الحماية القانونية من التزوير الرقمي في القانون الجزائري

The Legal Protection against Digital Forgery in Algerian Legislation



د.ايمان بغدادي
جامعة المجاهد عبد الحفيظ بوالصوف-ميلة-كلية الحقوق
baghdadi.i@centre-univ-mila.dz

تاريخ الإرسال: 17 / 08 /2026 تاريخ القبول: 10 / 11 /2026 تاريخ النشر: 17 / 11 /2026

ملخص:
المشرع الجزائري إنتهج سياسة تشريعية متكاملة لتعزيز الإطار القانوني للمعاملات الإلكترونية، من خلال تكريس الإعتراف بها وتوفير حماية جزائية فعالة لها وفي هذا السياق وسع نطاق التجريم ليشمل مختلف صور التزوير التي تمس المحررات والمعطيات الرقمية دون تمييز بينها، بإعتبار أن جوهر الجريمة يكمن في تغيير الحقيقة بقصد إحداث الضرر كما عزز هذا التوجه بإضفاء بعد سيادي على حماية البيانات والهوية الرقمية، من خلال اعتبار سلامتها جزءًا من متطلبات الأمن القومي في الجزائر، بما يعكس إهتمامه المتزايد بتعزيز الثقة والأمن في البيئة الرقمية.
كلمات مفتاحية: المشرع، المعاملات الإلكترونية، التزوير، الأمن القومي، الجزائر.

Abstract:

The Algerian legislator has adopted a comprehensive legislative policy to strengthen the legal framework governing electronic transactions by formally recognizing their legal validity and ensuring effective criminal protection, In this context, it has broadened the scope of criminalization to encompass all forms of forgery affecting both electronic documents and digital data without distinguishing between them,

ايمان بغدادي baghdadi.i@centre-univ-mila.dz

on the grounds that the essence of the offense lies in the alteration of the truth with the intent to cause harm, Furthermore this approach has been reinforced by granting the protection of digital data and digital identity a sovereign dimension, considering their integrity an essential component of Algeria's national security, This reflects the legislator's growing commitment to enhancing trust and security within the digital environment.

Keywords: *Legislator, Electronic Transactions, Forgery, National Security, Algeria.*

مقدمة :

من خلال التطور التشريعي الذي عرفته الجزائر، ولا سيما النصوص القانونية الصادرة خلال سنتي 2024 و2026، أن المشرع الجزائري اتجه نحو إرساء إطار قانوني متكامل لتنظيم وتأمين البيئة الرقمية. فقد شكل القانون رقم **24-06** المؤرخ في 28 أفريل 2024، المعدل والمتمم للأمر رقم **66-15** المؤرخ في 8 جوان 1966 والمتضمن قانون العقوبات، نقطة تحول مهمة من خلال تكريس الاعتراف القانوني الكامل بالتعاملات الإلكترونية، وهو ما استوجب بالضرورة توفير حماية جزائية فعالة لها وانسجاما مع هذا التوجه، جاء القانون رقم **24-02** المؤرخ في 26 فيفري 2024 والمتعلق بمكافحة التزوير واستعمال المزور، ليعزز هذه الحماية من خلال عدم التمييز في التجريم والعقاب بين تزوير المحررات الرقمية وتزوير المعطيات الرقمية، بإعتبار أن العبرة ليست بوعاء المعلومة وإنما بالنتيجة الإجرامية المتمثلة في تغيير الحقيقة بقصد إحداث ضرر ولم يقتصر الأمر على ذلك، بل تعزز هذا المسار بصدور القانون رقم **26-02** المؤرخ في 17 فيفري 2026 المتعلق بالخدمات العامة لخدمات الثقة للمعاملات الإلكترونية والتعريف الإلكتروني، الذي منح حماية المعطيات الرقمية بعدًا سياديًا، من خلال اعتباره أن سلامة

البيانات والهوية الرقمية تمثل عنصرًا أساسيا من عناصر الأمن القومي، بما يعكس انتقال المشرع من مجرد حماية المعاملات الإلكترونية إلى حماية الثقة الرقمية والسيادة الرقمية للدولة، فالعلاقة المنطقية بين القوانين الثلاثة تكمن في أن الأول قد أرسى الأساس القانوني للإعتراف بالمعاملات الإلكترونية، والثاني وفر لها حماية جزائية مشددة ضد جرائم التزوير، أما الثالث فارتقى بهذه الحماية إلى مستوى السيادة الوطنية والأمن القومي، بما يعكس تطور السياسة التشريعية الجزائرية في مجال الأمن الرقمي.

فإلى أي مدى يضمن الإطار القانوني الجزائري حماية فعالة وأمنا قانونيا متكاملا للمستندات والبيانات الرقمية ضد جرائم التزوير الرقمي، وفي أي مدى تستجيب القواعد الإجرائية والموضوعية الحالية للتحديات المستحدثة التي تفرضها تقنيات التزوير الحديثة كالذكاء الاصطناعي والهوية الرقمية؟

1. تعزيز الثقة في المعاملات الإلكترونية كآلية للوقاية من التزوير الرقمي

صدر القانون رقم 26-02 في 17 فيفري 2026 ليحدد القواعد العامة المتعلقة بخدمات الثقة للمعاملات الإلكترونية وبالتعريف الإلكتروني[1]، في خطوة تهدف إلى تعزيز موثوقية البيئة الرقمية وضمان أمن المعاملات المنجزة عبر الوسائط الإلكترونية وقد نظم القانون آليات إنشاء التوقيع الإلكتروني والختم الإلكتروني، وبين البيانات التقنية اللازمة لإنشائهما، إضافة إلى الشهادات الإلكترونية المرتبطة بهما، مثل شهادة التوقيع الإلكتروني وشهادة الختم الإلكتروني، والتي تصدر عن مؤدي خدمات الثقة وفق ضوابط قانونية محددة، كما عرف القانون خدمات الثقة وخدمات الثقة المعتمدة، واشترط ممارستها من قبل مؤدين مرخص لهم ومسجلين في قائمة رسمية تعدها السلطة المختصة وتقوم بتحيينها ونشرها بوسائل آمنة، بما يضمن سلامة عمليات التوثيق الإلكتروني ومصداقيتها.

ومن جهة أخرى، كرس القانون نظام التعريف الإلكتروني، بإعتباره وسيلة للتحقق من العلاقة بين الشخص الطبيعي أو المعنوي وهويته الرقمية، من خلال مجموعة من الخصائص والبيانات التي تمكن من التعرف عليه بصورة فريدة داخل البيئة الإلكترونية، وهو ما يعزز الثقة في المعاملات الرقمية ويضمن إثبات هوية أطرافها، وترتبط هذه الأحكام إرتباطا وثيقا بمكافحة التزوير الرقمي، إذ أن تنظيم وسائل التوقيع والختم والتعريف الإلكتروني وإنشاء منظومة قانونية لخدمات الثقة يسهم في الحد من إمكانية إنتحال الهوية أو إصطناع التوقيعات والأختام الإلكترونية أو التلاعب بالمحررات والبيانات الرقمية، كما توفر هذه الآليات وسائل فنية وقانونية للتحقق من أصالة الوثائق الإلكترونية وسلامتها ونسبتها إلى منشئها الحقيقي، مما يعزز إكتشاف جرائم التزوير الرقمي وإثباتها، ويحد من الإعتداء على الثقة في المعاملات الإلكترونية وبذلك يشكل القانون رقم **26-02** أحد أهم المرتكزات التشريعية الداعمة لحماية المحررات والبيانات الإلكترونية من صور التزوير المختلفة، إلى جانب النصوص الجزائية التي تجرم هذه الأفعال وتعاقب مرتكبيها.

1.1 مفهوم التزوير الرقمي

إن إقرار المشرّع الجزائري للتزوير الرقمي كجريمة قائمة بذاتها يجد مبرره في المكانة القانونية التي أضحت تحتلها البيانات المعلوماتية، باعتبارها تتمتع بذات الحجية القانونية المقررة للمحررات الورقية ويستند هذا التجريم إلى أحكام المادة 394 مكرر 1 من قانون العقوبات في القسم السابع مكرر المعنون بالمساس بأنظمة المعالجة الآلية للمعطيات، التي تجرّم كل فعل من شأنه المساس بسلامة المعطيات المعلوماتية، حيث نصّت على معاقبة "كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدّل بطريق الغش المعطيات التي يتضمنها"، بما يؤكد اتجاه المشرّع نحو توفير حماية جزائية للثقة والأمان في البيئة الرقمية.

وطبقا للمادة 03 من قانون رقم 24-02 مؤرخ في 26 فيفري 2024 الذي يتعلق بمكافحة التزوير وإستعمال المزور [2]، يعرف التزوير بأنه كل تغيير للحقيقة يتم بسوء نية وبطريقة احتيالية في محرر أو وثيقة أو دعامة من الدعامات التي يحددها القانون، بأي وسيلة كانت، متى كان من شأن هذا التغيير إحداث ضرر، كما يشترط أن يكون من شأن الفعل أو الغرض منه ترتيب آثار قانونية، سواء من خلال إقرار حق أو اكتساب صفة أو إثبات واقعة ذات حجية قانونية ويشمل مفهوم التزوير صورًا متعددة من الأفعال، من بينها التقليد والتزييف، وفقًا لما يحدده التشريع.

ومنه فإن التزوير الرقمي يعرف بأنه كل تغيير أو تحريف أو إدخال أو حذف غير مشروع يتم بطريقة إلكترونية على البيانات أو المعطيات المعلوماتية أو المحررات الرقمية، باستعمال وسائل تقنية من شأنها المساس بصحتها أو سلامتها أو مصداقيتها، بهدف إظهارها على غير حقيقتها أو ترتيب آثار قانونية عليها أو إحداث ضرر بالغير ويشمل ذلك مختلف صور العبث بالمعلومات المخزنة أو المتداولة عبر الأنظمة المعلوماتية، بما يؤدي إلى فقدان الثقة في حجيتها الإلكترونية.

فالتغيير الزائف للمحتويات الرقمية مثل: الصور والصور الفوتوغرافية والوثائق، والموسيقى...الخ وقد يكون ذلك بهدف تحقيق مكاسب اقتصادية وقد يشمل هذا النوع من التزوير، التزوير الإلكتروني وانتحال الهوية.[3]

أ-الضوابط القانونية والتقنية للتوقيع والختم الإلكترونيين المعتمدين كآلية لحماية المعاملات الرقمية من التزوير

تنص المادة 04 من القانون رقم **26-02** المتعلق بالقواعد العامة لخدمات الثقة للمعاملات الإلكترونية والتعريف الإلكتروني، على مجموعة من الشروط الواجب توافرها حتى يكتسب التوقيع الإلكتروني والختم الإلكتروني صفة

الموثوقية، حيث يشترط أن يكون كل منهما مرتبطًا بالموقع أو بمنشئ الختم ارتباطًا فريدا يسمح بتحديد هويته، وأن يكون مرتبطا بالبيانات الإلكترونية التي اقترن بها بطريقة تضمن كشف أي تعديل يطرأ عليها لاحقا، كما يجب أن يتم إنشاؤهما بواسطة بيانات إنشاء التوقيع الإلكتروني أو الختم الإلكتروني التي تمكن الموقع أو منشئ الختم من استعمالها بدرجة عالية من الثقة وتحت سيطرته الخاصة، بما يضمن سلامة عملية الإنشاء وعدم إمكانية استخدامها من طرف الغير.

أما المادة 05 من القانون ذاته فقد خصت التوقيع الإلكتروني المعتمد والختم الإلكتروني المعتمد بشروط أكثر صرامة، حيث أوجبت أن يتم إنشاؤهما استنادًا إلى شهادة إلكترونية معتمدة، وبواسطة آلية إنشاء توقيع إلكتروني أو ختم إلكتروني معتمدة، بما يحقق مستوى أعلى من الأمان والموثوقية، كما حددت البيانات الإلزامية التي يجب أن تتضمنها شهادة التوقيع الإلكتروني المعتمد أو شهادة الختم الإلكتروني المعتمد، ومن بينها الإشارة إلى كونها شهادة معتمدة، والبيانات التي تسمح بالتعرف بشكل واضح على مزود خدمات الثقة الذي أصدرها، بما في ذلك تسميته ورقم تسجيله عند الاقتضاء وفقًا للتشريع المعمول به.

كما اشترط المشرع تضمين شهادة التوقيع الإلكتروني المعتمد اسم الموقع أو اسمًا مستعارًا له مع ضرورة الإشارة صراحة إلى استعمال الاسم المستعار في حين يجب أن تتضمن شهادة الختم الإلكتروني المعتمد تسمية منشئ الختم ورقم تسجيله عند الاقتضاء، إضافة إلى ذلك يجب أن تحتوي الشهادة على بيانات التحقق من صحة التوقيع أو الختم الإلكتروني بما يتطابق مع بيانات إنشائهما، إلى جانب تحديد مدة صلاحية الشهادة من خلال بيان تاريخ بدايتها ونهايتها، ووضع رمز تعريف فريد لها يميزها لدى مزود خدمات الثقة.

كما أوجب القانون إدراج توقيع موثوق أو معتمد أو ختم إلكتروني موثوق أو معتمد خاص بمزود خدمات الثقة الذي أصدر الشهادة، فضلاً عن توفير رابط إلكتروني يسمح بالوصول المجاني إلى الشهادة التي يستند إليها التوقيع أو الختم الإلكتروني، بالإضافة إلى المعلومات أو الخدمات اللازمة للتحقق من حالة صلاحية الشهادة وفي حال كانت بيانات إنشاء التوقيع أو الختم الإلكتروني محفوظة داخل آلية الإنشاء وجب تضمين بيان يوضح ذلك بطريقة قابلة للمعالجة الآلية.

ويبرز من خلال هذه الأحكام أن المشرع الجزائري لم يكتف بالاعتراف القانوني بالتوقيع والختم الإلكترونيين [4]، بل وضع منظومة تقنية وقانونية متكاملة تهدف إلى ضمان سلامتهما وإثبات نسبتهما إلى أصحابها الحقيقيين وهو ما يرتبط مباشرة بمكافحة التزوير الرقمي، باعتبار أن هذه الشروط توفر وسائل للتحقق من مصدر الوثيقة الإلكترونية، وكشف أي تعديل أو تحريف يطرأ عليها، ومنع إنشاء توقيعات أو أختام إلكترونية مزيفة، مما يعزز حجية المحررات الإلكترونية ويحمي الثقة في المعاملات الرقمية.

ب- دور خدمات الثقة الرقمية في مكافحة التزوير الإلكتروني وتعزيز حجية الوثائق الرقمية

يكرس القانون رقم 26-02 المتعلق بخدمات الثقة مبدأ إلزامية توطين جميع المعطيات التي يتم جمعها من طرف مؤدي خدمات الثقة داخل التراب الوطني، مع إمكانية نقلها إلى الخارج في إطار ممارسة نشاطهم، شريطة عدم مخالفة أحكام التشريع والتنظيم المعمول بهما، كما يشترط لممارسة المتدخلين في المجال الحكومي مهام الطرف الثالث الموثوق الحصول على موافقة مسبقة من السلطة المختصة، وذلك بعد تقديم طلب وفق الإجراءات المحددة قانونا.

ويخضع تقديم خدمات الثقة لضرورة إجراء تدقيق تقييمي يثبت فعالية ومطابقة الوسائل المعتمدة، تقوم به السلطة أو الهيئة الوطنية المكلفة بأمن الأنظمة المعلوماتية، ويترتب عن نجاح هذا التدقيق منح صفة الطرف الثالث الموثوق للمتدخلين في المجال الحكومي ويتم إجراء هذا التدقيق بناءً على طلب المؤسسة المعنية الموجه إلى السلطة الوطنية للتصديق الإلكتروني ويقدم الطرف الثالث الموثوق خدمات الثقة وخدمات الثقة المعتمدة مجانا في حدود مجال اختصاصه.

ويقصد بخدمة الثقة وفقا لهذا القانون، كل خدمة إلكترونية تهدف إلى ضمان خصائص معينة للوثيقة الإلكترونية، وتشمل على وجه الخصوص آليات إنشاء وإدارة التوقيع الإلكتروني، والختم الإلكتروني، وختم الوقت الإلكتروني إضافة إلى توثيق مواقع الإنترنت، والحفظ الإلكتروني، وخدمات الإرسال الإلكتروني المضمون.

ويلتزم الطرف الثالث الموثوق باحترام متطلبات تقديم خدمات الثقة التي تحددها السلطة المختصة، والمحافظة على سرية البيانات والمعلومات المرتبطة بهذه الخدمات، كما يلتزم، بالتنسيق مع السلطة الوطنية للتصديق الإلكتروني بحفظ الشهادات الإلكترونية بعد انتهاء صلاحيتها وفقًا لسياسات التصديق الإلكتروني المعتمدة، كما يخضع لأحكام التدقيق الدوري المنصوص عليها في القانون.

ولا يجوز للطرف الثالث الموثوق الاحتفاظ أو نسخ بيانات إنشاء التوقيع الإلكتروني الخاصة بالشخص الحاصل على الشهادة الإلكترونية إلا بعد الحصول على موافقته الصريحة، كما أخضع القانون تقديم خدمات الثقة في المجال الاقتصادي لنظام الترخيص المسبق الذي تمنحه السلطة المختصة، ويُمنح هذا الترخيص حسب طبيعة الخدمة المقدمة، ويرفق بدفتر شروط تعده

السلطة الوطنية للتصديق الإلكتروني يحدد مدة الترخيص وشروط وكيفيات ممارسة النشاط.

وقد حددت المادة 34 من القانون شروط منح ترخيص تقديم خدمات الثقة، حيث يسبق الحصول عليه منح شهادة تأهيل لمدة سنتين قابلة للتجديد مرة واحدة، تمنح لكل شخص يستوفي الشروط القانونية اللازمة قصد تهيئة الوسائل التقنية والتنظيمية الضرورية لممارسة نشاط خدمات الثقة ويمنح الترخيص النهائي لحامل شهادة التأهيل بعد اجتياز تدقيق تقييمي يثبت مدى استيفائه للمتطلبات القانونية والتنظيمية.

كما تضمنت المواد 40 وما يليها من القانون مجموعة من الالتزامات المفروضة على مؤدي خدمات الثقة، بهدف ضمان موثوقية هذه الخدمات، وحماية البيانات الإلكترونية، وتعزيز الثقة في المعاملات الرقمية.

2.1 التزوير الرقمي وأمن المعاملات الرقمية في ظل المنصة الوطنية الموحدة للخدمات الرقمية

يمثل التزوير الرقمي أحد أبرز التحديات التي تهدد أمن المعاملات الرقمية، لما ينطوي عليه من تزوير للوثائق والبيانات والهويات الإلكترونية بما ينعكس سلباً على الثقة في الخدمات الرقمية وفي هذا الإطار تسعى الجزائر من خلال المنصة الوطنية الموحدة للخدمات الرقمية إلى تعزيز أمن المعاملات الإلكترونية عبر توفير بيئة رقمية آمنة تعتمد على التحقق الإلكتروني وحماية البيانات وتوحيد الخدمات الرقمية، كما تسهم هذه المنصة في الحد من مخاطر التزوير الرقمي من خلال تعزيز آليات المراقبة والتوثيق الإلكتروني وضمان سلامة وتكامل المعاملات الرقمية.

أ-أشكال التزوير الإلكتروني الحديثة وأثرها على أمن المعاملات الرقمية

على الرغم من التطور المستمر الذي شهدته آليات الحماية الرقمية، فإن أساليب التزوير الإلكتروني لا تزال في تطور متسارع، إذ يعمل الفاعلون غير المشروعون على تطوير تقنياتهم بالاعتماد على فهم عميق للبنى الرقمية والثغرات التي قد تعتريها، بهدف اختراق دائرة الثقة القائمة بين المستخدمين والمؤسسات، والاستيلاء على الهوية الرقمية أو البيانات المصرفية أو إنشاء وثائق إلكترونية مزورة تبدو في ظاهرها صحيحة ويصعب اكتشاف زيفها.

ويتخذ التزوير الإلكتروني صورا متعددة ومتجددة، تبدأ من التلاعب بالتوقيعات الرقمية وانتحال الهويات الإلكترونية، وصولا إلى تقليد المنصات والمواقع الرسمية، فضلا عن تعديل الصور والمحررات الرقمية باستخدام تقنيات الذكاء الاصطناعي القادرة على إنتاج محتويات وملفات بالغة الواقعية يصعب تمييزها عن النسخ الأصلية وقد أدى ذلك إلى إثارة إشكالات جوهرية في المجالات القانونية والاقتصادية والبحثية بشأن مدى إمكانية الحفاظ على المصداقية والثقة في بيئة رقمية أصبح التحقق التقليدي فيها غير كاف لمواجهة أساليب التزييف الحديثة.

ولعل الجانب الأكثر خطورة في هذا التطور يتمثل في أن أدوات التزوير الإلكتروني لم تعد تقتصر على المحررات والوثائق الرقمية، بل امتدت لتشمل إنتاج تسجيلات صوتية ومقاطع مرئية مفبركة تتمتع بدرجة عالية من الواقعية، الأمر الذي يفاقم صعوبة عمليات الكشف والتحقيق، ويهدد موثوقية الأدلة الرقمية والشهادات المعتمدة في المجالات القضائية والإعلامية والبحثية، وتبرز خطورة تقنيات التزييف العميق (Deepfake) بإعتبارها من أبرز صور التلاعب الرقمي الحديثة، إذ أصبحت تستخدم لانتحال أصوات وصور الأشخاص، وخاصة الشخصيات العامة، بهدف نسب تصريحات أو أفعال غير حقيقية إليهم، وهو ما قد يترتب عليه آثار خطيرة تمس الاستقرار السياسي والاجتماعي والاقتصادي، لا سيما في الفترات الحساسة كالانتخابات أو

الأزمات، حيث يمكن توظيف محتويات مزيفة يصعب تفنيدها دون الاستعانة بتقنيات متقدمة للتحليل الرقمي والتحقق من صحتها.[5]

تشمل أشكال التزوير الإلكتروني الحديثة عدة صور مستحدثة تعتمد على التكنولوجيا الرقمية والذكاء الاصطناعي، ومن أبرزها [6]:

- تزوير الهوية الرقمية: انتحال شخصية الأفراد أو المؤسسات عبر إنشاء حسابات وهمية أو سرقة بيانات الهوية الإلكترونية.
- تزوير التوقيع الإلكتروني: تقليد أو سرقة التوقيعات الإلكترونية والشهادات الرقمية لاستعمالها في إبرام العقود أو إجراء المعاملات.
- تزوير المستندات الإلكترونية: تعديل أو إنشاء وثائق رقمية مزورة مثل العقود والفواتير والشهادات الإدارية باستخدام برامج متطورة .
- التصيد الإلكتروني: (Phishing) إنشاء مواقع أو رسائل إلكترونية مزيفة بهدف الحصول على البيانات الشخصية أو البنكية للضحايا .
- التزييف العميق: (Deepfake) استخدام تقنيات الذكاء الاصطناعي لتزوير الصور أو مقاطع الفيديو أو الأصوات بصورة يصعب اكتشافها .
- تزوير وسائل الدفع الإلكترونية: مثل تزوير البطاقات البنكية، والمحافظ الإلكترونية، وأوامر التحويل الإلكتروني .
- تزوير البيانات المخزنة في الأنظمة المعلوماتية: اختراق قواعد البيانات وتعديل أو حذف أو إضافة معلومات غير صحيحة .
- تزوير العملات والأصول الرقمية: إنشاء رموز رقمية وهمية أو التلاعب بالمعاملات المتعلقة بالعملات المشفرة.

ب-اطلاق المنصة الوطنية الموحدة للخدمات الرقمية ودورها في مكافحة التزوير الرقمي

أفادت المحافظة السامية للرقمنة في بيان لها، أن الرابط الرسمي والوحيد للبوابة الوطنية للخدمات الرقمية Dzair Digital Services هو [7] dzds.dz

يمثل انتقال الجزائر إلى الرقمنة عبر المنصة الوطنية الموحدة للخدمات الرقمية والمركز الوطني للخدمات الرقمية نقلة نوعية تهدف إلى تبسيط الإجراءات ويُرتقب أن يشكل المركز الوطني الجزائري للخدمات الرقمية، الذي دشنه مؤخرا، نقطة تحول في مسار الرقمنة بالجزائر، لما سيتيحه من تسريع غير مسبوق في تقديم الخدمات الإدارية، واستخراج الوثائق، ومعالجة الملفات التي تتطلب تبادل المعلومات بين مختلف الإدارات، من دون إلزام المواطن بالتنقل أو إعادة تقديم وثائق تمتلكها هيئات أخرى، وتشمل أبرز هذه المميزات ما يلي [8]:

- القضاء على البيروقراطية: إنهاء معاناة التنقل المستمر بين الإدارات وإلغاء الطابع المادي (سياسة "صفر ورق") لمعالجة الملفات.
- تبادل البيانات الآني: ربط مختلف المنصات الحكومية ببعضها البعض، مما يتيح للإدارات الوصول إلى الوثائق المشتركة دون طلبها من المواطن في كل مرة.
- تسهيل الإجراءات عن بعد: توفير واجهة تفاعلية آمنة تُمكّن المواطنين من استخراج الوثائق الرسمية ومتابعة الطلبات رقمياً بسرعة وسهولة.
- تعزيز الشفافية والرقابة: قطع الطريق أمام الممارسات السابقة كالتزوير والإدلاء بمعلومات خاطئة، إلى جانب دعم دقة الإحصائيات.
- السيادة الرقمية: تأمين بيانات الدولة وبنيتها التحتية الرقمية بمركز بيانات وطني متطور يعتمد على أحدث المعايير الدولية.
- الارتقاء بالخدمة العمومية: تقليص أوقات الانتظار ومعالجة الطلبات بشكل أسرع وأكثر كفاءة، مما يرفع من جودة الخدمات العامة المقدمة.

ان المركز الوطني للخدمات الرقمية يوفّر أيضا ضمانات قوية لحماية المعطيات الشخصية، ويطمئن المواطنين إلى أن بياناتهم أصبحت مخزّنة داخل الجزائر، وليس في مراكز بيانات أجنبية، مع تطبيق معايير عالمية في الأمن السيبراني وحماية التجهيزات والتطبيقات واستمرارية الخدمة.

2. الردع القانوني للتزوير الرقمي في الجزائر

يمثل الردع القانوني للتزوير الرقمي في الجزائر أحد الآليات الأساسية لحماية الثقة في المعاملات الإلكترونية وضمان أمن الوثائق والبيانات الرقمية، وذلك من خلال تجريم مختلف صور التلاعب بالمحررات والبيانات الإلكترونية، وفرض عقوبات جزائية على مرتكبيها، إلى جانب اعتماد آليات إجرائية وتقنية لمكافحة هذه الظاهرة.

1.2 التجريم بالقوانين القديمة

بدأ المشرّع الجزائري في مواجهة ظاهرة الإجرام المعلوماتي من خلال تعديل قانون العقوبات سنة 2004 بموجب القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، حيث تم استحداث قسم خاص بالمساس بأنظمة المعالجة الآلية للمعطيات[9]، وذلك استجابة لظهور أفعال إجرامية جديدة مرتبطة باستخدام الحاسوب والأنظمة الرقمية وقد جاء هذا التدخل التشريعي لسد الفراغ القانوني وحماية البيانات والأنظمة المعلوماتية من الاعتداءات التي تهدد سلامة المعاملات الإلكترونية والثقة في البيئة الرقمية، وكان لزوما معه أيضا وضع احكام خاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها في قانون اخر، ليكون بعده كذلك ضرورة وجود قانون متعلقا بحماية المعطيات ذات الطابع الشخصي لتوفير حماية قانونية من مختلف الأفعال المرتبطة بهذه الجريمة.

أ-التجريم في قانون العقوبات الجزائري القديم

تم تعديل قانون العقوبات الجزائري من خلال استحداث القسم السابع مكرر تحت عنوان **"**المساس بأنظمة المعالجة الآلية للمعطيات**"**، وذلك ضمن المواد من 394 مكرر إلى 394 مكرر 7، حيث تضمن هذا القسم تجريم مجموعة من الأفعال المرتبطة بالاعتداءات على الأنظمة المعلوماتية، وذلك على النحو الآتي:

- جرم المشرع الجزائري الدخول أو البقاء غير المشروع داخل كل أو جزء من نظام للمعالجة الآلية للمعطيات، متى تم ذلك بطريقة احتيالية، أو مجرد محاولة القيام به، وقرر لذلك عقوبة الحبس من ثلاثة أشهر إلى سنة، وغرامة مالية تتراوح بين 50.000 و200.000 دج، كما شدّد العقوبة في حال أدى الفعل إلى حذف أو تغيير البيانات الموجودة بالنظام، بينما تكون العقوبة أشد إذا ترتب عن ذلك تعطيل أو تخريب سير عمل النظام، حيث تصبح الحبس من ستة أشهر إلى سنتين والغرامة من 50.000 إلى 300.000 دج .
- اعتبر المشرّع إدخال بيانات بطريقة احتيالية إلى نظام المعالجة الآلية للمعطيات، أو حذف أو تعديل البيانات الموجودة به دون وجه حق، من الأفعال المجرّمة، ورتب عليها عقوبة الحبس من ستة أشهر إلى ثلاث سنوات، وغرامة مالية تتراوح بين 500.000 و4.000.000 دج .
- جرّم الأفعال العمدية المرتكبة بوسائل احتيالية والمتعلقة بالمعطيات المعلوماتية، والمتمثلة في تصميم أو إعداد أو جمع أو توفير أو نشر أو الاتجار في البيانات المخزنة أو المعالجة أو المرسلة عبر نظام معلوماتي، متى كانت قابلة للاستعمال في ارتكاب الجرائم المنصوص عليها في هذا القسم، كما شمل التجريم حيازة أو كشف أو نشر أو استعمال البيانات المتحصل عليها نتيجة ارتكاب إحدى هذه الجرائم،

وقرر لهذه الأفعال عقوبة الحبس من شهرين إلى ثلاث سنوات وغرامة من 1.000.000 إلى 10.000.000 دج.

- رفع المشرّع مستوى الحماية الجنائية عندما تستهدف الجرائم المعلوماتية مصالح حساسة، حيث تُضاعف العقوبات المقررة إذا كان محل الجريمة يتعلق بالدفاع الوطني أو بالهيئات والمؤسسات الخاضعة للقانون العام، وذلك دون المساس بتطبيق أي عقوبات أشد قد تنص عليها تشريعات أخرى.
- امتدت المسؤولية الجزائية إلى الشخص المعنوي في حال ارتكابه إحدى الجرائم المنصوص عليها ضمن هذا القسم، حيث يعاقب بغرامة مالية تساوي خمسة أضعاف الحد الأقصى للغرامة المقررة للشخص الطبيعي.
- جرّم المشرّع الاشتراك في جماعة أو اتفاق يهدف إلى التحضير لارتكاب جريمة أو أكثر من الجرائم المعلوماتية المنصوص عليها في هذا القسم، متى تجسد هذا التحضير في أفعال مادية، وقرر معاقبة المشاركين بالعقوبات نفسها المقررة للجريمة محل التحضير.
- أقرّ المشرّع إمكانية الحكم بمصادرة الوسائل المستعملة في ارتكاب الجرائم المعلوماتية، بما في ذلك الأجهزة والبرامج والوسائل التقنية، مع إمكانية غلق المواقع الإلكترونية التي كانت محلاً للجريمة، وكذا غلق المحل أو مكان الاستغلال إذا ثبت علم مالكه بارتكاب الجريمة، مع مراعاة حقوق الغير حسن النية.
- أخضع الشروع في ارتكاب الجنح المنصوص عليها ضمن هذا القسم للعقوبات نفسها المقررة للجريمة التامة، تأكيداً على السياسة الجنائية الوقائية الرامية إلى الحد من الاعتداءات على أنظمة المعالجة الآلية للمعطيات.

ب-التجريم في القانون الخاص بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها

ان قانون رقم 09-04 المؤرخ في 5 أوت 2009 جاء متضمنا القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها [10]، وهي جرائم المساس بالانظمة المعالجة الآلية للمعطيات الواردة في قانون العقوبات أعلاه وأي جريمة أخرى ترتكب أو يسهل إرتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية.

تنص المادة 11 من هذا القانون على أنه، مع مراعاة طبيعة الخدمات المقدمة ونوعيتها، يلتزم مقدمو خدمات الاتصال الإلكتروني، سواء كانوا أشخاصاً طبيعيين أو معنويين من القطاعين العام أو الخاص وكل جهة تتولى معالجة البيانات المعلوماتية أو تخزينها لصالح خدمات الاتصال أو لفائدة مستعمليها بالاحتفاظ بمجموعة من البيانات الضرورية وتشمل هذه البيانات ما يسمح بتحديد هوية مستعملي الخدمة والبيانات المتعلقة بالأجهزة الطرفية المستخدمة في الاتصال، والخصائص التقنية للاتصالات، وتاريخها ووقتها ومدتها، فضلاً عن البيانات الخاصة بالخدمات التكميلية المطلوبة أو المستعملة والجهات المقدمة لها، إضافة إلى البيانات التي تمكن من التعرف على متلقي الاتصال وعناوين المواقع الإلكترونية التي تمت زيارتها.

وفيما يتعلق بخدمات الهاتف، يلتزم المتعامل بحفظ البيانات التي تسمح بتحديد هوية مستعملي الخدمة، وكذا البيانات التي تمكن من تحديد مصدر الاتصال وموقعه الجغرافي وقد حدد المشرع مدة الاحتفاظ بجميع هذه البيانات بسنة واحدة تبدأ من تاريخ تسجيلها.

كما قرر المشرع، إلى جانب الجزاءات الإدارية المترتبة على الإخلال بهذه الالتزامات، قيام المسؤولية الجزائية للأشخاص الطبيعيين والمعنويين متى أدى عدم احترام هذه الالتزامات إلى عرقلة السير الحسن للتحريات القضائية ويعاقب الشخص الطبيعي في هذه الحالة بالحبس لمدة تتراوح بين ستة أشهر وخمس سنوات وبغرامة مالية من 50.000 دج إلى 500.000 دج، في حين يعاقب الشخص المعنوي بالغرامة وفق الأحكام والقواعد المنصوص عليها في قانون العقوبات.

ج-التجريم في قانون حماية المعطيات الشخصية

كرّس القانون رقم 18-07 حماية جزائية للمعطيات ذات الطابع الشخصي[11] من خلال تجريم الأفعال التي تمس بسرية البيانات وخصوصية الأفراد ومن بين هذه الأفعال الحصول على المعطيات الشخصية بوسائل غير مشروعة، كاللجوء إلى الغش أو الاختراق أو أي أساليب تدليسية أخرى، حيث يعاقب مرتكب هذا الفعل بالحبس من سنة إلى ثلاث سنوات وبغرامة تتراوح بين 100.000 دج و300.000 دج، كما يجرّم القانون جمع أو الاحتفاظ بالبيانات المتعلقة بالوضعية الجزائية للأشخاص خارج الحالات المقررة قانوناً، ويعاقب على ذلك بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 60.000 دج إلى 300.000 دج.

وفيما يتعلق بالمخالفات المرتبطة بإنشاء معالجة المعطيات الشخصية، فقد أخضع المشرّع عمليات المعالجة لجملة من الضوابط القانونية، إذ يعاقب على معالجة البيانات دون موافقة صاحبها أو رغم اعتراضه المشروع بالحبس من سنة إلى ثلاث سنوات وبغرامة من 100.000 دج إلى 300.000 دج. كما شدّد العقوبة بالنسبة لإنجاز أو الأمر بإنجاز معالجة للمعطيات الشخصية دون استيفاء إجراءات التصريح أو الحصول على الترخيص المسبق من السلطة

الوطنية المختصة، حيث تتراوح العقوبة بين سنتين وخمس سنوات حبساً، بالإضافة إلى غرامة من 200.000 دج إلى 500.000 دج.

ومن جهة أخرى، رتّب القانون مسؤولية جزائية على عاتق القائم بمعالجة المعطيات الشخصية عند الإخلال بالالتزامات المفروضة عليه، لاسيما فيما يتعلق بضمان حقوق الأشخاص المعنيين بالمعالجة كحقهم في الإعلام والاطلاع على بياناتهم وتصحيحها أو الاعتراض على معالجتها ويعاقب على إنكار هذه الحقوق بالحبس من شهرين إلى سنتين وبغرامة من 20.000 دج إلى 200.000 دج أو بإحدى هاتين العقوبتين، كما يعاقب على الإخلال بواجب المحافظة على سرية وأمن المعطيات الشخصية بغرامة تتراوح بين 200.000 دج و500.000 دج، فضلاً عن تجريم كل إخلال بواجب التعاون والتواصل مع السلطة الوطنية لحماية المعطيات الشخصية.

كذلك يجرّم القانون كل استغلال للمعطيات الشخصية خارج الأهداف التي جُمعت من أجلها أو خلافاً لشروط التصريح أو الترخيص الممنوح، بما في ذلك الاحتفاظ بها بعد انتهاء المدة القانونية أو إفشاؤها للغير غير المؤهل للاطلاع عليها، سواء كان ذلك عمداً أو نتيجة إهمال، لما يشكله هذا السلوك من مساس بحق الأفراد في حماية حياتهم الخاصة وبياناتهم الشخصية.

2.2 التجريم بالقوانين الجديدة

أدى التطور المتسارع لتكنولوجيا المعلومات والاتصالات وانتشار المعاملات الإلكترونية في الجزائر إلى ظهور أنماط جديدة من الجرائم، وعلى رأسها التزوير الرقمي والنصب الإلكتروني، والتي تتسم بالسرعة والتعقيد وصعوبة اكتشاف مرتكبيها، كما أن اتساع استخدام المنصات الرقمية والخدمات الإلكترونية أوجد مخاطر متزايدة تهدد أمن المعاملات الرقمية والثقة في البيئة

الإلكترونية، الأمر الذي استدعى تدخل المشرع الجزائري من خلال تعديل النصوص القانونية واستحداث أحكام جزائية جديدة تواكب التطور التقني وتوفر حماية قانونية فعالة للأفراد والمؤسسات.

أ- التجريم بقانون العقوبات الجزائري المعدل

وفقاً لأحكام القانون رقم 24-06 المؤرخ في 28 أفريل 2024 والمتضمن تعديل وتتميم قانون العقوبات، نصت المادة 394 مكرر على معاقبة كل من يتسلل أو يحاول التسلل بطريق الغش إلى منظومة للمعالجة الآلية للمعطيات، كلياً أو جزئياً، بعقوبة الحبس من ستة (06) أشهر إلى سنتين وبغرامة تتراوح بين 60.000 دج و200.000 دج وتُشدد العقوبة إذا ترتب عن هذا الفعل حذف أو تعديل للمعطيات الموجودة داخل المنظومة، بينما ترتفع إلى الحبس من سنة إلى ثلاث (03) سنوات وغرامة من 100.000 دج إلى 300.000 دج إذا أدى الفعل إلى الإخلال أو التخريب في سير نظام المعالجة الآلية.

كما تقضي المادة 394 مكرر 1 بمعاقبة كل من يقوم بإدخال معطيات إلى نظام المعالجة الآلية أو حذفها أو تعديلها باستعمال وسائل احتيالية، بعقوبة الحبس من سنة إلى ثلاث (03) سنوات وبغرامة تتراوح بين 500.000 دج و2.000.000 دج.

أما المادة 394 مكرر 2، فقد قررت عقوبة الحبس من سنة إلى خمس (05) سنوات وغرامة من 1.000.000 دج إلى 5.000.000 دج لكل من يتعمد، وبطرق احتيالية، تصميم أو إعداد أو تجميع أو توفير أو نشر أو المتاجرة بمعطيات مخزنة أو معالجة أو مرسلة عبر منظومة معلوماتية يمكن استعمالها في ارتكاب الجرائم المنصوص عليها في هذا القسم، كما تشمل العقوبة كل

صور حيازة أو إفشاء أو استخدام المعطيات المتحصل عليها من إحدى هذه الجرائم، مهما كان الغرض من ذلك.

وبخصوص المادة 394 مكرر 3، فقد شددت العقوبة إلى الحبس من سنتين إلى عشر (10) سنوات وغرامة من 700.000 دج إلى 2.000.000 دج عندما تستهدف الجرائم المنصوص عليها في هذا القسم الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، وذلك دون المساس بإمكانية تطبيق العقوبات الأشد متى اقتضى الأمر ذلك.

ب-التجريم في قانون مكافحة التزوير واستعمال المزور

جاء القانون رقم 24-02 المؤرخ في 26 فيفري 2024 المتعلق بمكافحة التزوير واستعمال المزور بإطار قانوني شامل يهدف إلى مواجهة مختلف صور التزوير، حيث امتد نطاق التجريم فيه ليشمل تزوير الوثائق الإدارية والشهادات، والمحررات العمومية أو الرسمية، وكذا المحررات العرفية والتجارية والمصرفية، وذلك ضمن الأحكام الممتدة من المادة 22 إلى المادة 37 منه، كما شمل التجريم صورا أخرى تتمثل في التزوير بغرض الاستفادة من الإعانات والمساعدات العمومية أو الحصول على الإعفاءات، وتزوير النقود والسندات، فضلا عن تقليد الأختام والدمغات والطوابع والعلامات، إضافة إلى تجريم شهادة الزور واليمين الكاذبة، وانتحال الوظائف أو الألقاب أو الأسماء أو إساءة استعمالها، وهي الأفعال التي نظمها المشرع ضمن المواد 38 إلى 70 من القانون ذاته.

ولا يقتصر نطاق تطبيق هذه الأحكام على المحررات والوثائق في صورتها التقليدية الورقية، بل يمتد كذلك إلى البيئة الإلكترونية، وهو ما يتضح من خلال إدراج المشرع للبعد الرقمي ضمن أحكام القانون، لاسيما من خلال

تعريف المحرر في المادة الأولى باعتباره كل دعامة مكتوبة، سواء كانت ورقية أو إلكترونية، تمكن من تحديد هوية الشخص الصادرة عنه، كما أكد المشرع على ضرورة اعتماد تدابير وقائية لحماية الوثائق والمحررات من مخاطر التزوير، حيث أوجب على السلطات الإدارية والهيئات والمؤسسات العمومية والخاصة اتخاذ الإجراءات التقنية والتنظيمية الكفيلة بتأمينها، من خلال اعتماد مواصفات فنية تحد من إمكانية العبث بها، ووضع آليات للتحكم في الولوج إلى قواعد البيانات وحماية المعلومات ذات الطابع الحساس.

وفي السياق ذاته، أقر القانون آليات للتنسيق وتبادل المعلومات بين مختلف المصالح والجهات المعنية بالرقابة، سواء بصورة مباشرة أو بواسطة المنصات الرقمية المخصصة لذلك، مع الاستعانة بقواعد البيانات المرتبطة بالوثائق للتحقق من صحتها، كما ألزم الإدارات والمؤسسات والهيئات العمومية والجماعات المحلية والمصالح التابعة لها بالتحقق من سلامة وصحة الوثائق والمحررات المقدمة إليها بمختلف الوسائل المتاحة، خاصة عبر الرجوع إلى قواعد البيانات الخاصة بها لدى الجهات المصدرة لها، بما يعزز الثقة في المعاملات الإدارية والرقمية ويحد من انتشار صور التزوير الإلكتروني.

ج-التجريم في قانون خدمات الثقة للمعاملات الالكترونية

إلى جانب الجزاءات الإدارية والمالية المنصوص عليها في المواد من 88 إلى 93 من القانون رقم 26-02، فقد أقر المشرع مجموعة من الأحكام الجزائية الواردة في المواد من 94 إلى 108، بهدف ضمان حسن استعمال خدمات الثقة الرقمية وحماية المعاملات الإلكترونية من مختلف صور الاعتداء أو الاستعمال غير المشروع.

فقد رتب المشرع غرامة مالية تتراوح بين 50.000 دج و200.000 دج على كل شخص يستعمل خدمة الثقة في غير الأغراض التي منحت من أجلها، كما يعاقب بالحبس من شهرين إلى سنة وبغرامة من 200.000 دج إلى 1.000.000 دج أو بإحدى هاتين العقوبتين كل مؤدي خدمات ثقة يمتنع عن إعلام السلطة المختصة بتوقف نشاطه، أو يخل بالالتزامات المتعلقة بسرية البيانات والمعلومات المرتبطة بتقديم خدمات الثقة، أو يستأنف أو يواصل نشاطه بعد تعليق ترخيصه أو انقضاء مدة صلاحيته.

ويعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 200.000 دج إلى 1.000.000 دج كل من يتعمد الإخلال بالتزام التحقق من هوية طالب الشهادة المعتمدة للتوقيع الإلكتروني أو الختم الإلكتروني، أو يدلي بتصريحات كاذبة بغرض الاستفادة من خدمة ثقة، أو يمتنع عن احترام الأحكام المتعلقة بجمع البيانات الشخصية الضرورية لتقديم هذه الخدمات، وتشدد العقوبة إلى الحبس من ستة أشهر إلى ثلاث سنوات وغرامة من 1.000.000 دج إلى 5.000.000 دج في حق كل من يحوز أو يفشي أو يستعمل بيانات إنشاء التوقيع الإلكتروني أو الختم الإلكتروني الخاصة بالغير، وكذلك في حق الشخص المكلف بالتدقيق الذي يتعمد إفشاء المعلومات السرية التي اطلع عليها أثناء أداء مهامه لأشخاص غير مرخص لهم.

كما يعاقب بالحبس من سنة إلى ثلاث سنوات وبغرامة من 1.000.000 دج إلى 5.000.000 دج كل من يقدم خدمات ثقة للجمهور دون الحصول على الترخيص اللازم أو يواصل نشاطه بعد سحب الترخيص، فضلاً عن كل من يتعمد إتلاف أو إخفاء الوثائق أو المعلومات التي تطلبها السلطة المختصة وفقا لأحكام المادة 49 وتخضع التجهيزات والوسائل المستعملة في ارتكاب هذه الجرائم للمصادرة طبقاً للتشريع الساري المفعول.

وفي حالة العود، تتضاعف العقوبات المقررة في هذا القانون، كما يجوز للجهات القضائية المختصة توقيع عقوبة تكميلية أو أكثر من العقوبات المنصوص عليها في قانون العقوبات ويُسأل الشخص المعنوي جزائياً عن الجرائم المنصوص عليها في هذا القانون وفق القواعد العامة المقررة في التشريع الجزائي.

الخاتمة:

مما سبق نستنتج أن أثر التزوير الإلكتروني على أمن المعاملات الرقمية يكمن في:

- فقدان الثقة في التجارة الإلكترونية والخدمات الرقمية.
- تعريض البيانات الشخصية والمالية للخطر وسرقتها.
- زيادة الخسائر المالية للأفراد والمؤسسات.
- المساس بسرية وسلامة البيانات داخل الأنظمة المعلوماتية.
- إضعاف حجية المحررات الإلكترونية وصعوبة إثبات صحتها.
- تهديد الأمن السيبراني والاقتصاد الرقمي وتعطيل الخدمات الإلكترونية.
- زيادة النزاعات القانونية المتعلقة بإثبات المعاملات الإلكترونية وتحديد المسؤولية.

وتكمن جهود الجزائر في مكافحة التزوير الإلكتروني من خلال:

- تخصيص المركز الوطني الجزائري للخدمات الرقمية منظومة رقمية سيادية متكاملة، أُنشئت في إطار استراتيجية الدولة الرامية إلى تطوير بنية رقمية وطنية حديثة قائمة على توظيف التكنولوجيات الرقمية وإدارة البيانات، بما يساهم في تعزيز السيادة الرقمية من خلال ضمان استضافة ومعالجة بيانات الدولة داخل الإقليم الوطني، وفقًا لأعلى

معايير الأمن المعلوماتي والموثوقية والاستمرارية، ويعتمد هذا المركز على مركزين وطنيين للبيانات مجهزين بقدرات متقدمة في مجال المعالجة والاستضافة، ومصممين وفق المعايير الدولية المعتمدة، حيث تم إنجازهما بالتعاون مع شركاء تقنيين دوليين، من أبرزهم مجمع شركات "هواوي" الصينية، مع الاستفادة من أحدث الحلول التكنولوجية، إلى جانب برامج نقل المعرفة وتطوير مهارات الكفاءات الوطنية المتخصصة في المجال الرقمي.

- صور الردع القانوني للتزوير الرقمي في الجزائر تكمن في:
  - الردع الموضوعي: ويتمثل في تجريم أفعال تزوير البيانات والوثائق الإلكترونية، ومعاقبة مرتكبيها بعقوبات سالبة للحرية وغرامات مالية حسب طبيعة الفعل والضرر الناتج عنه .
  - الردع الإجرائي: من خلال منح جهات التحقيق والقضاء صلاحيات البحث والتحري في الجرائم الإلكترونية، واعتماد وسائل تقنية لجمع الأدلة الرقمية .
  - الردع الوقائي: عبر تعزيز أنظمة التوقيع الإلكتروني، التشفير، وحماية قواعد البيانات ورفع مستوى الأمن السيبراني داخل المؤسسات.
- تُظهر الأحكام التي أتى بها توجه المشرّع الجزائري نحو تعزيز الحماية الجنائية للبيئة الرقمية في قانون العقوبات وهو أول نص مجرم، من خلال تجريم مختلف صور الاعتداء على الأنظمة المعلوماتية والبيانات الإلكترونية، ومواجهة المخاطر الناتجة عن الاستخدام غير المشروع للتكنولوجيا.
- رغم التطور النسبي للإطار التشريعي الجزائري، إلا أن مواجهة التزوير الرقمي ما تزال تواجه عدة تحديات، منها سرعة تطور التقنيات المستخدمة في ارتكاب الجريمة، وصعوبة تحديد هوية الجناة بسبب

الطابع العابر للحدود للفضاء الرقمي، إضافة إلى الحاجة إلى تكوين متخصص للقضاة وأعوان الضبطية القضائية في مجال الأدلة الرقمية، وعليه فإن فعالية الردع القانوني للتزوير الرقمي في الجزائر لا تتوقف على وجود النصوص القانونية فقط، بل تتطلب تكاملًا بين التشريع والتقنيات الحديثة، والتعاون الدولي، وتطوير آليات التحقيق الرقمي لضمان حماية المعاملات الإلكترونية وتعزيز الثقة في البيئة الرقمية.

المراجع:

1-القانون رقم 26-02 في 17 فيفري 2026 ليحدد القواعد العامة المتعلقة بخدمات الثقة للمعاملات الإلكترونية وبالتعريف الإلكتروني، الجريدة الرسمية العدد 14، المؤرخ في 18 فيفري 2026.

2-قانون رقم 24-02 مؤرخ في 26 فيفري 2024 الذي يتعلق بمكافحة التزوير وإستعمال المزور، الجريدة الرسمية العدد 15، المؤرخ في 29 فيفري 2024.

[3]- M. N. O. Sadiku, Sarhan M. Musa, and S. R. Nelatury, DIGITAL FORGERY, International Journal of Advances in Scientific Research and Engineering (ijasre), Vol. 03, Issue 4, May -2017, p 26.

[4]- أنظر القانون رقم 15-04 المؤرخ في 1 فيفري 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، الجريدة الرسمية العدد 06، المؤرخ في 1 فيفري 2015.

[5]- https://elbadilabc-ar.dz/%D8%A7%D9%84%D8%

6- Khiari Rayane, Selmani Hayette, Electronic Forgery As a Manifestation of Digital Corruption, Journal of Legal Studies and Researche, Vol: 11 No 1, January 2026, p 19.

7- https://www.hcn.dz/

[8]- https://www.echoroukonline.com/%D9%87

[9]-القانون رقم 15/04 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر 156/66 المؤرخ في 08 جوان 1966 والمتضمن قانون العقوبات الجزائري، الجريدة الرسمية عدد 71 المؤرخ في 27 جوان 2001.

10-قانون رقم 09-04 المؤرخ في 5 أوت 2009 جاء متضمنا القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، الجريدة الرسمية العدد 47 المؤرخ في 16 أوت 2009.
11- القانون رقم 18-07 المؤرخ في 10 يونيو 2018 يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية العدد 34 المؤرخ في 10 يونيو 2018، المعدل والمتمم بالقانون رقم 25-11 المؤرخ في 24 يوليو 2025 يعدل ويتمم القانون رقم 18-07 لسنة 2018 والمتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية العدد 48 المؤرخ في 24 يوليو 2025.