الفساد**، وكالة الأنباء الجزائرية، منشور بتاريخ 30 أفريل 2026، تم الاطلاع عليه يوم 13 ماي 2026، على الساعة 15:28، على الرابط: https://www.aps.dz/algerie/societe/mols6aqk

[2] عزة خولة، ربيع شيماء، **اليات مكافحة الجرائم الالكترونية في التشريع الجزائري**، مذكرة ماستر تخصص قانون الاعلام والانترنت، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الابراهيمي- برج بوعريريج، السنة الجامعية: 2024/2023، ص 64.

[3] بوعجاجة بلال، عراب ربيعة، **الجريمة المعلوماتية وسبل مكافحتها في التشريع الجزائري**، مذكرة ماستر تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة عباس لغرور- خنشلة، الموسم الجامعي: 2024/2023، ص 21.

[4] **الدعوة الى التعجيل باصدار التنظيم المتعلق بتدابير حماية المبلغين عن الفساد**، وكالة الأنباء الجزائرية، منشور بتاريخ 30 أفريل 2026، تم الاطلاع عليه يوم 13 ماي 2026، على الساعة 16:03، على الرابط: https://www.aps.dz/algerie/societe/mols6aqk

للمبلغين سرية الهوية عند الإبلاغ إذا لزم الأمر، وضمان سلامة المبلغين وحماية مصالحهم، وذلك بهدف تشجيع الإبلاغ دون خوف[1]، ومع ذلك، تشير الدراسات الأكاديمية إلى الحاجة إلى آليات تقنية حديثة للحفاظ على سرية المبلغين، خاصة معالجة فعالة للبلاغات المجهولة والمشفرة، بالإضافة إلى تكثيف الدورات التكوينية للقضاة لزيادة كفاءتهم في التعامل مع القضايا السيبرانية، كما يدعو البعض إلى تعديلات تشريعية لتعزيز الحماية القانونية الشاملة، مثل إشكاليات تنظيم التوقيع الإلكتروني في الأمر 15-04 التي تستدعي معالجة الثغرات القانونية[2].

المطلب الثالث: التعاون الدولي في مكافحة التزوير الرقمي

إن الطبيعة العابرة للحدود للإنترنت تجعل من جريمة التزوير الرقمي ظاهرة دولية بامتياز، إذ قد يرتكب الجاني فعله من دولة، مستخدماً خادماً إلكترونياً في دولة أخرى، ليؤثر في ضحية تقع في دولة ثالثة، وهذا الواقع يجعل الملاحقة القضائية الوطنية وحدها عاجزة عن مواجهة هذا النوع من الجرائم مهما بلغت كفاءة الآليات المؤسساتية الداخلية، ومن ثم يصبح التعاون الدولي سواء على مستوى تسليم المجرمين أو المساعدة القضائية المتبادلة أو التنسيق عبر المنظمات الدولية ضرورة قصوى لا محيد عنها.

وقد سعت الجزائر إلى الانخراط في هذا التعاون الدولي من خلال الانضمام إلى اتفاقية بودابست حول جرائم المعلوماتية الموقعة بتاريخ 23 نوفمبر 2001، وكذا اتفاقية العربية لمكافحة جرائم تقنية المعلومات المنعقدة بالقاهرة بتاريخ 21 سبتمبر 2010، مما يعكس إرادة واضحة في مواءمة تشريعها الوطني مع المعايير الدولية.

الفرع الأول: اليات تسليم المجرمين والمساعدة القضائية المتبادلة

يفرض القانون رقم 24-02 المتعلق بمكافحة التزوير واستعمال المزور الصادر في 26 فيفري 2024 إطاراً قانونياً صارماً يجرّم التزوير الرقمي ويوسّع نطاق العقوبات لتشمل المحررات الإلكترونية والتوقيعات الرقمية بما يتجاوز الأطر التقليدية المقتصرة على الوثائق المادية[3]، كما يُعدّ هذا القانون استكمالاً للقانون 09-04 المؤرخ في 05 أوت 2009 المتعلق بالوقاية من الجرائم المرتبطة بالتكنولوجيات الإعلامية والاتصال، والذي

[1] بن لعربي أسماء، الفحلة مديحة، **المرجع السابق**، ص 450.

[2] مصطفاوي اسامة، **المرجع السابق**، ص48.

[3] القانون رقم 24-02 المؤرخ في 26 فيفري 2024، المتعلق بمكافحة التزوير واستعمال المزور، الجريدة الرسمية، العدد 15، الصادر بتاريخ 29 فيفري 2024.

يُعتبر حجر الزاوية في المنظومة القانونية الجزائرية لمكافحة الجرائم الإلكترونية[1]، وفي سياق التعاون الدولي يخضع تسليم المجرمين في الجزائر لأحكام قانون الإجراءات الجزائية بالإضافة إلى اتفاقيات دولية ثنائية ومتعددة الأطراف، منها اتفاقية بودابست واتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة (اتفاقية باليرمو)، التي تُعدّ معياراً دولياً للتزامات الدول في مكافحة الجرائم الإلكترونية العابرة للحدود[2]، كما تبرز أهمية حماية التوقيع الإلكتروني كركيزة أساسية في مكافحة جريمة التزوير الرقمي إذ تلعب التوقيعات الرقمية دوراً حيوياً في تحديد صحة المستندات الرقمية وسلامتها وهو ما يؤثر بشكل مباشر على قبول الأدلة في إجراءات تسليم المجرمين والمساعدة القضائية المتبادلة[3].

أولا- شروط وإجراءات تسليم المجرمين في قضايا التزوير الرقمي

تخضع عملية تسليم المجرمين في الجزائر لشروط وإجراءات محددة تنظمها نصوص قانون الإجراءات الجزائية بالتوازي مع الاتفاقيات الدولية، حيث يُشترط مبدأ الازدواجية الجنائية باعتباره شرطاً أساسياً، أي أن الفعل المطلوب تسليم المجرم بسببه يجب أن يكون مجرماً في كل من الدولة الطالبة والدولة المطلوب منها التسليم، كما يجب أن يكون المطلوب للتسليم قد ارتكب فعلاً يعاقب عليه القانون في كلا البلدين بعقوبة سالبة للحرية تزيد عن سنة واحدة على الأقل[4]، ويتم تقديم طلب التسليم بشكل رسمي عبر وزارة العدل، مرفقاً بالوثائق والمستندات القانونية اللازمة التي تثبت هوية المطلوب وصحة الأحكام أو مذكرات التوقيف الصادرة بحقه[5]، ويُمنع التسليم إذا كانت الجريمة سياسية أو عقوبتها الإعدام، كما يُمنع إذا كانت الدولتان قد أبرمتا اتفاقية تستبعد

---

[1] القانون رقم 09-04 المؤرخ في 05 أوت 2009، المتعلق بالوقاية من الجرائم المرتبطة بتكنولوجيات الاعلام والاتصال، الجريدة الرسمية، العدد 47، الصادر بتاريخ 16 أوت 2009.

[2] **دليل عملي لصياغة طلب تعاون فعال للدول الأعضاء في فرقة العمل المشتركة لمنطقتي الشرق الأوسط وشمال افريقيا**، مكتب الأمم المتحدة المعني بالمخدرات والجريمة، تم الاطلاع عليه يوم 16 ماي 2026، على الساعة 16:35، على الرابط: https://www.unodc.org/documents/terrorism/Publications/MATF_Practical_Guide_AR/MATF_Practical_Guide_AR_UNODC_final.pdf

[3] حسام بن ميسية، عبد المولى حملاوي، **اليات مكافحة الجريمة الالكترونية في التشريع الجزائري**، مذكرة ماستر تخصص قانون جنائي، معهد الحقوق، المركز الجامعي عبد الحفيظ بوالصوف- ميلة، السنة الجامعية 2025/2024، ص 70.

[4] العنيد محمد زيد، عصماني ليلى، **شروط تسليم المجرمين في النظام القانوني الجزائري**، مجلة الاجتهاد القضائي، جامعة محمد خيضر بسكرة، المجلد 13، العدد 02، منشور بتاريخ 31 مارس 2021، ص 627.

[5] امل المرشدي، **بحث قانوني كبير عن نظام تسليم المجرمين**، موقع محاماة نت، منشور بتاريخ 05 أكتوبر 2016، تم الاطلاع عليه يوم 16 ماي 2026، على الساعة 16:54، على الرابط: https://www.mohamah.net

هذه الجريمة من نطاق التسليم[1]، وفي إطار مكافحة التزوير الرقمي تكتسي هذه الشروط أهمية بالغة نظراً لطبيعة الجريمة العابرة للحدود وصعوبة تحديد مكان ارتكاب الفعل في الفضاء السيبراني[2].

ندرك أن شروط التسليم التقليدية قد تكون عائقاً أمام فعالية ملاحقة مرتكبي التزوير الرقمي حيث أن مبدأ الازدواجية الجنائية يصعب تطبيقه عملياً في ظلّ التباين الكبير بين التشريعات الوطنية في مجال الجرائم الإلكترونية، كما نرى أن شرط العقوبة السالبة للحرية لمدة سنة قد لا يتناسب مع الخطورة النسبية لبعض أشكال التزوير الرقمي التي تستوجب تسليماً سريعاً حتى وإن كانت العقوبة أقل، ونؤكد أن الإجراءات البيروقراطية المتعلقة بتقديم الطلب عبر القنوات الدبلوماسية تتناقض مع سرعة انتشار الجريمة الرقمية مما يستدعي تبسيط الإجراءات وتخصيص قنوات رقمية للتعاون القضائي الدولي. ونعتقد أن المشرع الجزائري كان بإمكانه إدراج نصوص خاصة في القانون 24-02 تُيسّر إجراءات التسليم في الجرائم الرقمية دون الإخلال بالضمانات الأساسية.

ثانيا- المساعدة القضائية المتبادلة وتبادل الأدلة والمعلومات الرقمية

تُعدّ المساعدة القضائية المتبادلة (MLA) جزءاً لا يتجزأ من آليات التعاون الدولي في مكافحة جريمة التزوير الرقمي، إذ تهدف إلى تسهيل الإجراءات القضائية بين الدول المتعاونة وتبادل المعلومات والأدلة والخبرات الفنية[3]، ويشمل نطاق المساعدة القضائية في الجزائر جمع الأدلة الرقمية المتعلقة بجرائم التزوير الإلكتروني، والاستماع للشهود عن بعد، وتجميد الأصول الإلكترونية، بالإضافة إلى تبادل المصاريف القضائية والمنازعات الإجرائية المترتبة عن التعاون[4]، وتتم هذه الإجراءات عبر قنوات التعاون الدولي المتعددة، منها قنوات الاتصال المباشرة والمنتظمة بين النيابات، وقنوات الشرطة الدولية (الإنتربول)، واتفاقيات التعاون الثنائية

---

[1] سيليني نسيمة، **عدم تسليم المجرمين في الجرائم السياسية وفقا للاتفاقيات الدولية**، المجلة الأكاديمية للبحوث القانونية والسياسية، جامعة عمار ثليجي الأغواط، المجلد 05، العدد 01، منشور بتاريخ 14 مارس 2021، ص 261.

[2] وفاء صدراتي، **اليات مكافحة جريمة التزوير الالكتروني**، أطروحة دكتوراه العلوم في القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي- تبسة، السنة الجامعية 2021/2020، ص 275.

[3] **المساعدة القضائية**، موقع مجلس قضاء الجزائر، تم الاطلاع عليه يوم 16 ماي 2026، على الساعة 17:05، على الرابط: https://cour-alger.mjustice.dz

[4] **قانون المساعدة القضائية الأمر رقم 71-57 المعدل والمتمم بالقانون رقم 01-06**، موقع طريق العدالة، منشور بتاريخ 25 فيفري 2020، تم الاطلاع عليه يوم 16 ماي 2026، على الساعة 17:11، على الرابط: https://www.abridh.com/aide-judiciaire/

بين الجزائر ودول أخرى كتونس والمغرب وفرنسا[1]، كما تلعب شبكات الإنتربول دوراً متزايد الأهمية في مكافحة الجرائم الإلكترونية المتعلقة بالتزوير والمحاكمات الرقمية، مع ضرورة التأكيد على احترام الخصوصية والحقوق الأساسية أثناء تبادل البيانات[2].

نرى أن المساعدة القضائية المتبادلة تمثل الآلية الأنسب للتعامل مع جريمة التزوير الرقمي نظراً لطبيعتها غير المادية، غير أننا نعتقد أن القنوات الحالية للتعاون تفتقر إلى السرعة والمرونة المطلوبة في عالم يتسم بالتغير التقني المستمر، كما نلاحظ أن جمع الأدلة الرقمية عبر الحدود يواجه عقبات تقنية ولغوية وقانونية كبيرة، خاصة في ظلّ تباين معايير حماية البيانات بين الدول، وندرك أن الإنتربول رغم أهميته إلا أن آلياته قد لا تكون مصممة خصيصاً للتعامل مع الأدلة الرقمية المعقدة، ونؤكد أن تجميد الأصول الإلكترونية يظلّ تحدياً كبيراً في ظلّ استخدام المجرمين للعملات المشفرة والمحافظ الرقمية مما يستدعي تطوير اتفاقيات دولية خاصة بالأدلة الرقمية والأصول الافتراضية.

الفرع الثاني: دور المنظمات الدولية (الانتربول والاتفاقيات الدولية)

يُعتبر القانون رقم 24-02 المتعلق بمكافحة التزوير واستعمال المزور، الصادر بتاريخ 26 فيفري 2024، من أهم النصوص التشريعية الجزائرية التي استجابت للتحديات الرقمية المستجدة، إذ أقرّ المشرع من خلاله إطاراً قانونياً صارماً يجرّم التزوير الرقمي ويوسّع نطاق العقوبات لتشمل المحررات الإلكترونية والتوقيعات الرقمية بما يتجاوز الأطر التقليدية المقتصرة على الوثائق المادية، كما يُكمّل هذا القانون القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتعلق بالوقاية من الجرائم المرتبطة بالتكنولوجيات الإعلامية والاتصال، والذي يُعتبر حجر الزاوية في المنظومة القانونية الجزائرية لمكافحة الجرائم الإلكترونية بوجه عام، وفي ظلّ طبيعة الجريمة الرقمية العابرة للحدود برزت أهمية حيوية للتعاون الدولي والمنظمات الدولية كالإنتربول والاتفاقيات الدولية في مكافحة جريمة التزوير الرقمي حيث تتطلب هذه الجريمة استجابة قانونية وتشغيلية مرنة وتعاونية لمواجهة التحديات المتزايدة.

---

[1] دنيا حفصة، **البرلمان يصادق على مشروع قانون اتفاقية تسليم المجرمين بين تونس والجزائر: وزيرة العدل: 28 انابة قضائية صادرة من تونس و110 واردة من الجزائر و199 سجينا جزائريا في تونس، موقع المغرب يومية مستقلة**، منشور بتاريخ 17 جانفي 2024، تم الاطلاع عليه يوم 16 ماي 2026، على الساعة 17:17، على الرابط: https://ar.lemaghreb.tn

[2] **قانون نموذجي بشأن تسليم المجرمين (2004)**، الأمم المتحدة المكتب المعني بالمخدرات والجريمة، تم الاطلاع عليه يوم 16 ماي 2026، على الساعة 17:20، على الرابط: https://www.unodc.org/documents/organized-crime/Publications/Model_Law_extradition_AR.pdf

أولا- دور الإنتربول كشبكة عالمية لمكافحة الجريمة السيبرانية

تُعتبر منظمة الشرطة الجنائية الدولية (الإنتربول) حجر الزاوية في التعاون الشرطي العالمي لمكافحة جريمة التزوير الرقمي بشتى أشكالها، إذ يمتد دور الإنتربول ليشمل جوانب حيوية تدعم الجهود المبذولة من الدول الأعضاء ومنها الجزائر في معركتها ضد هذه الجريمة، ويساعد الإنتربول في تنسيق الجهود بين سلطات الشرطة في 196 دولة عضو، ويشمل ذلك جمع وتحليل المعلومات وتبادلها بشكل آمن عبر منصة خاصة، مما يمكن من تتبع المجرمين وتحليل أنماط الجريمة على نطاق عالمي، كما يسهم الإنتربول في دعم العمليات الميدانية المشتركة، ومنها على سبيل المثال حملة "سيرينغيتي 2.0" التي استهدفت الشبكات الإجرامية للاحتيال الرقمي في أفريقيا، والتي أسفرت عن توقيف المئات من المشتبه بهم واستعادة مبالغ مالية كبيرة [1]، ويعمل الإنتربول أيضاً على تطوير البنية التحتية للاتصالات الشرطية الآمنة وتعزيز القدرات التحليلية للبيانات الجنائية بالإضافة إلى تنظيم فعاليات لزيادة الوعي بمخاطر الجرائم الإلكترونية وتعزيز الأمن على الإنترنت[2].

ثانيا- اتفاقية الأمم المتحدة لمكافحة الجريمة واتفاقية بودابست

تشكل الاتفاقيات الدولية الأساس القانوني العالمي لمكافحة جريمة التزوير الرقمي والجرائم السيبرانية، إذ توفر هذه الاتفاقيات إطاراً موحداً لتجريم الفعال الإجرامية وتسهيل التعاون القضائي بين الدول، وتُعدّ اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة (اتفاقية باليرمو) من أهم هذه الاتفاقيات، حيث تدعو الدول الأعضاء إلى تبني مضامينها وتنفيذها، وتهدف إلى توحيد تعريف الجرائم الإلكترونية وتحديد آليات التعاون الدولي لتقديم المساعدة القضائية المتبادلة وتبادل المعلومات[3]، كما تُعتبر اتفاقية بودابست من أبرز الاتفاقيات التي وضعت إطاراً قانونياً موحداً للاستجابة الوطنية المتناسقة في مجال معالجة الجرائم المعلوماتية، وتساهم في تنسيق التشريعات الوطنية لمواجهة التهديدات السيبرانية، وتلتزم الجزائر بالعديد من الاتفاقيات الدولية المتعلقة بمكافحة الجريمة المنظمة والإرهاب، حيث تتطلب هذه الالتزامات تكييف التشريعات الوطنية بما يتوافق مع المعايير

[1] **الانتربول يضرب شبكات الاحتيال الرقمي بافريقيا ويوقف المئات**، قناة الجزيرة، منشور بتاريخ 24 أوت 2025، تم الاطلاع عليه يوم 16 ماي 2026، على الساعة 17:44، على الرابط: https://www.aljazeera.net/news

[2] **فعالية للانتربول تقدم نصائح لصون السلامة عبر الانترنت**، الانتربول (المنظمة الدولية للشرطة الجنائية)، منشور بتاريخ 13 مارس 2025، تم الاطلاع عليه يوم 16 ماي 2026، على الساعة 17:58، على الرابط: https://www.interpol.int/en/News-and-Events/News/2025/INTERPOL-event-shares-tips-for-staying-safe-online

[3] وفاء صدراتي، **المرجع السابق**، ص279.

الدولية، مما يعزز قدرة الجزائر على التعاون مع المنظمات الدولية وتبادل الأدلة الرقمية وملاحقة الجناة عبر الحدود[1].

الفرع الثالث: تقييم مدى مواءمة التشريع الجزائري للاتفاقيات الدولية (اتفاقية بودابست)

يُعتبر تقييم مدى مواءمة التشريع الجزائري للاتفاقيات الدولية وخاصة اتفاقية بودابست من المسائل القانونية الحيوية في عصر التحول الرقمي المتسارع إذ تفرض الجرائم الرقمية العابرة للحدود تحديات تنظيمية وقانونية تتطلب تكاملاً بين النصوص الوطنية والمعايير الدولية[2]، وقد أصبحت اتفاقية بودابست الموقعة في بودابست بتاريخ 23 نوفمبر 2001 والمصادق عليها بالمرسوم رقم 2006-580 المؤرخ في 23 ماي 2006، من أهم الإطارات القانونية الدولية في مجال مكافحة الجرائم المعلوماتية حيث تضع معايير دولية لحماية البيانات الشخصية وتجريم الفعل المعلوماتي وتسهيل التعاون الدولي، وفي السياق الجزائري يُعدّ القانون رقم 24-02 المتعلق بمكافحة التزوير واستعمال المزور، الصادر بتاريخ 26 فيفري 2024، إضافة نوعية إلى المنظومة التشريعية الوطنية إذ وسّع نطاق التزوير ليشمل المحررات الرقمية والإلكترونية والتوقيعات الرقمية[3]، كما يُكمّل هذا القانون القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتعلق بالوقاية من الجرائم المرتبطة بالتكنولوجيات الإعلامية والاتصال، والذي يُعتبر حجر الزاوية في المنظومة القانونية الجزائرية لمكافحة الجرائم الإلكترونية.

أولا- مواءمة أحكام جمع الأدلة والتعاون الدولي

تتطلب اتفاقية بودابست من الدول الأطراف وضع إجراءات فعالة لجمع الأدلة الرقمية وتبادل المعلومات مع الجهات الدولية لمكافحة الجريمة العابرة للحدود، وقد أظهر التحليل أن التشريع الجزائري يتمتع بدرجة مواءمة جيدة في هذا المحور[4]، وقد أسست الجزائر مبادرات للتعاون الدولي في مجال تبادل المعلومات والأدلة مع الجهات الدولية، خاصة في إطار التعاون الجزائري-الأوروبي، مما يعكس إرادة حقيقية في التفاعل مع المجتمع

---

[1] حسام بن ميسية، عبد المولى حملاوي، **المرجع السابق**، ص78.

[2] **ندوة جزائرية- أوروبية حول "الجريمة المعلوماتية"**، موقع الشروق أونلاين، منشور بتاريخ 24 سبتمبر 2023، تم الاطلاع عليه يوم 16 ماي 2026، على الساعة 17:58، على الرابط: https://www.echoroukonline.com

[3] بوديسة بجاد عبد الرؤوف، **اليات التحري عن الجريمة الالكترونية في القانون الجزائري**، مذكرة ماستر تخصص قانون الاعلام الالي والانترنت، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الابراهيمي- برج بوعريريج، السنة الجامعية 2022/2021، ص 73.

[4] قطاف سليمان، بوقرين عبد الحليم، **الاليات القانونية الموضوعية لمكافحة الجرائم السيبرانية في ظل اتفاقية بودابست والتشريع الجزائري**، المجلة الاكاديمية للبحوث القانونية والسياسية، جامعة عمار ثليجي- الاغواط، المجلد 06، العدد 01، منشور بتاريخ 31 مارس 2022، ص 337.

الدولي[1]، كما يتجسد دور المؤسسات القضائية الجزائرية العليا، كالمحكمة العليا، في تطبيق هذه التشريعات وتفسيرها بما يتوافق مع المعايير الدولية.

ثانيا: التعاون الدولي وتبادل المعلومات في إطار المواءمة

تظهر الجزائر التزاماً واضحاً بتعزيز التعاون الدولي في مجال مكافحة الجرائم المعلوماتية، بما في ذلك جريمة التزوير الرقمي، حيث تشارك في ندوات ونقاشات حول التعاون الجزائري–الأوروبي في مجال الجريمة المعلوماتية، مما يعكس رغبتها في التفاعل مع المجتمع الدولي، وقد أظهر التحليل أن جانب التعاون الدولي يتميز بدرجة مواءمة مرتفعة بين التشريع الجزائري ومعايير اتفاقية بودابست، إذ أن القانون 09–04 والقانون 24–02 قد أقرّا آليات للتعاون مع المنظمات الدولية والجهات الأجنبية في مجال تبادل المعلومات والأدلة الرقمية، كما أن الجزائر قد أصدرت قوانين جديدة وعدّلت قوانين قائمة في إطار سعيها لتحقيق مواءمة أكبر مع المعايير الدولية، خاصة في مجال جريمة التزوير الرقمي، مما يدل على إدراك المشرع الجزائري لأهمية التكامل بين التشريع الوطني والالتزامات الدولية[2].

[1] **ندوة جزائرية– أوروبية حول "الجريمة المعلوماتية"**، موقع الشروق أونلاين، منشور بتاريخ 24 سبتمبر 2023، تم الاطلاع عليه يوم 16 ماي 2026، على الساعة 18:01، على الرابط: https://www.echoroukonline.com

[2] قطاف سليمان، بوقرين عبد الحليم، **المرجع السابق**، ص 341.

خلاصة الفصل الثاني

يتضح من دراسة هذا الفصل أن مكافحة جريمة التزوير الرقمي لا تتوقف عند حدود التجريم، بل تمتد لتشمل منظومة متكاملة من الإجراءات والآليات المؤسساتية التي تضمن فعالية التحقيق وسلامة الإثبات وسرعة الملاحقة، فالخصوصية التي تكتسيها الجريمة المعلوماتية، من حيث خفاء الفاعل وسرعة الانتشار وطبيعة الأدلة الرقمية القابلة للتلف، تجعل من الإطار الإجرائي التقليدي غير كافٍ لمواجهتها، مما يستدعي تطوير آليات خاصة تتماشى مع طبيعة هذا النوع من الجرائم.

وفي المبحث الأول، تبين أن إجراءات البحث والتحري في جرائم التزوير الرقمي تتطلب خبرة تقنية خاصة، إذ إن التفتيش الإلكتروني يختلف جوهرياً عن نظيره التقليدي، سواء من حيث طرق الولوج إلى الأنظمة المعلوماتية أو ضبط البيانات وحفظها، وقد أكدت الدراسة ضرورة احترام ضوابط قانونية صارمة أثناء إجراءات التفتيش، تضمن التوازن بين فعالية التحقيق وحماية الحريات الفردية وخاصة الحق في الخصوصية، كما تبين أن ضبط الأدلة الرقمية يخضع لقواعد فنية دقيقة، تتمثل في إجراءات التحريز الرقمي (Hash Value) التي تضمن عدم تغيير البيانات المضبوطة وسلامتها طوال مراحل التقاضي، أما الأساليب التحقيقية الخاصة، كاعتراض المراسلات الإلكترونية والمراقبة الرقمية، فتظل خاضعة لرقابة قضائية مشددة تمنع أي تجاوز أو إخلال بالحقوق الأساسية للأفراد.

أما المبحث الثاني، فقد أوضح أن إثبات جريمة التزوير الرقمي يواجه تحديات جوهرية تتعلق بموثوقية الدليل الرقمي وحجيته أمام القضاء، فالأدلة الرقمية – رغم ما تتمتع به من دقة وغنى في المعلومات – تظل قابلة للتزوير ذاتها مما يفرض إثبات سلامتها ونزاهتها وفق معايير فنية وقانونية محددة، وقد تبين من الدراسة أن الخبرة القضائية المعلوماتية أضحت ركيزة أساسية في كشف آثار التلاعب وتحليل البيانات المزورة، وأن تقرير الخبير الرقمي يكتسب حجية علمية كبيرة أمام قاضي الموضوع، شريطة استيفائه شروط الشكل والموضوع، كما برزت إشكالية الاختصاص القضائي كأحد التحديات الجوهرية إذ إن الجرائم المرتكبة عبر الإنترنت تثير صعوبات في تحديد المكان والجهة المختصة، مما يستدعي تخصيص أقطاب قضائية مدربة على التعامل مع القضايا المعلوماتية، وتطوير قواعد الاختصاص المحلي بما يواكب طبيعة هذه الجرائم العابرة للحدود.

وفي المبحث الثالث، اتضح أن مكافحة التزوير الرقمي تقتضي تنسيقاً مؤسساتياً واسعاً يتجاوز الأجهزة الأمنية والقضائية لتشمل هيئات وطنية متخصصة، كالهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ومركز مكافحة الجرائم المعلوماتية، والسلطة الوطنية لحماية المعطيات ذات الطابع

الشخصي، التي تلعب أدواراً تكميلية في الوقاية والرقابة والتنسيق، كما تبين أن القطاع الخاص – وخاصة مقدمو خدمات الإنترنت والمؤسسات المالية – يتحملون التزامات قانونية في الكشف عن التزوير وحماية البيانات، وأن التعاون الدولي يمثل ضرورة حتمية في ظل طبيعة الجريمة العابرة للحدود، سواء من خلال آليات تسليم المجرمين والمساعدة القضائية المتبادلة، أو عبر دور المنظمات الدولية كالإنتربول والاتفاقيات الدولية ذات الصلة، وعلى رأسها اتفاقية بودابست، غير أن الدراسة كشفت عن ثغرات في مواءمة التشريع الجزائري مع هذه الاتفاقيات، مما يقتضي مراجعات تشريعية لضمان اندماج أفضل في المنظومة الدولية لمكافحة الجرائم المعلوماتية.

ويمكن الاستنتاج من هذا الفصل بأجمعه أن فعالية مكافحة التزوير الرقمي في الجزائر ترتكز على ثلاث ركائز متكاملة: إجراءات تحقيق تقنية دقيقة تحترم الحريات، ونظام إثبات قادر على ضمان حجية الأدلة الرقمية، وهيكل مؤسساتي وطني ودولي متكامل، غير أن هذا الإطار لا يزال يواجه تحديات تتعلق بالتكوين القضائي والأمني، وتطوير البنية التحتية التقنية، وتعزيز التعاون بين القطاعين العام والخاص، مما يفرض مواصلة الجهود لبلورة استراتيجية شاملة تضع الجزائر في مصاف الدول الفاعلة في مكافحة الجرائم المعلوماتية.

الخاتمة

الخاتمة

لقد كان موضوع الحماية القانونية من جرائم التزوير الرقمي في التشريع الجزائري محط اهتمام هذه الدراسة، انطلاقاً من الإدراك بأن التحول الرقمي الذي يشهده العالم اليوم لم يقتصر على تغيير أدوات التواصل والتعامل، بل امتد ليشمل طبيعة الجرائم ذاتها وآليات مكافحتها، وقد حاولنا من خلال هذه المذكرة تقديم قراءة علمية متكاملة للإطار الموضوعي والإجرائي والمؤسساتي لجريمة التزوير الرقمي، من خلال استقراء النصوص القانونية المنظمة لهذا النوع من الجرائم، وتحليل أركانها المادية والمعنوية، وتقييم السياسة العقابية المعتمدة، فضلاً عن الوقوف على الآليات الإجرائية المتاحة لضبط الأدلة الرقمية وإثباتها، ودور الهيئات الوطنية والتعاون الدولي في مجال الملاحقة والوقاية، وقد تبين لنا أن التشريع الجزائري قد خطا خطوات مهمة نحو التجريم والحماية، غير أن هذه الخطوات لا تزال بحاجة إلى مزيد من التطوير والتحديث لتواكب التطورات التقنية المتسارعة والأساليب الإجرامية المستجدة.

وإذا كانت الإشكالية المركزية للبحث قد تمحورت حول مدى كفاية الحماية القانونية التي يوفرها التشريع الجزائري من جرائم التزوير الرقمي، وقدرة النصوص الجزائية والإجرائية الحالية على مواجهة التحديات التقنية والإجرامية المستجدة، فإن الإجابة عنها تقتضي التمييز بين مستويين: فمن حيث المبدأ، يتوفر التشريع الجزائري على نصوص تجريمية تغطي أشكال التزوير الرقمي الرئيسية، وتنظيمية تعترف بالمحرر الإلكتروني والتوقيع الرقمي، مما يشكل أساساً قانونياً للحماية، غير أن هذا الأساس لا يخلو من ثغرات، سواء على مستوى دقة التجريم وملاءمة العقوبات، أو على مستوى الآليات الإجرائية المعقدة التي تتطلب تدخلاً تقنياً متخصصاً يفوق في كثير من الأحيان إمكانيات الأجهزة الأمنية والقضائية التقليدية، وعليه، يمكن القول إن الحماية القانونية موجودة لكنها غير كافية بشكل مطلق، وأن النصوص الحالية قادرة على مواجهة بعض التحديات، لكنها تظل عاجزة عن استيعاب كل الابتكارات الإجرامية في ظل ثورة الذكاء الاصطناعي والعملات الرقمية والعقود الذكية.

من خلال ما تقدم، يمكن حصر أهم النتائج التي توصل إليها البحث في النقاط التالية:

• التزوير الرقمي ليس مجرد امتداد للتزوير التقليدي، بل هو جريمة مستقلة ذات خصائص مميزة، تتمثل في عدم المادية، وسهولة النسخ والتعديل، وصعوبة الكشف عنها، وطبيعتها العابرة للحدود، مما يستدعي نظاماً قانونياً خاصاً لا يكتفي بتطبيق قواعد التزوير العادية.

• الاعتراف القانوني بالمحرر الإلكتروني والتوقيع الرقمي يشكل ركناً أساسياً في الحماية من التزوير، لكن هذه الحماية تبقى رهينة بتوفر شروط تقنية وقانونية صارمة تضمن سلامة البيانات ونزاهتها، وهو ما يفرض ضرورة التوعية والتكوين في هذا المجال.

• أركان جريمة التزوير الرقمي تطرح إشكاليات نظرية وعملية، خاصة فيما يتعلق بتحديد السلوك الإجرامي المادي في الفضاء الافتراضي، والعلاقة السببية بين الفعل والنتيجة، والقصد الجنائي الخاص المتمثل في نية الاستعمال، وهي إشكاليات تتطلب تأويلاً قضائياً دقيقاً.

• السياسة العقابية المعتمدة في التشريع الجزائري تتسم بالتنوع بين العقوبات الأصلية والتكميلية، غير أنها تفتقر في بعض جوانبها إلى التناسب مع خطورة الجريمة، خاصة في ظل غياب عقوبات خاصة بالجرائم المرتكبة باستخدام الذكاء الاصطناعي أو تقنيات التشفير المتقدمة.

• الإثبات في جرائم التزوير الرقمي يواجه تحديات جسيمة تتمثل في هشاشة الدليل الرقمي وإمكانية تلفه أو تزويره، مما يجعل الخبرة القضائية المعلوماتية ضرورة حتمية لا غنى عنها، غير أنها لا تزال تواجه نقصاً في التكوين والتنظيم في الجزائر.

• الاختصاص القضائي في الجرائم العابرة للحدود يظل من أكثر المسائل إشكالاً، حيث تتداخل الاختصاصات المحلية والنوعية، وتبرز صعوبة تسليم المجرمين وتنفيذ الأحكام في ظل غياب اتفاقيات ثنائية متخصصة.

• التعاون الدولي يمثل ركيزة أساسية في مكافحة التزوير الرقمي، لكن فعاليته تبقى محدودة بالاختلافات بين التشريعات الوطنية وضعف آليات المساعدة القضائية المتبادلة في الجرائم المعلوماتية.

وبناءً على ما توصل إليه البحث من نتائج، نقدم مجموعة من التوصيات التي نرجو أن تسهم في تطوير الإطار القانوني والمؤسساتي لمكافحة التزوير الرقمي:

• على المستوى التشريعي: ضرورة مراجعة النصوص الجزائية المنظمة للجرائم المعلوماتية بشكل دوري لضمان مواكبتها للتطورات التقنية، مع إدخال مصطلحات تقنية دقيقة تضمن اليقين القانوني، وتجريم أشكال جديدة من التزوير الرقمي الناشئة.

• على المستوى العقابي: تطوير السياسة العقابية بما يتناسب مع خطورة الجريمة الرقمية، من خلال تشديد العقوبات في الحالات التي يكون فيها الفاعل موظفاً عاماً أو متخصصاً في المعلوماتية، وإقرار عقوبات تكميلية فعالة مثل المنع الدائم من ممارسة المهن المعلوماتية.

• على المستوى الإجرائي: تطوير دليل إجرائي خاص بالجرائم المعلوماتية ينظم عمليات الضبط والتفتيش والمعاينة الإلكترونية بما يحفظ حقوق الأفراد ويضمن سلامة الأدلة الرقمية، مع اعتماد معايير دولية في التحريز الرقمي.

• على المستوى المؤسساتي: تعزيز قدرات الهيئات الوطنية المكلفة بمكافحة الجرائم المعلوماتية، وإنشاء وحدات متخصصة في الدرك والأمن الوطني تعنى بالتحري الرقمي، وتطوير مراكز التكوين القضائي والأمني في مجال الجريمة المعلوماتية.

• على المستوى القضائي: إحداث أقطاب قضائية متخصصة في الجرائم المعلوماتية على المستوى الوطني، تضم قضاة مدربين تقنياً، وتسهيل استعانة القضاء بخبراء معتمدين في المعلوماتية، مع ضمان استقلاليتهم وحياديتهم.

• على المستوى الدولي: تعزيز التعاون القضائي الدولي من خلال الانضمام إلى الاتفاقيات الدولية المتخصصة في الجرائم المعلوماتية، وإبرام اتفاقيات ثنائية لتسليم المجرمين وتبادل الأدلة الرقمية، والمشاركة الفاعلة في شبكات التحري الدولية.

• على المستوى الوقائي: إطلاق حملات توعية وطنية للمواطنين والمؤسسات حول مخاطر التزوير الرقمي وسبل الوقاية منه، وتشجيع اعتماد أنظمة أمنية متقدمة في المعاملات الإلكترونية، وإلزام مقدمي الخدمات الرقمية بالتبليغ عن الجرائم.

• على المستوى الأكاديمي: تشجيع البحث العلمي في مجال الجرائم المعلوماتية من خلال تخصيص منح وبرامج دكتوراه في هذا المجال، وتنظيم ندوات ومؤتمرات علمية تجمع بين القانونيين والتقنيين لمناقشة الإشكاليات الناشئة.

ختاماً، يظل التزوير الرقمي تحدياً مستمراً يفرض على المشرع والقضاء والمجتمع بأسره ضرورة التعاون والتكامل بين الأدوات القانونية والتقنية والمؤسساتية، فالقانون وحده غير كافٍ ما لم يصحبه وعي مجتمعي

وتكوين مهني وتعاون دولي فعال، وإذا كانت هذه الدراسة قد أسهمت في تسليط الضوء على بعض جوانب الإشكال، فإنها تدرك في الوقت ذاته أن الجريمة الرقمية تتطور بوتيرة أسرع من قدرة القانون على ملاحقتها، وهو ما يجعل البحث في هذا المجال مفتوحاً على الدوام، ويستدعي من الباحثين القادمين مواصلة الاستكشاف والتأصيل، لعلهم يصلون إلى نموذج قانوني متكامل يحقق التوازن بين حماية النظام الرقمي وصون الحريات الفردية في عالم يزداد رقمنة يوماً بعد يوم.

قائمة المصادر و المراجع

قائمة المصادر والمراجع

أولا: المصادر:

1) المعاجم والقواميس

معجم المعاني الجامع، "تزوير"، تاريخ الاطلاع 12 مارس2026، على الساعة 22:02، عبر الرابط: https://www.almaany.com/ar/dict/ar-ar/التزوير/

2) النصوص القانونية

أ- النصوص التشريعية

- الدستور:

دستور الجمهورية الجزائرية الديمقراطية الشعبية لسنة 1996 المعدل والمتمم، الجريدة الرسمية، العدد 82، الصادر بتاريخ 30 ديسمبر 2020.

- المعاهدات الدولية:

1. Convention on Cybercrime (Budapest Convention), 2001.

- الأوامر والقوانين:

1. الامر رقم 66-156 المؤرخ في 8 جوان 1966 المتضمن قانون العقوبات ، المعدل والمتمم بموجب القانون رقم 24-06 المؤرخ في 28 افريل 2024 ، الجريدة الرسمية للجمهورية الجزائرية ، العدد 30 ، 30 أفريل 2024.
2. القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، المعدل و المتمم للأمر رقم 66-156 والمتضمن قانون العقوبات، الجريدة الرسمية، العدد 71، الصادرة بتاريخ 10 نوفمبر 2004.
3. الامر رقم 75-58 المؤرخ في 26 سبتمبر 1975، المتضمن القانون المدني المعدل والمتمم بموجب القانون رقم 05-10 المؤرخ في 20 جوان 2005، الجريدة الرسمية، العدد 44، 2005.
4. القانون رقم 06-01 المؤرخ في 20 فيفري 2006، المتعلق بالوقاية من الفساد ومكافحته، موقع الديوان المركزي لقمع الفساد، تم الاطلاع عليه يوم 14 أفريل 2026، على الساعة 14:24، على الرابط: https://ocrc.gov.dz.

5. القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006، المتضمن قانون الاجراءات الجزائية، الجريدة الرسمية، العدد 84، الصادر بتاريخ 24 ديسمبر 2006.

6. القانون رقم 08-09 المؤرخ في 25 فيفري 2008، المتضمن قانون الاجراءات المدنية والادارية المعدل والمتمم بالقانون رقم 22-13 المؤرخ في 12 جويلية 2022، الجريدة الرسمية، العدد48، الصادر بتاريخ 17 جويلية 2022.

7. القانون 09-04 المؤرخ في 5 أوت 2009 المتعلق بالوقاية من الجرائم المرتبطة بتكنولوجيات الاعلام والاتصال لمكافحتها، الجريدة الرسمية، العدد 47، الصادر بتاريخ 16 أوت 2009.

8. Code pénal français, Articles 323-3 & 226-4-1(modifiér par le loi n° 2014-617 du 13 juin 2014)

9. Code pénal français, Articles 323-1 & 323-3 (modifiér par le loi n° 2015-912 du 24 juillet 2015)

10. القانون رقم 15-04 المؤرخ في 1 فيفيري 2015، المتعلق بالتوقيع والتصديق الالكتروني، الجريدة الرسمية، العدد06، الصادر بتاريخ 10 فيفري2015.

11. القانون رقم 18-05، المؤرخ في 10 ماي2018، المتعلق بالتجارة الالكترونية، الجريدة الرسمية، العدد28، الصادر بتاريخ 16 ماي 2018.

12. القانون رقم 18-07 المؤرخ في 10 جوان 2018 المعدل والمتمم بالقانون رقم 25-11 المؤرخ في 24 جويلية 2025، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية، العدد 34، الصادر بتاريخ 10 جوان 2018.

13. الأمر رقم 21-11 المؤرخ في 25 أوت 2021 المعدل والمتمم للأمر رقم 66-153 المؤرخ في 08 جوان 1966، المتضمن قانون الاجراءات الجزائية، الجريدة الرسمية، العدد 65، الصادر بتاريخ 26 أوت 2021.

14. القانون رقم 23-14 المؤرخ في 27 أوت 2023، المتعلق بالاعلام، الجريدة الرسمية، العدد 56، الصادر بتاريخ 29 أوت 2023.

15. قانون رقم 24-02 المؤرخ في 26 فيفري 2024، يتعلق بمكافحة التزوير و استعمال المزور، ج.ر، عدد 15، 29 فيفري 2024.

16. القانون رقم 24-06 المؤرخ في 28 افريل 2024 ، المعدل و المتمم للامر 66-156 المتضمن قانون العقوبات ، الجريدة الرسمية للجمهورية الجزائرية ، العدد 30 ، 30 أفريل 2024.

17. القانون 24-02 المؤرخ في 26 فيفري 2024، المتعلق بمكافحة التزوير واستعمال المزور، الجريدة الرسمية، العدد 15، الصادر بتاريخ 29 فيفري 2024.

18. القانون 24-06 المؤرخ في 28 أفريل 2024 المعدل والمتمم للأمر رقم 66-156 المؤرخ في 8 جوان 1966، المتضمن قانون العقوبات، الجريدة الرسمية، العدد 30، الصادر بتاريخ 30 أفريل 2024.

19. القانون رقم 25-11 المؤرخ في 24 جويلية 2025 المعدل والمتمم للقانون رقم 18-07 المؤرخ في 10 جوان 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية، العدد 48، الصادر بتاريخ 24 جويليلة 2025.

20. القانون رقم 25-11 المؤرخ في 24 جويلية 2025، المتعلق بحماية الاشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية، العدد 48، الصادر بتاريخ 24 جويلية 2025.

21. القانون رقم 15-04 المؤرخ في 1 فيفري2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، الجريدة الرسمية، العدد 06، الصادر بتاريخ 10 فيفري2015.

ب- النصوص التنظيمية

- المراسيم:

1. المرسوم التفيذي رقم 16-135 المؤرخ في 25 ماي 2016 المتعلق بالتوقيع الالكتروني، الجريدة الرسمية، العدد 32، الصادر بتاريخ 29 ماي 2016.

- القرارات الوزارية والادارية:

1. بنك الجزائر، تعليمات رقم 01-25، المؤرخة في 02 مارس 2025، المتعلقة بشروط الترخيص بتأسيس واعتماد بتك ومؤسسة مالية، الجزائر، سنة 2025.

ج- الأحكام والقرارات القضائية

1. قرار صادر عن المحكمة العليا، غرفة الجنح والمخالفات، ملف رقم 1185414، المؤرخ في 20 جويلية 2023، قضية (ع.م) ومن معه ضد (د.م) والنيابة العامة، منشور على الموقع الالكتروني للمحكمة العليا، تم الاطلاع عليه يوم 25 مارس 2026، على الساعة 23:30، على الرابط: https://www.coursupreme.dz

2. قرار صادر عن المحكمة العليا، الغرفة الجزائية، ملف رقم 1168028، المؤرخ في 09 فيفري 2023، قضية (ب.ب) ضد (ب.ع) والنيابة العامة، موقع المحكمة العليا، تم الاطلاع عليه يوم 05 ماي 2026، على الساعة 00:28، على الرابط: https://coursupreme.dz/

ثانيا: المراجع:

1) الكتب

1. احمد فتحي سرور، **الوسيط في قانون العقوبات–القسم الخاص**، الطبعة الرابعة، دار النهضة العربية، القاهرة، سنة 2006.
2. امال قارة، **الحماية الجنائية للمعلوماتية في التشريع الجزائري**، الطبعة الثانية، دار هومة، الجزائر، 2010.
3. جمال نجيمي، **جرائم التزوير في قانون العقوبات الجزائري**، دار هومة، الطبعة الثانية، الجزائر، 2014.
4. زيدان زبيحة ، **الجريمة المعلوماتية في التشريع الجزائري و الدولي** ، دار الهدى ، د.ط، الجزائر ، 2011.
5. علي عبد القادر القهوجي، **قانون العقوبات–القسم الخاص**، الطبعة الأولى، الدار الجامعية، الاسكندرية، سنة 2003.
6. محمد سعيد نمور، **جرائم الحاسوب والانترنت**، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، سنة 2010.
7. محمود نجيب حسني، **شرح قانون العقوبات–القسم الخاص**، الطبعة السادسة، دار النهضة العربية، القاهرة، سنة 1989.
8. نجيمي جمال، **جرائم التزوير في قانون العقوبات الجزائري**، د.ط، دار هومة للطباعة والنشر، الجزائر، د.ت.ن.
9. يزيد بوحليط، **الجرائم الالكترونية والوقاية منها في القانون الجزائري**، د.ط، دار الجامعة الجديدة، الاسكندرية، سنة 2019.
10. Garçon émile, **Code pénal annoté**, Tome 02, Librairie du Recueil Sirey, Paris, 1956.
11. Jean Pradel, **Droit pénal spécial**, 16e édition, Cujas, paris, 2011.

ثالثا: الأطروحات والمذكرات:

- أطروحات دكتوراه

1. درابلة العمري سليم، **حجية الدليل الرقمي في الاثبات الجنائي**، أطروحة دكتوراه علوم تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر 01، السنة الجامعية 2024/2025.

2. غولم بونفلة، **أثر اليقظة الاستراتيجية على الأداء المتميز للمؤسسات الاقتصادية: دراسة حالة عينة من المؤسسات الجزائرية**، أطروحة دكتوراه تخصص ادارة الأعمال، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة 08 ماي 1945 قالمة، سنة 2021.

3. قمراوي حفيظة، **الحماية القانونية لبطاقة الدفع الالكتروني في التشريع الجزائري**، اطروحة دكتوراه تخصص قانون الاعمال المقارن، كلية الحقوق والعلوم السياسية، جامعة وهران2 محمد بن أحمد، سنة 2025.

4. وفاء صدراتي، **اليات مكافحة جريمة التزوير الالكتروني**، أطروحة دكتوراه العلوم في القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي– تبسة، السنة الجامعية 2020/2021.

- رسائل الماجستير ومذكرات الماستر

- رسائل الماجستير

1. الفالح نافل، عبد الكريم العقلة، **جريمة التزوير الالكتروني: دراسة تحليلية مقارنة**، رسالة ماجستير، كلية الحقوق، جامعة الاسراء بالأردن، سنة 2014.

2. أحمد مسعود مريم، قريشي محمد، **اليات مكافحة جرائم تكنولوجيات الاعلام والاتصال في ضوء القانون رقم 09/04**،رسالة ماجستير تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح ورقلة، السنة الجامعية 2012/2013.

3. ايمان مكري، **الجريمة الالكترونية في التشريع الجزائري**، رسالة ماجستير تخصص تشريعات اعلامية، كلية الاعلام والاتصال، جامعة الجزائر 3، السنة الجامعية 2014/2015.

4. عمر عبد السلام حسن الجبوري، **جريمة تزوير الالكتروني في تشريع الاردني دراسة مقارنة**، رسالة ماجستير، جامعة شرق الاوسط، كلية الحقوق، 2017، الأردن.

5. هاجر طبا، صبرينة مقالتي، **الأدلة الرقمية ودورها في الإثبات الجنائي**، رسالة ماجستير في الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي – برج بوعريريج، السنة الجامعية 2020-2021.

- مذكرات الماستر

6. أبو بكر التيتاوي، الياس مالك قرادي، **جرائم النصب والاحتيال الالكتروني في التشريع الجزائري**، مذكرة ماستر تخصص القانون الجنائي والعلوم الجنائية، معهد الحقوق، المركز الجامعي المقاوم الشيخ امود بن مختار ايليزي، السنة الجامعية 2024/2025.

7. ألجية قريب، **دور الشرطة العلمية في اثبات جريمة التزوير في المحررات**، مذكرة ماستر تخصص قانون جنائي وعلوم جنائية، كلية الحقوق، جامعة الجزائر1- بن يوسف بن خدة، سنة 2025.

8. أوساسي فؤاد، **دور الدليل الرقمي في الاثبات الجنائي**، مذكرة ماستر تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور بالجلفة، الموسم الجامعي 2019/2020.

9. التجاني ايمان واخرون، **المسؤولية الجزائية عن الاستخدام غير المشروع للذكاء الاصطناعي**، مذكرة ماستر تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية جامعة قاصدي مرباح ورقلة، السنة الجامعية 2023/2024.

10. اية بن ميسية، **الجريمة الالكترونية واليات مكافحتها في التشريع الجزائري**، مذكرة ماستر في القانون الجنائي، معهد الحقوق، المركز الجامعي عبد الحفيظ بوالصوف ميلة، 2025.

11. بساحة سليمة، **جريمة التزوير الالكتروني**، مذكرة ماستر في القانون القضائي، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس، مستغانم، 2025.

12. بن داني راضية، **الرقابة والاشراف على الأعمال الضبطية القضائية في التشريع الجزائري**، مذكرة ماستر تخصص قانون جنائي، كلية الحقوق والعلوم الساسية، جامعة عبد الحميد بن باديس مستغانم، السنة الجامعية 2019/2020.

13. بن صويلح سفيان، حريدي الياس، **مكافحة التزوير واستعمال المزور في ظل القانون 24-02**، مذكرة ماستر تخصص قانون الأعمال، كلية الحقوق والعلوم السياسية، جامعة 8 ماي 1945 قالمة، السنة الدراسية 2024/2025.

14. بوجلال كواشي، بوريو فيصل، **جريمة التزوير واستعمال المزور وفق القانون رقم 24-02**، مذكرة ماستر تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة باتنة 1 الحاج لخضر، السنة الجامعية 2024/2025.

15. بوديسة بجاد عبد الرؤوف، **اليات التحري عن الجريمة الالكترونية في القانون الجزائري**، مذكرة ماستر تخصص قانون الاعلام الالي والانترنت، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الابراهيمي- برج بوعريريج، السنة الجامعية 2021/2022.

16. بوعجاجة بلال، عراب ربيعة، **الجريمة المعلوماتية وسبل مكافحتها في التشريع الجزائري**، مذكرة ماستر تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة عباس لغرور- خنشلة، الموسم الجامعي: 2023/2024.

17. بيكة باكة، موساوي لمياء، **اليات مكافحة الجريمة الالكترونية في التشريع الجزائري**، مذكرة ماستر تخصص قانون جنائي وعلوم جنائية، معهد الحقوق، المركز الجامعي الشيخ أمود بن مختار اليزي، السنة الجامعية 2022/2023.

18. جليلة بلعلمي، صالح مزري، **الدليل الرقمي والاثبات الجنائي**، مذكرة ماستر تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح ورقلة، السنة الجامعية 2021/2022.

19. جنيدي محمد الصغير، منصوري محمد عبد الوهاب، **الأقطاب الجزائية المستحدثة في التشريع الجزائري**، مذكرة ماستر تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح- ورقلة، السنة الجامعية 2021/2022.

20. حسام بن ميسية، عبد المولى حملاوي، **اليات مكافحة الجريمة الالكترونية في التشريع الجزائري**، مذكرة ماستر تخصص قانون جنائي، معهد الحقوق، المركز الجامعي عبد الحفيظ بوالصوف- ميلة، السنة الجامعية 2024/2025.

21. ديابي زينب، **جرائم التزوير واستعمال المزور في التشريع الجزائري**، مذكرة ماستر تخصص قانون خاص، معهد الحقوق، المركز الجامعي مغنية، السنة الجامعية 2023/2024.

22. زعيون عبد الوهاب، بشكيط يوسف، **مكافحة جريمة تزوير المحررات الرسمية في ظل أحكام القانون رقم: 24-02**، مذكرة ماستر تخصص قانون جنائي، معهد الحقوق، المركز الجامعي عبد الحفيظ بوالصوف- ميلة، السنة الجامعية 2024/2025.

23. زيداني جمال الدين، **مهام الأقطاب الجزائية المتخصصة في القضاء الجزائري**، مذكرة ماستر تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف- المسيلة، السنة الجامعية 2021/2022.

24. سعيد بن لحرش، **الحماية الجزائية للتوقيع الالكتروني**، مذكرة ماستر في الحقوق تخصص قانون أعمال، جامعة زيان عاشور، الجلفة، 2021.

25. سلاوي مارية، يوسفي عفاف، **أحكام الجرائم السيبرانية في التشريع الجزائري**، مذكرة ماستر تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة 1، السنة الجامعية 2024/2025.

26. سيق الدين الخليفي واخرون، **حماية المعطيات الشخصية في زمن الذكاء الاصطناعي**، ماستر قانون العقود والانظمة العقارية، كلية العلوم القانونية والاقتصادية والاجنماعية، ماي 2025.

27. شهيرة مسعود، **الجريمة الالكترونية في التشريع الجزائري**، مذكرة ماستر تخصص قانون عام، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس مستغانم، 14 جويلية 2021.

28. عبد القادر دارم، جلال حدوش، **السياسة الجنائية في ظل القانون 24-02 يتعلق بمكافحة التزوير واستعمال المزور**، مذكرة ماستر تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة غرداية، السنة الجامعية 2024/2025.

29. عزة خولة، ربيع شيماء، **اليات مكافحة الجرائم الالكترونية في التشريع الجزائري**، مذكرة ماستر تخصص قانون الاعلام والانترنت، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الابراهيمي- برج بوعريريج، السنة الجامعية: 2023/2024.

30. عمار حشمان، **الجريمة المعلوماتية في التشريع الجزائري**، مذكرة ماستر تخصص ادارة التحقيقات الاقتصادية والمالية، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، جامعة قاصدي مرياح ورقلة، السنة الجامعية 2018/2019.

31. عمور زهير، **الخبرة القضائية في المواد الجنائية**، مذكرة ماستر تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس- مستغانم، السنة الجامعية 2020/2021.

32. عواشرة ياسر، **دور السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي**، مذكرة ماستر تخصص قانون الأعمال، كلية الحقوق والعلوم السياسية، جامعة محمد الصديق بن يحي- جيجل، السنة الجامعية 2021/2022.

33. قسمية نجاة، **الحماية الجزائية للخصوصية الرقمية في التشريع الجزائري**، مذكرة ماستر تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة باتنة 1 الحاج لخضر، السنة الجامعية 2024/2025.

34. كيحول عبد القادر، **التفتيش الالكتروني كاجراء للتحقيق في الجرائم المعلوماتية**، مذكرة ماستر تخصص قانون جنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة زيان عاشورالجلفة، السنة الجامعية 2019/2020.

35. لشخب عبد الحق، جبايلي عبد الرحيم، **جريمة التزوير في التشريع الجزائري**، مذكرة ماستر تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة عباس لغرور خنشلة، السنة الجامعية 2024/2025.

36. لمصارة أنفال، محلول منال، **اجراءات التفتيش الالكتروني في التشريع الجزائري**، مذكرة ماستر تخصص قانون جنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة باتنة1 الحاج لخضر، السنة الجامعية 2024-2025.

37. محمد الشريف بوالعراس، أسامة طلحي، **جريمة التزوير المعلوماتية**، مذكرة ماستر تخصص قانون اعلام الي وانترنت، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الابراهيمي- برج بوعريريج، السنة الجامعية 2021/2022.

38. مروة ظافري، نهى ياسمين يونس، **حماية المستهلك من مخاطر الدفع الالكتروني**، مذكرة ماستر تخصص قانون أعمال، كلية الحقوق والعلوم السياسية، جامعة 20 أوت 1955 سكيكدة، جوان 2023

39. مروى بن بوزيد، نجوى هداج، **الحماية الجنائية لبطاقات الدفع الالكتروني من التزوير**، مذكرة ماستر تخصص قانون اعلام الي والانترنت، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الابراهيمي برج بوعريريج، 12 جوان 2025.

40. مريم دوش، سميحة هلالي، **مدى مواجهة المشرع الجزائري للجرائم الالكترونية**، مذكرة ماستر تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة حمه لخضر- الوادي، سنة 2029.

41. مريم عيسات، **تزوير التوقيع الالكتروني**، مذكرة ماستر تخصص قانون الدولة والمؤسسات، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، سنة 2017

42. مصطفاوي أسامة، **التزوير في المستندات الالكترونية في القانون الجزائري**، مذكرة ماستر تخصص الادارة الالكترونية، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف بالمسيلة، سنة 2025.

43. معزوز راضية، **الحماية الجزائية للبيانات الرقمية في التشريع الجزائري**، مذكرة ماستر تخصص القانون القضائي، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس مستغانم، السنة الجامعية 2023/2024.

44. معزوزي نادية، زنير ريان، **النظام القانوني للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي**، مذكرة ماستر تخصص دولة ومؤسسات، كلية الحقوق والعلوم السياسية، جامعة 20 أوت 1955–سكيكدة، دورة جوان 2025.

45. مكري ايمان، **الجريمة الالكترونية في التشريع الجزائري**، رسالة ماجستير، جامعة الجزائر3، سنة 2016.

46. مليكة سعيدان، **تتبع الدليل الرقمي في جرائم المعلوماتية في التشريع الجزائري**، مذكرة ماستر تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر– بسكرة، الموسم الجامعي 2016/2017.

47. هشام بن سليمان، **تزوير المحررات الرسمية في القانون الجزائري**، مذكرة ماستر تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس مستغانم، السنة الجامعية 2023/2024.

48. والي أمير، بلعلمي اسحاق، **مكافحة جريمة التزوير الالكتروني في الجزائر**، مذكرة ماستر تخصص قانون اعلام الي، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الابراهيمي،– برج بوعريريج، السنة الجامعية 2022/2023 .

رابعا: المقالات:

1. أجعود سعاد، **الحماية الجزائية لتكنولوجيات الاعلام والاتصال في التشريع الجزائري "دراسة على ضوء النصوص المستحدثة"**، مجلة الرسالة للدراسات والبحوث الانسانية، جامعة العربي التبسي– تبسة، المجلد 07، العدد 04، منشور بتاريخ 14 جوان 2022.

2. أحمد غلاب، زهرة كيسي، **اجراءات اعتراض المكالمات السلكية واللاسلكية كالية لمتابعة جرائم المخدرات**، مجلة تحولات، جامعة قاصدي مرباح ورقلة، المجلد 02، العدد 01، منشور بتاريخ 01 جانفي 2019.

3. أحمد محمد محروس عبدالعال، **التزوير الاكتروني بين التشريع التقليدي واليات المواجهة الحديثة،** المجلة الأكاديمية للأبحاث والنشر العلمي، الاصدار 70، فيفري 2025.

4. أسامة بلحاج، خليفي سمير، **خصوصيات مكافحة الجريمة الالكترونية في الجزائر على ضوء التشريع والممارسة القضائية،** مجلة القانون والمجتمع، جامعة أدرار، المجلد 13، العدد 02، منشور بتاريخ 01 ديسمبر 2025.

5. أميمة لعروسي، **حجية المحرر الالكتروني،** مجلة القانون والأعمال الدولية، منشور بتاريخ 22أفريل2020، تم الاطلاع يوم 21 مارس2026 ، على الساعة 16:53، على الرابط: https://www.droitetentreprise.com.

6. **الأعذار القانونية والظروف القضائية المخففة والمشددة،** مجلة المخبر القانوني ، تم الاطلاع عليه يوم 10 أفريل 2026، على الساعة 21:00، على الرابط: https://labodroit.com.

7. محمود محمد الشحات محمود، **التوازن بين حماية الحق في الخصوصية ومشروعية الدليل الجنائي الرقمي،** المجلة الافريقية للدراسات القانونية والسياسية، جامعة أحمد دراية– أدرار، المجلد 07، العدد 02، منشور بتاريخ 04 جانفي 2024.

8. السائح ايمان، **الحماية القانونية للتوقيع الالكتروني،** منشورات المجلة المغربية للدراسات والاستشارات القانونية، جامعة محمد الأول وجدة، العدد 01، سنة 2016.

9. العنيد محمد زيد، عصماني ليلى، **شروط تسليم المجرمين في النظام القانوني الجزائري،** مجلة الاجتهاد القضائي، جامعة محمد خيضر بسكرة، المجلد 13، العدد 02، منشور بتاريخ 31 مارس 2021.

10. القينعي بن يوسف، **اليات الكشف عن جرائم التزوير ومعرفة مرتكبيها على ضوء القانون رقم 24-02،** المجلة الجزائرية للحقوق والعلوم السياسية، جامعة أحمد بن يحي الونشريسي تيسيمسيلت، المجلد 09، العدد 02، منشور بتاريخ 01 جانفي 2024.

11. الكثيري سعيد مسعود، **الجريمة الالكترونية في ضوء اتفاقية بودابست: الاطار المفاهيمي والتصنيفي،** مجلة البحوث القانونية والاقتصادية، المركز الجامعي أفلو، المجلد 09، العدد 01، منشور بتاريخ 01 جانفي 2026.

12. ايمان بغدادي، **التوقيع الالكتروني كبديل للتوقيع التقليدي في التجارة الالكترونية،** مجلة الاقتصاد الدولي والعولمة، جامعة زيان عاشور بالجلفة، المجلد 02، العدد 04، تم النشر بتاريخ 01 ديسمبر 2019.

13. ايمان بغدادي، **أثر تعديل قانون العقوبات الجزائري في التصدي للجريمة الالكترونية**، مجلة افاق للبحوث والدراسات، المركز الجامعي ايليزي، المجلد 02، العدد 02، جويلية 2019.

14. بلحاج أسامة، خليفي سمير، **خصوصيات مكافحة الجريمة الالكترونية في الجزائر على ضوء التشريع والممارسة القضائية**، مجلة القانون والمجتمع، جامعة البويرة، المجلد 13، العدد 02، منشور سنة 2025.

15. بلقاسم بوزيدي، **السياسة الجنائية لمواجهة جرائم التزوير المعلوماتي في التشريع الجزائري**، مجلة الدراسات الحقوقية، جامعة سعيدة، المجلد08، العدد02.

16. بن زهرة السعيد، بلعربي بلقاسم، **القطب الجزائي الوطني المتخصص في مكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال: دراسة في المفهوم والاختصاص**، مجلة الدراسات القانونية والاقتصادية، المركز الجامعي سي الحواس– بريكة، المجلد 08، العدد 02، منشور بتاريخ 20 ديسمبر 2025.

17. بن لعربي أسماء، الفحلة مديحة، **التزوير المعلوماتي في عصر الرقمنة: بين قابلية الخضوع للقواعد العامة وضرورة تبني نصوص خاصة**، مجلة الفكر القانوني والسياسي، جامعة عمار ثليجي الأغواط، المجلد 08، العدد 02، بتاريخ 20 نوفمبر 2024.

18. بهادي عبد القادر، الصادق عبد القادر، **الحق في خصوصية البيانات الشخصية عبر المجال الرقمي وسبل حمايتها في التشريع الجزائري**، مجلة الحقيقة، جامعة احمد دراية بأدرار، المجلد 24، العدد 02، 05 ماي 2025.

19. بوجمعة شهرزاد، عيشاوي امال، **مظاهر الحماية القانونية لوسائل الدفع الالكتروني في التشريع الجزائري**، مجلة البحوث والدراسات القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة البليدة 2 – لونيسي علي، المجلد 13، العدد 01، جانفي 2024.

20. بوحديد فارس، قرانة عادل، **مهام السلطة الوطنية لحماية المعطيات الشخصية في التشريع الجزائري**، مجلة العلوم القانونية والاجتماعية، جامعة زيان عاشور الجلفة كلية الحقوق والعلوم السياسية، المجلد06، العدد02، جوان 2021.

21. بورطل أمينة، **اثبات الجريمة الالكترونية بالدليل الرقمي وفق التشريع الجزائري**، المجلة الجزائرية للعلوم القانونية والسياسية، جامعة عين تموشنت، المجلد 61، العدد 01، منشور سنة 2024.

22. بوزينة امنة امحمدي، **النظام القانوني للتعامل ببطاقة الائتمان المتداولة في البنوك الجزائرية**، مجلة القانون، معهد العلوم القانونية والادارية، المركز الجامعي أحمد زبانة بغليزان، العدد 08، جوان 2018.

23. بوضياف اسمهان، **الجريمة الالكترونية والاجراءات التشريعية لمواجهتها في الجزائر**، مجلة الاستاذ الباحث للدراسات القانونية والسياسية، العدد 11، ماي 2018.

24. بومدين رحال، **محل التفتيش في مجال جرائم التجارة الالكترونية وفق القانون الجزائري**، المجلة الجزائرية للحقوق والعلوم السياسية، جامعة أحمد بن يحي الونشريسي تيسمسيلت، المجلد 03، العدد 02، 01 ديسمبر 2018.

25. جميلة محلق، **اعتراض المراسلات، تسجيل الأصوات والتقاط الصور في قانون الاجراءات الجزائية الجزائري**، مجلة التواصل في الاقتصاد والادارة والقانون، جامعة باجي مختار عنابة، العدد 42، جوان 2015.

26. حايطي فاطيمة، هروال نبيلة هبة، **الحماية الاجرائية للحق في الخصوصية الرقمية في مواجهة الجريمة المعلوماتية**، مجلة الدراسات القانونية، جامعة يحيى فارس بالمدية، المجلد 07، العدد 02، منشور بتاريخ 24 جوان 2021.

27. حسونة عبد الغني، **المعالجة القانونية لتزوير بطاقات الدفع الالكترونية**، مجلة الحقوق والحريات، جامعة محمد خيضر – بسكرة، المجلد 12، العدد 01، منشور بتاريخ 05 أفريل 2024.

28. حسين فريجة، **الجرائم الالكترونية والانترنت**، مجلة المعلوماتية، السعودية، العدد 36، أكتوبر 2011

29. حسينة شرون، عبد الحليم بن مشري، **الحماية القانونية لبطاقات الدفع الالكترونية** ، مجلة الاجتهاد القضائي، جامعة محمد خيضر بسكرة، المجلد 12، العدد 01، مارس 2019.

30. حنان براهيمي، **المحررات الالكترونية كدليل اثبات**، مجلة المفكر، جامعة محمد خيضر بسكرة، المجلد08، العدد01، ماي2013.

31. خالد تومي، **تأثير الرقمنة على الثقة الرقمية في القانون الجزائري**، مجلة الحقوق و لعلوم السياسية، جامعة محمد لمين دباغين سطيف2، مجلد11، العدد1، سنة 2024.

32. خميس جمعة الشهواني، **اشكالية تحديد الاختصاص القضائي في الجرائم الالكترونية**، مجلة الشرق الأوسط للدراسات القانونية والفقهية، جامعة صفاقس، المجلد 06، العدد 01، منشور بتاريخ 13 فيفري 2026.

33. راضية مشري، **جريمة تزوير التوقيع الالكتروني في التشريع الجزائري**، حوليات جامعة قالمة للعلوم الاجتماعية والانسانية، جامعة 8 ماي 1945 قالمة، المجلد 19، العدد 20، جوان 2017.

34. رحال علي، **حجية المحررات الالكترونية في الاثبات على ضوء التشريع الجزائري والتشريع المقارن**، مجلة طبنة للدراسات العلمية الأكاديمية، المجلد 04، العدد02، نوفمبر 2021.

35. رحموني محمد، بن الطيبي امبارك، **شروط قبول الدليل الرقمي كدليل اثبات في الجريمة الالكترونية**، مجلة القانون والعلوم السياسية، المركز الجامعي صالحي أحمد – النعامة، المجلد 05، العدد 02، منشور بتاريخ 31 أكتوبر 2019.

36. زعيطي امنة، **مكافحة الجرائم الالكترونية في ضوء قانون العقوبات الجزائري**، مجلة حقوق الانسان والحريات العامة، جامعة عبد الحميد بن باديس– مستغانم، المجلد 20، العدد 07، منشور بتاريخ جوان 2019.

37. زكريا بوعون، **دور الهيئة الوطنية للوقاية من الجرائم الالكترونية في حماية المستهلك**، مجلة العلوم الانسانية، جامعة منتوري قسنطينة، المجلد 29، العدد 01، منشور بتاريخ 30 جوان 2018.

38. سعيدة بوزنون، **مكافحة الجريمة الالكترونية في التشريع الجزائري**، مجلة العلوم الانسانية، جامعة منتوري بقسنطينة، المجلد 30، العدد 05، ديسمبر 2019.

39. سويلم فضيلة، **ضوابط التسويق الالكتروني في التشريع الجزائري**، مجلة القانون والعلوم السياسية، المركز الجامعي صالحي أحمد بالنعامة، المجلد 09، العدد 01، تاريخ النشر 30 أفريل 2023.

40. سيليني نسيمة، **عدم تسليم المجرمين في الجرائم السياسية وفقا للاتفاقيات الدولية**، المجلة الأكاديمية للبحوث القانونية والسياسية، جامعة عمار ثليجي الأغواط، المجلد 05، العدد 01، منشور بتاريخ 14 مارس 2021.

41. شعباني نوال، **مظاهر تفعيل قواعد مكافحة جرائم التزوير المقررة بموجب القانون رقم 24-02 المتعلق بمكافحة التزوير واستعمال المزور**، المجلة النقدية للقانون والعلوم السياسية، جامعة مولود معمري تيزي وزو، المجلد 20، العدد 01، منشور بتاريخ 30 جوان 2025.

42. شهيرة بولحية، **الاحتيال الالكتروني**، مجلة الدراسات القانونية والاقتصادية، جامعة باتنة 1، الجزائر، العدد 04، ديسمبر 2019.

43. طباش عزالدين، **الحماية الجزائية للمعطيات الشخصية في التشريع الجزائري دراسة في ظل القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي**، المجلة الأكاديمية للبحث القانوني، العدد 02، 2018.

44. عبد الرزاق بن خيرة، **الحماية الجنائية للمحررات الالكترونية في ظل القانون 04-15 و القوانين المكملة له**، مجلة المفكر، جامعة بسكرة، مجلد 16، العدد 2، سنة 2021.

45. عبد العزيز بن خدة، **الخصوصية الاجرامية لجرائم التزوير في المحررات الالكترونية**، مجلة الفقه و القانون، جامعة الوادي، مجلد10، عدد3، سنة2023.

46. عبد النبي سلمى، **دور القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال في مواجهة الاعتداءات الواقعة على المعطيات المعلوماتية**، مجلة الحقوق والعلوم السياسية، جامعة عباس لغرور – خنشلة، المجلد 11، العدد 02، منشور بتاريخ 26 جوان 2024.

47. عبدالنبي مصطفى، **قراءة في النصوص القانونية المنظمة للهيئة الوطنية للوقاية من جرائم تكنولوجيات الاعلام والاتصال ومكافحتها**، دفاتر السياسة والقانون، جامعة قاصدي مرباح–ورقلة، المجلد 13، العدد 03، منشور بتاريخ 21 جوان 2021.

48. عبيزة منيرة، **الحماية القانونية للبيانات الشخصية من الجرائم المعلوماتية في ضوء التشريع الجزائري**، مجلة الاجتهاد القضائي، جامعة محمد خيضر بسكرة، المجلد 15، العدد 02، منشور بتاريخ 30 نوفمبر 2023.

49. عجابي الياس، **الطبيعة القانونية للتوقيع الالكتروني**، مجلة دراسات وأبحاث، جامعة الجلفة ، المجلد 01، العدد 01.

50. عز الدين العثماني، **اجرائات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلوماتية**، مجلة دائرة البحوث والدراسات القانونية والسياسية، جامعة تبسة، العدد الرابع، جانفي 2018.

51. علمي مخلوف، بومحراث ليندة، **ضوابط التفتيش في الجرائم الالكترونية**، مجلة المعيار، جامعة الأمير عبد القادر للعلوم الاسلامية قسنطينة، المجلد 28، العدد 01، 15 جانفي 2024.

52. عمار فتيحة، **جريمة التزوير الالكتروني**، مجلة القانون والمجتمع، جامعة أدرار، المجلد 07، العدد 01، جوان 2019.

53. عيمور راضية، **الجريمة الالكترونية واليات مكافحتها في التشريع الجزائري**، المجلة الأكاديمية للبحوث القانونية والسياسية، جامعة عمار ثليجي الأغواط، المجلد 06، العدد 01، منشور بتاريخ 31 مارس 2022.

54. غزالي نزيهة، **الاليات القانونية لحماية وسائل الدفع الالكتروني في التشريع الجزائري**، مجلة البحوث السياسية والادارية، جامعة محمد لمين دباغين سطيف 2، المجلد 06، العدد 01.

55. غلاب عبد الحق، **خصوصية جريمة تزوير التوقيع الالكتروني في التشريع الجزائري**، مجلة الدراسات القانونية والسياسية، جامعة عمار ثليجي الأغواط، المجلد 08، العدد 01، جانفي 2022.

56. فتيحة معمري، **تحديات الامن السيبراني والسيادة الرقمية في ظل التشريع الجزائري الحديث**، مجلة الحقوق والعلوم السياسية، جامعة خنشلة، مجلد9، عدد2، جوان 2021.

57. فريدة عيادي، **الجريمة المعلوماتية في التشريع الجزائري**، المجلة الجزائرية للعلوم القانونية والسياسية، جامعة بن يوسف بن خدة الجزائر، المجلد 55، العدد 2، منشور يوم 15 جوان 2018.

58. فضيلة يسعد، **القوة الثبوتية للتوقيع الالكتروني في التشريع الجزائري**، مجلة العلوم الانسانية، جامعة20 أوت1955 سكيكدة، المجلد 30، العدد52، ديسمبر2019.

59. فلاك مراد، **اليات الحصول على الأدلة الرقمية كوسائل اثبات في الجرائم الالكترونية**، مجلة الفكر القانوني والسياسي، جامعة عمار ثليجي– الاغواط، المجلد 03، العدد 01، منشور بتاريخ 23 سبتمبر 2019.

60. قرانة عادل، بوحديد فارس، **مهام السلطة الوطنية لحماية المعطيات الشخصية في التشريع الجزائري**، مجلة العلوم القانونية والاجتماعية، جامعة زيان عاشور الجلفة، المجلد 06، العدد 02، جوان 2021.

61. قطاف سليمان، بوقرين عبد الحليم، **الاليات القانونية الموضوعية لمكافحة الجرائم السيبرانية في ظل اتفاقية بودابست والتشريع الجزائري**، المجلة الاكاديمية للبحوث القانونية والسياسية، جامعة عمار ثليجي– الاغواط، المجلد 06، العدد 01، منشور بتاريخ 31 مارس 2022.

62. كعوان محمد، بلعزام مبروك، **مسؤولية البنك المحسوب عليه عند الوفاء للشيك المتقن التزوير عبر المقاصة الالكترونية**، مجلة العلوم القانونية والاجتماعية، جامعة زيان عاشور– الجلفة، المجلد 08، العدد 03، منشور بتاريخ 01 سبتمبر 2023.

63. كوثر سعدي، رضوان بن صاري، **حماية وسائل الدفع الالكتروني The Electronic Payment Protection**، مجلة الدراسات القانونية، جامعة يحي فارس بالمدية ، سنة 2023، تم الاطلاع عليه يوم 28 مارس 2026، على الساعة 12:54، على الرابط: https://theses-algerie.com/artivle/details/35728.

64. لموسخ محمد، **تنازع الاختصاص في الجرائم الالكترونية**، دفاتر السياسة والقانون، جامعة قاصدي مرباح– ورقلة، المجلد 09، العدد 02، منشور بتاريخ 31 ديسمبر 2009.

65. ليلى بن برغوث، **الأمن السيبراني وحماية خصوصية البيانات الرقمية في الجزائر في عصر التحول الرقمي والذكاء الاصطناعي**، المجلة الدولية للاتصال الاجتماعي ، جامعة عبد الحميد بن باديس- مستغانم، المجلد 10، العدد 01، منشور بتاريخ 31 مارس 2023.

66. مجدوب لامية، **اجراء التفتيش في التزوير الالكتروني**، مجلة التواصل في العلوم الانسانسة والاجتماعية، جامعة باجي مختار عناية، المجلد 25، العدد 03، 30 سبتمبر 2019.

67. **مجموعة القانون الجنائي**، موقع مجلة مغرب القانون، منشور بتاريخ 19 سبتمبر 2016، تم الاطلاع عليه يوم 10 أفريل 2026، على الساعة 21:08، على الرابط: https://maroclaw.com.

68. محمد العيداني ، يوسف زروق، **حماية المعطيات الشخصية في الجزائر على ضوء القانون رقم 18-07 (المتعلق بحماية الاشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي)**، مجلة معالم للدراسات القانونية والسياسية، المركز الجامعي تندوف، المجلد 02، العدد 03، ديسمبر 2018.

69. محمد العيداني، يوسف زروق، **حماية المعطيات الشخصية في الجزائر على ضوء القانون رقم 18-07**، معالم للدراسات القانونية والسياسية، المركز الجامعي تندوف، المجلد 02، العدد 03، منشور بتاريخ 20 ديسمبر 2018.

70. محمد بودالي، **الجريمة المعلوماتية في القانون الجزائري**، مجلة الفقه و القانون، جامعة الوادي، المجلد11، العدد01، سنة 2012.

71. محمد طلعت يدك، **الحجية القانونية لتوثيق المحررات الالكترونية: دراسة مقارنة**، مجلة جيل الأبحاث القانونية المعمقة، مركز جيل البحث العلمي، مصر، العدد 50.

72. مريم عراب، **الاختصاص القضائي في الجرائم المعلوماتية**، حوليات كلية الحقوق والعلوم الساسية، جامعة وهران 2 محمد بن أحمد، المجلد 07، العدد 03، منشور بتاريخ 22 ديسمبر 2015.

73. مشري راضية، السعيد زيدان، **جريمة تزوير التوقيع الالكتروني في التشريع الجزائري**، حوليات جامعة قالمة، جامعة 8 ماي 1945 قالمة، المجلد 2017، العدد 20، 30 جوان 2017.

74. مطلق بن مقحص بن مطلق السهلي، **حجية التوقيع الالكتروني في الاثبات**، مجلة ابن خلدون للدراسات والأبحاث، المجلد 03، العدد 07، جويلية 2023.

75. **مقال: التنظيم القانوني للجريمة الالكترونية في التشريع الجزائري**، مجلة الفكر القانوني والسياسي، جامعة ابن خلدون تيارت، ردمد: 2112-2588، تم الاطلاع عليه عبر منصة مركز المعرفة الرقمي، بتاريخ 3 أفريل 2026، على الساعة: 20:24، على الرابط: https://ddl.ae.

76. مقلاتي مونة، بوخميس سهيلة، **الحق في اعتراض سرية الاتصالات والمراسلات في التشريع الجزائري**، المجلة الأكاديمية للبحوث القانونية والسياسية، جامعة عمار ثليجي الأغواط، المجلد 03، العدد 02، منشور بتاريخ 24 أكتوبر 2019.

77. مهداوي حنان، **التنظيم القانوني للجريمة الالكترونية في التشريع الجزائري**، مجلة الفكر القانوني والسياسي، جامعة محمد لمين دباغين، سطيف 2، المجلد 06، العدد 02، منشور بتاريخ 02 نوفمبر 2022.

78. موسى لسود، **معايير الاختصاص القضائي في جرائم قانون التجارة الالكترونية الجزائري 05/18**، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة العربي التبسي– تبسة، المجلد 04، العدد 02، منشور بتاريخ 08 جانفي 2020.

79. نزيهة علال، **الاطار القانوني لحماية المعطيات ذات الطابع الشخصي في الفضاء الالكتروني في ظل القانون 18-07**، مجلة دائرة البحوث والدراسات القانونية والسياسية، المركز الجامعي مرسلي عبد الله – تيبازة، المجلد04، العدد09، جوان 2020.

80. نورهان محمد الربيعي، **اليات الحصول على الأدلة الرقمية واستخدامها كوسائل اثبات في الجرائم الالكترونية**، مجلة الباحث في العلوم القانونية، كلية القانون جامعة اوروك– بغداد، المجلد 05، العدد 2، منشور بتاريخ ديسمبر 2024.

81. وفاء صدراتي، **اليات الحماية القانونية للتوقيع الالكتروني من جرائم التزوير الالكتروني في التشريع الجزائري**، مجلة العلوم القانونية والسياسية، جامعة الشهيد حمه لخضر بالوادي ، المجلد 11، العدد 01، منشور بتاريخ 28 أفريل 2020.

82. وليد لعماري، **الضمانات القانونية ضد مخاطر استخدام وسائل الدفع الالكتروني، مجلة العلوم القانونية والسياسية**، جامعة الشهيد حمه لخضر الوادي، المجلد 11، العدد 01، جانفي 2020.

83. يوسف حمداني، تطور الجرائم الالكترونية في الجزائر، مجلة القانون والمجتمع، العدد 45، 2025.

84. يوسف مسعودي، رحاب أرجيلوس، **مدى حجية التوقيع الالكتروني في الاثبات في التشريع الجزائري (دراسة على ضوء أحكام القانون 15-04)**، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المركز الجامعي لتامنغست بأدرار، المجلد 06، العدد 01، جانفي 2017.

85. Rayan Khiari, Hayette Selmani, **Electronic Forgery As a Manifestation of Degital Corruption**, Journal of Legal Studies and Researches, volume 11, number 1, 15 january 2026.

86. Zerrouki Assia & Hamel Mohamed, **"Cybercrime Follow-up Procedures : A Comparative Study of Algeria and Qatari Legislation",** Journal of Legal Studies, University og Ghardaia, 2024.

خامسا: المداخلات العلمية:

1. أومدور رجاء، **مفهوم الدليل الرقمي**، مداخلة في الملتقى الدولي حول: أدلة الاثبات الجنائية الحديثة في التشريعات المقارنة، جامعة طاهري محمد – بشار، المنعقد يومي 25 و 26 أفريل 2018.

2. بن زيدان زوينة، **التأسيس النظري لعقود الأعمال الرقمية**، ندوة تكوينية لصالح الطلبة تحت عنوان: التحديات القانونية لعقود الأعمال الرقمية ، جامعة الجزائر 1.

3. بومحراث ليندة، **الأقطاب الجزائية المتخصصة كالية لمكافحة الجرائم الالكترونية**، مداخلة في ملتقى دولي بعنوان: التكنولوجيات الحديثة والجريمة، جامعة الأمير عبد القادر للعلوم الاسلامية– قسنطينة، المنعقد يوم 23 نوفمبر 2022.

4. سويسي فتيحة، **التكييف القانوني لجرائم المعلوماتية والاشكالات العلمية المترتبة عنها**، مداخلة مقدمة خلال الندوة البحثية المنظمة من طرف مركز البحوث القانونية والقضائية، المنعقد بتاريخ 18 جانفي 2022.

5. فريد مشري واخرون، **الحماية القانونية لوسائل الدفع الالكتروني –الجزائر نموذجا–** ، مداخلة في ملتقى وطني بعنوان: المستهلك والاقتصاد الرقمي: ضرورة الانتقال وتحديات الحماية، المركز الجامعي عبد الحفيظ بوالصوف–ميلة، يومي 23 و24 افريل 2018.

6. معمري ايمان، فضيلة شعبان، **مدى مواجهة المشرع الجزائري للجرائم الالكترونية "جريمة التزوير الالكتروني نموذجا"**، مداخلة في ملتقى:الدكتوراه الدولي متعدد الاختصاصات، جامعة الشهيد حمه لخضر الوادي، من 23 الى 26 فيفري 2020.

سادسا: المواقع الالكترونية:

1. أركان جريمة التزوير في المحررات الرسمية أو العمومية في القانون الجزائري، مدونة القانون والتعليم، منشور منذ 7 سنوات (سنة 2019)، تم الاطلاع عليه يوم 10 أفريل 2026، على الساعة 20:14، على الرابط: https://droit7.blogspot.com

2. أمينة داودي، هذه عقوبة تزوير الوثائق الادارية والشهادات، الصادر عن موقع النهار أنلاين، بتاريخ 11 أكتوبر 2023، تم الاطلاع عليه بتاريخ 25 مارس 2026، على الساعة 22:33، على الرابط: https://www.ennaharonline.com

3. أنواع وأمثلة على الجرائم الالكترونية، منشور على موقع قانون تك، بتاريخ 17 جوان 2025، تم الاطلاع عليه يوم 7 أفريل 2026، على الساعة 16:17، على الرابط: https://www.9anon4dz.com

4. الأحكام الجديدة في قانون مكافحة التزوير واستعمال المزور، موقع هوريزونز، منشور بتاريخ 30 جوان 2024، تم الاطلاع عليه يوم 14 أفريل 2026، على الساعة: 15:28، على الرابط: https://horizons.dz

5. الأحكام الجديدة في قانون مكافحة التزوير واستعمال المزور محور دراسي بالجزائر العاصمة، موقع الان، منشور منذ 2024، تم الاطلاع عليه يوم 07 ماي 2026، على الساعة 20:27، على الرابط: https://elaane.dz

6. الأحكام الجديدة في قانون مكافحة التزوير واستعمال المزور: تعزيز الردع وحماية الثقة العامة، موقع وكالة الأنباء الجزائرية، 30 جوان 2024، تم الاطلاع عليه يوم 25 مارس 2026، على الساعة 23:56، على الرابط: https://www.aps.dz/ar/algerie/164434-2024-06-30-14-15-54

7. الاحكام الجديدة في قانون مكافحة التزوير واستعمال المزور محور دراسي بالجزائر العاصمة، وكالة الأنباء الجزائرية، منشور بتاريخ 30 جوان 2024، تم الاطلاع عليه يوم 6 أفريل 2026، على الساعة 22:07، على الرابط: https://www.aps.dz/ar/algerie/164434

8. الاستراتيجية الوطنية للتحول الرقمي في الجزائر، المندوبية العليا للرقمنة، منشور في أوت 2024، تم الاطلاع عليه يوم 25 أفريل 2026، على الساعة 16:04، على الرابط: https://hcn.dz/SNTN-Ar.pdf

9. الاعذار القانونية في قانون العقوبات الجزائري، موقع المحاكم والمجالس القضائية، منشور بتاريخ 19 جانفي 2016، تم الاطلاع عليه يوم 10 أفريل 2026، على الساعة 20:47، على الرابط: https://tribunaldz.com

10. الانتربول يضرب شبكات الاحتيال الرقمي بافريقيا ويوقف المئات، قناة الجزيرة، منشور بتاريخ 24 أوت 2025، تم الاطلاع عليه يوم 16 ماي 2026، على الساعة 17:44، على الرابط: https://www.aljazeera.net/news

11. التزوير الالكتروني يهدد الثقة الرقمية في عصر الذكاء الاصطناعي، منشور على موقع البديل ABC، تم الاطلاع عليه يوم 7 أفريل 2026، على الساعة 16:05، على الرابط: https://elbadilabc-ar.dz

12. التزوير واستعمال المزور..القوانين المحينة والعقوبات في القانون الجزائري، منصة اليوتيوب على قناة الشروق نيوز، منشور بتاريخ 10 جويلية 2023، تم الاطلاع عليه يوم 14 أفريل 2026، على الساعة 15:38، على الرابط: https://youtu.be/SW0Wu00MIiY?si=f-wUNMsiAp5yoOxm

13. التسرب الالكتروني: دوافع نفسية وامكانات ضئيلة، موقع الرأي، منشور بتاريخ 28 نوفمبر 2020، تم الاطلاع عليه يوم 25 أفريل 2026، على الساعة 16:22، على الرابط: https://alrai.com/article/10564648

14. التفتيش والانابة القضائية في القانون الجزائري، موقع قانون تك، منشور بتاريخ 12 أفريل 2023، تم الاطلاع عليه يوم 17 أفريل 2026، على الساعة 16:32، على الرابط: https://www.9anon4dz.com

15. الجزائر تتجه الى اصدار قانون جديد للحد من جرائم التزوير، منصة العربي الجديد، منشور بتاريخ 29 ماي 2023، تم الاطلاع عليه يوم 1 ماي 2026، على الساعة 15:09، على الرابط: https://www.alaraby.co.uk/society

16. الجزائر تتشدد في محاربة التزوير والاحتيال، موقع الشرق الأوسط، منشور بتاريخ 22 نوفمبر 2023، تم الاطلاع عليه يوم 10 أفريل 2026، على الساعة 20:02، على الرابط: https://aawsat.com

17. الجزائر تراهن على الأقمار الصناعية لضمان استمرارية الانترنت، موقع العربي الجديد، منشور بتاريخ 10 فريل 2026، تم الاطلاع عليه يوم 14 أفريل 2026، على الساعة 17:05، على الرابط: https://www.aajae.co/entertainment_media

18. الدعوة الى التعجيل باصدار التنظيم المتعلق بتدابير حماية المبلغين عن الفساد، وكالة الأنباء الجزائرية، منشور بتاريخ 30 أفريل 2026، تم الاطلاع عليه يوم 13 ماي 2026، على الساعة 15:28، على الرابط: https://www.aps.dz/algerie/societe/mols6aqk

19. الزام المؤسسات والادارات والهيئات العمومية باستحداث هيكل مكلف بأمن أنظمتها المعلوماتية وحماية معطياتها، موقع الحراك الاخباري، منشور بتاريخ 21 جانفي 2026، تم الاطلاع عليه يوم 17 أفريل 2026، على الساعة 15:36، على الرابط: https://alhirak-alikhbari.dz

20. السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، الصادر عن الموقع الرسمي للسلطة الوطنبة لحماية المعطيات ذات الطابع الشخصي ، تم الاطلاع يوم 25 مارس 2026، على الساعة 23:07، على الرابط: https://anpdp.dz

21. الشروط الشكلية والموضوعية لعملية التسرب في القانون الجزائري، مدونة القانون والتعليم، منشور سنة 2020، تم الاطلاع عليه يوم 25 أفريل 2026، على الساعة 16:20، على الرابط: http://droit7.blogspot.com/2019/09/blog-post_91.html

22. الفرقة الخاصة للتدخل، منشور على موقع الدرك الوطني، تم الاطلاع عليه يوم 08 ماي 2026، على الساعة 20:07، على الرابط: https://www.mdn.dz/site_cgn/sommaire/presentation/unit_spe/dsi/dsi_ar.php

23. القانون الجديد: مكافحة التزوير واستعمال المزور في الجريدة الرسمية، موقع ديزاد news، منشور بتاريخ 13 مارس 2024، تم الاطلاع عليه يوم 13 ماي 2026، على الساعة 13:51، على الرابط: https://dznews.dz

24. الكشف عن مضمون الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية للفترة 2025-2029، وكالة الأنباء الجزائرية، منشور بتاريخ 3 مارس 2026، تم الاطلاع عليه يوم 17 أفريل 2016، على الساعة 17:36، على الرابط: https://www.aps.dz

25. المجلس الشعبي الوطني: المصادقة على مشروع القانون المتعلق بمكافحة التزوير واستعمال المزور، الاذاعة الجزائرية، تم النشر يوم 21 ديسمبر 2023، تم الاطلاع عليه يوم 3 افريل 2026، على الساعة 21:23، على الرابط: https://news.radioalgerie.dz

26. المحامي سفران الشمراني، جريمة التزوير في النظام السعودي، منشور على موقع مكتب المحامي والمستشار القانوني سفران مشبب الشمراني، بتاريخ 15 ماي 2025، تم الاطلاع عليه يوم 6 أفريل 2026، على الساعة 21:30، على الرابط: https://lawyesafran.com

27. المحامية مروة أبو العلا، بحث متميز حول خصوصية الجرائم الالكترونية في التشريع الجزائري والتشريعات المقارنة، منشور على موقع محاماة نت، بتاريخ 20 أفريل 2018، تم الاطلاع عليه بتاريخ 2 أفريل 2026، على الساعة 19:07، على الرابط: https://mohamah.net

28. المحامية مروة أبو العلا، بحث ودراسة حول الأعذار القانونية في القانون الجنائي، موقع محاماة نت، منشور بتاريخ 14 أكتوبر 2018، تم الاطلاع عليه يوم 10 أفريل 2026، على الساعة 20:49، على الرابط: https://mohamah.net

29. المديرية العامة للضرائب تحذر المواطنين من منصات الدفع الالكترونية غير الرسمية، صادر عن موقع أخبار بلا حدود، منشور في مارس 2026، تم الاطلاع عليه يوم 28 مارس 2026، على الساعة 22:47، على الرابط: https://unlimited-news

30. المرسوم التنفيذي رقم 20-332 المؤرخ في 22 نوفمبر 2020، المتعلق بتحديد كيفيات ممارسة نشاط الاعلام عبر الانترنت ونشر الرد أو التصحيح عبر الموقع الالكتروني، الجريدة الرسمية، العدد 70، الصادر بتاريخ 25 نوفمبر 2020

31. المسؤولية الجزائية للشخص المعنوي في ظل قانون العقوبات الجزائري، موقع أنامل الحقوق، منشور بتاريخ 19 جويلية 2013، تم الاطلاع عليه يوم 9 أفريل 2026، على الساعة 23:45، على الرابط: https://enamilsdroit.ahladalil.com

32. المسؤولية الجزائية للشخص المعنوي والشخص الطبيعي، منشور على منتدى المحاكم والمجالس القضائية، بتاريخ 21 جوان 2018، تم الاطلاع عليه يوم 9 أفريل 2026ن على الساعة 23:49، على الرابط: https://www.tribunaldz.com

33. المساعدة القضائية، موقع مجلس قضاء الجزائر، تم الاطلاع عليه يوم 16 ماي 2026، على الساعة 17:05، على الرابط: https://cour-alger.mjustice.dz

34. المستشار القانوني يكشف عن الحالات التي يتم فيها تطبيق قانون التزوير التي تصل عقوبته ل30 سنة سجن، منصة اليوتيوب على قناة الشروق نيوز، منشور بتاريخ 3 جوان 2025، تم الاطلاع عليه يوم 14 أفريل 2026، على الساعة 15:42، على الرابط: https://youtu.be/U7mjzYzo1Pw?si=Hd3soooE-krl12-f

35. امل المرشدي، بحث قانوني كبير عن نظام تسليم المجرمين، موقع محاماة نت، منشور بتاريخ 05 أكتوبر 2016، تم الاطلاع عليه يوم 16 ماي 2026، على الساعة 16:54، على الرابط: https://www.mohamah.net

36. اية الوصيف، جرائم التزوير في القانون الجزائري، موقع محاماة نت، بتاريخ 12 أكتوبر 2019، اطلع عليه بتاريخ 9 مارس 2026، الساعة 02:37، عبر الرابط: https://www.mohamah.net

37. اية الوصيف، بحث ودراسة قانونية حول التفتيش الالكتروني، موقع محاماة نت، منشور بتاريخ 4 أكتوبر 2019، تم الاطلاع عليه يوم 17 أفريل 2026، على الساعة 16:05، على الرابط: https://www.mohamah.net

38. ايهاب فوزي السقا، جريمة التزوير في المحررات الالكترونية، منصة المحكمة العليا، منشور سنة 2008، تم الاطلاع عليه يوم 25 أفريل 2026، على الساعة 14:25، على الرابط: https://coursupreme.dz

39. تحديد المسؤولية الجزائية للشخص الاعتباري في التشريع الجزائري والقانون المقارن، موقع WordPress، منمنشور بتاريخ 6 أكتوبر 2013، تم الاطلاع عليه يوم 9 أفريل 2026، على الساعة 23:58، على الرابط: https://norbertnoland.wordpress.com

40. تساؤلات: قانون مكافحة التزوير واستعمال المزور.. هذه هي التفاصيل، منصة اليوتيوب على قناة النهار tv ، منشور بتاريخ 20 ماي 2024، تم الاطلاع عليه يوم 14 أفريل 2026، على الساعة 15:50، على الرابط: https://youtu.be/Y5kjKn9r1ys?si=Is0LiqFMMu4oysT6

41. تعليمات صارمة لمنع العملات المشفرة في الجزائر، موقع العربي الجديد، منشور بتاريخ 01 ديسمبر 2025، تم الاطلاع عليه يوم 13 ماي 2026، على الساعة 14:17، على الرابط: https://www.aajsa.com/economy

42. تفاصيل مشروع قانون مكافحة التزوير واستعمال المزور، الاذاعة الجزائرية، منشور بتاريخ 21 نوفمبر 2023، تم الاطلاع عليه يوم 10 أفريل 2026، على الساعة 00:26، على الرابط: https://news.radioalgerie.dz

43. تقسيم الجرائم من حيث ركنها المعنوي والشرعي، المحاضرة الثامنة والعشرون، الجامعة المستنصرية، بغداد، تم الاطلاع عليه يوم 7 أفريل 2026، على الساعة: 18:28، على الرابط: https://uomustansiriyah.edu.iq

44. جريمة التزوير التقليدي في القانون الجزائري، مدونة الحقوق والعلوم السياسية (APP-ON)، منشور بتاريخ 22 أكتوبر 2013، تم الاطلاع عليه يوم 7 أفريل 2026، على الساعة: 16:57، على الرابط: https://www.app-on.com/2013/10/blog-post9260.html

45. جريمة التزوير في القانون المغربي والعقوبات، موقع محامي بهيئة الدار البيضاء CLF AVOCAT، تم الاطلاع عليه يوم 6 أفريل 2026، على الساعة 21:36، على الرابط: https://calavpcat.ma

46. جريمة تزوير المحررات (التزوير الخطي) في القانون الجزائري، مدونة الحقوق والعلوم السياسية (APP-ON)، منشور بتاريخ 22 أكتوبر 2013، تم الاطلاع عليه يوم 10 أفريل 2026، على الساعة 20:10، على الرابط: https://www.app-on.com/2013/10/blog-post9260.html

47. جريمة تزوير المحررات في التشريع الجزائي الجزائري، منشورات جامعة الدكتور مولاي الطاهر بسعيدة، كلية الحقوق والعلوم السياسية، تم الاطلاع عليه بتاريخ 3 أفريل 2026، على الساعة 20:36، على الرابط: https://budsp.univ-saida.dz/doc_num.php?explnum_id=2701

48. حظر العملات الرقمية وتجميد الاصول..الجزائر تشدد قبضتها على المال غير المشروع، موقع تدامسا نيوز، منشور بتاريخ 28 جويلية 2025، تم الاطلاع عليه يوم 14 أفريل 2026، على الساعة 17:02، على الرابط: https://tadamsanews.dz

49. حل سؤال عملية ايصال محتوى الوسائط الرقمية التي تم شراؤها عبر التجارة الالكترونية ، موقع المتوفر، منشور بتاريخ 23 أكتوبر 2021، تم الاطلاع عليه يوم 19 أفريل 2026، على الساعة 07:41، على الرابط: https://ask.tanfis.com/28661

50. خمسة اجهزة محظورة عند دخول الجزائر، منشور على منصة اخر الأخبار، بتاريخ 17 ديسمبر 2024، تم الاطلاع عليه يوم 14 أفريل 2026، على الساعة 14:32، على الرابط: https://elikhbaria.dz

51. دليل عملي لصياغة طلب تعاون فعال للدول الأعضاء في فرقة العمل المشتركة لمنطقتي الشرق الأوسط وشمال افريقيا، مكتب الأمم المتحدة المعني بالمخدرات والجريمة، تم الاطلاع عليه يوم 16 ماي 2026، على الساعة 16:35، على الرابط: https://www.unodc.org/documents/terrorism/Publications/MATF_Practical_Guide_AR/MATF_Practical_Guide_AR_UNODC_final.pdf

52. دنيا حفصة، البرلمان يصادق على مشروع قانون اتفاقية تسليم المجرمين بين تونس والجزائر: وزيرة العدل: 28 انابة قضائية صادرة من تونس و110 واردة من الجزائر و199 سجينا جزائريا في تونس، موقع المغرب يومية مستقلة، منشور بتاريخ 17 جانفي 2024، تم الاطلاع عليه يوم 16 ماي 2026، على الساعة 17:17، على الرابط: https://ar.lemaghreb.tn

53. دور المركز الوطني للتصديق الرقمي في تعزيز المعاملات الرقمية الامنة، منشور على موقع Signit، تم الاطلاع عليه يوم 08 ماي 2026، على الساعة 20:16، على الرابط: https://signit.sa/ar/blogs

54. راغب ملي، قانون الاعلام الجديد في الجزائر: ضبط المحتوى حتى على الانترنت، منصة سمكس، منشور بتاريخ 02 أكتوبر 2023، تم الاطلاع عليه يوم 19 أفريل 2026، على الساعة 07:44، على الرابط: https://smex.org

55. رياض/خ، قانون مكافحة جرائم التزوير في الجريدة الرسمية، جريدة البلاد، بتاريخ 13 مارس 2004، تم الاطلاع عليه يوم 3 أفريل 2026، على الساعة 20:16، على الرابط: https://elbilad.net

56. رياض/خ، قانون مكافحة جرائم التزوير في الجريدة الرسمية، منشور على موقع البلاد نت، بتاريخ 13 مارس 2024، تم الاطلاع عليه يوم 6 أفريل 2026، على الساعة 21:11، على الرابط: https://www.elbilad.net

57. رياض/خ ، قانون مكافحة جرائم التزوير في الجريدة الرسمية، منصة البلاد نت، منشور بتاريخ 13 مارس 2024، تم الاطلاع عليه يوم 08 ماي 2026، على الساعة 19:05، على الرابط: https://www.elbilad.net

58. زعموش فوزية، خوادجية سميحة حنان، النظام القانوني للاعلام الالكتروني في الجزائر بين الضمانات والضوابط: دراسة مقارنة، موقع اليف، منشور بتاريخ 22 نوفمبر 2024، تم الاطلاع عليه يوم 19 أفريل 2026، على الساعة 08:13، على الرابط: https://aleph.edinum.org/13306

59. سلطة ضبط البريد والاتصالات الالكترونية، الصفحة الرئيسية، تم الاطلاع عليه بتاريخ 19 أفريل 2026، عللى الساعة 08:04، على الرابط: https://www.arpce.dz

60. سيد طنطاوي محمد سيد، الجريمة المعلوماتية: الصعوبات التي تواجه التعاون الوطني والدولي وكيفية مكافحتها، المركز الديمقراطي العربي، منشور بتاريخ 17 جوان 2018، تم الاطلاع عليه يوم 7 أفريل 2026، على الساعة 18:11، على الرابط: https://democraticac.de

61. شيخ سناء، شيخ محمد زكرياء، مكافحة الجرائم الالكترونية في القانون الجزائري، مقال بحثي منشور على منصة وميض الفكر، تم الاطلاع عليه بتاريخ 27 مارس 2026، على الساعة 18:07، على الرابط: https://wameedalfiker.com

62. شيخ سناء، شيخ محمد زكرياء، مكافحة الجرائم الالكترونية في القانون الجزائري، موقع وميض الفكر، تم الاطلاع عليه يوم 7 أفريل 2026، على الساعة 17:47، على الرابط: https://wameedalfikr.com

63. شيخ سناء وشيخ محمد زكرياء، مكافحة الجرائم الالكترونية في القانون الجزائري ، تم الاطلاع عليه يوم 16 مارس 2026، على الساعة 00:06، متاح على الرابط: https://wameedalfiker.com

64. عبد الرؤوف حرشاوي، صدور قانون جديد يسلط عقوبات ردعية على المزورين، موقع أوراس ، منشور بتاريخ 13 مارس 2024، تم الاطلاع عليه يوم 9 أفريل 2026، على الساعة 23:07، على الرابط: https://awra.com

65. عثمان لحياني، الجزائر تتجه الى اصدار قانون جديد للحد من جرائم التزوير، العربي الجديد، منشور بوم 29 ماي 2023، تم الاطلاع عليه يوم 3 أفريل 2026، على الساعة 28:42، على الرابط: https://www.alaraby.co.uk

66. عقوبة التصوير في الدوائر الحكومية، موقع محامي النخبة، تم الاطلاع عليه يوم 14 أفريل 2026، على الساعة 14:55، على الرابط: https://arablawfirm.org

67. عمارة فوزي، اعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كاجراءات تحقيق قضائي في المواد الجنائية، مركز المعرفة الرقمي، منشور سنة 2010، تم الاطلاع عليه يوم 25 أفريل 2026، على الساعة 13:46، على الرابط: https://ddl.ae/book/5180436

68. فراجي عماد الدين، التزوير وأحكامه في الجزائر على ضوء القانون المستحدث 24-02، موقع ResearchGate، منشور بتاريخ افريل 2024، تم الاطلاع عليه يوم 7 أفريل 2026، على الساعة 15:41، على الرابط: https://researchgate.net

69. فعالية للانتربول تقدم نصائح لصون السلامة عبر الانترنت، الانتربول (المنظمة الدولية للشرطة الجنائية)، منشور بتاريخ 13 مارس 2025، تم الاطلاع عليه يوم 16 ماي 2026، على الساعة 17:58، على الرابط: https://www.interpol.int/en/News-and-Events/News/2025/INTERPOL-event-shares-tips-for-staying-safe-online

70. فيصل محمودي، "المحامي فيصل محمودي يوضح مفهوم الجرائم الالكترونية بنظر القانون'، فيديو يوتيوب على قناة Echorouk News، تم النشر يوم 12 جانفي 2026، تم الاطلاع عليه بتاريخ 24 مارس2026، على الساعة 17:45، على الرابط: https://www.youtube.com/watch?v=jC6e05PxCQq

71. قانون المساعدة القضائية الأمر رقم 71-57 المعدل والمتمم بالقانون رقم 01-06، موقع طريق العدالة، منشور بتاريخ 25 فيفري 2020، تم الاطلاع عليه يوم 16 ماي 2026، على الساعة 17:11، على الرابط: https://www.abridh.com/aide-judiciaire/

72. قانون مكافحة التزوير واستعمال المزور يصدر في الجريدة الرسمية، موقع الشروق أونلاين، منشور بتاريخ 12 مارس 2024، تم الاطلاع عليه يوم 17 أفريل 2026، على الساعة 15:14، على الرابط: https://www.echoroukonline.com

73. قانون نموذجي بشأن تسليم المجرمين (2004)، الأمم المتحدة المكتب المعني بالمخدرات والجريمة، تم الاطلاع عليه يوم 16 ماي 2026، على الساعة 17:20، على الرابط: https://www.unodc.org/documents/organized-crime/Publications/Model_Law_extradition_AR.pdf

74. كل الوثائق الادارية قابلة للتزوير في الجزائر، موقع الشروق أنلاين، منشور بتاريخ 25 سبتمبر 2012، تم الاطلاع عليه يوم 14 أفريل 2026، على الساعة: 15:30، على الرابط: https://echoroukonline.com

75. كلمة الوزير الأول خلال اشرافه على وضع المنظومة الوطنية لحوكمة البيانات حيز الخدمة، منشور على الموقع مصالح الوزير الأول، بتاريخ 9 فيفري 2026، تم الاطلاع عليه يوم 3 أفريل 2026، على الساعة 1:39، على الرابط: https://premier-minister.gov.dz

76. كيف تحمي خصوصيتك؟، موقع الجزيرة، منشور بتاريخ 5 أكتوبر 2025، تم الاطلاع عليه يوم 17 أفريل 2016، على الساعة 17:28، على الرابط: https://www.aljazeera.net

77. ما هي العقوبة التي حددها القانون الجزائري للجريمة الالكترونية؟، موقع تخصصات بيت.كوم، منشور عام 2015، تم الاطلاع عليه يوم 19 أفريل 2026، على الساعة 08:18، على الرابط: https://www.bayt.com

78. مجلس الأمة: المصادقة على القانون المحدد للقواعد العامة المتعلقة بخدمات الثقة للمعاملات الالكترونية، وكالة الأنباء الجزائرية، منشور بتاريخ 21 جانفي 2026، تم الاطلاع عليه يوم 3 أفريل 2026، على الساعة 01:07، على الرابط: https://aps.dz

79. مجلس الأمة: المصادقة على نص قانوني بمكافحة التزوير واستعمال المزور، الاذاعة الجزائرية، تم النشر يوم 30 جانفي 2024، تم الاطلاع عليه يوم 3 افريل 2026، على الساعة 20:28، على الرابط: https://news.radioalgerie.dz

80. محكمة النقض توضح القصد الجنائي في جرائم التزوير، نقابة المحامين المصرية، منشور بتاريخ 26 جويلية 2023، تم الاطلاع عليه يوم 7 أفريل 2026، على الساعة 17:10، على الرابط: https://egyls.com

81. محمد أمين زيان، اشكالية الركن المعنوي في الجرائم الجمركية دراسة مقارنة، مركز جيل البحث العلمي، منشور بتاريخ 28 ديسمبر 2017، تم الاطلاع عليه يوم 7 أفريل 2026، على الساعة: 18:04، على الرابط: https://jilrc.com

82. محمد سعيد عبد المولى، الاثبات بالمحررات الالكترونية، موقع حماة الحق للمحاماة والاستشارات القانونية، نشر بتاريخ 27أكتوبر 2021، تم الاطلاع عليه يوم 21 مارس 2026، على الساعة 17:10، على الرابط: https://jordan-lawyer.com

83. مخاطر الجريمة الالكترونية في عام 2026: قراءة قانونية- تقنية في التهديدات المستجدة وسبل الوقاية، منصة مكتب النشاشيبي للمحاماة، منشور سنة 2026، تم الاطلاع عليه يوم 25 أفريل 2026، على الساعة 14:22، على الرابط: https://nashashibilaw.weebly.com/magazine/-20257338351

84. مدونة: كيف تبدأ مشروع تجارة الكترونية في الجزائر: الدليل الشامل، افاكت (Evact)، تم الاطلاع عليه يوم 27 مارس 2026، على الساعة 17:32، على الرابط: https://evact.net

85. مدى حجية التوقيع الالكتروني في الاثبات في التشريع الجزائري: دراسة على ضوء أحكام القانون 15-04، تم الاطلاع عليه يوم 24 مارس 2026، على الساعة 00:49، على الرابط: https://platform.almanhal.com

86. مصالح شرطة مكافحة الجرائم الالكترونية تسجل 567 قضية تتعلق بجرائم الانترنت، صادر عن الموقع الرسمي للشرطة الجزائرية، تم الاطلاع عليه يوم 24 مارس 2026، على الساعة 2:13، على الرابط: https://www.algeriepolice.dz

87. معلومة قانونية: عقوبة التزوير أو التحريف في وثائق الحالة المدنية، منصة اليوتيوب على قناة النهار tv ، منشور بتاريخ 16 جوان 2025، تم الاطلاع عليه يوم 14 أفريل 2026، على الساعة 15:48، على الرابط: https://youtu.be/uAlPN5_sBwA?si=m89ts0tLgvel8uWK

88. مقال: الاحكام الجديدة في قانون مكافحة التزوير واستعمال المزور محور يوم دراسي بالجزائر العاصمة، جريدة هورايزون ((Horizons، 30 جوان 2024، تم الاطلاع عليه بتاريخ 27 مارس 2026، على الساعة 18:48، على الرابط: https://www.horizons.dz

89. مقال: التصديق الالكتروني (Electronic certification)، صادر عن الموقع الرسمي لسلطة ضبط البريد والاتصالات الالكترونية، تم الاطلاع يوم 24 مارس 2026، على الساعة 01:40، على الرابط: https://www.arpce.dz/en/big-folders/electronic-certification

90. مقال: التوقيع والتصديق الالكترونيين، صادر عن الموقع الرسمي لوزارة البريد والمواصلات السلكية واللاسلكية ، تم الاطلاع عليه يوم 24 مارس 2026، على الساعة 2:04، على الرابط: https://www.mpt.gov.dz

91. مقال: الجزائر: اقرار قانون جديد يتصدى لجرائم تزوير الوثائق، الصادر عن موقع العربي الجديد، تم الاطلاع عليه يوم 25 مارس 2026، على الساعة 22:25، على الرابط: https://www.alaraby.co.uk

92. مقال: بحث و دراسة حول الجرائم الالكترونية وأنواعها والاجراءات القانونية لمكافحتها، صادر عن الموقع السوري للاستشارات والدراسات القانونية، اطلع عليه بتاريخ 15 مارس 2026، على الساعة 20:55، الرابط: www.syrianalaw.net

93. مقال: صدور قانون مكافحة التزوير واستعمال المزور في الجريدة الرسمية، الصادر عن موقع الجزائر الان، بتاريخ 13 مارس 2024، تم الاطلاع عليه بتاريخ 25 مارس 2026، على الساعة 23:14، على الرابط: https://algeriemaintenant.dz

94. مكافحة الجريمة الالكترونية: بوغالي يبرز ضرورة تحديث المنظومة التشريعية الوطنية، منصة الاذاعة الجزائرية، منشور بتاريخ 30 جوان 2025، تم الاطلاع عليه يوم 08 ماي 2026، على الساعة 19:09، على الرابط: http://news.radioalgerie.dz/ar/node/67139

95. منير ركاب، توظيف الذكاء الاصطناعي و"البلوك تشين" والدينار الرقمي لحماية السيادة المالية بالجزائر، موقع الشروق أونلاين، منشور بتاريخ 27 أفريل 2026، تم الاطلاع عليه يوم 13 ماي 2026، على الساعة 14:09، على الرابط: https://www.echoroukonline.com

96. مهام الدرك الوطني، منشور على موقع الدرك الوطني، تم الاطلاع عليه يوم 08 ماي 2026، على الساعة 20:05، على الرابط: https://www.gendarmerie.mr/ar/missions

97. مواجهة الجريمة المعلوماتية في التشريع الجزائري، موقع جامع الكتب الاسلامية، تم الاطلاع عليه يوم 10 أفريل 2026، على الساعة 20:06، على الرابط: https://ketabonline.com

98. موسى قرومي: جريمة التزوير واستعمال المزور أخذت ابعادا خطيرة، الاذاعة الجزائرية، تم النشر يوم 30 جوان 2024، تم الاطلاع عليه يوم 7 افريل 2026، على الساعة 15:53، على الرابط: https://news.radioalgerie.dz

99. مي أحمد، محكمة النقض توضح القصد الجنائي في جرائم التزوير، موقع قاضي أنلاين، منشور منذ 3 سوات (2023)، تم الاطلاع عليه يوم 7 أفريل 2026، على الساعة 17:06، على الرابط: https://kadyonline.com

100. مينا فايق، جرائم التزوير في المحررات الرسمية والعرفية، منشور على موقع الدكتور مينا فايق، بتاريخ 9 سبتمبر 2025، تم الاطلاع عليه يوم 6 أفريل 2026، على الساعة 21:20، على الرابط: https://menafayq.com

101. نور اليقين، شرح برنامج DSploit لاختراق الأجهزة المتصلة بنفس الشبكة، موقع لوك ويب، بتاريخ 06 مارس 2021، تم الاطلاع عليه يوم 14 أفريل 2026، على الساعة 14:36، على الرابط: https://loqweb.com

102. هذه أهم الشروط الخاصة بانشاء بنك رقمي في الجزائر، موقع ايكو ألجيريا، منشور بتاريخ 22 نوفمبر 2024، تم الاطلاع عليه يوم 13 ماي 2026، على الساعة 13:57، على الرابط: https://www.eco-algeria.dz/content

103. يعيش تمام شوقي، خليفة محمد، نظام المعالجة الالية للمعطيات الالكترونية كأساس للحماية الجزائية في التشريع الجزائري، مركز جيل البحث العلمي، بتاريخ 16 أوت 2018، تم الاطلاع عليه بتاريخ 2 أفريل 2026، على الساعة 19:14، على الرابط: https://jilrc.com

104. The legality of accessing blocked websites and using web proxy servers, Site web Masaar, Publié le 7 mars 2021, Consulté le 14 avril 2026, à 17:12, Sur le lien: https://masaar.net

الفهرس

➢ الفهرس

المحتوى	رقم الصفحة
المقدمة	أ – ج
الفصل الأول: الإطار المفاهيمي لجريمة التزوير الرقمي في القانون الجزائري	
المبحث الأول: ماهية التزوير الرقمي في التشريع الجزائري	02
المطلب الأول: تعريف التزوير الرقمي وخصائصه	03
الفرع الأول: التعريف اللغوي والاصطلاحي للتزوير الرقمي.	04
الفرع الثاني: الخصائص المميزة للتزوير الرقمي عن التزوير التقليدي.	07
الفرع الثالث: علاقة التزوير الرقمي بالجرائم المعلوماتية الأخرى.	10
المطلب الثاني: محل جريمة التزوير الرقمي (المحرر الإلكتروني)	16
الفرع الأول: تعريف المحرر الإلكتروني في التشريع الجزائري.	16
الفرع الثاني: شروط الاعتراف بالقيمة القانونية للمحرر الإلكتروني.	19
الفرع الثالث: التوقيع الإلكتروني كهدف لعمليات التزوير.	23
المطلب الثالث: صور التزوير الرقمي في الواقع العملي	27
الفرع الأول: تزوير البيانات والمعطيات المخزنة.	27
الفرع الثاني: تزوير المواقع الإلكترونية والبريد الإلكتروني.	31
الفرع الثالث: تزوير البطاقات البنكية ووسائل الدفع الإلكتروني.	35
المبحث الثاني: الأركان القانونية لجريمة التزوير الرقمي	40
المطلب الأول: الركن الشرعي (محل الحماية)	41
الفرع الأول: النظام المعلوماتي أو نظام المعالجة الآلية للمعطيات.	42
الفرع الثاني: البيانات الرقمية ذات الحجية القانونية.	46
الفرع الثالث: المصلحة المحمية من تجريم التزوير الرقمي.	51
المطلب الثاني: الركن المادي للجريمة	55
الفرع الأول: السلوك الإجرامي (تغيير الحقيقة بالوسيلة الرقمية)	55
الفرع الثاني: النتيجة الإجرامية (احتمال وقوع ضرر)	58
الفرع الثالث: العلاقة السببية في الجريمة الرقمية.	62
المطلب الثالث: الركن المعنوي (القصد الجنائي)	64
الفرع الأول: القصد الجنائي العام (العلم والإرادة)	64
الفرع الثاني: القصد الجنائي الخاص (نية استعمال المحرر المزور)	67
الفرع الثالث: وقت توافر الركن المعنوي في الجرائم العابرة للحدود.	70

المبحث الثالث: النظام العقابي لجرائم التزوير الرقمي	74
المطلب الأول: العقوبات الأصلية المقررة	74
الفرع الأول: العقوبات المقررة للشخص الطبيعي.	74
الفرع الثاني: المسؤولية الجزائية والعقوبات المقررة للشخص المعنوي.	76
الفرع الثالث: عقوبة الشروع والمشاركة في التزوير الرقمي.	78
المطلب الثاني: الظروف المشددة والأعذار القانونية	81
الفرع الأول: تشديد العقوبة في حالة المساس بمؤسسات الدولة.	81
الفرع الثاني: صفة الفاعل (الموظف العام أو المتخصص في المعلوماتية)	84
الفرع الثالث: الأعذار المعفية والمخففة للعقوبة.	86
المطلب الثالث: العقوبات التكميلية والتدابير الأمنية	88
الفرع الأول: المصادرة (الأجهزة والبرامج المستخدمة)	88
الفرع الثاني: المنع من الإقامة أو ممارسة النشاط المهني.	93
الفرع الثالث: غلق المواقع الإلكترونية أو المنصات الرقمية محل الجريمة.	95
الفصل الثاني: مظاهر الحماية القانونية من جرائم التزوير الرقمي في التشريع الجزائري	
المبحث الأول: إجراءات البحث والتحري في جرائم التزوير الرقمي	109
المطلب الأول: المعاينة والتفتيش الإلكتروني	111
الفرع الأول: خصوصية تفتيش الأنظمة المعلوماتية.	111
الفرع الثاني: شروط وضوابط التفتيش الإلكتروني في القانون الجزائري.	113
الفرع الثالث: حماية الخصوصية أثناء إجراءات البحث والتحري.	116
المطلب الثاني: ضبط البيانات الرقمية وحفظها	119
الفرع الأول: طرق ضبط الوسائط الإلكترونية وتأمينها.	119
الفرع الثاني: القواعد الفنية لضمان عدم تغيير البيانات المضبوطة.	123
الفرع الثالث: إجراءات التحريز الرقمي.(Hash Value)	126
المطلب الثالث: الأساليب التحقيقية الخاصة	130
الفرع الأول: اعتراض المراسلات الإلكترونية وتسجيلها.	130
الفرع الثاني: المراقبة الإلكترونية والولوج إلى الأنظمة.	134
الفرع الثالث: التسرب الإلكتروني كآلية لكشف المزورين.	137
المبحث الثاني: إثبات جريمة التزوير الرقمي والملاحقة القضائية	140
المطلب الأول: حجية الدليل الرقمي في القضاء الجزائري	141

الفرع الأول: مفهوم الدليل الرقمي وشروطه (الموثوقية والنزاهة)	141
الفرع الثاني: القيمة القانونية للمستخرجات الرقمية في الإثبات.	144
الفرع الثالث: تحديات تزوير الأدلة الرقمية ذاتها.	146
المطلب الثاني: دور الخبرة القضائية والمعلوماتية	150
الفرع الأول: استعانة القضاء بالخبراء في المعلوماتية.	151
الفرع الثاني: مهام الخبير الرقمي في كشف التزوير.	152
الفرع الثالث: حجية تقرير الخبير أمام قاضي الموضوع.	153
المطلب الثالث: الاختصاص القضائي في جرائم التزوير الرقمي	155
الفرع الأول: الاختصاص النوعي (الأقطاب القضائية المتخصصة)	156
الفرع الثاني: الاختصاص المحلي في الجرائم المرتكبة عبر الإنترنت.	159
الفرع الثالث: مشكلة تنازع الاختصاص في الجرائم الدولية.	162
المبحث الثالث: الآليات المؤسساتية والتعاون الدولي لمكافحة التزوير الرقمي	164
المطلب الأول: الهيئات الوطنية المتخصصة في الجزائر	166
الفرع الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.	166
الفرع الثاني: دور مركز مكافحة الجرائم المعلوماتية (الدرك والأمن الوطني)	169
الفرع الثالث: دور السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي.	171
المطلب الثاني: دور مقدمي الخدمات والقطاع الخاص	173
الفرع الأول: التزامات مقدمي خدمات الإنترنت في الكشف عن التزوير.	174
الفرع الثاني: مسؤولية البنوك في حماية المحررات المالية الرقمية.	176
الفرع الثالث: التبليغ عن الجرائم الرقمية وحماية المبلغين.	178
المطلب الثالث: التعاون الدولي في مكافحة التزوير الرقمي	180
الفرع الأول: آليات تسليم المجرمين والمساعدة القضائية المتبادلة.	180
الفرع الثاني: دور المنظمات الدولية (الإنتربول والاتفاقيات الدولية)	183
الفرع الثالث: تقييم مدى مواءمة التشريع الجزائري للاتفاقيات الدولية (اتفاقية بودابست)	185
الخاتمة	190
قائمة المصادر والمراجع	195
الفهرس	–
الملخص	–

الملخص

الملخص

تناولت هذه الدراسة موضوع الحماية القانونية من جرائم التزوير الرقمي في التشريع الجزائري، وذلك في سياق التحول الرقمي المتسارع الذي غيّر من طبيعة المحررات والمعاملات القانونية، وقد هدف البحث إلى تقديم قراءة تحليلية متكاملة للإطار القانوني الموضوعي والإجرائي والمؤسساتي لهذه الجرائم، انطلاقاً من الإشكالية المتمثلة في مدى كفاية النصوص الجزائية والإجرائية الجزائرية في مواجهة التحديات التقنية والإجرامية المستجدة.

تضمنت الدراسة فصلين رئيسيين: خصص الفصل الأول للإطار الموضوعي لجريمة التزوير الرقمي، فتناول ماهية هذه الجريمة وخصائصها المميزة عن التزوير التقليدي، ومحلها المتمثل في المحرر الإلكتروني والتوقيع الرقمي، فضلاً عن صورها العملية المتنوعة من تزوير البيانات والمواقع الإلكترونية ووسائل الدفع الرقمي، كما تطرق هذا الفصل إلى دراسة الأركان القانونية للجريمة من ركن مادي ومعنوي، وانتهى بتحليل النظام العقابي المعتمد وتقييم العقوبات الأصلية والتكميلية والظروف المشددة.

أما الفصل الثاني فقد ركز على الآليات الإجرائية والمؤسساتية لمكافحة التزوير الرقمي، من خلال دراسة إجراءات البحث والتحري الإلكتروني وضبط الأدلة الرقمية وحفظها، وأساليب التحقيق الخاصة كالمراقبة والاعتراض، وتناول كذلك مسائل الإثبات وحجية الدليل الرقمي أمام القضاء، ودور الخبرة القضائية المعلوماتية في كشف التلاعب، فضلاً عن الاختصاص القضائي في الجرائم العابرة للحدود، واختتم الفصل بدراسة الآليات المؤسساتية الوطنية ودور مقدمي الخدمات والقطاع الخاص، وانتهاءً بالتعاون الدولي في مجال الملاحقة والمساعدة القضائية المتبادلة.

وقد توصل البحث إلى مجموعة من النتائج أبرزها أن التشريع الجزائري قد أرسى قاعدة قانونية للحماية من التزوير الرقمي، غير أن هذه الحماية لا تزال تواجه تحديات تتعلق بدقة التجريم وملاءمة العقوبات وتعقيد الإجراءات الإثباتية، مما يستدعي تطويراً تشريعياً ومؤسساتياً ودولياً متواصلاً.

الكلمات المفتاحية:

التزوير الرقمي، المحرر الإلكتروني، التوقيع الإلكتروني، الجرائم المعلوماتية، الدليل الرقمي، الخبرة القضائية المعلوماتية، التعاون الدولي، التشريع الجزائري.

Summary

This study examined the legal protection against digital forgery crimes in Algerian legislation, within the context of the rapid digital transformation that has changed the nature of legal documents and transactions, The research aimed to provide a comprehensive analytical reading of the substantive, procedural, and institutional legal framework for these crimes, starting from the central problem concerning the adequacy of Algerian criminal and procedural texts in addressing emerging technical and criminal challenges.

The study comprised two main chapters: The first chapter addressed the substantive framework of digital forgery crime, covering the definition of this crime and its distinguishing characteristics from traditional forgery, its object represented by the electronic document and digital signature, as well as its practical forms including data forgery, website manipulation, and digital payment fraud, This chapter also examined the legal elements of the crime, both material and moral, and concluded with an analysis of the applicable penal system and an evaluation of original and complementary penalties and aggravating circumstances.

The second chapter focused on the procedural and institutional mechanisms for combating digital forgery, through studying electronic investigation and inquiry procedures, digital evidence seizure and preservation, and special investigative methods such as surveillance and interception, It also addressed issues of proof and the legal value of digital evidence before the judiciary, the role of judicial informatics expertise in detecting manipulation, as well as judicial jurisdiction in cross-border crimes, The chapter concluded with an examination of national institutional mechanisms, the role of service providers and the private sector, and finally international cooperation in prosecution and mutual legal assistance.

The research reached several conclusions, most notably that Algerian legislation has established a legal basis for protection against digital forgery; however, this protection still faces challenges related to the precision of criminalization, adequacy of penalties, and complexity of evidentiary procedures, necessitating continuous legislative, institutional, and international development.

Keywords:

Digital Forgery, Electronic Document, Digital Signature, Cybercrimes, Digital Evidence, Judicial Informatics Expertise, International Cooperation, Algerian Legislation.