



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



الرقم التسلسلي:

الرمز:

قسم: الحقوق

الشعبة: الحقوق

التخصص: قانون جنائي

المسؤولية القانونية للتزوير في المعاملات الرقمية
والوثائق الإلكترونية

مذكرة ضمن متطلبات نيل شهادة الماستر

إشراف الأستاذة:

د. مقورة مفيضة

إعداد الطالبتين:

* إيمان قساس .

* نهى معاش.

السنة الجامعية: 2025 - 2026



وزارة التعليم العالي والبحث العلمي
جامعة المجاهد عبد الحفيظ بوصوف - ميله
كلية الحقوق



الرقم التسلسلي:

الرمز:

قسم: الحقوق

الشعبة: الحقوق

التخصص: قانون جنائي

المسؤولية القانونية للتزوير في المعاملات الرقمية
والوثائق الإلكترونية

مذكرة ضمن متطلبات نيل شهادة الماستر

إشراف الأستاذة:

د. مقورة مفيضة

إعداد الطالبتين:

* إيمان قساس.

* نهى معاش.

أعضاء لجنة المناقشة

رئيسا	أستاذة محاضرة - ب	منصور نورة. - جامعة عبدالحفيظ بوصوف - ميله
مشرفا ومقررا	أستاذة محاضر - ب	مقورة مفيضة. - جامعة عبدالحفيظ بوصوف - ميله
عضوا مناقشا	أستاذة محاضرة - ب	بوخنوف سمية. - جامعة عبدالحفيظ بوصوف - ميله

السنة الجامعية: 2025 - 2026

ملخص

ملخص

تناولت هذه الدراسة موضوع "المسؤولية القانونية للتزوير في المعاملات الرقمية والوثائق الإلكترونية في التشريع الجزائري، من خلال توضيح مفهوم التزوير الإلكتروني وتمييزه عن التزوير التقليدي، مع بيان أركان الجريمة وصورها المختلفة كالتعديل والحذف والتلاعب بالتوقيع الإلكتروني. كما تطرقت إلى الحجية القانونية للمحررات الإلكترونية ودور التوقيع والتصديق الإلكترونيين في تعزيز الثقة في المعاملات الرقمية، اعتمدت الدراسة على المنهج الوصفي التحليلي لتحليل النصوص القانونية المتعلقة بالجرائم المعلوماتية والتزوير الإلكتروني.

توصلت الدراسة إلى أن المشرع الجزائري وفر حماية قانونية للوثائق الإلكترونية، إلا أن التطور التكنولوجي المتسارع يفرض ضرورة تحديث التشريعات وتعزيز وسائل الإثبات الرقمي. **الكلمات المفتاحية:** التزوير الإلكتروني، المعاملات الرقمية، الوثائق الإلكترونية، التوقيع الإلكتروني، المسؤولية القانونية.

Abstract

This study addressed the issue of legal responsibility for forgery in digital transactions and electronic documents under Algerian legislation. It clarified the concept of electronic forgery and distinguished it from traditional forgery, white highlighting the elements of the crime and its various forms, such as alteration, deletion, and manipulation of electronic signatures. It also discussed the legal evidentiary value of electronic documents and the role of electronic signatures and certification in enhancing trust in digital transactions. The study adopted the descriptive analytical method to analyze Algerian legal texts related to cybercrime and electronic forgery.

The study concluded that the Algerian legislator has provided legal protection for electronic documents, however, the rapid technological development requires continuous updating of legislation and strengthening digital evidentiary tools.

Keywords; electronic forgery, digital transaction, electronic documents, electronic signature, legal responsibility.

شكر و عرفان

الحمد لله الواحد الأحد الذي لم يلد ولم يولد ولم يكن له كفوا أحد،
الحمد لله الذي أعاننا ويسر لنا أمرنا ووفقنا،
والصلاة والسلام على النبي الكريم ومن تبعه بإحسان إلى يوم الدين
الداعي إلى التحلي بكل فضيلة والبعد عن كل رذيلة.
ولا يسعنا إلا أن نتقدم بجزيل الشكر وعظيم الامتنان ونخص بالذكر الأستاذة
المشرفة

" مقورة مفيدة "

على ما قدمه لنا من ملاحظات وتوجيهات.
والى السادة الأساتذة أعضاء لجنة المناقشة على قبول وتقييم وتصويب
هذا العمل وإثرائه بملاحظاتهم القيمة.
إلى كل من مد يد العون والمساعدة إلى الذين طوقونا بجميل صنيعهم وأفادونا
بالرأي ولا يفوتنا
تقديم شكرنا وامتناننا إلى الزملاء والزميلات
وإلى كل طالب علم.
نقول جزاكم الله خيرا وأعانكم

الإهداء

بسم الله الرحمن الرحيم

(... قَدْ جَعَلَهَا رَبِّي حَقًّا...)

أهدي تخرجي إلى

كل من كلل العرق جبينه ومن علمني أن النجاح لا يأتي إلا بالصبر والإصرار
إلى النور الذي أضاء دربي والسراج الذي لا ينطفئ نوره بقلبي أبداً
من بدل الغالي والنفيس الذي استمدت منه قوتي واعتزازي بداتي
والدي العزيز.

إلى من جعل الجنة تحت أقدامها وسهلت لي الشدائد بدعائها إلى الإنسانية العظيمة
التي طالما تمنيت أن تقر عينها لرؤيتي في هذا اليوم إلى
أمي العزيزة

ضلعي الثابت وأمان أيامي إلى من شددت عضدي بهم وكانوا ينباع أرتوى بهم إلى
إخواني وأخواتي الغاليين

لكل من كان عونا وسندا لي في هذا الطريق أهدىكم هذا الإنجاز وثمره النجاح أنا
اليوم أكملت وأنهيت ثمرة نجاحي بفضل الله والحمد لله على ما وهبني وأن يجعلني
مباركاً فمن قال أنا لها نالها فأنا لها وإن أتت رغما عنها أتت بها فالحمد لله
شكراً وحبا وامتناناً على البدئ والختام وآخر دعواي أنه الحمد لله رب العالمين

نهى و

إيمان

الفهرس

فهرس المحتويات

الصفحة	المحتوى
	ملخص
	شكر وتقدير.
	الإهداء.
أ-هـ	مقدمة.
	الفصل الأول: الإطار القانوني لجريمة التزوير في البيئة الرقمية.
08	المبحث الأول: مفهوم التزوير الإلكتروني وتمييزه عن التزوير التقليدي.
08	المطلب الأول: مفهوم التزوير في القانون التقليدي.
09	أولاً : تعريف التزوير في الفقه.
10	ثانياً : تعريفه في التشريع.
11	ثالثاً : عناصره الأساسية في المحررات الورقية.
13	المطلب الثاني: مفهوم التزوير في البيئة الرقمية.
13	أولاً : تعريف التزوير الإلكتروني .
14	ثانياً : صور التزوير في المعاملات الورقية.
17	ثالثاً : الفروق الجوهرية بين التزوير التقليدي والتزوير الإلكتروني .
18	المطلب الثالث: خصائص المعاملات الرقمية والوثائق الإلكترونية وأثرها على التجريم.
19	أولاً : الطبيعة غير المادية للبيانات.
20	ثانياً : الطابع التقني للوسائط الإلكترونية.
21	ثالثاً : إشكالية الحجية القانونية للوثيقة الإلكترونية.
23	المبحث الثاني: أركان جريمة التزوير الإلكتروني وأثرها في قيام المسؤولية القانونية.
23	المطلب الأول: الركن المادي للتزوير الإلكتروني.
24	أولاً : تغيير الحقيقة في محرر إلكتروني.
25	ثانياً : وسائل التزوير (التعديل، الحذف، الاصطناع).

26	ثالثا : النتيجة الإجرامية وعلاقة السببية.
26	المطلب الثاني: الركن المعنوي.
27	أولا : العلم بتغيير الحقيقة.
27	ثانيا: نية استعمال المحرر المزور.
29	ثالثا: قصد الإضرار بالغير.
31	المطلب الثالث: محل جريمة التزوير الإلكتروني.
31	أولا : البيانات الرقمية.
32	ثانيا : التوقيع الإلكتروني.
33	ثالثا : السجلات وقواعد البيانات الإلكترونية.
35	خلاصة الفصل.
الفصل الثاني: المسؤولية القانونية المترتبة عن المعاملات الرقمية والوثائق الإلكترونية.	
38	المبحث الأول: المسؤولية الجنائية عن التزوير الإلكتروني.
38	المطلب الأول: الأشخاص المسؤولون جنائياً.
39	أولا : الفاعل الأصلي.
41	ثانيا: الشريك.
44	ثالثا: مسؤولية الشخص المعنوي.
50	المطلب الثاني: العقوبات المقررة لجريمة التزوير الإلكتروني.
50	أولا :العقوبات الأصلية.
52	ثانيا: العقوبات التكميلية.
54	ثالثا : الظروف المشددة.
56	المطلب الثالث: خصوصية الإثبات في جرائم التزوير الإلكتروني.
56	أولا : حجية المحرر الإلكتروني .
59	ثانيا: وسائل الإثبات الرقمية.
61	ثالثا : الخبرة التقنية ودورها في الإثبات.

64	المبحث الثاني: المسؤولية المدنية والتحديات العملية.
65	المطلب الأول: المسؤولية المدنية والتعويض عن الضرر.
65	أولاً : أركان المسؤولية المدنية.
66	ثانياً : الضرر الرقمي وإثباته.
67	ثالثاً: تقدير التعويض.
68	المطلب الثاني: صعوبات المتابعة القانونية في البيئة الرقمية.
69	أولاً : صعوبة تحديد الفاعل.
70	ثانياً: إشكالية الاختصاص القضائي.
72	ثالثاً: الطابع العابر للحدود للجريمة.
73	المطلب الثالث: آليات الحماية القانونية والوقاية من التزوير الإلكتروني.
74	أولاً : دور التشريع.
75	ثانياً : الحماية التقنية.
77	ثالثاً: دور التوعية والرقابة.
79	خلاصة الفصل.
81	الخاتمة.
85	قائمة المصادر والمراجع.

مقدمة

عرف العالم في السنوات الأخيرة تطورا متسارعا في مجال التكنولوجيا والاتصالات، الأمر الذي أدى إلى الانتقال من البيئة التقليدية القائمة على المحررات الورقية إلى بيئة رقمية تعتمد على المعاملات الإلكترونية والوثائق الرقمية في مختلف المجالات الإدارية والتجارية والمالية. وقد ساهم هذا التحول الرقمي في تسهيل المعاملات وتسريعها وتحقيق الدقة والمرونة في تبادل المعلومات، غير أن هذا التطور صاحبه ظهور أنماط جديدة من الجرائم المستحدثة، وفي مقدمتها التزوير الإلكتروني التي أصبحت تشكل تهديدا حقيقيا لأمن المعاملات الرقمية للثقة المفترضة في الوثائق الإلكترونية.

ويعد التزوير الإلكتروني من الجرائم الحديثة المرتبطة بالتقدم التقني، حيث يتمثل في تغيير الحقيقة في محرر أو وثيقة إلكترونية باستعمال وسائل تقنية بهدف استعمالها على نحو يسبب ضررا للغير. ويختلف ها النوع من التزوير عن التزوير التقليدي من حيث الوسائل المستعملة وطبيعة المحرر محل الجريمة، إذ أصبحت البيانات الرقمية والتوقيع الإلكتروني والسجلات المعلوماتية محلا للاعتداء والتلاعب، وهو ما استوجب تدخل التشريعات الحديثة من أجل توفير حماية قانونية فعالة للمعاملات الإلكترونية.

وفي هذا الإطار سعى المشرع الجزائري إلى مواكبة التطورات التقنية من خلال سن مجموعة من النصوص القانونية التي تنظم المعاملات الإلكترونية وتجرم الأفعال الواقعة على نظم المعالجة الآلية للمعطيات والوثائق الإلكترونية، خاصة قانون العقوبات والقانون رقم 15-04 المتعلق بالتوقيع والتصديق الإلكتروني، وذلك بهدف ضمان أمن البيئة الرقمية وتحقيق الثقة في التعاملات الإلكترونية.

وبناء على ما سبق ذكره فإن الإشكال الذي يمكن طرحه في هذا الإطار يتمثل في:

أولاً: الإشكالية.

ما مدى فعالية السياسة الجنائية في تجريم ومكافحة التزوير الإلكتروني في المعاملات الرقمية والوثائق الإلكترونية؟

وتتفرع عن هذه الإشكالية مجموعة من التساؤلات الفرعية أهمها:

- ما هو الإطار المفاهيمي والقانوني التزوير الإلكتروني والتزوير التقليدي؟
- ماهي أركان جريمة التزوير الإلكتروني؟
- من هم الأشخاص المسؤولون جنائيا عن جريمة التزوير الإلكتروني؟

– ماهي العقوبات المقررة لجريمة التزوير الإلكتروني في التشريع الجزائري؟

ثانيا: فرضيات الدراسة.

للإحاطة بجوانب الإشكالية والإجابة عن تساؤلات المطروحة، يمكن اقتراح الفرضيات التالية:
يساهم تحيين المشرع الجزائري للقوانين المتعلقة بالجرائم الإلكترونية في الحد من الجرائم التزوير الإلكتروني وتعزيز الحماية القانونية للمعاملات الرقمية والوثائق الإلكترونية.
كما يساعد تطوير التشريع الجزائري وتحديث آليات الرقابة والإثبات الرقمي على تعزيز فعالية مكافحة جرائم التزوير الإلكتروني والحد من انتشارها.

ثالثا: أهمية الدراسة.

تتجلى أهمية هذه دراسة في كونها تعالج أحد المواضيع القانونية المعاصرة المرتبطة بحماية المعاملات الإلكترونية من الاعتداءات التقنية. وتكمن أهمية الدراسة من الناحية النظرية في إثراء الدراسات القانونية المتعلقة بجرائم التزوير الإلكتروني وبيان الأحكام القانونية المنظمة لها، أما من الناحية العملية فتظهر من خلال إبراز الآليات القانونية والتقنية التي تساعد الجهات القضائية في مكافحة هذه الجريمة وإثباتها وحماية حقوق المتعاملين إلكترونيا.

رابعا: أسباب اختيار الموضوع.

يرجع سبب اختيارنا لهذا الموضوع إلى جملة من الأسباب الذاتية والموضوعية دفعتنا لاختياره، فمن الناحية الذاتية يتمثل ذلك الميول الشخصي نحو دراسة الجرائم الإلكترونية والرغبة في التعمق في المواضيع القانونية الحديثة المرتبطة بالتكنولوجيا الرقمية، خاصة موضوع التزوير الإلكتروني باعتباره من المواضيع المعاصرة ذات الأهمية كبيرة. إضافة إلى أهمية الموضوع في التكوين الأكاديمي والبحث العلمي.

أما الأسباب الموضوعية فتتمثل في الانتشار المتزايد للمعاملات الإلكترونية وما نتج عنه من تزايد جرائم الإلكترونية فضلا عن حداثة الموضوع وتشعبه في ظل التطور التكنولوجي، حيث أصبح الاعتماد على الوثائق والمعاملات الإلكترونية أمرا شائعا في مختلف المجالات، إضافة إلى أهمية الوقوف على مدى فعالية التشريع الجزائري في توفير الحماية للوثائق الإلكترونية ومواكبته للتطورات التقنية الحديثة.

خامسا: أهداف الدراسة.

- تهدف هذه الدراسة إلى تحقيق جملة من الأهداف تتمثل أساسا في:
- تحديد مفهوم التزوير الإلكتروني وتمييزه عن التزوير التقليدي.
 - بيان أركان جريمة التزوير الإلكتروني وصورها المختلفة.
 - تحديد المسؤولية الجنائية والمدنية المترتبة عنها، إضافة إلى دراسة العقوبات المقررة لها وآليات الإثبات في البيئة الرقمية.
 - إبراز الصعوبات العملية التي تواجه مكافحة هذا النوع من الجرائم واقتراح الوسائل القانونية والتقنية الكفيلة بالحد منها.

سادسا: دراسات السابقة.

- لقد حظي موضوع التزوير باهتمام المتزايد من طرف الباحثين، بالنظر إلى التطور التكنولوجي المتسارع وما صاحبه من انتشار الجرائم الإلكترونية، خاصة جرائم التزوير التي تمس المحررات والوثائق الإلكترونية والمعاملات الرقمية. ومن بين الدراسات التي تم الاطلاع عليها:
- دراسات تناولت الجانب المفاهيمي والتنظيمي للتزوير الإلكتروني، حيث ركزت على تعريف التزوير الإلكتروني وبيان خصائصه وأركانه القانونية، إضافة إلى دراسة حجية المحرر الإلكتروني والتوقيع الإلكتروني في الإثبات، لكنها لم تتوسع بشكل كاف في إبراز المسؤولية القانونية المترتبة عن هذا النوع من الجرائم، سواء المسؤولية الجنائية أو المدنية. ومن بين هذه الدراسات:
 - كتاب الدكتور "جمال نجيمي" بعنوان "جرائم التزوير في قانون العقوبات الجزائري" الصادر سنة 2013، والذي تناول فيه مختلف صور جرائم التزوير في التشريع الجزائري، خاصة التزوير في المحررات، مع تحليل أركان الجريمة والعقوبات المقررة لها، أفادت هذه الدراسة في توضيح الإطار الجنائي لجريمة التزوير وإسقاطه على البيئة الرقمية.
 - رسالة ماجستير الباحث "الجبوري عبد السلام حسين" بعنوان "جريمة التزوير الإلكتروني" تناول فيها ماهية التزوير الإلكتروني وخصائصه، إضافة إلى دراسة موقف التشريعات الحديثة من تجريم هذا النوع من الجرائم والعقوبات المقررة.
 - دراسة مقال الباحث "عبد الله بلقاسم" بعنوان "الطبيعة الخاصة للتزوير في المحررات الإلكترونية" (27 ديسمبر 2020) تناول فيه خصوصية جريمة التزوير الإلكتروني وتمييزها عن التزوير التقليدي، إضافة إلى التحديات القانونية المتعلقة بالإثبات الحماية الجزائية.

كما توجد دراسات ركزت على المسؤولية القانونية الناشئة عن الجرائم الإلكترونية بصفة عامة، من خلال بيان صور المسؤولية الجنائية للفاعل الأصلي ومسؤولية الأشخاص المعنوية ومزودي الخدمات التصديق الإلكتروني، غير أنها تناولت التزوير الإلكتروني بصورة مختصرة، دون التعمق فيه كدراسة مستقلة، من بين هذه الدراسات:

- أطروحة الدكتوراه الأستاذ "فارس بوبكر" بعنوان "المسؤولية المدنية في مجال المعاملات الإلكترونية" الذي تناول فيها أحكام المسؤولية المدنية الناشئة عن استخدام الوسائل الإلكترونية في إبرام وتنفيذ المعاملات الرقمية.
- مقال الباحثة "زهيرة عبوب" بعنوان "المسؤولية المدنية لمقدم خدمات التصديق الإلكتروني دراسة تحليلية لما جاء في قانون 04-15" تناولت فيه الإطار القانوني المنظم لخدمات التصديق الإلكتروني، مع بيان مسؤولية مقدمي هذه الخدمات عن الأضرار الناتجة عن الإخلال بالتزاماتهم القانونية.
- كتاب الباحث "هشام بحوش" بعنوان "الجرائم المتصلة بتكنولوجيا الإعلام والاتصال في ظل التشريع جزائري" تناول فيه مختلف الجرائم المعلوماتية المرتبطة باستعمال وسائل التكنولوجيا الحديثة، مع التركيز على الجرائم الواقعة على نظم المعلومات والمعاملات الإلكترونية.

سابعاً: منهج الدراسة.

للإجابة عن الإشكالية الرئيسية والتساؤلات الفرعية، تم الاعتماد على المنهج الوصفي والمنهج التحليلي، حيث استخدم الوصفي لتحديد المفاهيم المتعلقة بالتزوير الإلكتروني، بينما شخر التحليلي لفحص النصوص القانونية (قانون رقم 02-24، قانون رقم 09-15، قانون العقوبات الجزائري) وغيرها من القوانين المستعملة، مع الاستعانة بالمنهج المقارن في بعض المواضع لإبراز أوجه الاختلاف والتشابه بين التزوير التقليدي والإلكتروني.

ثامناً: حدود الدراسة.

تقتصر حدود هذه الدراسة مكانياً على نطاق التشريع الجزائري، من خلال تحليل النصوص القانونية المنظمة لجريمة التزوير الإلكتروني وحماية الوثائق الإلكترونية، مع الاستعانة ببعض الآراء الفقهية كلما اقتضت الضرورة العلمية. بينما تتحدد زمانياً خاصة بعد صدور القانون رقم 04-09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، وقانون العقوبات الجزائري والقانونين رقم 15-04 و 02-24 وما يلحقهما من نصوص تنظيمية وتعديلات سارية المفعول إلى غاية سنة 2025.

تاسعا: صعوبات الدراسة.

على الرغم من الأهمية العلمية للموضوع، إلا أن هذه الدراسة اصطدمت بجملة من الصعوبات أهمها حداثة الموضوع وتشعبه وارتباطه بالتطور التقني المستمر، مما جعل بعض المعلومات والنصوص القانونية عرضة للتجدد والتعديل، كما واجهت الدراسة صعوبة في الإحاطة بجميع الجوانب التقنية المرتبطة بالجريمة الإلكترونية، فضلا عن محدودية الاجتهادات القضائية والتطبيقات العملية المنشورة المتعلقة بالتزوير في المعاملات الرقمية والوثائق الإلكترونية.

عاشرا: خطة الدراسة.

قصد الإحاطة بمختلف جوانب الموضوع والإلمام بالأبعاد القانونية له، وتماشيا مع المنهجية المتبعة في معالجة الإشكالية المطروحة، تم اعتماد خطة مقسمة إلى فصلين:

- **الفصل الأول:** الإطار القانوني لجريمة التزوير الإلكتروني في البيئة الرقمية، من خلال دراسة مفهوم التزوير الإلكتروني وأركانه وخصائص المعاملات الرقمية والوثائق الإلكترونية.
- **الفصل الثاني:** المسؤولية القانونية المترتبة عن التزوير في المعاملات الرقمية والوثائق الإلكترونية، خصص لدراسة المسؤولية الجنائية والمدنية مع التطرق إلى العقوبات وخصوصية الإثبات وآليات الحماية القانونية والوقاية من هذه الجريمة.

الفصل الأول

الإطار القانوني لجريمة التزوير في البيئة الرقمية

يشهد العالم المعاصر تغييرا جذريا بفعل التطور التكنولوجي المتسارع، الذي أدى إلى بروز ما يعرف بالبيئة الرقمية، حيث أصبحت المعاملات الإلكترونية والوثائق الرقمية جزءا لا يتجزأ من الحياة اليومية، سواء في المجال الإداري أو الاقتصادي أو القانوني. وقد ترتب عن هذا التحول ظهور أنماط جديدة من السلوك الإجرامي، من أبرزها جريمة التزوير الإلكتروني التي تمثل امتدادا حديثا لجريمة التزوير التقليدي، لكنها تتميز عنها بخصائص تقنية وقانونية خاصة.

وإذا كان التزوير في صورته التقليدية يقوم على تغيير الحقيقة في محررات مادية بهدف إحداث ضرر، فإن التزوير في البيئة الرقمية يثير إشكالات قانونية معقدة، تتعلق بطبيعة الدعاية غير المادية للبيانات وسهولة التلاعب بها، وصعوبة اكتشافها، مما يستدعي إعادة النظر في المفاهيم القانونية الكلاسيكية وتكييفها مع المستجدات التكنولوجية.

وعليه يهدف هذا الفصل إلى تحديد الإطار القانوني لجريمة التزوير في البيئة الرقمية من خلال دراسة مفهوم التزوير الإلكتروني وتمييزه عن التزوير التقليدي، وذلك عبر التطرق في المبحث الأول إلى مفهوم التزوير في القانون التقليدي ثم في البيئة الرقمية، مع إبراز أهم الفروق الجوهرية بينهما.

كما يتناول المبحث الثاني خصائص المعاملات الرقمية والوثائق الإلكترونية، وبيان أثر هذه الخصائص على قيام الجريمة وإثباتها، خاصة من حيث الطبيعة غير المادية للبيانات والطابع التقني للوسائط الرقمية، وكذا إشكالية الحجية القانونية للوثيقة الإلكترونية.

وبذلك يشكل هذا الفصل مدخلا أساسيا لفهم الأبعاد القانونية لجريمة التزوير في العصر الرقمي، وتمهيدا لدراسة المسؤولية القانونية المترتبة عنها.

المبحث الأول: مفهوم التزوير الإلكتروني وتمييزه عن التزوير التقليدي.

يشكل التزوير جريمة معروفة منذ القدم، نظرا لما ينطوي عليه من مساس مباشر بالثقة التي تقوم عليها العلاقات بين الأفراد والمؤسسات. وقد ارتبط مفهوم التزوير تقليديا بالمحررات الورقية، حيث يتم تغيير الحقيقة فيها، سواء بطريقة مادية أو معنوية، يقصد استعمالها على نحو يسبب ضررا للغير.

غير أن التطور السريع في تكنولوجيا المعلومات والاتصالات، أدى إلى ظهور أنماط جديدة من المعاملات التي تعتمد على الوثائق الرقمية والإلكترونية. وقد أفرز هذا التحول أشكالاً حديثة من التزوير تختلف في طبيعتها ووسائلها عن التزوير التقليدي.

وأمام هذه التحولات، سعى المشرع إلى مواكبة التطور من خلال سن تشريعات تنظم البيئة الرقمية، وتجرم الأفعال التي تمس بسلامة وصحة البيانات الإلكترونية.

بناء على ذلك، يهدف هذا البحث إلى دراسة مفهوم التزوير بنوعيه: التقليدي والرقمي، حيث سيتم أولاً التطرق إلى التزوير في القانون التقليدي والرقمي، ثم الانتقال إلى التزوير في البيئة الرقمية وأنواعه، مع إبراز أهم الفروقات بينهما. كما سيتم التطرق إلى خصائص المعاملات الرقمية والوثائق الإلكترونية وتحديد عناصرها في هذا السياق الحديث.

المطلب الأول: مفهوم التزوير في القانون التقليدي.

يعد التزوير في المحررات التقليدية من أقدم الجرائم التي اهتمت بها التشريعات الجنائية، بسبب خطورته على استقرار المعاملات القانونية والثقة العامة في الأوراق المكتوبة. وقد انصب اهتمام الفقه والقضاء على تحديد مفهومه وضبط عناصره، ومن هذا المنطلق نتناول في هذا المطلب تعريف التزوير في الفقه.

ثم بيان موقف التشريع منه من خلال النصوص القانونية، وذلك بهدف تأسيس الإطار المفاهيمي يمكن من فهم هذا النوع من الجرائم في صورته التقليدية.

أولاً: تعريف التزوير في الفقه.

يعدّ التزوير من الجرائم التي حظيت باهتمام واسع في الفقه القانوني، حيث تعددت تعريفاته بتعدد اجتهادات الفقهاء، غير أنها تلتقي جميعاً في عناصر جوهرية مشتركة.

فقد عرفه الفقيه غارسون على أنه تغيير للحقيقة بوسائل قانونية قصد الخداع، ويترتب عن هذا التغيير ضرر للغير.¹

كما عرفه أيضا الأستاذ جون بول دوسي بأنه كل تغيير أو تزيف أو نفي للحقيقة أو الواقع أو الأصل، يكون الهدف منه خداع الآخرين.²

في حين عرفه فقيه آخر بأنه كل تحريف للحقيقة، مهما كانت وسيلته سواء تعلق بالمحرر ذاته أو بالدعامة التي يتضمنها أو بطريقة توثيقه، متى كانت هذه الدعامة معدة لإثبات حق أو من شأنها إنتاج آثار قانونية معينة.

كما اعتبر بلحاج العربي أن التزوير هو تغيير للحقيقة، أي تحريف واقعة مع العلم بمخالفتها للواقع، ويشمل هذا المفهوم كل وسيلة يستعملها الشخص بقصد خداع الغير، غير أن المشرع الجنائي لا يجرم جميع صور الغش، بل يقتصر على الأفعال التي تتسم بالخطورة فيخضعها للتجريم ويوفر لها الحماية القانونية. أما باقي صور الغش، فتظل في نطاق المسؤولية المدنية، حيث يترتب عنها فقط إلزام الفاعل بتعويض الضرر الناتج عنها.³

أما الفقه الجنائي عرف التزوير على أنه كل تعديل متعمد للحقيقة في المستندات أو الوثائق أو أي محررات أخرى، باستخدام إحدى الوسائل التي يحددها القانون، بحيث يكون هذا التغيير قادرا على إلحاق الضرر بالمصلحة العامة أو بمصلحة فرد معين، ويرافقه قصد استخدام المحرر المزور للغرض الذي أعد من أجله.⁴

من خلال التعريفات السابقة اتفق الفقهاء على أن جوهر التزوير يكمن في تغيير الحقيقة بقصد الغش أو التضليل. فالتزوير هو فعل متعمد يقوم به الشخص لتغيير أصل المستند، مع علمه بأن هذا التغيير يخالف الحقيقة، ويهدف من خلاله إلى خداع الآخرين، كما يشير غارسون إلى أن وسائل التزوير قد تكون قانونية الشكل لكنها تستعمل لإيهام الغير. ويركز بلحاج العربي على أن القانون الجنائي يختار الأفعال الأكثر خطورة التي قد تلحق ضررا بالمصلحة العامة أو بمصلحة أفراد.

¹ سفيان بن صويلح، مكافحة التزوير واستعمال المزور في ظل القانون 24-02، مذكرة مكملة لمتطلبات نيل شهادة ماستر في قانون، كلية الحقوق، جامعة 08 ماي 1945، قالمة، الجزائر، 2025، ص 9.

² جمال نجيمي، جرائم التزوير في قانون العقوبات الجزائري، ب.د.ن طبعة، دار هومة، الجزائر، 2013، ص 270.

³ بلحاج العربي، أبحاث ومذكرات في قانون والفقه الإسلامي، ديوان المطبوعات الجامعية، بن عكنون، الجزائر، 1996، ص 465.

⁴ سرور أحمد فتحي، الوسيط في قانون العقوبات، القسم الخاص، طبعة 4، دار النهضة العربية، 1991، ص 402.

وبناء على ذلك يعرف التزوير بأنه فعل متعمد يتمثل في تغيير الحقيقة في مستند أو وثيقة بقصد الغش والتضليل، ويترتب عليه ضرر بالمصلحة العامة أو الخاصة، حيث يجمع بين الواقعة المادية والقصد الجنائي الأثر الضار على الثقة العامة.

ثانياً: تعريفه في التشريع.

يعدّ التزوير من الجرائم التي أولتها التشريعات الجنائية أهمية خاصة نظراً لخطورته على الثقة العامة والمعاملات القانونية، لذلك سعت مختلف التشريعات إلى وضع تعريف واضح يحدد مفهومه وأركانه، وعلى رأسها كلّ من المشرع الجزائري والمشرع الفرنسي.

عرفه المشرع الجزائري وفق ما ورد في الجريدة الرسمية في مادة الثالثة من قانون 02-24، على أنه كل تغيير للحقيقة عن طريق الغش في أحد المحررات أو الوثائق أو الدعائم المنصوص عليها في هذا القانون بأي وسيلة، بحيث يهدف إلى إلحاق ضرر من شأنه أن يترتب عليه إقرار حق أو صفة أو واقعة ترتب آثاراً قانونية ويشمل التقليد والتزييف.¹

وعليه من خلال تحليل نص المادة بشكل مبسط ومختصر نستنتج أن جريمة التزوير تقوم على مجموعة عناصر أساسية، تتمثل في تغيير الحقيقة باستعمال طرق احتيالية في محرر أو وثيقة أو دعامة قانونية، مع اشتراط حدوث ضرر أو احتمال وقوعه.

كما يستفاد منها ضرورة توافر القصد الجنائي واتجاه إرادة الجاني إلى تحقيق غاية محددة، وهي إقرار حق أو صفة أو واقعة ذات أثر قانوني، وقد وسع المشرع نطاق هذه الجريمة ليشمل صورتَي التقليد والتزييف.

أما المشرع الفرنسي عرفه في مادته 441 الفقرة 01 المعدلة في 1 جانفي 2000 بموجب مرسوم رقم 2000-916 على أنه كل تغيير احتيالي للحقيقة، من شأنه أن يسبب ضرراً ويتم ارتكابه بأي وسيلة كانت على محرر مكتوب أو أي دعامة أخرى للتعبير عن الفكر والتي يكون هدفها إثبات حق أو حقيقة ذات تبعات قانونية، يشكل تزويراً.

« Constitue un faux toute altération frauduleuse de la vérité, de nature à causer un préjudice et accomplie par quelque moyen que ce soit, dans un écrit ou tout support

¹ المادة الثالثة، قانون رقم 02-24، يتعلق بمكافحة التزوير واستعمال المزور، المؤرخ في 26 فيفري 2024، الجريدة الرسمية، عدد 15، 2025.

d'expression de la pensée qui a pour objet ou qui peut avoir pour effet d'établir la preuve d'un fait ayant des conséquences juridiques ».¹

ثالثا: عناصره الأساسية في المحررات الورقية.

يعد المحرر الورقي الدعامة المادية التقليدية التي تجسد التصرفات القانونية وهو الوعاء الذي يحمل الحقيقة التي يسبغ عليها القانون حمايته. ولكي يكتسب الورق صفة المحرر القانوني القابل للتزوير هناك مجموعة من العناصر الجوهرية التي تمنحه كيانه المادي والمعنوي.

تكمن أهمية دراسة هذه العناصر في كونها تمثل "المعيار المرجعي" الذي سيتم القياس عليه عند دراسة المحرر الإلكتروني حيث أن أي عبث بهذه العناصر يغير من مراكز يخل بالثقة العامة التي تضعها الدولة في الأوراق الرسمية والعرفية.

1- العناصر الذاتية (التوقيع).

يمثل التوقيع الركن المادي الأكثر أهمية في المحرر الورقي فهو الأداة القانونية التي تربط بين مضمون الورقة وإدارة صاحبها. وفي الفقه القانوني الجزائري لا تكتسب الورقة حجيتها إلا بالتوقيع الذي قد يتخذ عدة صور مادية مثل التوقيع الخطي أو البصمة أو الختم الشخصي.

أ- الوظيفة التعريفية: تعتبر الوظيفة التعريفية الركيزة الأساسية في المحرر الورقي حيث تهدف الى ربط المحرر بشخص معين بذاته وتتجلى هذه الوظيفة في:

- **تحديد الهوية:** التوقيع هو الوسيلة التي تسمح "بشخصنة"² المحرر بحيث يمكن من خلاله معرفة من هو الطرف الذي صدر عنه هذا التصرف القانوني.
- **نسبة المحرر لصاحبه:** لا يمكن الاحتجاج بأي وثيقة ورقية ضد أي شخص إلا إذا حملت توقيع (خطي بصمة أو ختم شخصي) وهو ما يمنح المحرر قوته في الإثبات.
- **الصلة المادية:** في المحرر الورقي تلتصق الوظيفة التعريفية بالدعامة المادية (الورقة) مباشرة مما يجعل أي تغيير في التوقيع تزويرا ماديا ظاهرا.

¹ Code pénal français dernière modification, 9 juillet 2025

<https://www.legifrance.gouv.fr/codes/article-ic/LEGIARTI000006418753>. ساعة 03:49

² أحسن بوسفيعة، الوجيز في القانون الجنائي الخاص (الجرائم ضد الثقة العامة)، دار هومة، الجزائر، 2022، ص145

ب- **الوظيفة التعبيرية:** وهي التي تعكس رضا الموقع على مضمون المحرر بوضع التوقيع يعلن الشخص عن موافقته النهائية على الالتزامات الواردة في الورقة وبذلك يتحول مجرد الورق الى سند قانوني يرتب مسؤولية.

2- العناصر الشكلية للبيانات المكملّة

بجانب التوقيع يستلزم المحرر الورقي وجود بيانات شكلية تمنحه كيانه الكامل وتساهم في حمايته من التزوير وتتمثل أساسا في:

- **الدمغة (l'entête) وأهميتها التعريفية:** تعرف الدمغة بأنها مجموعة الرموز الشعارات أو البيانات النصية المطبوعة التي تعلق صدر المحرر الورقي وتهدف الى بيان الجهة المصدرة له (سواء كانت سلطة عامة في المحررات العرفية)¹ وهي تمثل العنوان البصري للمحرر الذي يضيف عليه صفة الجدية وقرينة الصحة الظاهرية، مما يجعلها عنصرا جوهريا في تكوين الشكل المادي للمحرر الخاضع للحماية القانونية من التزوير.

- **بيانات المرسل والمرسل إليه:** تعتبر بيانات الأطراف (الأسماء، الصفات، والعناوين) من البيانات الجوهرية المكملّة للمحرر الورقي تعريفيا وإثباتيا حيث تلعب دورا مزدوجا.

3- تحديد نطاق المسؤولية القانونية.

من خلال ذكر اسم المرسل (مصدر المحرر) والمرسل إليه (المستفيد أو الموجه إليه الخطاب) يتم تحديد الأشخاص الملزمين قانونيا بمضمون المحرر، مما يسهل عملية إسناد المسؤولية القانونية وحصر أطراف النزاع في حالة حدوث تزوير أو إنكار للالتزام.²

■ **حماية المحرر من التزوير المعنوي:** تساهم دقة بيانات الأطراف في منع تغيير حقيقة التصرف القانوني المضمن في الورقة، ففي المحرر الورقي التقليدي، أي شطب تعديل، أو إضافة في أسماء الأطراف أو صفاتهم مثل تغيير صفة دائن الى مدين يعتبر تزويرا ماديا ملموسا يسهل كشفه بالعين المجردة أو الخبرة الفنية، وهو ما يحافظ على استقرار المعاملات.

¹أوبكر سلطان محمد الخضر، عفاف مصطفى حامد كروم، وصف البيانات الرقمية - دراسة تقويمية، المجلة العربية للمعلوماتية وأمن المعلومات، 2021، ص40.

²محمد صلاح، شادي حمادة، البيانات الرقمية في مصر دراسة قانونية تحليلية، مجلة الدراسات القانونية والاقتصادية، 2025، ص2380.

- **الختم Le Sceau / cachet:** يعتبر الختم عنصرا ماديا شكليا يدعم التوقيع ويمنحه قوة إضافية، خاصة في المحررات الرسمة وظيفته لتوثيق والتأكيد على الورقة عن جهة معينة (إدارة، شركة أو هيئة) حيث يحمل الختم غالبا شعارا أو اسما محفورا بطريقة يصعب تقليديا يدويا. علاقته بالتزوير في المحرر التقليدي، الختم هو "أداة مادية" تترك أثرا حبريا على ألياف الورق، وتزويره يتطلب جهدا في المحاكاة يسهل كشفه تقنيا، مما يجعله من الضمانات الشكلية الهامة لصحة المحرر.¹
- **تاريخ ومكان الصدور:** يعتبر ذكر التاريخ ومكان تحرير المحرر الورقي من البيانات الجوهرية، حيث يسمح التاريخ بتحديد الزمان الذي اكتملت فيه أركان التصرف القانوني، مما يساعد في كشف حالات التزوير الزمني (تزوير معنوي) من خلال تقديم أو تأخير زمن المحرر، بينما يحدد المكان الاختصاص القضائي والقانون الواجب التطبيق.²

المطلب الثاني: مفهوم التزوير في البيئة الرقمية.

مع توسع استخدام التقنيات الرقمية واعتماد الوسائط الإلكترونية في إبرام المعاملات وتبادل المعلومات، لم يعد التزوير محصورا في المحررات الورقية التقليدية، بل امتد ليشمل البيانات والمستندات ذات الطابع الرقمي. وقد أدى هذا التحول إلى ظهور تحديات قانونية جديدة، تتعلق أساسا بتحديد مفهوم التزوير الإلكتروني وبيان أشكاله المختلفة، نظرا للطبيعة غير المادية للبيانات وسهولة التلاعب بها.

أولا: تعريف التزوير الإلكتروني.

في العصر الرقمي الحديث، أصبحت التكنولوجيا جزءا لا يتجزأ من حياتنا اليومية، مما أدى إلى تسهيل العديد من المعاملات وتبسيط الوصول إلى المعلومات. ومع ذلك هذا التطور السريع صاحبه نوع جديد من الجرائم الإلكترونية، من بينها التزوير الإلكتروني.

يقصد بالتزوير الإلكتروني ذلك السلوك غير المشروع الذي يتمثل في التلاعب بالحقيقة أو تحريفها في البيانات أو الوثائق ذات الطبيعة الرقمية، بقصد تضليل أو الاحتيال من أجل تحقيق منافع غير مشروعة. ويتجسد هذا النوع من التزوير في عدة صور، من بينها اصطناع أو تقليد التوقيعات الرقمية،

¹ مهند فايز الدويكات ، حسين مجد الشبلي، صور الاحتيال والتزوير في البطاقات الائتمانية، جامعة نايف العربية للعلوم الأمنية، 2013، ص 89.

² حابس يوسف زيدات، مدى استيعاب النصوص التقليدية للسرقة الإلكترونية، دراسة مقارنة، 2019، ص 95.

والتدخل غير المشروع لتعديل محتوى المستندات الإلكترونية، فضلا عن إدخال تغييرات غير مصرح بها على البيانات المخزنة ضمن قواعد المعلومات.¹

يمكن تعريف التزوير الإلكتروني بأنه: التسلل إلى قواعد البيانات ضمن النظم المعلوماتية، سواء بوسائل قانونية أو غير قانونية، بقصد إجراء تعديلات على المعطيات، وذلك من خلال حذف بيانات قائمة أو إضافة بيانات لم تكن موجودة مسبقا.²

ويعرف أيضا: بأنه كل تغيير للحقيقة يتم بوسائل تقنية، ويترتب عليه التأثير في مخرجات الحاسوب، سواء تجسدت هذه المخرجات في مستندات ورقية مطبوعة أو في أشكال ورسومات رقمية.³ وفي تعريف مغاير عرّف بأنه أي استخدام لبرامج معالجة آلية أو برمجيات اختراق بهدف تعديل البيانات أو المعلومات بغرض الحصول على البيانات الأصلية أو التلاعب بها بنية استخدامها.⁴

من خلال التعريفات السابقة نستنتج أن التزوير الإلكتروني كل تغيير متعمد للحقيقة يتم باستخدام الوسائل والتقنيات المعلوماتية، من خلال التلاعب بالبيانات أو المعطيات أو الوثائق الرقمية، سواء بالإضافة أو الحذف، وذلك بقصد التضليل أو تحقيق مصلحة غير مشروعة، ويكون من شأنه إحداث ضرر مع إمكانية تجسده في مخرجات الحاسوب بمختلف أشكالها، سواء كانت مستندات مطبوعة أو محتوى رقميا.

ثانيا: صور التزوير في المعاملات الرقمية.

لم يعد التزوير مقتصرًا على شكله التقليدي، بل تطوّر ليواكب البيئة الرقمية فظهرت صور حديثة تستهدف المعاملات الإلكترونية بمختلف وسائلها. وفي هذا السياق، برزت أشكال جديدة من التزوير، لاسيما تزوير التوقيع الإلكتروني، وتزوير المحررات الإلكترونية، وكذا تزوير بطاقات الدفع، وهي صور تعكس مدى تعقّد هذا النوع من الجرائم وخطورته في العصر الرقمي.

¹ عبد الله بن سعود مجد السرائي، فاعلية الأساليب المستخدمة في إثبات جريمة التزوير الإلكتروني، الطبعة 1، دار جامعة نايف العربية للعلوم الأمنية، المملكة العربية السعودية، 2011، ص 54.

² الجبوري عمر عبد السلام حسين، جريمة التزوير الإلكتروني في التشريع الأردني، رسالة ماجستير، جامعة الشرق الأوسط، الأردن، 2017، ص 17.

³ عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت دراسة عملية في جرائم الحاسوب الآلي والإنترنت، طبعة 1، دار الكتب القانونية، القاهرة، مصر، 2005، ص 170.

⁴ حفصي عباس، جرائم التزوير الإلكتروني، أطروحة دكتوراه جامعة وهران، كلية الحقوق والعلوم السياسية، قسم الحقوق، الجزائر، 2015، ص 2.

1- تزوير التوقيع الإلكتروني.

عرفت المادة 02 من قانون 04-15، المؤرخ 11 ربيع الثاني 1436 الموافق ل أول فبراير سنة 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين على أنه: "بيانات في شكل إلكتروني مرفقة أو مرتبطة منطقيا ببيانات إلكترونية أخرى تستعمل كوسيلة توثيق".¹

من خلال هذا التعريف، يتبين أن المشرع الجزائري لم يحدد شكلا محددا للتوقيع الإلكتروني، بل اعتمد تعريفا واسعا يشمل مختلف الأشكال، أما في مادة 03 من نفس القانون فقد ركز على الوظيفة القانونية للتوقيع (التوثيق، تحديد الهوية، سلامة المحرر) وليس على شكله.

هذا استجابة للتطور التكنولوجي المتسارع والمستمر، سعى المشرع إلى مواكبة هذا التحول من خلال تكييف الإطار القانوني بما يتلاءم مع المستجدات التقنية، وذلك بهدف ضمان سلامة ونجاح المعاملات الإلكترونية، ولا سيما في ظل الانتشار الواسع للتجارة الإلكترونية، وكذا التعامل عبر البنوك والمصارف الإلكترونية.

يتخذ التوقيع الإلكتروني صورا متعددة، من بينها التوقيع الرقمي، والبيو متري، والتوقيع بالقلم الإلكتروني، وكذا التوقيع الممسوح ضوئيا، وغيرها من الوسائل التقنية الحديثة، وهو ما يعكس عدم تقيد المشرع بشكل محدد، واعتماده على معيار وظيفي يقوم على تحقيق التوثيق وتحديد هوية الموقع.

يتم تزوير التوقيع الإلكتروني بطرق مختلفة تماما، حيث يكون التوقيع المزور مطابقا تماما للتوقيع الأصلي. يتم ذلك من خلال اختراق نظام التوقيع الإلكتروني عبر التجسس الإلكتروني أو التلصص الرقمي، مما يتيح للمعتدي الحصول غير المشروع على بيانات التوقيع واستعمالها في توقيع الوثائق والمحركات. ورغم أن التوقيع المزور قد يبدو صحيحا من الناحية الشكلية عند مقارنته بالتوقيع الأصلي، إلا أنه في الحقيقة لا ينسب إلى صاحبه الشرعي، وإنما يكون صادرا عن شخص آخر تمكن من اختراق النظام والاستيلاء على بيانات التوقيع.²

¹ المادة 02 ، القانون رقم 04-15 ، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، المؤرخ في 01 فبراير 2015 ، الجريدة الرسمية، عدد 06، 2015.

² عبد الله بن سعود محمد السراي، المرجع السابق، ص 40.

2- تزوير المحررات الإلكترونية.

هو كل فعل يقوم على تغيير الحقيقة في محرر إلكتروني أو إنشاء محرر إلكتروني مزيف أو تعديل بيانات محرر قائم أو إدخال معلومات غير صحيحة أو حذف بيانات صحيحة، باستخدام وسائل تقنية أو معلوماتية، بقصد استعماله فيما بعد كحقيقة قانونية والإضرار بالغير أو تحقيق منفعة غير مشروعة، بما يمس حجية المحررات الإلكترونية.¹

يتضح مما سبق أن صور تزوير المحررات الإلكترونية تعددت تبعا للوسائل التقنية المستعملة في ارتكابها، حيث يمكن أن يتم ذلك عن طرق التعديل على محتوى محرر إلكتروني قائم من خلال الحذف أو الإضافة أو الاستبدال، أو عن طريق الاصطناع المتمثل في إنشاء محرر إلكتروني مزور بالكامل ونسبه إلى غير صاحبه. كما قد يتحقق التزوير من خلال انتحال الهوية الرقمية باستعمال بيانات أو صفة الغير إنشاء أو تعديل محررات الإلكترونية، أو عبر التلاعب بالأنظمة المعلوماتية بإدخال أو تغيير معطياتها بما يؤدي إلى إنتاج محررات غير مطابقة للحقيقة.

2- تزوير بطاقات الدفع.

تعددت تعريفات بطاقات الدفع الإلكترونية فهناك من عرفها بأنها البطاقة التي تصدر عن مؤسسة مالية لمصلحة علمية يعطيه الحق على ما يلزمه من سلع وخدمات مقابل الوفاء بقيمة السلع التي حصل عليها حامل هذه البطاقة والتزاما بالشروط المنققة عليها.²

أما المشرع الجزائري فقد عرف بطاقة الدفع في المادة 543 مكرر 23 من القانون التجاري المعدل والمتمم بموجب قانون رقم 05-02 التي تنص على ما يلي: "تعتبر بطاقة الدفع كل بطاقة صادرة عن البنوك والهيئات المالية المؤهلة قانونا وتسمح لصاحبها بسحب أو تحويل أموال.³

تتعرض بطاقات الدفع كغيرها من المحررات والمستندات إلى التزوير بمختلف أشكاله وطرقه، والذي يكون عن طريق التلاعب بالبيانات والمعلومات التي تمس المادة المكونة لبطاقة الدفع، حيث يتم

¹ عبد الله بلقاسم، الطبيعة الخاصة لجريمة التزوير في المحررات الإلكترونية، مجلة الدراسات القانونية المقارنة، جامعة التكوين متواصل مركز تيزي وزو، المجلد 06، العدد 02، 2020/12/27، ص 981.

² نوال حاج مخناش، التعاون الدولي ومدى فعاليته في مكافحة جرائم تزوير بطاقات الدفع الإلكترونية، مجلة العلوم القانونية والسياسية، جامعة يحي فارس المدينة، المجلد 10، العدد 01، 28 جانفي 2019، ص 1120.

³ المادة 543 مكرر 23، قانون رقم 05-02، المتضمن القانون التجاري، المؤرخ في 6 فبراير 2005، المعدل والمتمم لأمر رقم 59-75 مؤرخ في 26 سبتمبر 1975، الجريدة الرسمية، العدد 11، 2005.

اصطناع بطاقة كاملة ثم يتم تقليد الرسوم الخاصة على هيكل البطاقة، وتغليفها وتلصيق الشريط المغنط وشريط التوقيع ثم القيام بالطباعة النافرة وتشغيلها عن طريق إشباعها بالمعلومات التي حصل عليها المزور من البطاقة الصحيحة، بعد ذلك يتم القيام بنسخ نسخ عديدة من البطاقة المزورة ليتم تسويقها بهدف استخدامها استخدام غير مشروع¹.

ثالثاً: الفروق الجوهرية بين التزوير التقليدي والتزوير الإلكتروني.

سبقت الإشارة أن التزوير هو تغيير حقيقة محرر، بإحدى الطرق المقررة قانوناً تغييراً من شأنه إحداث ضرر، وبنية استعماله كمحرر صحيح، هذا بالنسبة للتزوير التقليدي، أما التزوير الإلكتروني فه كل تغيير في حقيقة مستند معلوماتي يهدف الجاني من وراءه لاستخدامه والاستفادة منه.

بمعنى يتفق التزوير الإلكتروني مع التزوير التقليدي من حيث الغاية الإجرامية، والمتمثلة في تغيير الحقيقة بقصد تحقيق مصلحة غير مشروعة، وكذلك من حيث الأثر الضار الذي يلحق بالغير. غير أنه يختلف عنه من حيث الوسائل، إذ تعتمد على تقنيات حديثة وأدوات معلوماتية، ويرد على المحررات ووثائق ذات طابع إلكتروني يتم إنشاؤه أو معالجته بواسطة الحاسب الآلي أو غيره من الأجهزة الإلكترونية².

يشارك التزوير التقليدي والإلكتروني في نفس الأركان القانونية (المادي والمعنوي) بحيث يقوم الركن المادي على السلوك الإجرامي المتمثل في تغيير الحقيقة، وهو ما يؤدي إلى إلحاق ضرر بالغير، بينما الركن المعنوي يتطلب توافر القصد الجنائي العام (العلم والإرادة) إلى جانب القصد الجنائي الخاص، المتمثل في نية استعمال المحرر.

على الرغم من التشابه الكبير بين التزوير الإلكتروني والتزوير التقليدي، إلا أنه يمكن تحديد مجموعة من الفروق الجوهرية التي تميّز بينهما:

❖ التزوير التقليدي يقع على محرر مادي كالوثائق الورقية، بينما التزوير الإلكتروني يقع على محرر رقمي أو مستند معلوماتي.

¹ رياض فتح الله بصله، جرائم بطاقة الائتمان، دار الشرق، بيروت، لبنان، 1995، ص 108.

² رياء بنت عبد الرحمن الثنيان، القصد الجنائي في جريمة التزوير المعلوماتية دراسة مقارنة، مجلة كلية الشريعة والقانون، المجلد 29، العدد 9، ديسمبر 2024، جامعة القصيم، المملكة العربية السعودية، ص 4205.

❖ التزوير التقليدي غالبا ما يترك آثارا يمكن ملاحظتها، أما التزوير الإلكتروني فيصعب اكتشافه لعدم ترك آثارا مادية واضحة.

❖ التزوير التقليدي محدود النطاق، أما الإلكتروني فيمكن أن ينتشر بسرعة وعلى نطاق واسع عبر الأنظمة والشبكات.

إن جريمة التزوير الإلكتروني تتصف بخاصية تفرد شخصية الجاني فهذا الأخير يتمتع بحرفية عالية في مجال الحاسب الآلي وثقافة إلكترونية كبيرة حتى يتم تزوير البيانات والمعلومات بدقة كبيرة، في حين أن مرتكب جريمة التزوير التقليدي وبالرغم من كونه جاني مثقفا، إلا أنه لا يحتاج إلى مثل هذه الثقافة والقدرات والمهارات.¹

ويستنتج مما تم بيانه لأوجه الشبه والاختلاف بين التزوير التقليدي والإلكتروني أن الاختلاف بينهما هو اختلاف شكلي، يتعلق بالتقنية الحديثة وما أفرزته من صعوبة في إثبات الجرائم المرتكبة في وسطها، ومن مجرمين جدد لم تعهدهم البشرية من قبل، وذلك الاختلاف لا يمس الأركان الرئيسية لجريمتين.

المطلب الثالث: خصائص المعاملات الرقمية والوثائق الإلكترونية وأثرها على التجريم.

إن الانتقال من بيئة المحررات الورقية التقليدية الى بيئة المعاملات الرقمية لم يكن مجرد تغيير في وسيلة الكتابة فحسب، بل هو تحول جذري في طبيعة المحرر ذاته. فالمحرر الإلكتروني يتمتع بخصائص ذاتية وفنية تتفرد بها الوسائط الرقمية، وهي خصائص تجعل منه كيانا لا ماديا عصيا على القواعد التقليدية للتزوير التي وضعت أساسا لحماية الورق.

ومن هذا المنطق، تبرز أهمية دراسة هذه الخصائص، ليس فقط من الناحية التقنية بل من زاوية أثرها المباشر على السياسة الجنائية وكيفية تجريم الاعتداء على هذه المحررات، فعدم وجود أثر مادي ملموس وسهولة محو آثار الجريمة الرقمية فرضا تحديات جديدة أمام القضاء والتشريع، وهو ما سنحاول تسليط الضوء عليه من خلال تبيان الطبيعة غير المادية للبيانات، والطابع التقني للوسائط، وصولا إلى إشكالية الحجية القانونية للوثيقة الإلكترونية.

¹ الهام بن خليفة، الحماية الجنائية للمحررات الإلكترونية من التزوير، أطروحة الدكتوراه، كلية الحقوق والعلوم السياسية، جامعة باتنة، الجزائر، 2016، ص 56.

أولاً: الطبيعة غير المادية للبيانات.

تتمثل أبرز خاصية تميز المعاملات الرقمية والوثائق الإلكترونية في كونها قائمة على بيانات غير مادية أي أنها لا تتخذ شكلاً مادياً يمكن رؤيته أو لمسها بالمعنى التقليدي. فالبيانات الإلكترونية هي، مجرد نبضات إلكترونية وإشارات رقمية" يتم تخزينها على وسائط مغناطيسية أو ضوئية، ولا يمكن إدراكها بشكل مباشر إلا بعد تحويلها إلى صورة مقروءة عبر أجهزة إلكترونية محددة.

إن هذه الطبيعة غير المادية للبيانات تترتب عليها عدة نتائج جوهرية من حيث التجريم، أولها صعوبة تطبيق مفهوم المحل المادي للجريمة. ففي التزوير التقليدي، كان المحل هو المحرر الورقي (المادة)، بينما في التزوير الإلكتروني، ينصب السلوك الإجرامي على بيانات غير ملموسة، مما يثير تساؤلاً حول إمكانية اعتبار هذه البيانات شيئاً يصلح لأن يكون محلاً لجريمة التزوير، ويذهب جانب من الفقه إلى أن الطبيعة غير المادية لا تمنح البيانات صفة الشيء، غير أن الرأي الراجح يؤكد أنها أصبحت تمثل قيمة اقتصادية وقانونية، وبالتالي تصلح محلاً للاعتداء.¹

فكما أن الكهرباء والغاز ليستا مادتين بالمعنى الحرفي، إلا أن القانون يعترف بهما كمواضع يقع عليها الاعتداء، فالأمر نفسه ينطبق على البيانات الإلكترونية، بل أن قيمتها تفوق في كثير من الأحيان قيمة الأشياء المادية.

ثاني هذه النتائج: إمكانية إعادة إنتاج البيانات وتعدد نسخها دون فقدان الأصل، فالوثيقة الورقية التقليدية، إذ تم تزويرها، فإن الأصل يبقى وحيداً. ويمكن كشف التزوير من خلال فحص الورقة أو الحبر أو التوقيع، أما الوثيقة الإلكترونية، فيمكن نسخها آلاف المرات، ويكون كل نسخة مطابقة تماماً للأصل، بل يصبح من المستحيل تقريباً التمييز بين النسخة والأصل. هذه الخاصية تجعل من السهل إخفاء أثر التزوير، حيث يمكن للمرور أن يتلف النسخ الأصلية أو يعدلها، ويبقى على النسخ المزورة التي لا يمكن تمييزها، مما يعقد مهمة الإثبات الجنائي.²

ارتباط الوجود القانوني للبيانات بوسيط تقني فالبيانات غير المادية لا يمكن أن توجد في الفراغ، بل تحتاج إلى وسيط مادي (شريحة ذاكرة، خادم سحابي) لتخزينها، ولكن هذا الوسيط ليس هو البيانات

¹ شيماء علوان حسن، الصعوبات القانونية في مكافحة الجريمة الإلكترونية، مجلة العلوم الإنسانية الطبيعية، 2024، ص45.

² حابس يوسف زيدات، مدى استيعاب النصوص التقليدية للسرقة الإلكترونية دراسة مقارنة، مجلة مركز حكم القانون ومكافحة الفساد، المجلد 2، العدد 9، سنة 2019، ص34.

ذاتها. وهنا تبرز إشكالية: هل الاعتداء على الوسيط المادي يعتبر اعتداءات على البيانات؟ والعكس صحيح، فهل يمكن تزوير البيانات دون المساس بالوسيط؟ في الواقع. هذا الانفصال بين الدعم المادي والمضمون غير أن المادي يخلق منطقة رمادية في القانون التقليدي الذي اعتاد التعامل مع الشيء كوحدة مادية.¹

النتيجة الرابعة والأخيرة الصعوبة في تحديد مكان وقوع الجريمة. ففي البيئة الرقمية، يمكن أن تكون البيانات المخزنة على خادم في الدولة، ويتم الوصول إليها من دولة ثانية، والتلاعب بها عبر دولة ثالثة. والطبيعة غير المادية تجعل مفهوم "مكان ارتكاب الجريمة" فضفاضا وغير محدد، مما يثير إشكاليات تتعلق بالاختصاص القضائي الدولي، خاصة في جرائم التزوير التي تطل وثائق إلكترونية ذات طابع عبر الحدود.²

ثانيا: الطابع التقني للوسائط الرقمية.

لا تقتصر خصوصية البيئة الرقمية على كون بياناتها غير مادية، بل تمتد الى الطابع التقني الشديد للوسائط التي تعمل عليها هذه البيانات. فالوثيقة الإلكترونية لا توجد إلا في إطار نظام تقني معقد يتكون من أجهزة وبرمجيات وشبكات اتصال، وهذه الوسائط هي التي تمنحها الوجود والوظيفة. هذا الطابع التقني له انعكاسات عميقة على جريمة التزوير من حيث إمكانية ارتكابها، ومن حيث طرق اكتشافها وإثباتها.

اعتماد صحة الوثيقة الإلكترونية على سلامة النظام التقني بأكمله. ففي المحرر الورقي، يمكن التحقق من صحة التوقيع من خلال مقارنته بتوقيع سابق، أو فحص الورقة بالعين المجردة أو بالمهجر، ما في الوثيقة الإلكترونية، فصحة التوقيع الإلكتروني (مثلا) تعتمد على مفاتيح التشفير والشهادات الرقمية، وسلامة الخوارزميات المستخدمة. أي خلل في أحد هذه العناصر -سواء كان ناتجا عن عطل تقني أو عن اختراق معتمد- يمكن أن يؤدي الى اعتبار الوثيقة مزورة حتى لو كان السلوك البشري سليما

¹ علي صاحب تقني، حماية المستفيد من المخاطر الناشئة عن الدفع الإلكتروني دراسة مقارنة، مجلة دجلة للعلوم 2025، ص 12.

² هشام محمد مهدي صالح، محمد هاني فرحات، الصور المستحدثة للجريمة الإلكترونية، مجلة العلوم الإنسانية والطبيعية، 2026ص22.

في الظاهر. وهذا يخلق نوعاً من "التعبية التقنية" التي لم تكن موجودة في القانون التقليدي، حيث كان الإنسان هو محور العملية.¹

إمكانية التلاعب بالبيانات على مستويات متعددة وبطرق غير مرئية، فالتزوير الورقي يتطلب أما تغيير في الحبر أو مسح كلمة وكتابة أخرى، أو إضافة توقيع مزور، هذه التغييرات تترك: وجوداً مادياً أثراً مادية يمكن، من حيث المبدأ، اكتشافها بالخبرة الفنية، أما التزوير الإلكتروني، فيمكن أن يتم على مستوى التطبيق (مثل تعديل حقل في قاعدة بيانات)، أو حتى على مستوى نظام التشغيل (مثل تغيير إعدادات الوقت والتاريخ لإظهار أن وثيقة قد تم إنشاؤها في وقت سابق)، أو حتى على مستوى العتاد الصلب مثل اختراق الذاكرة، والأخطر من ذلك أن بعض هذه التغييرات لا تترك أي أثر ثابتة.

مادي يمكن ملاحظته، ولا يمكن اكتشافها إلا من خلال برامج فحص متخصصة وتحليل للبيانات الوصفية، وهذا يضع عبئاً كبيراً على جهات التحقيق التي تحتاج إلى خبراء في علوم الحاسوب Digital Forensic وليس في الخطوط والتوقيع.²

الدور المحوري للخبرة التقنية في الإثبات. في قضايا التزوير التقليدي، يكفي أحياناً الاستعانة بخبير خطوط أو خبير الوثائق. أما في قضايا التزوير الإلكتروني، فغالبا ما يحتاج القضاء إلى فريق متعدد التخصصات يضم مهندسي برمجيات، خبراء أمن معلومات محليي بيانات. وهذا ما يرفع من تكلفة التقاضي ويطيل أمد الإجراءات، كما يطرح إشكالية قبول الخبرة التقنية كدليل قضائي، خاصة عندما تكون المنهجيات المتبعة غير موحدة أو معترف بها قانونياً بعد.³

ثالثاً: إشكالية الحجية القانونية للوثيقة الإلكترونية.

تعد إشكالية الحجية القانونية للوثيقة الإلكترونية من أخطر الإشكاليات التي تواجه المشرع والقضاء على حد سواء. فالحجية في القانون التقليدي كانت مرتبطة بوجود محرر ورقي يمكن التحقق من مصدره وسلامته عبر التوقيع اليدوي والختم. لكن في البيئة الرقمية التزوير يفترض وجود وثيقة أصلية ذات حجية

¹ محمد توفيق بابا، الإثبات الجنائي بالوسائل العلمية الحديثة، مجلة العلوم الإنسانية والطبيعية، 2025، ص 18-20.

² M, Tampubalan, "Digital face forgery and the role of digital forensic, international", journal for the semiotics of law, 2024, p 5-7.

³ S. Bourouis et al., « Recent advances in digital multimedia tampering detection for forensics analysis, symmetry 2020, p3.

فإذا كانت الوثيقة الإلكترونية فاقدة للحجية أصلاً، فإن أي تغيير فيها قد لا يشكل "تزويراً" بالمعنى القانوني الدقيق¹.

مبدأ حرية مقابل الشكلية التقليدية. في القانون المدني والإداري، كانت القاعدة أن الإثبات بالكتابة هو أصل عام، خاصة بالنسبة للتصرفات القانونية التي تتجاوز قيمة معينة. وكانت الكتابة تعني بالضرورة الورق والتوقيع اليدوي. مع ظهور الوثيقة الإلكترونية، بدأ التشريعات تتجه نحو الاعتراف لها بحجية مماثلة، بشرط أن تتوفر فيها ضمانات تقنية معينة، وفي مقدمتها التوقيع الإلكتروني الموثوق غير أن هذا التحول لم يكن سلساً، إذ لا يزال هناك تردد في قبول الوثائق الإلكترونية كدليل كامل، خاصة في غياب التوقيع الإلكتروني أو في حال وجود شك حول سلامة نظام التقني².

معضلة ضمان سلامة الوثيقة واستمراريتها. الحجية القانونية للمحرر التقليدي تستند إلى افتراض أن المحرر لم يتم تغييره بعد توقيعه وأنه يمكن حفظه لسنوات طويلة دون تغيير. أما الوثيقة الإلكترونية، فسلامتها تعتمد على آليات تقنية معقدة مثل الذي يعتمد على التشفير غير المتماثل، والذي يضمن أن أي تغيير حتى في حرف واحد سيؤدي إلى إبطال التوقيع. غير أن هذه الآليات ليست عصية على الاختراق، كما أن التقادم التقني قد يجعل من المستحيل بعد سنوات فك تشفير وثيقة موقعة بنظام قديم.

التزوير كإخلال بالثقة الرقمية. إذا كانت الحجية القانونية للوثيقة الإلكترونية قائمة على الثقة في الأنظمة التقنية (البنية التحتية للمفاتيح العمومية، الشهادات الرقمية، جهات التصديق) فإن جريمة التزوير في هذا السياق لا تقتصر على التغيير المادي للبيانات، بل تتجاوز ذلك أضعاف هذه الثقة ذاتها.

فالمزور الذي يخترق نظام توقيع إلكتروني أو ينشئ شهادة رقمية مزورة لا يزور وثيقة معينة فحسب، بل يهدد سلامة النظام البيئي الرقمي بأكمله. وهذا يقتضي من المشرع أن يجرم ليس فقط فعل تزوير الوثيقة الإلكترونية، بل أيضاً الأفعال التحضيرية والتقنية التي تهدف إلى الإخلال بالآليات التوثيق الرقمي، مثل صنع برامج ضارة لتزوير التوقيعات أو انتحال هوية جهات التصديق³.

¹ Singh. R. Kamar, "image forgery detection: comprehensive review of digital forensics approaches", journal of computational social science, 2024, p15.

² IO Krystka, «Digitization of the criminal process: yesterday, today, tomorrow», publishing House Baltija publishing, 2021, p34.

³ G. Varbanova, «Electronic Documents as Electronic Evidence», International journal of law changing world, 2025.

المبحث الثاني: أركان جريمة التزوير الإلكتروني وأثرها في قيام المسؤولية القانونية

بعد التطرق في المبحث الأول إلى مفهوم التزوير الإلكتروني وتمييزه عن التزوير التقليدي، يقتضي استكمال الدراسة للانتقال بيان الأساس القانوني لقيام هذه الجريمة. إذ لا يكفي تحديد الإطار المفاهيمي لها، بل يتعين الوقوف على الأركان التي تقوم عليها جريمة التزوير الإلكتروني باعتبارها الأساس الذي تبنى عليه المسؤولية القانونية.

وعليه، يستلزم الأمر تحليل أركان جريمة التزوير الإلكتروني، سواء الركن المادي بما يتضمنه من سلوك إجرامي ونتيجة وعلاقة سببية، أو الركن المعنوي القائم على القصد الجنائي.

المطلب الأول: الركن المادي للتزوير الإلكتروني.

يعدّ الركن المادي لجريمة التزوير الإلكتروني المظهر الخارجي لها، من خلال الأفعال التي تؤدي إلى تغيير الحقيقة في المحررات الرقمية باستعمال وسائل تقنية. ويقتضي ذلك بيان السلوك الإجرامي والنتيجة المترتبة عنه، إضافة إلى العلاقة السببية بينهما.

أولاً: تغيير الحقيقة في محرر الإلكتروني.

يتمثل الركن المادي لجريمة التزوير الإلكتروني في تغيير الحقيقة في محرر الإلكتروني، وذلك عن طريق إدخال تعديل أو تحريف على البيانات أو المعلومات المثبتة في دعامة إلكترونية، بما يؤدي إلى إحلال واقعة غير صحيحة محل واقعة صحيحة. ويعدّ هذا التغيير جوهر جريمة التزوير، إذ لا يتصور قيامها دون تحريف الحقيقة بإبدالها بما يخالفها، فلا تقوم الجريمة في حال عدم تحقق هذا التغيير، ولو كان الفاعل سيء النية.¹

ويتم هذا التغيير باستعمال وسائل تقنية حديثة، كبرمجيات المعالجة الآلية أو عبر الدخول غير المشروع إلى الأنظمة المعلوماتية، ويتميز بطابعه الخفي، إذ قد يقع دون أن يترك آثاراً مادية ظاهرة، مما يزيد من خطورته ويصعب اكتشافه مقارنة بالتزوير التقليدي. كما لا يشترط أن يكون التغيير شاملاً لكافة

¹ عبد الرحمن عبد الله حميد آل علي، جرائم التزوير المعلوماتي، الطبعة 1، دار حائل للطباعة والنشر، سوريا، 2009، ص 96.

عناصر المحرر، بل يكفي أن ينصب على جزء منه كان من شأنه التأثير على مضمونه أو دلالاته القانونية.

ويشترط لقيام الجريمة تحقق الضرر، والذي يتمثل في المساس بالثقة المفترضة في المحررات، خاصة إذا تعلق الأمر بمحرر إلكتروني رسمي، أو في الإضرار بحقوق الأفراد ومراكزهم القانونية في حالة المحررات العرفية. غير أنه لا يشترط تحقق ضرر فعلي، بل يكفي أن يكون من شأنه التغيير احتمال إحداثه. كما تقوم الجريمة بمجرد تحقق تغيير الحقيقة، دون اشتراط استعمال المحرر المزور.¹ ويقصد بالحقيقة في هذا السياق الحقيقة القانونية التي تعبر عما اتجهت إليه إرادة من نسب إليه المحرر، وليس الحقيقة الواقعة المطلقة، لذلك يكفي أن يكون التغيير نسبيا أو جزئيا متى كان من شأنه التأثير على القيمة القانونية للمحرر. أما إذا بلغ التغيير حدا يؤدي إلى محو البيانات كليا أو جعل المحرر غير صالح للاستعمال أو غير قابل للاحتجاج به، فإن الفعل يخرج من نطاق التزوير ويدخل في نطاق جريمة الإلتلاف.²

من خلال ما سبق، يتضح أن تغيير الحقيقة في المحرر الإلكتروني يشكل الركيزة الأساسية لقيام جريمة التزوير الإلكتروني، لما ينطوي عليه من مساس بمصداقية المحررات وبالثقة المفترضة في المعاملات الرقمية. وقد أدرك المشرع الجزائري خطورة هذا النوع من الجرائم، خاصة في ظل التطور التكنولوجي المتسارع، فسعى إلى تكريس حماية قانونية فعالة من خلال القانون رقم 24-02 المتعلق بمكافحة التزوير واستعمال المزور، الذي وسع نطاق التجريم ليشمل مختلف صور التزوير، بما فيها التزوير في المحررات الإلكترونية، مع تشديد العقوبات لمواجهة هذه الأفعال وضمان استقرار المعاملات الإلكترونية وتعزيز الثقة فيها.

¹ عبد الرحمن عبد حميد آل علي، مرجع سابق، ص 96.

² أحمد خليفة الملط، الجرائم المعلوماتية، الطبعة 2، دار الفكر الجامعي، الإسكندرية، مصر، 2006، ص 467.

ثانيا: وسائل التزوير الإلكتروني.

1- التعديل.

تغيير محتوى البيانات الأصلية، وتغيير التواريخ، أو الأرقام، أو الأسماء الواردة في المحرر الإلكتروني. يجب أن يكون هذا التغيير قد تم بوسائل إلكترونية أو رقمية، أن يكون من شأنه إحداث ضرر محتمل أو فعلي. كما أن استخدام المحرر المزيف أو البيانات المزورة يعد جزءا لا يتجزأ من الركن المادي للجريمة، حيث يكتمل بها السلوك الإجرامي.¹

2- الاصطناع.

يقصد بالاصطناع خلق محرر بأكمله ونسبه إلى غير محرره، ويتحقق الاصطناع بخلق محرر لم يكن له وجودا من قبل ونسبه زورا إلى غير محرره بشرط أن يكون المحرر المصطنع له مظهر قانوني، أي متضمنا لواقعة تترتب عليها آثار قانونية يحتج به في الإثبات. وبهذه الطريقة يقوم الجاني بخلق وثيقة معلوماتية أو محرر إلكتروني لم يكن موجودا بمحتوى غير صحيح، وكثيرا ما يقتزن التزوير بالاصطناع بطريقة وضع إمضاء أو ختم مزور، والغالب أن يحدث الاصطناع في المحررات الرسمية، كمن يصطنع صورة حكم وينسب صدوره لمحكمة معينة.² للاصطناع صورتان إحداها أن يخلق المتهم محررا لم يكن موجودا من قبل، أما الصورة الثانية فهي أن يخلق محررا آخر وذلك بعد التعديل أو بدون تعديل.³

3- الحذف.

ويقصد به إزالة أو محو جزء من البيانات أو المعلومات الموجودة في محرر إلكتروني بطريقة غير قانونية، بهدف تغيير الحقيقة وإحداث أثر قانوني مغاير للواقع. ويشمل ذلك حذف أرقام أو فقرات أو معطيات رقمية من عقد أو سجلات إلكترونية أو قواعد بيانات. ويكتسي هذا الفعل طابعا جرميا متى

¹ المسؤولية الجنائية عن الجرائم التزوير الإلكتروني، دون طبعة، 1 سبتمبر 2025، د. ب. ن، تم إطلاع على الموقع بتاريخ 20 أبريل 2026 الساعة 02:30 <https://www.menafayq.com/criminal-responsibility-electronic-forgery-02:30> crimes.

² عبد الله بن سعود محمد السيراني، مرجع سابق، ص 56.

³ عبد الفتاح بيومي حجازي، التزوير في جرائم الكمبيوتر والأنترنت، مرجع سابق، ص 266.

ترتب عنه إضرار بالغير أو تغيير في مركز قانوني، لأنه يمس بمصادقية المحرر الإلكتروني ويؤثر على حجته القانونية.¹

ثالثا: النتيجة الإجرامية وعلاقة السببية.

تتمثل النتيجة في جريمة التزوير الإلكتروني في الإضرار بسلامة ومصادقية المعطيات ذات المعالجة الآلية، وما يترتب عن ذلك من مساس بالثقة العامة أو بحقوق الغير، سواء كان الضرر ماديا كخسارة مالية أو معنويا كالمساس بالسمعة. وقد أخذ المشرع الجزائري بهذا المفهوم من خلال النصوص المواد المادة 394 مكرر وما يليها من قانون العقوبات، حيث جرم أفعال التعديل والاصطناع والحذف للمعطيات متى كان من شأنها إحداث ضرر، دون اشتراط تحققه فعليا.

أما العلاقة السببية، فتقوم على وجود رابطة مباشرة بين السلوك الإجرامي والنتيجة، بحيث يكون فعل التزوير الإلكتروني (كتغير البيانات أو إدخال معطيات مزورة أو حذفها) هو السبب في إحداث الضرر أو تعريض المصلحة المحمية للخطر. ويشترط لإثبات هذه العلاقة أن تكون النتيجة مترتبة منطقيا ومباشرة على فعل الجاني، بحيث لولا الفعل لما تحققت، ويقع على عاتق القضاء التحقق من هذه العلاقة اعتمادا على الوسائل التقنية والأدلة الرقمية لإسناد المسؤولية الجزائية.²

المطلب الثاني: الركن المعنوي.

لا يكفي لقيام جريمة التزوير الإلكتروني توافر الركن المادي فقط، بل يجب أن يقترن هذا الفعل بإرادة جنائية واعية، تتمثل في اتجاه نية الجاني إلى ارتكاب السلوك المجرم مع علمه بعدم مشروعيته. فالركن المعنوي يعدّ جوهر المسؤولية الجزائية، إذ يميز بين الفعل العمدى والخطأ غير العمدى. وفي إطار التزوير الإلكتروني، يتخذ القصد الجنائي صورا خاصة تفرضها طبيعة البيئة الرقمية، حيث يشترط علم الجاني بتغيير الحقيقة في محرر الإلكتروني، واتجاه إرادته إلى استعماله بما قد يسبب ضررا للغير. وعليه سيتم التطرق في هذا المطلب إلى عناصر القصد الجنائي من خلال بيان العلم بتغيير الحقيقة، ثم نية استعمال محرر مزور، وأخيرا قصد الإضرار بالغير.

¹ حفصي عباس، جرائم التزوير الإلكتروني، أطروحة مقدمة لنيل شهادة الدكتوراه، كلية العلوم الإنسانية والعلوم السياسية، جامعة وهران، الجزائر، 2014، ص 25.

² المرجع نفسه، ص 26.

أولاً: العلم بتغيير الحقيقة.

يعدّ العلم بتغيير الحقيقة عنصراً جوهرياً في الركن المعنوي لجريمة التزوير الإلكتروني، حيث يقتضي أن يكون الجاني مدركاً بأن فعله ينصب على تحريف الحقيقة في محرر إلكتروني أو معطيات الإلكترونية أو بيانات رقمية، سواء عن طريق التعديل أو الاصطناع أو الحذف. لا يكفي مجرد الخطأ غير المقصود لإثبات هذا الركن، بل يجب أن تتجه إرادة الجاني إلى تحقيق التزوير.

يتطلب هذا الركن أن يكون الجاني يعلم أن فعله سيؤدي إلى إحداث ضرر أو يهدف إلى تحقيق منفعة غير مشروعة. ويشمل القصد الجنائي أيضاً علم الجاني بأن المحرر أو البيانات ستستخدم في إثبات أمر مخالف للحقيقة، إثبات القصد الجنائي قد يكون صعباً ويتطلب جمع أدلة قوية حول نية المتهم وقت ارتكاب الجريمة.¹

ثانياً: نية استعمال المحرر المزور.

لا يكاد ينعقد الركن المعنوي في جريمة تزوير المحررات الرقمية بمجرد توفر القصد العام (العلم والإرادة)، بل استلزم الفقه والقضاء ضرورة اقترانه بقصد جنائي خاص يتمثل في "نية الاستعمال". وتعتبر هذه النية هي "المعيار الجوهرية" الذي يخرج فعل العبث بالبيانات من دائرة الخطأ التقني إلى دائرة الجريمة العمدية الموجهة ضد الثقة العامة الرقمية.

1- الطبيعة القانونية لنية استعمال في المعاملات الرقمية.

تعد نية الاستعمال عنصراً نفسياً باطنياً يرافق الفعل المادي للتزوير، وهي التي تضفي على فعل تغيير الحقيقة صبغته الإجرامية، فالمحرر الرقمي لا يشكل خطراً على "الثقة العامة" إلا إذا كانت هناك إرادة لإقحامه في التداول القانوني.² في الفقه يشترط ضرورة معاصرة هذه النية للفعل المادي، أي تتوفر لحظة التعديل أو الاصطناع الرقمي، فإذا قام الشخص بتعديل بيانات مستند إلكتروني بدافع الفضول أو التجربة الفنية دون نية استخدامه كوسيلة إثبات، فإن الركن المعنوي للجريمة يظل ناقضاً، مما قد يخرج الفعل من دائرة التزوير إلى نطاق جرائم معلوماتية أخرى أقل جسامة.³

¹ نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة 3، دار الثقافة للنشر والتوزيع، الأردن، 2010، ص 147.

² خالد ممدوح إبراهيم، التزوير في المحررات الإلكترونية، دار الفكر الجامعي، الإسكندرية، مصر، 2008، ص 115.

³ جميل عبد الباقي الصغير، جرائم تزوير المستندات المكتوبة بالحاسب الآلي، دار النهضة العربية، القاهرة، مصر، 2001، ص 48.

2- استقلالية نية الاستعمال عن الاستعمال الفعلي للمحرر.

من الضوابط الجوهرية في المسؤولية عن التزوير الرقمي أن جريمة التزوير هي جريمة شكلية أو جريمة خطر تكتمل أركانها بمجرد توفر نية الاستعمال دون اشتراط وقوع الاستعمال المادي فعليا.¹ فإذا قام الجاني بتزوير توقيع إلكتروني بنية استخدامه في إبرام عقد، فإن المسؤولية الجزائية تترتب في حقه بمجرد انتهاء فعل التزوير كفعل اصطناع مقرون بنية، وبين جريمة استعمال المزور التي تبدأ عند لحظة تقديم المحرر فعليا للاحتجاج به، وهي جريمة مستقلة قد تقع من شخص آخر غير مزور.²

3- إشكاليات إثبات النية في البيئة الرقمية.

تثير عملية إثبات نية الاستعمال في جرائم التزوير المعلوماتي إشكالات قانونية وتقنية معقدة، تنبع أساسا من الطبيعة " اللامادية" للمحررات الإلكترونية وسهولة طمس معالم الجريمة فيها مقارنة بالمحررات التقليدية.³ تتمثل هذه الإشكالات في "غموض الحدود بين العبث الفني والقصد الجرمي" ففي البيئة الرقمية قد يقوم المستخدم بتعديل بيانات أو اصطناع محررات بدافع التجربة التقنية أو " الهواية " البرمجية دون نية الاحتجاج بالمحرر، مما يضع جهات التحقيق أمام معضلة التمييز بين الخطأ التقني وبين الإرادة الآثمة الموجهة للإضرار بالغير.⁴

علاوة على ذلك تبرز إشكالية تلاشي الدليل المعنوي بفعل تقنيات التشفير المتقدمة وبرمجيات محو، التي تتيح للجاني التخلص من "قرائن النية" (مثل مسودات) (Wi Ping Software الآثار الرقمية الإرسال أو سجلات التصفح) بضغطة زر واحدة، مما يجعل استخلاص القصد الخاص من "المظاهر الخارجية للسلوك" أمرا في غاية الصعوبة.⁵ كما أن الاعتماد الكلي على الخبرة المعلوماتية في الإثبات يطرح تساؤلا حول مدى كفاية الدليل الفني وحده للاستدلال على حالة باطنية نفسية، خاصة وإن الأنظمة

¹ نورة مرابط، القصد الجنائي في جريمة التزوير المعلوماتي، مجلة الدراسات الحقوقية، العدد 02، جامعة تيبازة، الجزائر، 2019، ص242.

² الشتيان رياء، جريمة التزوير المعلوماتية - دراسة مقارنة، مجلة البحوث الفقهية والقانونية، العدد 46، السعودية، 2024، ص2915.

³ محمد الأمين البشري، التحقيق في الجرائم المستحدثة، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، 2004، ص102.

⁴ نورة مرابط، مرجع نفسه، ص251.

⁵ خالد ممدوح إبراهيم، مرجع سابق، ص 155.

الآلية قد تتعرض لاختراقات أو أخطاء تؤدي لتغيير الحقيقة دون تدخل إرادي مباشر من صاحب الجهاز، مما يفتح باب الشك برمجية حول وحدة القصد لدى المتهم¹.

وأخيرا تظهر إشكالية مشروعية التفتيش الإلكتروني لاستخلاص النية، حيث أن البحث عن قرائن القصد غالبا ما يتطلب الولوج الى مساحات خاصة للجاني (كالبريد الإلكتروني والسحب التخزينية)، وهو ما يصطدم بضمانات حماية الحياة الخاصة وحرمة المراسلات الرقمية في القانون الجزائري، ويجعل الدليل المستخلص على " النية" مهددا بالبطلان إذا لم تراعى فيه الإجراءات الدقيقة المنصوص عليها قانونا.²

ثالثا: قصد الإضرار بالغير.

لا يكتمل البنيان القانوني للجريمة بمجرد "نية الاستعمال" بل يجب أن يتوفر عنصر " الضرر" كعلة للتجريم. فالتزوير في المعاملات الرقمية لا يعاقب عليه إلا إذا كان من شأنه إحداث ضرر، سواء كان هذا الضرر محققا أو محتملا، أو سواء أصاب فردا بذاته أو مس بالمصلحة العامة.

1- مفهوم نية الإضرار في الوسط الرقمي وتصنيفاته.

تتمثل نية الإضرار في اتجاه إرادة الجاني الى تحقيق نتيجة ضار من وراء استعمال المحرر المزور. وفي البيئة الرقمية يتخذ الضرر صورا تتجاوز المفهوم التقليدي.

ويتمثل في المساس بالذمة المالية، كالحصول على مزايا مالية غير مستحقة عبر

- **الضرر المادي:** تزوير أوامر تحويل إلكترونية³.
- **الضرر المعنوي:** وهو الأشد انتشارا في الفضاء الرقمي، ويتمثل في المساس بسمعة الأشخاص أو اعتبارهم من خلال تزوير مراسلات إلكترونية أو وثائق تمس بكرامتهم، وهو ضرر يتسم بالسرعة والانتشار الواسع عبر الشبكات.⁴

¹ جميلة بن مسعود ، زينب بوطيمة، القصد الجنائي في الجرائم المعلوماتية، مجلة جامعة غرداية للعلوم القانونية، الجزائر، 2022، ص24.

² طهاري عبد الله، الحماية الجنائية للمحررات الإلكترونية في التشريع الجزائري، أطروحة دكتوراه، جامعة تلمسان، الجزائر، 2016، ص190.

³ خالد ممدوح إبراهيم، التزوير في المحررات الإلكترونية، دار الفكر الجامعي، الإسكندرية، مصر، 2008، ص162.

⁴ جميل عبد الباقي الصغير، جرائم تزوير المستندات المكتوبة بالحاسب الآلي، دار النهضة العربية، القاهرة، مصر، 2001، ص72.

- **الضرر الاجتماعي:** ويتمثل في الاعتداء على " الثقة العامة" فتزوير سجل إداري إلكتروني يزعزع ثقة الجمهور في المنظومة القانونية للدولة، وهو ما يراه الفقه "مفترضا" بمجرد وقوع التزوير في المحررات الرسمية.¹

2- معيار بين الاحتمالية والتحقق.

من اهم النقاط التي يجب إبرازها هي أن المشرع الجزائري (المواد 197 وما بعدها) لا يشترط وقوع الضرر فعليا. بل يكفي أن يكون الضرر محتملا.²

المحرر الرقمي المزور، طالما انه صالح للاحتجاج به ويحمل في طياته إمكانية الحاق الأذى بالغير، فان الجريمة تكتمل أركانها. فمجرد وجود عقد رقمي مزور محفوظ في السحابة الإلكترونية يمثل خطرا مستمرا يهدد المراكز القانونية، مما يستوجب التدخل الجنائي الاستباقي حتى قبل وقوع الخسارة المادية فعليا.³

3- إثبات قصد الضرر وسلطة التقديرية للقاضي.

يخضع إثبات نية الإضرار للسلطة التقديرية لقاضي الموضوع، الذي يستخلصها من ظروف الدعوى. وفي المعاملات الرقمية يستند القاضي على قرائن تقنية، مثل حجم المنفعة التي كان الجاني سيجنيها، أو جسامه التزوير ومدى قدرته على خداع أنظمة الحماية.⁴

ويجب أم يكون استخلاص القاضي للضرر سائغا، خاصة في المحررات العرفية الإلكترونية حيث لا يفترض الضرر فيها كما هو الحال في المحررات الرسمية.

المطلب الثالث: محل جريمة التزوير الإلكتروني.

بما أن جريمة التزوير في جوهرها هي اعتداء على الحقيقة التي يثبتها محرر ما، فان الانتقال من المحيط الورقي الى المحيط الرقمي استوجب إعادة تعريف "محل الجريمة" بما يتلاءم مع الطبيعة اللامادية للبيانات. فالمحل هنا ليس وعاء ماديا كالأوراق، بل هو كيانات منطقية وتقنية تحمل قيمة قانونية، وتتمثل

¹ ممدوح عبد الحميد عبد المطلب، الجرائم المعلوماتية، دار الكتب القانونية، مصر، 2005، ص225.

² نورة مرابط، مرجع سابق، ص256.

³ طهاري عبد الله، الحماية الجنائية للمحررات الإلكترونية، جامعة تلمسان، الجزائر، 2016، ص198.

⁴ محمد الأمين البشري، التحقيق في الجرائم المستحدثة، الرياض، السعودية، 2004، ص112.

في البيانات الرقمية المعالجة والتوقيعات الإلكترونية التي تضفي الحجية، وصولاً إلى السجلات وقواعد البيانات التي تحفظ هذه الحقوق وتعد بمثابة الأرشيف الرقمي الموثق.

أولاً: البيانات الرقمية.

تعد البيانات الرقمية المادة الأولية والجوهر الموضوعي الذي يقع عليه فعل التزوير في البيئة المعلوماتية وهي عبارة عن مجموعة من الرموز والنبضات التي يتم معالجتها آلياً لتعبر عن واقعة قانونية. ولا ينحصر هذا المحل في البيانات الظاهرة فقط بل يمتد ليشمل البيانات الواسفة والتي تعد الركيزة الأساسية في وصف العناصر الرقمية وتحديد مصادرها وتاريخ إنشائها، مما يجعلها دليلاً جنائياً لا يقل أهمية عن محتوى الوثيقة ذاته¹.

إن حماية هذه البيانات تشريعياً وتقنياً هي الضمانة الأساسية لإنجاح التحول الرقمي، حيث أن العبث بها لا يمثل مجرد غش إلكتروني، بل هو اعتداء على العمود الفقري للمعاملات اليومية للدولة والمواطنين².

عليه فإن البيانات الرقمية تكتسب صفة المحل في الجريمة متى كانت تتمتع بحجية قانونية تسمح بالاحتجاج بها، وهو ما يتطلب تدخلاً تشريعياً قعلاً لضمان أمنها من الابتزاز أو التغيير الذي يطال مراكز الأشخاص المالية والأدبية³.

وبهذا تبرز البيانات الرقمية ككيان مستقل يتمتع بحماية جنائية موضوعية، إلا أن هذه الحماية لا تكتمل إلا بوجود رابط قانوني ينسب هذه البيانات لصاحبها وهو ما ينقلنا للحديث عن التوقيع الإلكتروني باعتباره المحل الأكثر حساسية في منظومة الإثبات الرقمي.

ثانياً: التوقيع الإلكتروني.

يعد التوقيع الإلكتروني المحل الأكثر دقة وحيوية في جريمة التزوير الإلكتروني، فإذا كانت البيانات هي مضمون المحرر، فإن التوقيع هو سند صحته والركن الذي يضفي عليه صفة النسبة لمصدره. والتوسع في هذا العنصر يقتضي إدراك أن التوقيع في البيئة الرقمية ليس مجرد رسم شكلي، بل

¹ أبو بكر سلطان محمد الخضر، عفاف مصطفى حامد كروم، مرجع سابق، ص 40.

² محمد صلاح وشادي حمادة، البيانات الرقمية في مصر دراسة قانونية تحليلية، مجلة الدراسات القانونية والاقتصادية، 2025، ص 2370.

³ طه محمد إبراهيم، السلوك الاتصال وعلاقته بإدراك خصوصية البيانات الرقمية، المجلة العربية لبحوث الإعلام والاتصال، 2023، ص 440.

هو منظومة تقنية متكاملة تعمل بمثابة " مفتاح التوثيق للهوية الرقمية، وهو ما يجعله البديل الشرعي والقانوني للتوقيع اليدوي في المعاملات الرسمية والخدمات الحكومية.

تكمن خطورة الاعتداء على هذا المحل في كونه يمس بمبدأ الموثوقية الذي تقوم عليه كافة أشكال التعاقد الإلكتروني إذ أن تزوير التوقيع بالاصطناع أو الانتحال يمنح المحرر المزور قوة الإثبات كاذبة تضلل المتعاملين وترزعزع استقرار المراكز القانونية. وقد اصبح المشرع الجزائري حماية خاصة على هذا المحل، نظرا لان التوقيع هو الذي يضمن عدم إنكار التصرفات القانونية ويؤكد سلامة المحتوى من أي تعديل لا حق¹.

علاوة على ذلك، فإن التوقيع الإلكتروني كمحل للجريمة يرتبط ارتباطا وثيقا ب «الهوية الرقمية» فالتزوير هنا لا يطل مجرد توقيع بل يطل الشخصية القانونية لصاحبه في الفضاء الرقمي، مما يسهل ارتكاب جرائم أخرى كالاختيال والسرقة الإلكترونية. وهذا ما يفسر تشديد العقوبات في الأنظمة القانونية المعاصرة عند وقوع التزوير على مفاتيح التوثيق والشهادات الإلكترونية، لكونها تمثل راس المال الثقة في الاقتصاد الرقمي².

وبناء عليه، يظل التوقيع الإلكتروني محلا جوهريا يتطلب فحصا فنيا دقيقا لكشف التلاعب بخوارزمياته أو انتحال شهادته الموثقة، لضمان حماية حقوق الأفراد وصيانة هيبة المحررات الإلكترونية الرسمية والعرفية على حد سواء³.

ولا تقتصر حماية التوقيع الإلكتروني كمحل للجريمة على الرموز التقنية فحسب، بل تمتد لتشمل شهادات التصديق الإلكتروني التي تصدرها جهات التوثيق المعتمدة. فهذه الشهادات هي التي تمنح التوقيع شرعيته القانونية وتربطه بهوية صاحبه بيقين. وبناء عليه، فإن أي تزوير يطل بيانات هذه الشهادة أو اصطناع شهادة وهمية يعد اعتداء مباشر على محل الجريمة، نظرا لان المشرع الجزائري جعل من هذه الشهادات الضمانة السيادية التي تحمي المعاملات الرقمية من الإنكار أو الانتحال. وهذا ما يعطي للتوقيع الإلكتروني صبغة "المحرر الرسمي في كثير من الأحيان، خاصة عندما تصدر الشهادة عن سلطة تصديق حكومية، مما يرفع من جسامة فعل التزوير المرتكب ضدها⁴.

¹ عبد المنعم بوبتر، وليد بن شيخ، أثر التزوير على التعاقد الإلكتروني، جامعة برج بوعريبيج، الجزائر، 2022، ص 08.

² جميل عبد الباقي الصغير، مرجع سابق، ص 118.

³ نورة مرابط، مرجع سابق، ص 263.

⁴ قانون رقم 15-04 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين.

ثالثا: السجلات وقواعد البيانات الإلكترونية.

لا ينحصر محل التزوير الإلكتروني في معطيات فردية أو توقيعات معزولة، بل يمتد ليشمل الأوعية الشاملة التي تحتضن هذه الحقيقة الرقمية، وهي السجلات وقواعد البيانات الإلكترونية. وتعد هذه السجلات بمثابة الأرشيف السيادي الرقمي والعمود الفقري الذي تقوم عليه منظومة التعاقد الإلكتروني والخدمات الحكومية المعاصرة. أن تزوير هذه القواعد لا يمثل اعتداء على وثيقة وحيدة، بل هو اعتداء على نظام معلوماتي متكامل يتسم بالديمومة، حيث أن أي تحريف يطالها يظل منتجا لأثاره القانونية المظلمة الى حين كشفه، مما يجعل خطرا مستمرا يهدد الثقة العامة الرقمية.¹

والتوسع في تحليل هذا المحل يكشف عن دورها الجوهرية في مكافحة الفساد الإداري وضمان الشفافية إذ أن قواعد البيانات في المصارف، أو سجلات الحالة المدنية، أو العقود الموثقة رقميا، تعد هي المرجع القانوني اليقيني لإثبات الحقوق ومن هنا فإن التلاعب ب الميادات (بيانات الوصف) الخاصة لإخفاء آثار الجريمة، يمثل في جوهره تزويرا في (Log Files) محل يتمتع بحجية مطلقة.

وقد أكد الفقه الجزائري الحديث أن حماية هذه السجلات هي الضمانة الأساسية لاستقرار المعاملات المالية والاقتصادية، خاصة في ظل التحول نحو المحاكمة عن بعد، والخدمات الإلكترونية الشاملة، حيث أصبحت هذه الأوعية الرقمية هي البديل القانوني الكامل للسجلات الورقية التقليدية.²

وعلاوة على ذلك، فإن السجلات الإلكترونية كمحل للجريمة تتميز بخصائص تقنية تفرض على القضاء الجنائي ضرورة الاستعانة بالخبرة الفنية العالية لكشف التلاعب بها، نظرا لسهولة تغيير محتواها دون ترك أثر مادي مرئي. أن الاعتداء على هذا المحل لا يمس فقط بخصوصية الأفراد ومراكزهم القانونية، بل يمتد أثره ليعطل كفاءة سير المرافق العامة الرقمية، وهو ما يبرر إضفاء حماية جنائية مشددة عليها باعتبارها " محررات رسمية إلكترونية" متى صدرت جهات سيادية أو مؤسسات عمومية.³

¹ عبد المنعم بوبترة، ، وليد وبن شيخ ، مرجع سابق، ص15.

² امل خلف الحباشنة، الحماية المعلوماتية للمحاكمة عن بعد، مجلة العلوم الإنسانية والطبيعية، 2022، ص18.

³ محمد صلاح ، شادي حمادة، البيانات الرقمية - دراسة قانونية تحليلية، مجلة الدراسات القانونية والاقتصادية، مصر، 2025، ص2375.

وبذلك تشكل السجلات وقواعد البيانات المحل الشامل والنهائي الذي يجسد الحماية القانونية للمحرر الإلكتروني في أوسع صوره، بما يضمن سلامة المنظومة المعلوماتية من أي عبث يطل حقيقة بياناتها.¹

¹ عمر بن يونس، المسؤولية الجزائية عن الجرائم المعلوماتية، دار هومة، الجزائر، ص 160.

خلاصة الفصل.

يتضح من خلال ما سبق أن جريمة التزوير الإلكتروني لم تعد مجرد امتداد تقني بسيط لجريمة التزوير التقليدي، بل أضحت تشكّل نموذجاً قانونياً مستقلاً يفرض إعادة النظر في العديد من المفاهيم الكلاسيكية للقانون الجنائي. فانتقال التزوير من الدعامة الورقية إلى البيئة الرقمية أدى إلى بروز معطيات جديدة، أبرزها الطبيعة اللامادية للمحررات الإلكترونية، وسهولة تداولها وتعديلها، فضلاً عن الطابع العابر للحدود الذي يميز الجرائم المعلوماتية، كما أن خصوصية الوسائل المستعملة في التزوير الإلكتروني، والتي تعتمد على تقنيات متطورة كالمعالجة الآلية للبيانات والبرمجيات، تجعل من اكتشاف الجريمة وإثباتها أمراً أكثر تعقيداً مقارنة بالتزوير التقليدي، مما يستوجب تعزيز القدرات التقنية للجهات القضائية وأجهزة ضبط القضاء، وتطوير وسائل الإثبات الرقمي بما يضمن فعاليته وحجته القانونية.

ومن جهة أخرى، فإن قيام المسؤولية الجنائية في هذا النوع من الجرائم يظل رهيناً بتوافر أركانها الأساسية، سواء تعلق الأمر بالركن المادي المتمثل في تغيير الحقيقة في محرر إلكتروني، أو الركن المعنوي القائم على القصد الجنائي، غير أن خصوصية البيئة الرقمية تضيف على هذه الأركان طابعاً مميزاً يتطلب تفسيراً مرناً يتلاءم مع التطور التكنولوجي المستمر.

وعليه، فإن مواجهة جريمة التزوير الإلكتروني تقتضي تبني سياسة جنائية حديثة تقوم على التوفيق بين متطلبات الحماية الجنائية للثقة في المعاملات الرقمية، وبين تشجيع استخدام التكنولوجيا وتطوير الاقتصاد الرقمي. إلى جانب تعزيز التعاون الدولي نظراً للطبيعة العابرة للحدود لهذه الجرائم.

وبذلك يمكن القول إن فعالية الحماية القانونية في مجال التزوير الإلكتروني، لا تتحقق فقط من خلال تجريم الأفعال، بل تعتمد كذلك على تكامل المنظومة القانونية والتقنية، بما يضمن تحقيق الأمن القانوني والرقمي في آن واحد، وترسيخ الثقة في البيئة الرقمية كفضاء آمن لإبرام المعاملات وتبادل البيانات.

الفصل الثاني

المسؤولية القانونية المترتبة عن
المعاملات الرقمية والوثائق الإلكترونية

يمثل التزوير الإلكتروني أحد أخطر التحديات التي تواجه القانون المعاصر في ظل الثورة الرقمية المتسارعة، ذلك أنه لم يعد مجرد سلوك إجرامي يمس بمصادقية المحررات فحسب، بل أصبح ظاهرة مركبة تتطوي على أبعاد تقنية وقانونية متشابكة، تستدعي مقاربة متكاملة تتجاوز النظرة التقليدية للتزوير المادي. فإذا كان الفصل الأول من هذه الدراسة قد خصص لتأصيل المفهوم القانوني للتزوير الإلكتروني وتمييزه عن غيره من الأعمال المماثلة، فإن الفصل الثاني يأتي ليتناول الركن الأكثر حساسية في هذه الجريمة، ألا وهو المسؤولية القانونية بمختلف صورها وأنواعها. ذلك أن تحديد طبيعة المسؤولية المترتبة عن الفعل المزور يمثل القمة التي تلتقي عندها الأحكام الموضوعية للتجريم مع الآليات الإجرائية للمساءلة.

وسنتناول في هذا الفصل مبحثين رئيسيين: المبحث الأول يعنى بالمسؤولية الجنائية، حيث نبحث في الأشخاص المسؤولين، ثم العقوبات المقررة، وصولاً إلى إشكالية الإثبات التي تعد أخص مسائل الجرائم الرقمية. أما المبحث الثاني يخصص للمسؤولية المدنية وما تثيره من تحديات علمية، كتقدير الضرر الرقمي وصعوبات تحديد الفاعل، لنختم بآليات الحماية القانونية والتقنية والوقائية.

المبحث الأول: المسؤولية الجنائية عن التزوير الإلكتروني.

شهد العالم تحولاً رقمياً غير مسبوق طال مختلف المعاملات الإدارية والمالية، مما جعل المحررات الإلكترونية تكتسي حجية قانونية معادلة للمحررات الورقية. وتكتسي جريمة التزوير الإلكتروني خطورة خاصة لأنها تستهدف سلامة هذه المعاملات وتُضعف الثقة في الفضاء الرقمي، مما يستدعي دراسة دقيقة للمسؤولية الجنائية المترتبة عنها. ولا تقتصر صعوبة هذه المسألة على تحديد الفاعل المادي المباشر، بل تمتد لتشمل صور المشاركة الخاصة في البيئة الرقمية ومسؤولية الأشخاص المعنوية. ومن هنا تبرز إشكالية أساسية حول كيفية تحديد الأشخاص المسؤولين جنائياً عن هذه الجريمة والعقوبات المقررة لها وخصوصية إثباتها في ظل الطابع التقني للبيانات.

المطلب الأول: الأشخاص المسؤولون جنائياً.

تعد مسألة تحديد الأشخاص المسؤولين جنائياً عن جريمة التزوير الإلكتروني من أكثر المسائل تعقيداً في القانون الجنائي الحديث، وذلك بسبب الطابع التقني لهذه الجريمة وتعدد الأطراف التي يمكن أن تتدخل في ارتكابها. ففي البيئة الرقمية، لم تعد عملية التزوير قاصرة على فعل مادي ملموس يقوم به شخص واحد، بل يمكن أن تتم من خلال تدخلات تقنية متعددة، قد يكون بعضها بعيداً عن مكان ارتكاب الجريمة أو زمنها. وقد استوعب المشرع الجزائري هذه الخصوصية، فجاء بنصوص قانونية تكفل مساءلة كل من يسهم في ارتكاب هذه الجريمة، سواء كان فاعلاً أصلياً أو شريكاً أو شخصاً معنوياً أو مزوداً لخدمات التصديق الإلكتروني، وفق ضوابط دقيقة تحقق التوازن بين حماية المجتمع من هذه الجرائم وضمنان حقوق المتهمين.

أولاً: الفاعل الأصلي.

1- تعريف الفاعل الأصلي في قانون العقوبات الجزائري.

يعرف الفاعل الأصلي في القانون الجنائي الجزائري بأنه الشخص الذي يرتكب الفعل المكون للجريمة بنفسه أو بواسطة غيره، وذلك وفقاً للأحكام العامة الواردة في المادة 41 من قانون العقوبات. وتطبيقاً لهذه القواعد على جريمة التزوير الإلكتروني، يمكن القول إن الفاعل الأصلي فيها هو كل من يقوم بإدخال تغيير للحقيقة في محرر إلكتروني، بأي وسيلة كانت، بقصد إحداث ضرر واستعمال هذا المحرر كمحرر صحيح. غير أن خصوصية الجريمة الإلكترونية تستدعي تحليلاً دقيقاً للركن المادي

والركن المعنوي لهذه الجريمة في ضوء النصوص الخاصة الواردة في القانون رقم 09-04 والقانون رقم 15-04.¹

2- الركن المادي لدى الفاعل الأصلي.

يتجلى الركن المادي في جريمة التزوير الإلكتروني من خلال مجموعة من الأفعال المادية التي يقوم بها الفاعل الأصلي، والتي تختلف في طبيعتها عن أفعال التزوير التقليدي. فبينما كان التزوير الورقي يتطلب فعلاً مادياً ملموساً كالكتابة أو التوقيع أو التغيير في المحرر المادي، فإن التزوير الإلكتروني يتم من خلال أفعال تقنية قد لا يدركها الحس البشري المباشر. وتتعدد صور هذه الأفعال بحسب طبيعة المحرر الإلكتروني موضوع الجريمة.

فقد يتمثل الفعل المادي للتزوير في إدخال بيانات كاذبة إلى نظام معلوماتي بقصد تغيير الحقيقة، كأن يقوم موظف في بنك بإدخال أرقام حسابية خاطئة لتحويل أرصدة إلى حسابات أشخاص غير مستحقين. وقد يتخذ الفعل صورة تغيير أو حذف أو إضافة بيانات موجودة أصلاً في المحرر الإلكتروني، كأن يقوم شخص بتغيير تاريخ صدور عقد إلكتروني أو تعديل قيمة صفقة مالية مسجلة في نظام معلوماتي. وقد يتمثل أيضاً في استخدام برامج متخصصة لتزييف التوقيع الإلكتروني أو اصطناع شهادة رقمية مزورة. كما يمكن أن يتحقق الفعل المادي من خلال إنشاء محرر إلكتروني كامل يحمل بيانات غير صحيحة، كإنشاء موقع إلكتروني مزور يحاكي موقعاً رسمياً بهدف الحصول على بيانات المستخدمين.

وتجدر الإشارة إلى أن المشرع الجزائري قد وسع من نطاق الفعل المادي للتزوير الإلكتروني من خلال القانون رقم 09-04، حيث لم يقصره على الأفعال التي تستهدف المحتوى المعلوماتي فحسب، بل امتد ليشمل الأفعال التي تستهدف البنية التحتية للنظام المعلوماتي نفسه. فمن قبيل التزوير الإلكتروني، الدخول غير المشروع إلى نظام معلوماتي بقصد تغيير بياناته أو تعطيله، إذا رتب ذلك تغييراً للحقيقة في المحررات التي يحتويها.²

¹ للمادة 41 من القانون رقم 82-04 المؤرخ في 13 فيفري 1982، المتضمن قانون العقوبات.

² حابت أمال، "الجريمة المعلوماتية في التشريع الجزائري: بين قانوني 15-04 و 09-04"، مجلة هيروودوت للعلوم الإنسانية والاجتماعية، جامعة مولود معمري، الجزائر، المجلد 7، العدد 25، 2023، ص 60.

3- الركن المعنوي لدى الفاعل الأصلي.

لا يكتمل قيام المسؤولية الجنائية للفاعل الأصلي في جريمة التزوير الإلكتروني إلا بتوافر الركن المعنوي، الذي يتمثل في القصد الجنائي العام والخاص. فالقصد الجنائي العام يتمثل في علم الفاعل بأنه يقوم بفعل غير مشروع، وإرادته في القيام بهذا الفعل. بمعنى أن يكون الفاعل مدركاً أن ما يقوم به من إدخال بيانات كاذبة أو تغيير محرر إلكتروني يشكل تزويراً يعاقب عليه القانون، وأنه قد أقدم على هذا الفعل بإرادة حرة واعية.

أما القصد الجنائي الخاص، فيتمثل في نية استعمال المحرر المزور كمحرر صحيح. وهذا العنصر يميز جريمة التزوير عن غيرها من الجرائم المعلوماتية، كجريمة الدخول غير المشروع إلى نظام معلوماتي التي قد لا تقتزن بنية استعمال المحررات المزورة. وقد أكد المشرع الجزائري على أهمية هذا العنصر من خلال إيراد صراحة في نصوص التجريم. فإذا قام شخص بتغيير بيانات محرر إلكتروني دون أن يقصد استعمال هذا المحرر أو استعماله كمحرر صحيح، فإن فعله قد يشكل جريمة أخرى كإتلاف المال أو الدخول غير المشروع، ولكن لا تشكل جريمة تزوير إلكتروني بمعناها القانوني الدقيق.¹

وتثور إشكالية تتعلق بتوافر القصد الجنائي في الحالات التي يكون فيها التزوير قد تم بواسطة برامج أو أدوات تقنية لا إرادية. فإذا قام شخص بتركيب برنامج خبيث دون قصد التزوير، ولكن هذا البرنامج أدى إلى تعديل بيانات محرر إلكتروني، فإن القصد الجنائي لا يتوافر ما لم يثبت أن الشخص كان يعلم بقدرة هذا البرنامج على إحداث هذا التعديل وأراد ذلك. وهذا ما يؤكد أهمية البحث عن العنصر المعنوي في سلوك الفاعل وليس فقط في النتيجة المادية التي ترتبت عن فعله.

4- صور خاصة للفاعل الأصلي.

قد يتحقق الفاعل الأصلي في جريمة التزوير الإلكتروني من خلال وسيط، وذلك وفقاً لنظرية الفاعل غير المباشر. فإذا استغل شخص خبرته التقنية وأصدر تعليماته لآخر لا يعلم بحقيقة ما يقوم به، فإن الأول يعد فاعلاً أصلياً بالسبب. مثلاً، إذا قام مدير شركة بتوجيه موظف في قسم المعلوماتية لتعديل بعض البيانات في سجلات الشركة الإلكترونية، دون أن يخبره بأن هذه البيانات غير صحيحة، فإن المدير يكون فاعلاً أصلياً للجريمة حتى لو لم يقوم بنفسه بفعل التعديل المادي. أما الموظف الذي نفذ التعليمات دون علمه بحقيقة التزوير، فلا تتحقق مسؤوليتهم الجنائية لانقضاء الركن المعنوي لديه.²

¹ أحسن بوسقيعة، الوجيز في القانون الجزائري العام، الطبعة الثامنة عشرة، دار هومة، د. ب. ن، 2019، ص 142.

² أحسن بوسقيعة، مرجع نفسه، ص 144.

كما قد يتحقق الفاعل الأصلي في صورة الفاعل بالاشتراك، وذلك عندما يتفق عدة أشخاص على ارتكاب جريمة التزوير الإلكتروني ويقوم كل منهم بدور في تنفيذها. ففي هذه الحالة، يعتبر كل من المشاركين فاعلاً أصلياً للجريمة بأكملها، وليس فقط عن الجزء الذي قام به. وهذا ما تقرره أحكام المساهمة الجنائية في قانون العقوبات الجزائري.¹

5- العقوبات المقررة للفاعل الأصلي.

يخضع الفاعل الأصلي لجريمة التزوير الإلكتروني للعقوبات المنصوص عليها في قانون العقوبات الجزائري والقوانين الخاصة. فقد نصت المادة 394 مكرر 1 من قانون العقوبات على معاقبة كل من يدخل معطيات بطريق الغش، أو يزيلها، أو يعدلها، بالحبس من سنة إلى ثلاث سنوات وغرامة من 500.000 إلى 2.000.000 دينار جزائري. كما تتصاعد العقوبة إلى الحبس من سنتين إلى عشر سنوات وغرامة من 700.000 إلى 2.000.000 دينار جزائري إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات العمومية، وذلك وفقاً للمادة 394 مكرر 3 من قانون العقوبات.²

ثانياً: الشريك.

عرفه المشرع الجزائري في المادة 42 من قانون العقوبات الجزائري بأنه "يعتبر شريكاً في الجريمة من لم يشترك اشتراكاً مباشراً ولكنه ساعد بكل الطرق أو عاون الفاعل أو الفاعلين على ارتكاب الأفعال التحضيرية أو المسهلة أو المنفذة لها مع علمه بذلك"³

1- صور المشاركة في التزوير الإلكتروني.

تخضع المسؤولية الجنائية للشريك في جريمة التزوير الإلكتروني للأحكام العامة الواردة في قانون العقوبات الجزائري، والتي تنص على أن الشريك هو من يساعد أو يحرض على ارتكاب الجريمة، أو يقدم أدوات أو وسائل تسهل تنفيذها. غير أن الخصوصية التقنية للجريمة الإلكترونية تستدعي توسيعاً في فهم صور المشاركة الجنائية، حيث يمكن أن تتم المساعدة أو التحريض بوسائل إلكترونية لا وجود لها في الجرائم التقليدية.

¹ فرقد عبود العارضي، جريمة التزوير الإلكتروني-دراسة مقارنة، مجلة الكوفة للعلوم القانونية والسياسية، المجلد 1، العدد 13، د.ب.ن، 2012، ص 173.

² المادة 394 مكرر 1 والمادة 394 مكرر 3 من قانون العقوبات الجزائري، الأمر رقم 66-156 المؤرخ في 8 يونيو 1966 المعدل والمتمم.

³ المادة 42، من قانون العقوبات الجزائري، الأمر رقم 66-156.

تتنوع صور المشاركة في جريمة التزوير الإلكتروني بتنوع الوسائل والأدوار التي يمكن أن يقوم بها المشاركون في البيئة الرقمية. فقد يتمثل الشريك في الشخص الذي يقدم الدعم التقني للفاعل الأصلي عن علم بتوافر القصد الجنائي، كتوفير برامج التزوير المتخصصة أو تسهيل الدخول إلى الأنظمة المعلوماتية المحمية. ومثل هذا الشخص، لو كان يعلم أن البرامج التي يقدمها ستستخدم في تزوير محررات إلكترونية، فإنه يعد شريكاً في حتى لو لم يشارك في تنفيذها بشكل مباشر.

كذلك، يعتبر شريكا الجريمة من يضع خبرته التقنية في خدمة الفاعل الأصلي للمساعدة في تنفيذ التزوير، كمبرمج يقوم بكتابة أوامر برمجية خبيثة بناءً على طلب الفاعل، أو فني صيانة أنظمة معلوماتية يقدم معلومات عن نقاط الضعف في نظام ما تسهل اختراقه والتزوير فيه. وفي هذه الحالات، تكون خبرة الشريك هي العنصر الأساسي الذي مكن من ارتكاب الجريمة، مما يضيف على مشاركته خطورة خاصة تستدعي المساءلة الجنائية.

كما يمكن أن يتحقق دور الشريك من خلال التحريض على ارتكاب الجريمة بأي وسيلة كانت، سواء كان ذلك عبر الإنترنت من خلال منشورات تحرض على تزوير المحررات الإلكترونية أو تعليم كيفية القيام بذلك، أو بوسائل أخرى كالاتصال الهاتفي أو اللقاءات المباشرة. وقد نص المشرع الجزائري صراحة على تجريم التحريض على ارتكاب الجرائم المعلوماتية في القانون رقم 09-04، وذلك لما يشكله من خطورة على الأمن المعلوماتي¹

2- شروط قيام المسؤولية الجنائية للشريك.

لا تتحقق مسؤولية الشريك في جريمة التزوير الإلكتروني إلا بتوافر جملة من الشروط، يأتي في مقدمتها أن تكون هناك جريمة أصلية قد ارتكبت بالفعل أو شرع في ارتكابها. فإذا كان الفعل الذي ساعد فيه الشريك لا يشكل جريمة تزوير إلكتروني لعدم توافر أركانه، فلا مسؤولية جنائية على من قدم المساعدة، إلا إذا كان الفعل الذي قدمت المساعدة من أجله يشكل جريمة أخرى مستقلة.

كما يشترط أن يكون لدى الشريك علم بنية الفاعل الأصلي في ارتكاب الجريمة. فإذا قدم شخص دعماً تقنياً لآخر دون أن يعلم أن هذا الدعم سيستخدم في التزوير، فإنه لا يكون شريكاً في الجريمة لانقضاء الركن المعنوي. وهذه الجزئية تثير إشكالية كبيرة في مجال الجرائم الإلكترونية، خاصة في الحالات

¹ حابت آمال، مرجع سابق، ص 66.

التي يقدم فيها أشخاص خدمات تقنية بشكل مهني، كشركات الاستضافة أو مزودي خدمات الإنترنت، حيث قد لا يمكن إثبات علمهم بأن خدماتهم تُستخدم في نشاط غير مشروع. ويشترط أيضًا أن تكون المساعدة قد تمت قبل ارتكاب الجريمة أو إثباتها، وأن تكون قد ساهمت بشكل فعلي في تسهيل أو تمكين ارتكاب الجريمة. فإذا تم تقديم المساعدة بعد انتهاء الجريمة، فإن ذلك لا يرقى إلى مرتبة المشاركة الجنائية، بل قد يشكل جريمة أخرى كإخفاء الأدلة أو الإغانة على عدم الكشف عن الجناة.¹

3- عقوبة الشريك واستقلاليتها.

يعاقب الشريك في جريمة التزوير الإلكتروني بنفس العقوبات المقررة للفاعل الأصلي، وذلك وفقًا للأحكام العامة لقانون العقوبات. غير أن القاضي الجنائي يتمتع بسلطة تقديرية في توزيع العقوبة بين الفاعل والشريك وفقًا لدرجة مشاركة كل منهما في الجريمة وخطورة دوره فيها. فقد يقرر القاضي تخفيف العقوبة بالنسبة للشريك إذا كان دوره ثانويًا أو هامشيًا، كما قد يشدد العقوبة إذا كان دور الشريك هو الدافع الأساسي لارتكاب الجريمة.

وتجدر الإشارة إلى أن بعض صور المشاركة في جريمة التزوير الإلكتروني قد شكلها المشرع الجزائري كجرائم مستقلة بذاتها، وذلك في إطار سياسة جنائية تهدف إلى مكافحة الجرائم المعلوماتية في مراحلها المبكرة. فمن قبيل ذلك، تجريم صنع أو حيازة أو توفير برامج أو أدوات مصممة لارتكاب جرائم معلوماتية، حتى لو لم تُستخدم فعليًا في ارتكاب جريمة. وفي هذه الحالات، يكون الشخص مسؤولًا عن جريمة قائمة بذاتها، وليس مجرد شريك في جريمة لم ترتكب بعد. وقد نصت المادة 394 مكرر 2 من قانون العقوبات على معاقبة من يصمم أو يجمع أو يوفر أو ينشر أو يتجر في أدوات أو برمجيات خبيثة يمكن استخدامها لارتكاب الجرائم المعلوماتية، بالحبس من سنة إلى خمس سنوات وغرامة من 1.000.000 إلى 5.000.000 دينار جزائري.²

ثالثًا: مسؤولية الشخص المعنوي.

1- الأساس القانوني لمسؤولية الشخص المعنوي.

لم يعد الشخص المعنوي بمنأى عن المسؤولية الجنائية في القانون الجزائري، فقد أقر المشرع مبدأ مسؤولية الأشخاص المعنوية عن الجرائم المرتكبة باسمهم أو لحسابهم أو بواسطة أجهزتهم، وذلك وفقًا

¹ مجنوب لامية، مرجع سابق، ص 116.

² المادة 394 مكرر 2 من الأمر رقم 66-156، المتضمن قانون العقوبات .

لأحكام الواردة في قانون العقوبات. وتكتسي هذه المسؤولية أهمية خاصة في مجال التزوير الإلكتروني، حيث غالبًا ما تُرتكب هذه الجرائم في إطار نشاط الشركات والمؤسسات، سواء بقصد تحقيق منافع غير مشروعة للشخص المعنوي أو نتيجة إهمال في تنظيم أنظمته المعلوماتية.

يستند أساس مسؤولية الشخص المعنوي في القانون الجزائري إلى فكرة أن الشخص المعنوي، كالشركة أو المؤسسة، يتحمل تبعه الأفعال التي تصدر عن أعضائه أو ممثليه في إطار نشاطه ولحسابه. فقد نصت المادة 36 مكرر من قانون العقوبات الجزائري على أن "الأشخاص المعنوية عدا الدولة، تسأل جنائيًا عن الجرائم التي يرتكبها ممثلوها أو أجهزتها أو أعضاؤها باسمها أو لحسابها". وقد تمتد هذه المسؤولية لتشمل الأشخاص المعنوية الخاصة والعامة على حد سواء، باستثناء الدولة التي تتمتع بحصانة خاصة.

بخصوص جريمة التزوير الإلكتروني، فإن النصوص الخاصة الواردة في القانون رقم 04-09 والقانون رقم 04-15 لم تستثن الأشخاص المعنوية من نطاق التجريم، مما يعني أن هذه الأشخاص يمكن أن تسأل جنائيًا عن أفعال التزوير التي ترتكب في إطار نشاطها. وقد يكون هذا الأمر ذا أهمية كبيرة في مكافحة الجرائم التي ترتكبها الشركات الكبرى أو المؤسسات المالية أو شركات التكنولوجيا. وقد نص المشرع الجزائري على إمكانية مساءلة الأشخاص المعنوية عن الجرائم المنصوص عليها في القسم السابع مكرر من قانون العقوبات الخاص بالمساس بأنظمة المعالجة الآلية للمعطيات، وذلك وفقًا للقواعد العامة التي يحكمها مبدأ التخصص، والذي يقضي بأن لا مسؤولية جزائية للشخص المعنوي إلا بنص خاص.

إذ تستند هذه المسؤولية إلى نص المادة 51 مكرر من قانون العقوبات، والتي تنص على أنه "باستثناء الدولة والجماعات المحلية والأشخاص الخاضعة للقانون العام، يكون الشخص المعنوي مسؤولاً جزائياً عن الجرائم التي ترتكب لحسابه من طرف أجهزته أو ممثليه الشرعيين عندما ينص القانون على ذلك". ولما كانت جريمة التزوير الإلكتروني معاقب عليها بمقتضى النصوص الواردة في القسم السابع مكرر، فإن المادة 394 مكرر 4 من قانون العقوبات الجزائري تجسد هذا المبدأ بوضوح، حيث تعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمسة

أضعاف الحد الأقصى للغرامة المقررة للشخص الطبيعي عن ذات الجريمة، مما يكرس مبدأ الاستقلال والتبعية في آن معاً في مساءلة الأشخاص المعنوية.¹

2- شروط مسؤولية الشخص المعنوي.

تتحقق مسؤولية الشخص المعنوي عن جريمة التزوير الإلكتروني التي أشار إليها المشرع الجزائري بصورة غير مباشرة في نص المادة 51 مكرر إذا توافرت الشروط:

أولاً: أن يكون الفعل المكون للجريمة قد ارتكب باسم الشخص المعنوي أو لحسابه. فإذا قام أحد موظفي الشركة بتزوير محررات إلكترونية لمصلحته الشخصية ولأغراض خاصة به، فإن الشركة لا تسأل عن فعله، لأنه لم يرتكب باسمها أو لحسابها. أما إذا تم التزوير بغرض تحقيق منفعة للشركة، كتزوير تقارير مالية إلكترونية لتضليل الجهات الرقابية، فإن الشركة تسأل عن هذا الفعل.

ثانياً: أن يكون ارتكاب الجريمة قد تم بواسطة أحد أجهزة الشخص المعنوي أو ممثليه أو أعضائه. ويقصد بالأجهزة الهياكل التنظيمية التي يتكون منها الشخص المعنوي، كمجلس الإدارة أو الجمعية العامة أو الإدارة التنفيذية. ويقصد بالمثلين الأشخاص المخول لهم تمثيل الشخص المعنوي في مواجهة الغير، كرئيس مجلس الإدارة أو المدير العام. ويقصد بالأعضاء الأشخاص الذين ينتمون إلى هذه الأجهزة.

ثالثاً: أن يتوافر الركن المعنوي في الشخص الطبيعي الذي ارتكب الفعل وينسب إلى الشخص المعنوي. فإذا كان الشخص الطبيعي الذي قام بالتزوير قد فعل ذلك دون علم أو قصد، فلا تسأل الشخص المعنوي أيضاً، لأن المسؤولية الجنائية للشخص المعنوي تابعة للمسؤولية الجنائية للشخص الطبيعي في هذا الصدد. غير أن بعض الفقه يرى إمكانية قيام مسؤولية الشخص المعنوي بشكل مستقل عن مسؤولية الأشخاص الطبيعيين، خاصة في حالات الإهمال التنظيمي أو نقص الرقابة.²

3- العقوبات المطبقة على الشخص المعنوي.

تختلف العقوبات المقررة للشخص المعنوي عن تلك المقررة للشخص الطبيعي، وذلك لطبيعة الشخص المعنوي التي لا تسمح بتطبيق عقوبات سالبة للحرية كالسجن. وقد حدد المشرع الجزائري في قانون العقوبات قائمة العقوبات التي يمكن توقيعها على الأشخاص المعنوية، وتشمل:

¹ المادة 51 مكرر ، الأمر رقم 66-156، المتضمن قانون العقوبات الجزائري.

² أحسن بوسقيعة، الوجيز في القانون الجنائي العام، الديوان الوطني للأشغال التربوية، الجزائر، 2002، ص 56.

- الغرامة المالية التي تحدد وفقًا لجسامة الجريمة، وتكون عادة مضاعفة للغرامة المقررة للشخص الطبيعي. وقد نصت المادة 394 مكرر 4 من قانون العقوبات صراحة على أن عقوبة الشخص المعنوي هي غرامة مالية تعادل خمسة أضعاف الحد الأقصى للغرامة المقررة للشخص الطبيعي.
- الحل القضائي إذا ارتكبت الجريمة بقصد ارتكاب جرائم أو إذا كان الحل في المصلحة العامة.
- المنع من مزاولة النشاط المهني أو الاجتماعي الذي ارتكبت في نطاقه الجريمة لمدة لا تتجاوز خمس سنوات.

- المصادرة الكلية أو الجزئية للأموال التي استخدمت في ارتكاب الجريمة.
- نشر الحكم الصادر بالإدانة في الصحف أو بأي وسيلة أخرى على نفقة المحكوم عليه.
- الإغلاق المؤقت أو الدائم للمؤسسة أو الفرع الذي استخدم في ارتكاب الجريمة.¹

4- مسؤولية مزودي خدمات التصديق الإلكتروني

أ - الإطار التشريعي المنظم لخدمات التصديق الإلكتروني.

يمثل مزودو خدمات التصديق الإلكتروني ركناً أساسياً في البنية التحتية للمعاملات الإلكترونية، حيث يتولون مهام إصدار الشهادات الرقمية وإدارة مفاتيح التوقيع الإلكتروني والتحقق من هويات المستخدمين. وقد نظم المشرع الجزائري هذه الخدمات من خلال القانون رقم 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين، الذي حدد شروط مزاولة هذا النشاط والالتزامات الملقاة على عاتق مزودي الخدمة والجزاء المترتبة على إخلالهم بها.

استناداً إلى أحكام القانون رقم 15-04، تُعتبر الشهادة الإلكترونية المؤهلة، التي يتم إنشاؤها بواسطة شهادة إلكترونية مؤهلة وجهاز آمن، ذات حجية قانونية معادلة للحجية المقررة للتوقيع الخطي اليدوي. وقد أقر هذا القانون مبدأ الموثوقية كأهم المبادئ المكرسة لضمان أمان ومصداقية التوقيع الإلكتروني. ويترتب على ذلك أن مزودي خدمات التصديق يتحملون مسؤولية كبيرة في ضمان سلامة هذه العملية، حيث أن أي خلل أو تقصير في أدائهم لمهامهم قد يؤدي إلى تعريض سلامة المعاملات الإلكترونية للخطر، وقد يسهل ارتكاب جرائم التزوير الإلكتروني.

وقد حدد القانون رقم 15-04 شروط اعتماد مزودي خدمات التصديق، حيث لا يمكن لأي شخص أو مؤسسة مزاولة هذا النشاط دون الحصول على ترخيص من السلطة الوطنية المختصة، ودون استيفاء

¹ المادة 394 مكرر 4 من قانون العقوبات الجزائري.

مجموعة من الشروط التقنية والمالية والقانونية التي تضمن قدرته على أداء مهامه بكفاءة وأمان. كما ألزم القانون مزودي الخدمة بالاحتفاظ بسجلات دقيقة لجميع العمليات التي يقوم بها، وإخطار السلطات المختصة فور اكتشاف أي خرق أمني أو محاولة تزوير.¹

ب - نطاق مسؤولية مزودي الخدمات التصديق الإلكتروني.

يمكن تصنيف مسؤولية مزودي خدمات التصديق الإلكتروني في إطار جريمة التزوير الإلكتروني على عدة مستويات، تختلف بحسب درجة إسهامهم في الجريمة ومدى علمهم أو إهمالهم. فالمسؤولية المباشرة تتحقق إذا كان مزود الخدمة هو نفسه من قام بإصدار شهادة رقمية بناءً على معلومات غير صحيحة عن علم، أو إذا سهل عملية التزوير بإهماله في التحقق من هوية طالب الشهادة. فمثلاً، إذا قام مزود خدمة بإصدار شهادة رقمية لشخص لم يثبت من هويته بشكل صحيح، واستخدم هذا الشخص الشهادة في تزوير محررات إلكترونية، فإن مزود الخدمة يسأل جنائياً عن هذا الإهمال، خاصة إذا كان يشكل جريمة في حد ذاته وفقاً للقانون رقم 04-15.

أما المسؤولية بالتضامن، فتتأشأ إذا ساهم إهمال مزود الخدمة في تسهيل ارتكاب جريمة التزوير من قبل الغير. فإذا أهمل مزود الخدمة في تأمين أنظمتهم بشكل كاف، مما أتاح اختراقها واستغلال مفاتيح التوقيع الإلكتروني في تزوير محررات، فإنه يسأل بالتضامن مع الفاعل الأصلي عن الأضرار الناجمة عن هذا الاختراق. وفي هذه الحالة، تكون مسؤولية مزود الخدمة قائمة على أساس الخطأ في التنظيم والإدارة، وليس على أساس المشاركة المباشرة في الجريمة.

كما تنثور مسؤولية مزود الخدمة عن أعمال تابعيه وموظفيه في نطاق ممارستهم لمهامهم الوظيفية. فإذا قام موظف في شركة التصديق بتزوير شهادة رقمية أو تسريب مفاتيح توقيع عن علم أو عن إهمال، فإن الشركة تسأل عن هذه الأفعال لأنها صدرت عن أحد تابعيها في إطار العمل. وهذا ما تقرره القواعد العامة لمسؤولية المتبوع عن أعمال تابعه في القانون الجزائي والإداري.²

¹ نوي عبد النور، "مبدأ الموثوقية في ظل القانون 04/15 المتعلق بالتوقيع والتصديق الإلكترونيين"، مجلة صوت القانون، جامعة جيلالي بونعامة، خميس مليانة، المجلد 7، العدد 3، 28 ماي 2021، ص 257.

² زهيرة عبوب، المسؤولية المدنية لمقدم خدمات التصديق الإلكتروني، دراسة تحليلية القانون رقم 04-15، مجلة الدراسات القانونية المقارنة، كلية الحقوق والعلوم السياسية، جامعة حسيبة بن بوعلي، الشلف، المجلد 6، العدد 02، 27 ديسمبر 2020، ص 429.

ج - الالتزامات القانونية لمزودي الخدمات التصديق الإلكتروني.

- تقرض التشريعات المنظمة لخدمات التصديق الإلكتروني مجموعة من الالتزامات على مزودي الخدمة، والتي يعتبر الإخلال بها سبباً لقيام مسؤوليتهم الجنائية. ومن أبرز هذه الالتزامات:
- الالتزام بمعايير الأمان والجودة في إدارة الشهادات الرقمية، بما في ذلك استخدام تقنيات تشفير آمنة وحماية المفاتيح الخاصة من الاختراق أو الضياع.
 - الالتزام بالتحقق من هوية طالبي الشهادات الرقمية وفق إجراءات دقيقة، لا تقل صرامة عن تلك المتبعة في التحقق من هوية الأشخاص في المعاملات الورقية.
 - الاحتفاظ بسجلات دقيقة لجميع العمليات التي يقوم بها، بما في ذلك إصدار الشهادات وتجديدها وإلغاؤها، مع إمكانية تقديم هذه السجلات للسلطات القضائية عند الطلب.
 - إخطار الجهات المختصة فور اكتشاف أي خرق أمني أو محاولة تزوير أو اختراق لأنظمتها.
 - تقديم خدمة التحقق من صحة الشهادات، حيث تقدم سلطة التصديق خدمة مجانية للتحقق من صحة التوقيع أو الختم الإلكتروني وتأكيد صلاحيته لصالح الأطراف المستخدمة.
 - تعويض المتضررين عن الأضرار الناجمة عن إخلالهم بالالتزامات، وذلك وفقاً للقواعد العامة للمسؤولية المدنية¹.

ج - العقوبات المقررة لمزودي الخدمات التصديق الإلكتروني.

في حالة ثبوت مسؤولية مزود خدمات التصديق عن جريمة تزوير إلكتروني، يجوز توقيع مجموعة من الجزاءات تتناسب مع دوره في الجريمة وخطورة الإخلال الذي ارتكبه. فقد تقرر السلطة الوطنية المختصة سحب الترخيص الممنوح له بمزاولة النشاط، إما بشكل مؤقت أو دائم، إذا ثبت أنه لم يعد يستوفي شروط الاعتماد أو إذا ارتكب مخالفات جسيمة.

بالإضافة إلى العقوبات الإدارية، قد يتعرض مزود الخدمة للعقوبات الجنائية المقررة لجريمة التزوير إذا توافرت أركانها في حقه، خاصة في حالات التزوير المباشر أو المشاركة فيه. وفي هذا السياق، تنص المادة 394 مكرر 8 من قانون العقوبات على مسؤولية مزودي خدمات الإنترنت الذين يمتنعون عن التدخل الفوري لسحب أو حجب المحتويات التي تشكل جرائم قانونية رغم إنذارهم من الهيئة الوطنية المختصة أو أمر قضائي، ويعاقبون بالحبس من سنة إلى ثلاث سنوات وغرامة من 2.000.000 إلى

¹ زهيرة عبوب، مرجع سابق، ص 426.

10.000.000 دينار جزائري كما قد يحكم على مزود الخدمة بدفع تعويضات للمتضررين عن الأضرار المادية والمعنوية التي لحقت بهم نتيجة إخلاله بالتزاماته.¹

وتجدر الإشارة إلى أن القانون رقم 04-15 قد نص صراحة عن العقوبات المالية والإدارية لمزودي خدمات التصديق الإلكتروني في المادة 64 حيث تنص: "في حالة عدم احترام مؤدي خدمات التصديق الإلكتروني أحكام دفتر الأعباء أو سياسة التصديق الإلكتروني الخاصة به والموافق عليها من طرف السلطة الاقتصادية، تطبق عليه هذه السلطة عقوبة مالية يتراوح مبلغها بين مائتي ألف دينار 200.000 دج وخمسة ملايين دينار 5000.000 دج، حسب تصنيف الأخطاء المنصوص عليه في دفتر الأعباء الخاص بمؤدي الخدمات، وتعذر بالامتنال لالتزاماته في مدة تتراوح بين ثمانية أيام و30 يوما، حسب الحالة، وتبلغ المأخذ المتخذة ضد مؤدي الخدمات حتى يتسنى له تقديم مبرراته الكتابية ضمن الآجال المذكورة سابقا.

وفي حالة عدم امتثال مؤدي الخدمات للأعذار، تتخذ ضده السلطة الاقتصادية للتصديق الإلكتروني قرار سحب الترخيص الممنوح له وإلغاء شهادته، حسب الحالة، بعد موافقة السلطة.²

من خلال ما سبق نستنتج أن التشريعات المنظمة لخدمات التصديق الإلكتروني على مجموعة من العقوبات التي تسلط على مزودي الخدمة في حالة الإخلال بالتزاماتهم المهنية، حيث يمكن للسلطة الاقتصادية المختصة فرض عقوبات مالية تتراوح بين 200.000 دج و5000.000 دج، إضافة إلى اتخاذ تدابير إدارية قد تصل إلى سحب الترخيص وإلغاء شهادة التصديق الإلكتروني، وذلك بعد إعذار مسبق ومنح المهلة القانونية لتقديم المبررات.

¹ المادة 394 مكرر 8، الأمر رقم 66-156 المتضمن قانون العقوبات.

² المادة 64، قانون رقم 04-15، المتعلق بالتوقيع والتصديق الإلكترونيين، المؤرخ في 1 فبراير سنة 2015، الجريدة الرسمية، العدد 06، 2015.

المطلب الثاني: العقوبات المقررة لجريمة التزوير الإلكتروني

بعد تحديد نطاق المسؤولية الجنائية والأشخاص الذين يمكن مساءلتهم عن جريمة التزوير الإلكتروني، ننتقل إلى دراسة الجزاء المترتب على ثبوت هذه المسؤولية. لقد أدرك المشرع الجزائري خطورة هذه الجريمة على الثقة العامة في الاقتصاد الرقمي وفي سلامة المحررات الإلكترونية، فعمل على إرساء سياسة عقابية رادعة تقوم على مبدأي التناسب والتدرج. وتتميز هذه السياسة العقابية بكونها لم تقتصر على العقوبات الأصلية التقليدية المتمثلة في الحبس والغرامة، بل تجاوزتها لتشمل عقوبات تكميلية ذات طابع تقني تمس صميم النشاط الإلكتروني، فضلاً عن تغليظ العقوبة في حالات محددة ترتبط بمكانة المجني عليه أو جسامة الضرر. وقد استقى المشرع هذه الأحكام من القسم السابع مكرر من قانون العقوبات، الذي استحدث بموجب القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم بالقانون رقم 24-06 المؤرخ في 28 أبريل 2024، ليشكل إطاراً قانونياً متكاملاً للتصدي لهذه الجريمة المستحدثة.

أولاً: العقوبات الأصلية.

1- تعريف العقوبات الأصلية في جريمة التزوير الإلكتروني.

حدد المشرع الجزائري العقوبة الأصلية لجريمة التزوير الإلكتروني في نص المادة 394 مكرر 1 من قانون العقوبات، معتمداً في ذلك نظاماً عقابياً مزدوجاً يجمع بين العقوبة السالبة للحرية (الحبس) والعقوبة المالية (الغرامة). ويعكس هذا التوجه رغبة المشرع في تحقيق الردع بنوعيه العام والخاص، حيث يستهدف الحبس تقييد حرية الجاني وكفه عن معاودة الإجرام، بينما تستهدف الغرامة تجريده من أي عائد مالي قد يكون جناه من الجريمة. وقد روعي في تحديد العقوبة الطبيعة الخاصة للبيئة الرقمية، حيث تكون الأضرار فيها غالباً ذات طابع مالي أو معنوي يصعب جبره بالطرق التقليدية.¹

2- الركن المادي الموجب للعقوبة الأصلية.

تنص المادة 394 مكرر 1 من قانون العقوبات الجزائري صراحة على تجريم الأفعال المادية التالية متى ارتكبت بطريق الغش: إدخال معطيات في نظام للمعالجة الآلية للمعطيات، أو إزالة معطيات منه، أو تعديلها. ويُقصد بالمعطيات كل المعلومات أو البيانات المخزنة أو المعالجة أو المنقولة عبر النظام

¹ المادة 394 مكرر 1 الأمر رقم 66-156 المتضمن قانون العقوبات.

المعلوماتي، سواء تعلقت بأشخاص طبيعيين أو معنويين أو بوثائق إدارية أو مالية. وجدير بالملاحظة أن المشرع لم يقصر التجريم على التزوير بمعناه التقليدي (تغيير الحقيقة في محرر)، بل وسّع نطاقه ليشمل كل مساس بسلامة المعطيات المعلوماتية، إدراكاً منه بأن المحرر الإلكتروني بات يتمتع بذات الحجة القانونية التي يتمتع بها المحرر الورقي بموجب القانون رقم 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين.¹

3- الركن المعنوي الموجب للعقوبة الأصلية.

لا تقوم العقوبة الأصلية إلا بتوافر القصد الجنائي العام لدى الفاعل، والمتمثل في العلم والإرادة. فيشترط أن يكون الجاني عالماً بأنه يقوم بفعل غير مشروع يتمثل في إدخال معطيات أو إزالتها أو تعديلها بطريق الغش، وأن تتجه إرادته إلى تحقيق ذلك الفعل. كما يستلزم القانون توافر قصد خاص يتمثل في نية استعمال المحرر المزور كمحرر صحيح، وهو ما يميز جريمة التزوير الإلكتروني عن غيرها من جرائم المساس بأنظمة المعالجة الآلية للمعطيات، كجريمة الدخول غير المشروع المنصوص عليها في المادة 394 مكرر من قانون العقوبات. فإذا انتفى هذا القصد الخاص، انتفى وصف التزوير، وظل الفعل خاضعاً لنص تجريمي آخر إن توافرت أركانه.²

4- مقدار العقوبة الأصلية المقررة.

وفقاً لنص المادة 394 مكرر 1 من قانون العقوبات الجزائري، فإن عقوبة جريمة التزوير الإلكتروني هي الحبس من سنة (1) إلى ثلاث (3) سنوات، وغرامة مالية تتراوح بين 500.000 دينار جزائري و 2.000.000 دينار جزائري، أو بإحدى هاتين العقوبتين فقط. ويُلاحظ أن المشرع قد شدد العقوبة السالبة للحرية بموجب التعديل الأخير الصادر بالقانون رقم 24-06 المؤرخ في 28 أبريل 2024، حيث رفع الحد الأدنى للحبس من ستة (6) أشهر إلى سنة (1) كاملة، مما يعكس تشدد المشرع في مواجهة تنامي الجرائم المعلوماتية وتزايد خطورتها على الاقتصاد الوطني والأفراد على حد سواء. أما الغرامة المالية فقد أبقى عليها المشرع عند سقفها المرتفع، وهو ما يتناسب مع حجم الأضرار المالية التي يمكن أن تتجم عن التلاعب بالمعطيات المعلوماتية في الأنظمة المصرفية والتجارية.³

¹ المادة 394 مكرر 1، الأمر رقم 66-156، المتضمن قانون العقوبات.

² المادة 394 مكرر، الأمر رقم 66-156، المتضمن قانون العقوبات.

³ المادة رقم 394 مكرر 1، الأمر رقم 66-156، المتضمن قانون العقوبات.

5- السلطة التقديرية للقاضي في توقيع العقوبة الأصلية.

أجازت المادة 394 مكرر 1 من قانون العقوبات للقاضي الجنائي سلطة تقديرية واسعة في توقيع العقوبة، تبعاً لظروف الدعوى وملابساتها وجسامة الضرر الناجم عن الجريمة. فيمكن للقاضي أن يحكم بالحبس والغرامة معاً، وهو الأصل، أو أن يكتفي بإحدى العقوبتين فقط (الحبس دون غرامة، أو الغرامة دون حبس). وتستند هذه السلطة التقديرية إلى أحكام المادة 53 من قانون العقوبات التي تتيح للمحكمة النزول بالعقوبة عن حدها الأدنى إذا توافرت أعمار قانونية أو ظروف مخففة. غير أن ظروف التزوير الإلكتروني غالباً ما تقتضي التشديد لا التخفيف، نظراً لما تنطوي عليه من خيانة للأمانة الرقمية واستغلال للثقة التي يوليها الأفراد والمؤسسات للأنظمة المعلوماتية.¹

ثانياً: العقوبات التكميلية.

1- مفهوم العقوبات التكميلية وأساسها القانوني.

إلى جانب العقوبات الأصلية، أقر المشرع الجزائري طائفة من العقوبات التكميلية التي تهدف إلى تعزيز الردع ومنع استمرار النشاط الإجرامي أو تكراره. وهذه العقوبات منصوص عليها في المادة 394 مكرر 6 من قانون العقوبات، وتتميز بكونها ذات طبيعة وقائية وتحفظية أكثر منها عقابية بحتة. والملاحظ أن المشرع قد راعى في تقريرها الطبيعة التقنية لجريمة التزوير الإلكتروني، فجاءت عقوبات تمس الأدوات والوسائل المستخدمة في ارتكاب الجريمة، وتهدف إلى اجتثاث النشاط الإجرامي من جذوره بحرمان الجاني من الوسائل التي مكنته من ارتكاب الجريمة.²

2- مصادرة الأجهزة والبرامج والوسائل المستخدمة في الجريمة.

أولى العقوبات التكميلية التي نصت عليها المادة 394 مكرر 6 من قانون العقوبات هي مصادرة الأجهزة والبرامج والوسائل المستخدمة في ارتكاب الجريمة. ويشمل ذلك أجهزة الحاسوب والهواتف الذكية والأقراص الصلبة ووسائط التخزين والبرمجيات المستخدمة في التزوير. كما تمتد المصادرة لتشمل المعطيات والبيانات التي تم الحصول عليها نتيجة الجريمة. وتُعد المصادرة إجراءً ضرورياً لمنع الجاني من استئناف نشاطه الإجرامي باستخدام ذات الوسائل، كما تمنع تداول تلك المعطيات المزورة في الفضاء الرقمي. وتختلف المصادرة هنا عن المصادرة كعقوبة أصلية في كونها إجراءً احترازياً تفرضه المحكمة

¹ محمد الأمين شريط، "السياسة العقابية في جرائم تكنولوجيات الإعلام والاتصال في التشريع الجزائري"، مجلة القانون والمجتمع، جامعة أدرار، العدد 11، 2023، ص 115.

² المادة 394 مكرر 6، الأمر رقم 66-156، المتضمن قانون العقوبات.

بحكم القانون، ولا تملك سلطة تقديرية في إيقاعه إذا ما ارتأت أن الوسائل المضبوطة قد استخدمت فعلاً في ارتكاب الجريمة.¹

3- إغلاق المواقع الإلكترونية موضوع الجريمة.

ثاني العقوبات التكميلية المقررة بموجب المادة 394 مكرر 6 من قانون العقوبات هي إغلاق المواقع الإلكترونية التي كانت محل الجريمة. وهذه العقوبة تكتسي أهمية خاصة في جرائم التزوير الإلكتروني، حيث كثيراً ما تُرتكب الجريمة من خلال مواقع إلكترونية مزورة تحاكي مواقع رسمية أو تجارية بغرض تضليل المستخدمين والحصول على بياناتهم أو أموالهم. ويتم الإغلاق بأمر من الجهة القضائية المختصة، ويُنفذ بالتعاون مع مزودي خدمات الإنترنت والهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. ويهدف هذا الإجراء إلى منع استمرار الضرر وتجنب الجمهور الوقوع ضحية للموقع المزور، وهو ما ينسجم مع الوظيفة الوقائية للقانون الجنائي الحديث.²

4- إغلاق المحل أو مكان الاستغلال.

ثالث العقوبات التكميلية التي أوردتها المادة 394 مكرر 6 من قانون العقوبات هي إغلاق المحل أو مكان الاستغلال الذي ارتكبت فيه الجريمة بعلم مالكة. ويُقصد بالمحل كل مكان يمارس فيه نشاط تجاري أو مهني، كمقاهي الإنترنت ومحلات بيع وصيانة الحواسيب وشركات البرمجيات. واشترط المشرع لتوقيع هذه العقوبة أن يكون مالك المحل عالماً بأنشطة التزوير التي تمارس في محله، سواء بعلم فعلي أو بقرائن قاطعة تدل على علمه، ومع ذلك لم يتخذ الإجراءات الكفيلة بمنعها أو الإبلاغ عنها. فإذا انتفى علم المالك، فلا يمكن إغلاق المحل، حفاظاً على مبدأ شخصية العقوبة وعدم جواز مؤاخذة الشخص بفعل غيره.³

¹ المادة 394 مكرر 6، الأمر رقم 66-156، المتضمن قانون العقوبات .

² هشام بحوش، الجرائم المتصلة بتكنولوجيا الإعلام والاتصال في ظل التشريع الجزائري، مجلة الحقوق والعلوم السياسية، جامعة سوق أهراس، العدد 7، 2017، ص 199.

³ المادة 394 مكرر 6 الأمر رقم 66-156 المتضمن قانون العقوبات.

ثالثاً: الظروف المشددة.

1- أساس الظروف المشددة ونطاق تطبيقها.

لم يكتف المشرع الجزائري بالعقوبات المقررة للصورة البسيطة من جريمة التزوير الإلكتروني، بل نص في المادة 394 مكرر 3 من قانون العقوبات على ظرف مشدد يغلظ العقوبة بصورة ملحوظة. وهذا الظرف لا يشكل جريمة مستقلة بذاتها، بل هو وصف يلحق بالجريمة الأصلية فيرفع من مقدار عقوبتها. ويمتد نطاق تطبيق هذا الظرف المشدد ليشمل جميع الجرائم المنصوص عليها في القسم السابع مكرر من قانون العقوبات، بدءاً من المادة 394 مكرر المتعلقة بالدخول غير المشروع، ومروراً بالمادة 394 مكرر 1 المتعلقة بالتزوير الإلكتروني، وانتهاءً بالمادة 394 مكرر 2 المتعلقة بجرائم الأدوات والبرمجيات الخبيثة.¹

2- حالات الظرف المشدد.

حددت المادة 394 مكرر 3 من قانون العقوبات حالتين يتحقق بهما الظرف المشدد:

الحالة الأولى: استهداف الجريمة للدفاع الوطني.

وتشمل هذه الحالة كل فعل من أفعال التزوير الإلكتروني يكون محله معطيات أو أنظمة معلوماتية تخص وزارة الدفاع الوطني أو المصالح الأمنية أو أي هيئة أو مؤسسة تساهم في الدفاع عن الوطن أو حماية أمنه القومي. وقد أدرك المشرع أن استهداف المنظومات المعلوماتية العسكرية والأمنية بالتزوير يمكن أن يترتب أضراراً جسيمة بالأمن القومي، سواء بإضعاف القدرات الدفاعية للدولة أو بتسريب معلومات حساسة إلى جهات معادية. ولذلك، شدد العقوبة إلى درجة تحول الجريمة من جنحة إلى جناية، بالنظر إلى جسامه الفعل وخطورة نتائجه.

الحالة الثانية: استهداف الجريمة للهيئات والمؤسسات العمومية.

ويقصد بها كل مؤسسة أو هيئة خاضعة للقانون العام، كالوزارات والمصالح الإدارية والجماعات المحلية والمؤسسات العمومية ذات الطابع الإداري أو الاقتصادي. فإذا كان محل التزوير الإلكتروني معطيات تخص هذه الهيئات والمؤسسات، تشدد العقوبة. وتبرير ذلك أن هذه الهيئات تؤدي خدمات عامة جوهرية للمواطنين، وأن أي تزوير يطال معطياتها من شأنه زعزعة الثقة في الإدارة العامة والإضرار

¹ المادة 394 مكرر، المتضمن قانون العقوبات.

بمصالح المواطنين الأساسية. كما أن حماية المعطيات العمومية تُعد جزءاً لا يتجزأ من حماية السيادة الرقمية للدولة.¹

3- مقدار العقوبة في حالة توافر الظرف المشدد.

نصت المادة 394 مكرر 3 من قانون العقوبات على عقوبة مستقلة في حال توافر الظرف المشدد، وهي الحبس من سنتين (2) إلى عشر (10) سنوات، وغرامة مالية تتراوح بين 700.000 دينار جزائري و 2.000.000 دينار جزائري.² ويُلاحظ أن المشرع قد رفع الحد الأدنى للحبس من سنة إلى سنتين مقارنة بالصورة البسيطة، كما رفع الحد الأقصى من ثلاث سنوات إلى عشر سنوات، مما يُخرج الجريمة في هذه الحالة من نطاق الجناح لتدخل في نطاق الجنايات، وفقاً للتقسيم الثلاثي للجرائم المعتمد في قانون العقوبات الجزائري. وتترتب على هذا التصنيف آثار إجرائية مهمة، لعل أبرزها اختصاص محكمة الجنايات بنظر الدعوى بدلاً من المحكمة الابتدائية، وطول مدة تقادم الدعوى العمومية والعقوبة. أما الغرامة المالية فقد ارتفع حدّها الأدنى من 500.000 إلى 700.000 دينار، مع بقاء حدّها الأقصى عند 2.000.000 دينار.³

4- أثر الظرف المشدد على تكييف الجريمة.

يترتب على توافر الظرف المشدد المنصوص عليه في المادة 394 مكرر 3 من قانون العقوبات تغيير في التكييف القانوني للجريمة، من حيث درجة خطورتها ونوع المحكمة المختصة بمحاكمة المتهم. فإذا ارتكبت جريمة التزوير الإلكتروني في حق هيئة عمومية أو مساساً بالدفاع الوطني، فإنها تُعتبر جنائية وليس جنحة، وتُحال إلى محكمة الجنايات الابتدائية المختصة إقليمياً. وهذا التغيير في التكييف ليس مجرد مسألة شكلية، بل يترتب آثاراً موضوعية وإجرائية مهمة، منها: مدة تقادم الدعوى العمومية التي تصبح عشر (10) سنوات كاملة بدلاً من ثلاث (3) سنوات بالنسبة للجناح، وإمكانية إصدار أمر بالإيداع المؤقت للمتهم، وعدم جواز الصلح أو التنازل من قبل المجني عليه. كما أن الحكم الصادر في الجنائية يكون قابلاً للطعن بالنقض أمام المحكمة العليا وليس بالاستئناف.⁴

¹ المادة 394 مكرر، الأمر رقم 66-156، المتضمن قانون العقوبات.

² المادة 394 مكرر الأمر رقم 66-155، المتضمن قانون الإجراءات الجزائية، المعدل والمتمم، الجريدة الرسمية للجمهورية الجزائرية.

³ هشام بحوش، مرجع سابق، ص 198.

⁴ الأمر رقم 66-156، المتضمن قانون العقوبات.

المطلب الثالث: خصوصية الإثبات في جرائم التزوير الإلكتروني.

إذا كانت قواعد المسؤولية الجنائية والعقاب تشكل الإطار القانوني النظري لمكافحة جريمة التزوير الإلكتروني، فإن تفعيل هذه القواعد على أرض الواقع يظل رهيناً بإمكانية إثبات الجريمة وإقامة الدليل على وقوعها وعلى نسبة ارتكابها إلى المتهم. وتبرز خصوصية الإثبات في جرائم التزوير الإلكتروني من طبيعة البيئة الرقمية التي ترتكب فيها، حيث تغيب المحررات المادية الملموسة، وتحل محلها معطيات رقمية غير مرئية، قابلة للنسخ والتغيير والانتقال عبر الشبكات بصورة قد لا تترك أثراً مادياً محسوساً. وقد استشرع المشرع الجزائري هذه الخصوصية، فسعى إلى تكييف قواعد الإثبات الجنائي مع طبيعة الجرائم المعلوماتية من خلال جملة من النصوص التشريعية التي اعترفت بحجية المحرر الإلكتروني وأقرت وسائل إثبات رقمية متطورة، وأولت الخبرة التقنية دوراً محورياً في كشف ملابسات هذه الجرائم والتوصل إلى مرتكبيها.

أولاً: حجية المحرر الإلكتروني.

1- مفهوم المحرر الإلكتروني وحجيته في الإثبات.

يُقصد بالمحرر الإلكتروني في القانون الجزائري كل وثيقة تنشأ أو تخزن أو تُنقل بوسيلة إلكترونية، وتتضمن بيانات أو معلومات يمكن الرجوع إليها وفهمها. وقد أقر المشرع الجزائري حجية قانونية للمحرر الإلكتروني تعادل حجية المحرر الورقي التقليدي، وذلك بموجب القانون رقم 05-10 المؤرخ في 20 جوان 2005 المعدل والمتمم للقانون المدني، حيث تم تعديل المادة 323 مكرر 1 من القانون المدني لتنص صراحة على أن "الكتابة الإلكترونية نفس الحجية المقررة للكتابة على الورق، بشرط أن تتوفر فيها الضمانات الكافية لسلامتها ومطابقتها لأصلها". ويشكل هذا النص نقلة نوعية في مفهوم الإثبات في التشريع الجزائري، حيث ساوى بين المحرر الإلكتروني والمحرر الورقي في القوة الثبوتية، مما أزال أي شكوك كانت تحوم حول إمكانية الاعتماد على المحررات الإلكترونية كدليل في الدعاوى المدنية والجنائية¹.

2- الأساس القانوني لحجية المحرر الإلكتروني في المجال الجنائي.

على الرغم من أن النص المدني السالف ذكره يتعلق بالإثبات في المعاملات المدنية والتجارية، إلا أن أثره يمتد إلى المجال الجنائي بطبيعة الحال، إذ لا يتصور أن يعترف القانون للمحرر الإلكتروني

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

بالحجية في المجال المدني ثم يجدها في المجال الجنائي. بل إن القانون رقم 04-09 المتعلق بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال قد تضمن إشارات واضحة إلى اعتبار المعطيات والمعلومات المخزنة في الأنظمة المعلوماتية محلاً للحماية الجنائية، مما يفيد ضمناً الاعتراف بحجيتها كأدلة إثبات. كما أن القانون رقم 04-15 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين جاء ليعزز هذه الحجية من خلال وضع ضوابط وشروط فنية وقانونية دقيقة تضمن سلامة المحرر الإلكتروني وموثوقيته¹.

3- شروط اكتساب المحرر الإلكتروني للحجية القانونية.

لا يكتسب المحرر الإلكتروني حجيته القانونية بشكل مطلق، بل يتعين توافر جملة من الشروط والضمانات التي تكفل سلامته ومطابقته للحقيقة. وتتمثل أهم هذه الشروط في:

- أ- **ضمان هوية الشخص المصدر:** يجب أن يكون من الممكن التحقق من هوية الشخص الذي أصدر المحرر الإلكتروني أو وقّع عليه، ويتم ذلك عادة من خلال التوقيع الإلكتروني المؤمن أو الشهادة الرقمية التي تصدر عن مزود خدمات التصديق الإلكتروني المعتمد.
- ب- **سلامة المحرر الإلكتروني:** يجب أن تتوفر ضمانات كافية تثبت أن المحرر الإلكتروني لم يطرأ عليه أي تغيير أو تحريف أو تزوير منذ لحظة إنشائه أو توقيعه. ويتحقق ذلك من خلال تقنيات التشفير وخوارزميات التحقق من سلامة البيانات.
- ج- **إمكانية الاطلاع على المحرر:** يجب أن يكون المحرر الإلكتروني قابلاً للعرض والقراءة والفهم من قبل الأشخاص المخول لهم الاطلاع عليه، سواء من خلال الأجهزة الحاسوبية أو من خلال طباعته على الورق².

4- التوقيع الإلكتروني ودوره في تعزيز حجية المحرر الإلكتروني.

يُعد التوقيع الإلكتروني الركن الأساسي في إضفاء الحجية على المحرر الإلكتروني، حيث يؤدي ذات الوظائف التي يؤديها التوقيع اليدوي على المحررات الورقية. وقد عرّف القانون رقم 04-15 التوقيع

¹ القانون رقم 04-09، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، المؤرخ في 05 أوت 2009، العدد 47، الجريدة الرسمية.

² القانون رقم 04-15، المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، المؤرخ في 01 فبراير 2015، الجريدة الرسمية العدد 06.

الإلكتروني بأنه "بيانات في شكل إلكتروني ملحقة أو مرتبطة منطقياً بمحرر إلكتروني، يستخدمها الموقع لإظهار هويته والتعبير عن موافقته على مضمون المحرر". وقد ميز المشرع الجزائري بين نوعين من التوقيع الإلكتروني: التوقيع الإلكتروني البسيط، والتوقيع الإلكتروني المؤمن. ويتمتع التوقيع الإلكتروني المؤمن بحجية أقوى، لأنه يستند إلى شهادة تصديق إلكترونية صادرة عن مزود خدمات تصديق معتمد، ويتم إنشاؤه باستخدام أداة آمنة لإنشاء التوقيع، مما يجعله قرينة على صحة البيانات الموقعة ونسبتها إلى صاحبها.¹

5- حجية المحرر الإلكتروني في مواجهة جريمة التزوير.

إذا كان القانون قد اعترف للمحرر الإلكتروني بالحجية في الإثبات، فإن تزوير هذا المحرر يعد اعتداءً على هذه الحجية، ويستوجب توقيع العقاب على مرتكبيه. وهنا تثار إشكالية قانونية دقيقة: هل المحرر الإلكتروني المزور يفقد حجتيه القانونية بالكلية، أم يظل محتفظاً بها إلى أن يثبت تزويره بحكم قضائي؟ الأصل في القانون الجزائري أن المحررات الرسمية والعرفية تظل محتفظة بحجيتها إلى أن يطعن فيها بالتزوير ويثبت ذلك بحكم قضائي بات. ويسري هذا المبدأ على المحررات الإلكترونية أيضاً، فهي تظل منتجة لآثارها القانونية ما لم يتم إثبات تزويرها بالطرق المقررة قانوناً. ويقع عبء إثبات التزوير على عاتق من يدعيه، سواء كان متهماً بدفع التهمة عن نفسه أو مدعياً مدنياً يطالب بحقوقه.²

ثانياً: وسائل الإثبات الرقمية.

1- مفهوم الدليل الرقمي وخصائصه.

الدليل الرقمي هو أي مأو بيان إلكتروني يمكن استخلاصه من الأجهزة والأنظمة المعلوماتية وشبكات الاتصال، ويكون له قيمة في إثبات واقعة الجريمة أو نفيها. ويتميز الدليل الرقمي بخصائص فريدة تميزه عن الأدلة المادية التقليدية، وتؤثر في كيفية جمعه وتحليله والتعامل معه في الإجراءات الجنائية. ومن أبرز هذه الخصائص:

- الطبيعة غير الملموسة: حيث لا يمكن إدراك الدليل الرقمي بالحواس البشرية المباشرة، بل يحتاج إلى أجهزة وبرمجيات متخصصة لاستخلاصه.

¹ بلخير بلحاج، "حجية التوقيع الإلكتروني في الإثبات (الضوابط والشروط)"، مجلة القانون والعلوم السياسية، كلية الحقوق والعلوم السياسية، المركز الجامعي تندوف، المجلد 3، العدد 2، 2017، ص 270.

² غلاب عبد الحق، "خصوصية جريمة تزوير التوقيع الإلكتروني في التشريع الجزائري"، مجلة الدراسات القانونية والسياسية، المجلد 8، العدد 1، 2022، ص 500.

- **سهولة النسخ والانتقال:** مما يسمح بنقل الأدلة الرقمية عبر الشبكات بسرعة فائقة، ويصعب مهمة تحديد مكان وجودها.
- **قابلية التغيير والتعديل:** مما يهدد سلامة الدليل ويستدعي اتخاذ احتياطات تقنية خاصة عند جمعه وتحليله.
- **قابلية الاختفاء والتدمير عن بُعد:** حيث يمكن للجاني محو الأدلة الرقمية من أجهزته أو من الأنظمة المخترقة باستخدام برامج متخصصة أو أوامر بسيطة¹.

2- أنواع الأدلة الرقمية في جرائم التزوير الإلكتروني.

تتنوع الأدلة الرقمية التي يمكن الاعتماد عليها في إثبات جريمة التزوير الإلكتروني، ويمكن تصنيفها إلى الأنواع التالية:

- أ- **المحررات والملفات الإلكترونية المزورة.** وهي موضوع الجريمة ذاته، وتشمل الوثائق والعقود والفواتير والتقارير المالية الإلكترونية التي تم تغيير الحقيقة فيها. وتوجد هذه المحررات عادة في أجهزة الحاسوب أو الخوادم أو وسائط التخزين الرقمية، ويمكن استخلاصها وفحصها للكشف عن مواضع التزوير فيها.
- ب- **سجلات الأنظمة المعلوماتية.** تسجل الأنظمة المعلوماتية المختلفة أنشطة المستخدمين بشكل آلي، مما ينتج عنه سجلات رقمية (Log Files) تثبت عمليات الدخول إلى النظام والتعديلات التي أجريت على البيانات وتواريخها وأوقاتها. وتعد هذه السجلات من أقوى الأدلة في إثبات التزوير الإلكتروني، لأنها تسجل الأحداث بشكل موضوعي دون تدخل بشري.
- ج- **الرسائل الإلكترونية والمراسلات الرقمية.** قد تحتوي البريد الإلكتروني وتطبيقات المراسلة الفورية على مراسلات بين الفاعلين والشركاء تتضمن توجيهات أو تعليمات تتعلق بارتكاب التزوير، مما يشكل دليلاً قوياً على القصد الجنائي ودور كل متهم في الجريمة.
- ح- **البيانات المخفية والملفات المؤقتة.** تحتفظ أنظمة التشغيل والتطبيقات ببيانات مخفية وملفات مؤقتة قد تكشف عن وجود محررات تم حذفها أو تعديلها، ويمكن للخبراء التقنيين استعادة هذه البيانات واستخدامها كدليل².

¹ فيصل نسيغة، عبير بعقيقي، الإثبات في الجرائم المعلوماتية على ضوء القانون 04-09 مجلة العلوم القانونية والسياسية، جامعة محمد خيضر بسكرة، المجلد 9، العدد2، 11 جوان2018، ص36.

² الأمر رقم 66-155 المؤرخ في 8 يونيو 1966 المتضمن قانون الإجراءات الجزائية، المعدل والمتمم، الجريدة الرسمية.

3- الأحكام الإجرائية الخاصة بجمع الأدلة الرقمية.

نظراً للطبيعة الخاصة للدليل الرقمي، فقد تضمن القانون رقم 04-09 أحكاماً إجرائية خاصة بجمعه وتحريه، تهدف إلى الحفاظ على سلامته ومنع تغييره أو إتلافه. وتتمثل هذه الأحكام فيما يلي:

أ- **التفتيش الرقمي.** أجاز القانون لضباط الشرطة القضائية، بإذن من وكيل الجمهورية، تفتيش أنظمة المعالجة الآلية للمعطيات والاطلاع على محتوياتها. كما أجاز لهم الوصول إلى المعطيات المخزنة خارج الإقليم الوطني إذا كانت متاحة من داخل النظام المعلوماتي موضوع التفتيش.

ب- **الحفظ الاحتياطي للمعطيات.** للضبطية القضائية أن تأمر أي شخص طبيعي أو معنوي بحفظ المعطيات الرقمية التي يعتقد أنها ضرورية للتحقيق، وذلك لمدة لا تتجاوز سنة قابلة للتجديد. ويهدف هذا الإجراء إلى منع إتلاف الأدلة الرقمية في الفترة ما بين اكتشاف الجريمة وإتمام إجراءات جمعها.

ج- **التسليم الإجباري للمعطيات.** يجوز للسلطات القضائية إلزام مزودي خدمات الاتصالات والإنترنت بتسليم المعطيات المتعلقة بحركة الاتصالات والمشاركين، إذا كانت هذه المعطيات ضرورية لكشف الجريمة وتحديد مرتكبيها.

ح- **الاستعانة بخبراء تقنيين.** نظراً للطابع التقني للدليل الرقمي، فقد أوجب المشرع الاستعانة بخبراء متخصصين في مجال المعلوماتية والاتصالات عند إجراء عمليات التفتيش وجمع الأدلة الرقمية، لضمان سلامة هذه الإجراءات وعدم الإضرار بالبيانات¹.

4- مشروعية الدليل الرقمي وشروط قبوله في الإثبات الجنائي.

لا يكفي أن يكون الدليل الرقمي متوافراً من الناحية المادية، بل يجب أن يكون مشروعاً في طريقة الحصول عليه وفي كيفية عرضه على القضاء. فالقاضي الجنائي لا يقبل الدليل إلا إذا تم الحصول عليه وفقاً للإجراءات المقررة قانوناً، ودون مساس بالحقوق والحريات الأساسية للأفراد. وقد اشترط الفقه والقضاء لقبول الدليل الرقمي في الإثبات الجنائي الشروط التالية:

أ- **سلامة طريقة الحصول على الدليل.** يجب أن يتم جمع الدليل الرقمي وفقاً لأحكام قانون الإجراءات الجزائية والقانون رقم 04-09، وفي مقدمتها الحصول على إذن قضائي بالتفتيش عند الاقتضاء، واحترام حرمة الحياة الخاصة وسرية المراسلات.

¹ فيصل نسيغة، عبير بعقيقي، مرجع سابق، ص 41.

ب- **المحافظة على سلامة الدليل وسلامة سلسلة الحراسة.** يجب اتخاذ الاحتياطات الفنية اللازمة لضمان عدم تغيير الدليل الرقمي أو تبديله منذ لحظة جمعه وحتى عرضه على المحكمة. ويتم توثيق كل إجراء يُتخذ على الدليل في محاضر رسمية، لتكوين ما يُعرف بـ "سلسلة الحراسة" (Chain of Custody) التي تثبت سلامة الدليل وعدم العبث به.

ج- **مصادقية الخبرة التقنية.** إذا تطلب فحص الدليل الرقمي إجراء خبرة تقنية، فيجب أن تتم هذه الخبرة وفق الأصول العلمية المتعارف عليها، وأن يقدم الخبير تقريراً واضحاً ومفصلاً يمكن للقاضي الاعتماد عليه في تكوين قناعته.¹

ثالثاً: الخبرة التقنية ودورها في الإثبات

1- مفهوم الخبرة التقنية في جرائم التزوير الإلكتروني.

الخبرة التقنية في مجال الجرائم المعلوماتية هي إجراء من إجراءات التحقيق والاستدلال، يعهد بموجبه القاضي أو ضابط الشرطة القضائية إلى شخص مختص في تكنولوجيا المعلومات والاتصالات بمهمة فحص الأدلة الرقمية وتحليلها وتقديم تقرير فني حول المسائل التقنية التي تخرج عن نطاق المعرفة القانونية العادية. وتكتسي الخبرة التقنية أهمية بالغة في جرائم التزوير الإلكتروني، ذلك أن إثبات وقوع التزوير وتحديد كيفية ارتكابه والأدوات المستخدمة فيه، وكشف هوية الفاعل، هي مسائل تقنية بحتة لا يمكن للقاضي أو المحقق أن يحيط بها دون الاستعانة بخبير متخصص. فالخبير التقني هو الذي يستطيع قراءة السجلات الرقمية، واستعادة الملفات المحذوفة، وتحليل خصائص الملفات الرقمية للكشف عن مواطن التلاعب والتغيير.²

2- مجالات عمل الخبير التقني في إثبات التزوير الإلكتروني.

تتعدد المهام التي يمكن أن يضطلع بها الخبير التقني في إطار التحقيق في جريمة التزوير الإلكتروني، ويمكن إجمالها في المجالات التالية:

أ- **فحص الأجهزة ووسائط التخزين.** يقوم الخبير بفحص أجهزة الحاسوب والهواتف الذكية والأقراص الصلبة ووسائط التخزين المضبوطة، لاستخلاص الأدلة الرقمية الموجودة فيها. ويشمل ذلك نسخ

¹ فيصل نسيغة، عبير بعقيقي، مرجع سابق، ص42.

² فوزي عمار، نبيلة قنفود، الخبرة التقنية في مجال إثبات الجريمة الإلكترونية، مجلة جامعة الأمير عبد القادر للعلوم الإسلامية، قسنطينة، المجلد36، العدد2، 13 أكتوبر2022، ص408.

محتويات هذه الأجهزة بطريقة تحافظ على سلامتها الأصلية ((Forensic Imaging، ثم تحليل النسخ المستخلصة للبحث عن المحررات المزورة والأدلة الدالة على التزوير.

ب- **تحليل السجلات الرقمية.** يفحص الخبير سجلات الأنظمة المعلوماتية (Log Files) لتحديد من قام بالدخول إلى النظام في التواريخ والأوقات التي حدث فيها التزوير، وما هي العمليات التي قام بها. وهذه السجلات قد تكشف عن هوية الفاعل أو على الأقل عن الجهاز الذي تم استخدامه في ارتكاب الجريمة.

ج- **كشف التلاعب في المحررات الإلكترونية.** باستخدام أدوات وتقنيات متخصصة، يستطيع الخبير التقني اكتشاف ما إذا كان المحرر الإلكتروني قد تعرض للتغيير أو التعديل بعد إنشائه. فكل ملف رقمي يحمل بيانات خفية (Metadata) تسجل تاريخ إنشائه وتاريخ آخر تعديل عليه وخصائص أخرى، وأي تغيير في هذه البيانات يمكن أن يكون دليلاً على التلاعب.

ح- **تتبع الأثر الرقمي.** يمكن للخبير تتبع الأثر الرقمي الذي يتركه الجاني أثناء ارتكابه للجريمة عبر الشبكات، من خلال تحليل عناوين بروتوكول الإنترنت (P Addresses) وتحديد مسار الاتصالات، مما قد يقود إلى تحديد الموقع الجغرافي الذي انطلقت منه الجريمة أو تحديد هوية المشتبه به.¹

3- حجية تقرير الخبرة التقنية في الإثبات الجنائي.

يُعد تقرير الخبرة التقنية وسيلة من وسائل الإثبات في القانون الجزائري، إلا أنه لا يرقى إلى مرتبة الدليل القاطع الذي يلزم القاضي بالأخذ به. فالقاضي الجنائي يتمتع بسلطة تقديرية مطلقة في تقييم الأدلة المعروضة عليه، وله أن يأخذ بتقرير الخبرة كلياً أو جزئياً، كما له أن يطرحه جانباً إذا لم يقتنع بسلامة الأسس التي بني عليها أو إذا تعارض مع أدلة أخرى أكثر إقناعاً. غير أنه من الناحية العملية، تكتسي تقارير الخبرة التقنية أهمية استثنائية في مجال الجرائم المعلوماتية، نظراً للطبيعة التقنية البحتة لهذه الجرائم التي تجعل القاضي غير قادر على تكوين قناعته دون الاستعانة بالرأي الفني المتخصص. ولذلك، يحرص القضاة والمحققون على انتقاء خبراء ذوي كفاءة عالية، ويوجهون إليهم أسئلة محددة وواضحة، ويطلبون منهم تقديم تقارير مفصلة ومدعمة بالأدلة الفنية التي يمكن مناقشتها في الجلسات.²

¹ المادة 26 القانون رقم 09-04، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، المؤرخ في 05 أوت 2009، الجريدة الرسمية العدد 47.

² فيصل نسيغة، عبير بعقيقي، مرجع سابق، ص 45.

4- ضمانات الخبرة التقنية وشروط صحتها.

لكي تكتسب الخبرة التقنية قيمتها القانونية ويكون تقريرها صالحاً للاستناد إليه في الإثبات الجنائي، يجب أن تراعى فيها جملة من الضمانات الشكلية والموضوعية:

أ- **أهلية الخبير.** يجب أن يتمتع الخبير بالكفاءة العلمية والتقنية اللازمة في مجال تكنولوجيا المعلومات والاتصالات، ويفضل أن يكون مقيداً في جداول الخبراء القضائيين المعتمدين لدى المجالس القضائية، مما يضمن مستوى معيناً من التأهيل والخبرة العملية.

ب- **سلامة إجراءات الخبرة.** يجب أن تتم الخبرة وفق الأصول الفنية المتعارف عليها في مجال التحقيق الرقمي الجنائي Digital Forensics، مع استخدام أدوات وبرمجيات موثوقة ومعتمدة، وتوثيق كل خطوة من خطوات التحليل لضمان إمكانية مراجعتها والتحقق منها.

ج- **شمولية التقرير ووضوحه.** يجب أن يكون تقرير الخبرة شاملاً لكل المهام التي كلف بها الخبير، وأن يكون مكتوباً بلغة واضحة تمكن القاضي وأطراف الدعوى من فهم المسائل التقنية المعروضة فيه، مع تجنب المصطلحات التقنية المفرطة في التعقيد دون شرحها.

ح- **إمكانية المناقشة.** يخضع تقرير الخبرة لمبدأ التقاضي، فيحق للنيابة العامة والمتهم والمدعي المدني مناقشة الخبير في محتوى تقريره، وتوجيه الأسئلة إليه في الجلسة، كما يحق لهم طلب إجراء خبرة تكميلية أو خبرة مضادة إذا لم يقتنعوا بنتائج الخبرة الأولى¹.

5- التحديات التي تواجه الخبرة التقنية في الجزائر.

على الرغم من الأهمية البالغة للخبرة التقنية في إثبات جرائم التزوير الإلكتروني، إلا أن الواقع العملي في الجزائر يكشف عن وجود جملة من التحديات التي تعوق فعالية هذه الخبرة. من أبرزها: قلة عدد الخبراء المؤهلين في مجال التحقيق الرقمي الجنائي مقارنة بالعدد المتزايد من القضايا المعروضة على المحاكم، وعدم توافر المختبرات الرقمية المجهزة بأحدث التقنيات في كافة المجالس القضائية، وصعوبة مواكبة الخبراء للتطور المتسارع في تقنيات المعلومات والاتصالات. كما أن غياب معايير وطنية موحدة للتحقيق الرقمي الجنائي، وعدم وجود برامج تكوينية متخصصة كافية، يشكلان عائقاً إضافياً أمام تطوير الخبرة التقنية في الجزائر. ومع ذلك، فإن الجهود المبذولة من قبل وزارة العدل

¹ حابت آمال، مرجع سابق، ص 79.

والهيئات المختصة، ومنها سلطة الضبط للبريد والاتصالات الإلكترونية، تبشر بتحسين تدريجي في هذا المجال، خاصة مع إدراج تخصصات جديدة في التكوين القضائي والشرطي¹.

المبحث الثاني: المسؤولية المدنية والتحديات العملية

بعد التطرق إلى تحديد المسؤولية الجنائية والأشخاص الذين يمكن مساءلتهم عن جريمة التزوير الإلكتروني، تبرز أهمية دراسة الجزاء القانوني المترتب عن هذه الجريمة، باعتباره الأداة الأساسية لتحقيق الردع وحماية المعاملات الإلكترونية.

وقد اعتمد المشرع الجزائري سياسة عقابية تجمع بين الصرامة والتدرج، من خلال إقرار عقوبات أصلية وتكميلية، مع تشديدها في حالات معينة نظراً لخطورة الفعل المرتكب. وعليه، سيتم في هذا المبحث التطرق إلى مختلف العقوبات المقررة لجريمة التزوير الإلكتروني، مع بيان طبيعتها ونطاق تطبيقها.

المطلب الأول: المسؤولية المدنية والتعويض عن الضرر

تعدّ المسؤولية المدنية وسيلة قانونية لحماية الأفراد من الأضرار الناجمة عن الأفعال غير المشروعة، خاصة مع تطور الجرائم والأضرار في البيئة الرقمية. وقد أدى انتشار استخدام الوسائل الإلكترونية إلى ظهور أضرار رقمية تستوجب تعويض المتضرر وجبر الضرر الأحق به. وتقول المسؤولية على أركان أساسية تتمثل في الخطأ والضرر والعلاقة السببية، مع بروز صعوبات خاصة بإثبات الضرر الرقمي وتقدير التعويض عنه، وهو ما سيتم تناوله في هذا المطلب.

أولاً: أركان المسؤولية المدنية

تقوم المسؤولية المدنية، سواء كانت عقدية أو تقصيرية، على ثلاثة أركان أساسية لا يكتمل قيامها بدونها: الخطأ، والضرر، وعلاقة السببية بينهما. وفي مجال التزوير الإلكتروني، تظل هذه الأركان قائمة من حيث المبدأ، لكن طبيعة البيئة الرقمية تفرض تكييفاً خاصاً لكل ركن منها على حدة.²

أ- **الخطأ في المسؤولية المدنية الرقمية:** الخطأ في مفهومه العام هو انحراف في سلوك الشخص عن السلوك الذي كان ينبغي أن يصدر منه وفقاً لما يقتضيه العاديون من الناس. وفي البيئة الرقمية،

¹ عبد القادر هواري، المسؤولية المدنية المترتبة عن المعاملات الرقمية، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة عين تيموشنت، ص34.

² قارس بوبكر، "المسؤولية المدنية في مجال المعاملات الإلكترونية"، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة باتنة، 2021، ص 13.

يمكن أن يتمثل الخطأ في أفعال متعددة: تعديل البيانات الإلكترونية تحريفًا لها، حذفها عمدًا، استعمال توقيع إلكتروني مزور مع العلم بتزويره، تقديم معلومات كاذبة لمقدم خدمات التصديق، أو إهمال تطبيق التدابير الأمنية اللازمة. ويرى جانب من الفقه أن التأسيس القانوني الذي اعتمده المشرع الجزائري لإقرار مسؤولية الشخص المدنية والمتمثل في الخطأ واجب الإثبات قد أكد قصوره وعدم كفايته في مواجهة إرهابات التطور التكنولوجي.¹

- ب- **الضرر كأساس للمسؤولية:** لا تقوم المسؤولية المدنية إلا بوجود ضرر حقيقي ومحقق أصاب شخصًا معينًا. والضرر الموجب للمسؤولية يجب أن يكون محقق الوقوع، شخصيًا ومباشرًا. غير أن الطبيعة اللامادية للبيانات الإلكترونية تجعل من الصعب أحيانًا إثبات وقوع الضرر بالمعنى التقليدي.²
- ج- **علاقة السببية في الفضاء الإلكتروني:** علاقة السببية هي الرابط الذي يصل بين الخطأ الذي ارتكبه المزور والضرر الذي أصاب الضحية. وفي البيئة الرقمية، يصبح إثبات هذه العلاقة أكثر تعقيدًا بسبب تعدد المتدخلين في العملية الرقمية، وصعوبة تتبع مصدر الفعل الضار، وسهولة تداخل الأسباب. ويتقضي تحقيق هذه العلاقة إثبات أن الفعل الضار الإلكتروني هو السبب المباشر والمنتظم للضرر.³
- ح- **المسؤولية العقدية مقابل المسؤولية التقصيرية:** تتميز المسؤولية العقدية عن التقصيرية في أنها تنشأ من الإخلال بالتزام ناشئ عن عقد، بينما تنشأ التقصيرية من الإخلال بالالتزام العام بعدم الإضرار بالغير. وفي المجال الرقمي، قد يلتقي النوعان في الواقعة الواحدة، كما لو قام المزور بتزوير توقيع إلكتروني في عقد مبرم عبر الإنترنت.⁴

¹ محمد مختار السيد، "المسؤولية المدنية الناشئة عن الضرر الإلكتروني عبر الإنترنت - دراسة تحليلية"، مجلة الإلكترونية الدولية لنشر البحوث القانونية، 25 أبريل 2023، <https://www.reiprj.com/2023-04/articles.htm>، تاريخ الاطلاع 13 ماي 2026.

² محمد عبد المنعم الزهيري، "التحديات القانونية أمام إثبات الضرر السيبراني في ظل تطور التكنولوجيا"، المجلة القانون، كلية الحقوق، جامعة المنصورة، المجلد 25، العدد 4، أوت 2025، ص 119.

³ حسام أحمد كيلاني، "الدليل الرقمي ومعوقات إثبات الجريمة الإلكترونية"، مجلة القانون والقضاء، المجلد 47، العدد 47، أكتوبر 2024، ص 750.

⁴ قارس بوبكر، مرجع نفسه، ص 15.

ثانياً: الضرر الرقمي وإثباته.

يُعتبر الضرر الرقمي من أكثر الإشكاليات تعقيداً في مجال المسؤولية المدنية الناشئة عن التزوير الإلكتروني، إذ أن الضرر هنا لا ينحصر في الخسارة المادية المباشرة، بل يتسع ليشمل أضراراً غير ملموسة قد تستمر آثارها لفترات طويلة.¹

أ- **أنواع الضرر الرقمي:** يمكن تقسيم الضرر الرقمي إلى نوعين رئيسيين: الضرر المادي والضرر المعنوي. فالضرر المادي يتمثل في كل خسارة مالية ملموسة كتحويل مبالغ مصرفية بناءً على وثيقة مزورة، بينما الضرر المعنوي يتمثل في الأذى الذي يصيب الشخص في سمعته أو كرامته، مثل تشويه السمعة عبر نشر وثائق مزورة على الإنترنت.²

ب- **إشكالية إثبات الضرر الرقمي:** يواجه إثبات الضرر الرقمي عقبات جوهرية ترتبط بطبيعة الأدلة في الفضاء الإلكتروني، فالبيانات الرقمية غير مادية ويمكن التلاعب بها بسهولة. ويترتب على ذلك أن الخصم الذي يدعي حصول ضرر رقمي يقع على عاتقه عبء إثبات ليس فقط وقوع هذا الضرر، بل أيضاً صلة الوثيقة المزورة بالضرر، ونسبة التزوير إلى شخص معين³ وتتفاقم هذه الصعوبات عندما يتعلق الأمر بالضرر المعنوي، إذ لا يترك أثراً مادياً يمكن قياسه بسهولة.

ج- **حجية الدليل الرقمي في الإثبات:** للمشرع الجزائري موقف واضح من حجية الدليل الرقمي، حيث نص في قانون الإجراءات المدنية والإدارية على قبول المحررات الإلكترونية كدليل. وتنص المادة 323 مكرر من القانون المدني على مبدأ قبول الإثبات الإلكتروني بنفس درجة قبول الكتابة على الورق، وإن ظل تطبيق هذا المبدأ رهيناً بتوفر شروط فنية متطورة.⁴

ح- **دور الخبرة التقنية في كشف التزوير وإثبات الضرر:** نظراً للطابع التقني للدليل الرقمي، برزت الحاجة الملحة إلى الاستعانة بالخبرة التقنية. فالخبير المتخصص يمكنه الكشف عن التعديلات، تتبع أصل التوقيع المزور، استعادة البيانات المحذوفة، وإعداد تقرير فني يفهمه القاضي. وقد أكدت الدراسات

¹ حسام أحمد كيلاني، مرجع سابق، ص 755.

² محمد مختار السيد، مرجع سابق ص 19.

³ مباركية تقي، فاطمة الزهراء غريبي، "دور الخبرة في إثبات المعاملات الإلكترونية"، مجلة العلوم الإنسانية، جامعة الإخوة منتوري قسنطينة، المجلد 33، العدد 2، 9 ماي 2022، ص 131.

⁴ حابت آمال، مرجع سابق، ص 66.

الحديث أن اشتقاق الأدلة الرقمية المطلوبة في إثبات الجرائم المعلوماتية هو أمر يضطلع به الخبراء المتخصصون.¹

ثالثاً: تقدير التعويض.

إذا تم إثبات أركان المسؤولية المدنية، يأتي الدور على تحديد التعويض الذي سيحكم به للمتضرر. والتعويض في قواعد القانون المدني هو إجراء يهدف إلى جبر الضرر وإعادة الضحية إلى الحالة التي كان عليها لو لم يقع الفعل الضار.²

أ- **مبدأ التعويض العادل:** يستند التعويض في القانون المدني إلى مبدأ أساسي مفاده أن التعويض يجب أن يكون عادلاً ومنصفاً، أي أنه يجب أن يعوض كل الأضرار التي لحقت بالضحية دون أن يشكل مصدرًا لإثراء غير مشروع. وفي مجال التزوير الإلكتروني، يتطلب هذا المبدأ تقديرًا دقيقًا للخسائر المباشرة وغير المباشرة.³

ب- **صعوبة تقدير الضرر المعنوي الرقمي:** تكمن الصعوبة الكبرى في تقدير التعويض عن الضرر المعنوي الرقمي، مثل تشويه السمعة أو المساس بالخصوصية. فالقاضي يتمتع بسلطة تقديرية واسعة في تحديد هذا التعويض، غير أن غياب معايير موضوعية واضحة يؤدي إلى تباين الأحكام وعدم الاتساق في التقدير.⁴

ج- **معايير تقدير التعويض:** يمكن للقاضي الاسترشاد بعدة معايير عند تقدير التعويض، منها: مدى انتشار الوثيقة المزورة، مدة استمرار الضرر، درجة الضرر الذي لحق بالضحية، تكاليف إصلاح الضرر واستعادة السمعة، وأرباح المزور إن أمكن تحديدها. كما يمكن اللجوء إلى خبراء لتقييم الأضرار التقنية والاقتصادية.⁵

ح- **إجراءات المطالبة بالتعويض:** تختلف إجراءات المطالبة بالتعويض حسب طبيعة المسؤولية. ففي المسؤولية العقدية، يرفع الفعل أمام القضاء العادي بناءً على العقد المبرم، أما في المسؤولية التقصيرية،

¹ محمد عبد المنعم الزهيري، مرجع سابق، ص 120.

² قارس بوبكر، مرجع سابق، ص 19.

³ محمد مختار السيد، مرجع سابق، ص 21.

⁴ حسام أحمد كيلاني، مرجع سابق، ص 758.

⁵ مباركية تقي، فاطمة الزهراء غريبي، مرجع سابق، ص 135.

فيحق للمتضرر رفع دعوى مباشرة أمام القضاء المدني. ويوصى في كلتا الحالتين بالاستعانة بأدلة رقمية وخبرة تقنية منذ البداية لضمان إثبات الضرر.¹

المطلب الثاني: صعوبات المتابعة القانونية في البيئة الرقمية.

إذا كانت المسؤولية المدنية عن التزوير الإلكتروني تثير إشكاليات تتعلق بإثبات الضرر وتقدير التعويض، فإن المتابعة القانونية نفسها -سواء على المستوى المدني أو الجنائي- تواجه صعوبات جوهرية ترتبط بطبيعة الفضاء الرقمي. فهذه الصعوبات لا تقتصر على الجانب التقني فحسب، بل تمتد لتشمل الجوانب القانونية المرتبطة بتحديد الفاعل الحقيقي، ومعضلة الاختصاص القضائي عندما تتوزع عناصر الجريمة على عدة دول، والطابع العابر للحدود الذي يجعل من الجريمة الإلكترونية ظاهرة عالمية يصعب احتوائها بإطار قانوني محلي. وهذه الصعوبات مجتمعة تشكل عقبة كأداء أمام تحقيق العدالة الفعالة في قضايا التزوير الإلكتروني.

أولاً: صعوبة تحديد الفاعل.

تعتبر مسألة تحديد الفاعل الحقيقي لجريمة التزوير الإلكتروني من أبرز التحديات التي تواجه أجهزة العدالة. ففي البيئة الورقية التقليدية، كان الفاعل يترك آثاراً مادية يمكن تتبعها: بصمات أصابع، خطوط يد، تواجد مادي في مكان التزوير. أما في البيئة الرقمية، فالأمر مختلف تماماً، إذ يمكن للمزور أن يخفي هويته بسهولة باستخدام تقنيات متعددة، مما يجعل الوصول إليه عملية شاقة ومعقدة.²

أ- إمكانية إخفاء الهوية الرقمية: تتميز الشبكة العنكبوتية بإتاحة الفرصة للمستخدمين للتفاعل دون الحاجة إلى الكشف عن هوياتهم الحقيقية. فالمزور يمكنه استعمال عناوين بروتوكول الإنترنت (IP) مزورة، أو استخدام شبكات خاصة افتراضية (VPN) تخفي عنوانه الحقيقي، أو اللجوء إلى متصفحات مجهولة مثل متصفح "تور" (Tor) التي تعيد توجيه الاتصال عبر عدة خوادم في دول مختلفة، مما يجعل تتبع مصدر الرسالة أو الوثيقة المزورة عملية بالغة الصعوبة.³

ب- انتحال الشخصية الرقمية واستعمال حسابات مزورة: كثيراً ما يرتكب المزورون جرائمهم عبر حسابات بريد إلكتروني مؤقتة أو حسابات وهمية على منصات التواصل الاجتماعي، يتم إنشاؤها ببيانات

¹ حابت آمال، مرجع سابق، ص 70.

² شيماء علوان حسن، "الصعوبات القانونية في مكافحة الجريمة الإلكترونية"، مجلة العلوم الإنسانية والطبيعية، 2024، ص 45.

³ هشام محمد مهدي صالح، د. محمد هاني فرحات، "الصور المستحدثة للجريمة الإلكترونية"، مجلة العلوم الإنسانية والطبيعية، 2026، ص 110.

غير صحيحة. وعند الانتهاء من الفعل الإجرامي، يتم التخلي عن هذه الحسابات نهائياً، دون ترك أي رابط يمكن تتبعه إلى الشخص الحقيقي. كما يمكن للمزور أن ينقل هوية شخص آخر، فيصدر التزوير وكأنه صادر عن ضحية بريئة.¹

ج- استخدام أدوات إلكترونية خارج نطاق السلطة القضائية: قد يستعين المزور بخوادم موجودة في دول لا تتعاون قضائياً، أو بخدمات سحابية تخضع لقوانين دولة أجنبية ترفض تسليم البيانات. وفي هذه الحالة، حتى لو تمكنت السلطات المحلية من تحديد هوية الفاعل نظرياً، فإنها تعجز عملياً عن الوصول إلى الأدلة أو توقيفه إذا كان يقيم في الخارج. كما أن استعمال العملات الرقمية المشفرة (مثل بيتكوين) في عمليات الاحتيال المرتبطة بالتزوير يضيف طبقة إضافية من الإخفاء.²

ح- دور الخبرة التقنية في كشف الفاعل: رغم هذه الصعوبات، فإن الخبرة التقنية المتخصصة (الطب الشرعي الرقمي) يمكنها أن تساهم في كشف الفاعل. فمن خلال تحليل البيانات الوصفية (Metadata) للملفات، وتتبع مسارات الاتصالات في سجلات الخوادم، وتحليل التوقيات الزمنية للعمليات، والبحث عن بصمات رقمية فريدة تركها المزور دون قصد، يمكن في كثير من الأحيان بناء سلسلة من الأدلة تقود إلى الشخص المسؤول. غير أن نجاح هذه العملية يتطلب توفر كوادر مؤهلة وأجهزة تقنية متطورة، وهو ما لا يتوفر دائماً في جميع الأجهزة القضائية.³

ثانياً: إشكالية الاختصاص القضائي.

تُعد إشكالية الاختصاص القضائي من أكثر الإشكاليات تعقيداً في مجال الجرائم الإلكترونية عامة، وجريمة التزوير الإلكتروني خاصة. فبينما تخضع الجريمة التقليدية لمبدأ إقليمية القانون الجنائي (أي أن الجريمة تحاكم وفق قانون المكان الذي ارتكبت فيه)، فإن الجريمة الإلكترونية قد تقع عناصرها في عدة دول مختلفة في آن واحد، مما يثير تساؤلات حول أي محكمة تختص بنظر الدعوى وأي قانون يتم تطبيقه.⁴

¹ حابس يوسف زيدات، مرجع ، ص 34.

² علي صاحب تقي، "حماية المستفيد من المخاطر الناشئة عن الدفع الإلكتروني دراسة مقارنة"، مجلة دجلة للعلوم، المجلد 1، العدد2، 2025، ص 12.

³ M. Tampubolon, "Digital face forgery and the role of digital forensics", International Journal for the Semiotics of Law, 2024.

⁴ شيماء علوان حسن، مرجع سابق، ص 49.

أ- **تعارض مبادئ الاختصاص القضائي التقليدي:** يستند الاختصاص القضائي التقليدي إلى ثلاثة معايير رئيسية: إقليمية الجريمة (مكان وقوع الفعل أو النتيجة)، وشخصية الفاعل (جنسيته)، وحماية المصلحة الوطنية. وفي الجريمة الإلكترونية، كثيرًا ما تتصادم هذه المعايير. فالمزور قد يكون في دولة "أ" (تخضع لاختصاصها الشخصي)، والخادم الذي حُزنّت عليه الوثيقة المزورة في دولة "ب" (اختصاص إقليمي)، والضحية التي تضررت في دولة "ج" (مكان النتيجة)، والوثيقة تم استخدامها في دولة "د". أي من هذه الدول يحق لها ممارسة الاختصاص؟ وهل يجوز لدول متعددة أن تطالب بمحاكمة نفس الشخص عن نفس الفعل؟¹

ب- **مبدأ الإقليمية الواقعي والافتراضي:** يحاول الفقه الحديث التكيف مع هذه المعضلة بتوسيع مفهوم الإقليمية. فبالإضافة إلى الإقليمية الواقعية (المكان المادي الذي توجد فيه أجهزة الحاسوب والخوادم)، ظهر مفهوم الإقليمية الافتراضية (أي مكان وصول تأثير الجريمة أو ظهور نتائجها). وبموجب هذا التوسع، تعتبر الدولة التي وقع فيها الضرر الفعلي مختصة بنظر الدعوى، حتى لو لم يقع فيها الفعل المادي المكون للجريمة. غير أن هذا الاتجاه يثير مخاوف من تضارب الاختصاصات وازدواجية الملاحقة.²

ج- **الاتفاقيات الدولية كآلية لتنسيق الاختصاص:** لم تغفل المنظمات الدولية أهمية معالجة هذه الإشكالية، فصدرت عدة اتفاقيات تحاول تنسيق قواعد الاختصاص القضائي في مجال الجرائم الإلكترونية. وأبرزها اتفاقية بودابست لمكافحة الجريمة المعلوماتية الصادرة عن مجلس أوروبا سنة 2001، والتي وقعتها العديد من الدول العربية وغير العربية. وقد نصت هذه الاتفاقية على التزام الدول الأطراف بتبني تشريعات داخلية تمكنها من ممارسة الاختصاص على جرائم معلوماتية معينة، كما نصت على آليات للتعاون القضائي الدولي تشمل تبادل الأدلة الرقمية وتحديد الاختصاص الأكثر ملاءمة في حالات التضارب.³

ح- **موقف المشرع الجزائري من الاختصاص القضائي:** لم يغفل المشرع الجزائري هذه الإشكالية، فقد نص في قانون العقوبات على توسيع نطاق الاختصاص القضائي ليشمل الجرائم المرتكبة خارج الحدود

¹ هشام محمد مهدي صالح، محمد هاني فرحات، مرجع سابق، ص 31.

² حابت أمال، مرجع سابق، ص 57.

³ محمد توفيق بابا، الإثبات الجنائي بالوسائل العلمية الحديثة، مجلة العلوم الإنسانية والطبيعية، المجلد 6، العدد 9، 1 سبتمبر 2025، ص 59.

الوطنية في حالات معينة. فالمادة 36 مكرر من قانون العقوبات تعطي الاختصاص للمحاكم الجزائرية لمحاكمة أي شخص ارتكب خارج التراب الوطني جريمة من الجرائم المنصوص عليها في القسم السابع مكرر (المساس بأنظمة المعالجة الآلية للمعطيات)، إذا كان الفاعل جزائرياً أو كانت الضحية جزائرية أو كان الفعل معاقباً عليه بقانون الدولة التي وقع فيها. كما أن المادة 37 مكرر تعطي الاختصاص للمحاكم الجزائرية إذا كان الفاعل موجوداً على التراب الوطني ولم يتم تسليمه. غير أن تطبيق هذه النصوص يظل مرهوناً بوجود تعاون قضائي دولي فعال.¹

ثالثاً: الطابع العابر للحدود للجريمة.

إذا كانت إشكالية الاختصاص القضائي تتعلق بتحديد أي محكمة تختص، فإن الطابع العابر للحدود لجريمة التزوير الإلكتروني يتعلق بصعوبة تنفيذ الإجراءات القانونية عندما تمتد الجريمة عبر أراضي عدة دول ذات سيادة. فالحدود الجغرافية، التي كانت تشكل حاجزاً طبيعياً أمام الجرائم التقليدية، تصبح شبه معدومة في الفضاء الرقمي، بينما تظل القيود المفروضة على السلطة القضائية لكل دولة قائمة ومحددة بترابها²

أ- **صعوبة جمع الأدلة الرقمية عبر الحدود:** تعتمد الجريمة الإلكترونية على أدلة رقمية (Digital Evidence) قد تكون موزعة على خوادم في دول متعددة. فلو قام مزور بتغيير وثيقة إلكترونية مخزنة على خادم سحابي يديره مزود خدمة في دولة ثالثة، فإن الحصول على نسخة من هذه الوثيقة أو على سجلات الاتصال بالخادم يتطلب التعاون مع سلطات تلك الدولة. غير أن هذا التعاون يأخذ وقتاً طويلاً عبر القنوات الدبلوماسية التقليدية (كإنبات القضاء الدولية)، وفي كثير من الأحيان ترفض الدول التعاون لأسباب سياسية أو قانونية (مثل قوانين حماية البيانات أو السيادة الوطنية). ونتيجة لذلك، تضيع الأدلة أو تتلف قبل أن يتمكن المحققون من الوصول إليها.³

ب- **تباين التشريعات الوطنية وعقبة التجريم المزدوج:** لكي تتم الملاحقة القضائية الدولية، يشترط في أغلب الأنظمة القانونية مبدأ "التجريم المزدوج" (Double Criminality)، أي أن الفعل يجب أن يكون معاقباً عليه في كل من دولة طلب التسليم ودولة طلب الملاحقة. غير أن تشريعات الدول تختلف في تعريفها للتزوير الإلكتروني وعقوباته. فما يعتبره قانون دولة تزويراً معلوماتياً قد لا يعتبره قانون دولة أخرى

¹ المواد 36 مكرر و 37 مكرر، الأمر رقم 66-156، من قانون العقوبات الجزائري.

² شيماء علوان حسن، مرجع سابق، ص 53.

³ هشام محمد مهدي صالح، محمد هاني فرحات، مرجع سابق، ص 36.

إلا مخالفة بسيطة، أو قد لا يكون مجرمًا أصلاً. هذا التباين يعطل إجراءات التسليم والتعاون القضائي، ويوفر ملاد آمنة للمزورين في دول ذات تشريعات ضعيفة في مجال الجرائم الإلكترونية.¹

ج- دور اتفاقية بودابست والتحديات المرتبطة بها: تعتبر اتفاقية بودابست لمكافحة الجريمة المعلوماتية (2001) النص الدولي الأكثر شمولاً في هذا المجال. وقد وضعت الاتفاقية آليات للتعاون السريع بين الدول الأعضاء، مثل طلب الحصول على بيانات مخزنة في خوادم دولة أخرى خلال فترة زمنية قصيرة، وإمكانية القيام بعمليات بحث وتفتيش عابرة للحدود بموافقة الطرف المعني. غير أن هذه الاتفاقية تعرضت لانتقادات عديدة، أبرزها أنها صيغت وفق رؤية الدول الغربية وتهمل خصوصية بعض الدول، وأن بعض موادها تسمح بانتهاك سيادة الدول. كما أن الجزائر ليست من الدول الموقعة على هذه الاتفاقية، مما يزيد من عزلة النظام القانوني الجزائري في مجال التعاون الدولي لمكافحة الجريمة الإلكترونية.²

ح- آليات التعاون القضائي الدولي المتاحة للجزائر: في غياب الانضمام إلى اتفاقية بودابست، تظل الجزائر مرتبطة بالآليات التقليدية للتعاون القضائي الدولي، وهي: المعاهدات الثنائية (مع بعض الدول العربية والأوروبية)، والاتفاقيات الإقليمية (مثل اتفاقية جامعة الدول العربية لمكافحة الجريمة المعلوماتية)، وقواعد القانون الدولي العام المتعلقة بالإنبابات القضائية والتسليم. غير أن هذه الآليات تثبت عدم كفاءتها في مواجهة جرائم تتم في ثوانٍ وتتطلب ردود فعل سريعة. لذلك، يطالب فقهاء القانون الجزائري بضرورة تطوير هذه الآليات وإبرام اتفاقيات جديدة تراعي خصوصية الجرائم الإلكترونية، أو على الأقل الانضمام إلى بعض أطراف اتفاقية بودابست المعدلة بما يتناسب مع المبادئ القانونية الجزائرية.

خ- ضرورة التنسيق الدولي في مكافحة التزوير الإلكتروني: في النهاية، لا يمكن لأي دولة بمفردها أن تتصدى بشكل فعال لجريمة التزوير الإلكترونية ذات الطابع العابر للحدود. والحل الأمثل يكمن في تعزيز التعاون الدولي على عدة مستويات: تبادل المعلومات والخبرات بين أجهزة التحقيق، وضع معايير تقنية مشتركة للأدلة الرقمية، تنسيق التشريعات الوطنية لتقليل فجوة التجريم، إنشاء شبكة اتصالات سريعة بين النيابة العامة لمكافحة الجرائم الإلكترونية (مثل شبكة 7/24 المنصوص عليها في اتفاقية

¹ حابت أمال، مرجع سابق، ص 75.

² محمد توفيق بابا، مرجع سابق، ص 40.

بودابست)، وأخيرًا تبني مواثيق دولية ملزمة تحدد قواعد الاختصاص والتعاون بشكل واضح وعادل للجميع.¹

المطلب الثالث: آليات الحماية القانونية والوقاية من التزوير الإلكتروني

إذا كانت الصعوبات العملية والمتابعة القانونية تشكل عقبات كبيرة في مواجهة جريمة التزوير الإلكتروني، فإن وضع آليات فعالة للحماية والوقاية يبقى الخط الدفاعي الأول للحد من هذه الظاهرة. فلا يقتصر دور القانون على تجريم الفعل ومعاقبة الفاعل، بل يمتد إلى وضع إطار وقائي يسبق وقوع الجريمة، ويشمل تنظيمًا دقيقًا لوسائل التوقيع الإلكتروني، وإلزام الجهات المعنية بتطبيق معايير أمنية صارمة، وتوعية المستخدمين بمخاطر التزوير الرقمي. وتتوزع هذه الآليات بين دور المشرع في سن القوانين، ودور الخبراء التقنيين في تطوير وسائل الحماية، ودور مؤسسات المجتمع المدني والسلطات العامة في نشر الوعي والمراقبة.

أولاً: دور التشريع.

يمثل التشريع العمود الفقري لأي سياسة جنائية تهدف إلى مكافحة التزوير الإلكتروني. فالنصوص القانونية هي التي تحدد الأفعال المجرمة، وتضع العقوبات الرادعة، وتنظم آليات الإثبات، وتلزم الجهات المعنية (كالبنوك وشركات التكنولوجيا ومزودي خدمات التصديق) باتخاذ تدابير أمنية محددة. غير أن مجرد وجود النصوص لا يكفي، بل يجب أن تكون هذه النصوص متطورة ومواكبة للتغيرات التقنية السريعة، ومتكاملة مع بعضها البعض، وقابلة للتطبيق الفعلي على أرض الواقع.²

أ- النصوص التشريعية المنظمة للتوقيع والتصديق الإلكترونيين: تعتبر القوانين المنظمة للتوقيع الإلكتروني من أهم أدوات الوقاية من التزوير، لأنها تحدد الشروط التي تجعل التوقيع الإلكتروني موثقاً به قانوناً، وبالتالي يصعب تزويره. وقد أصدر المشرع الجزائري القانون رقم 15-04 المؤرخ في 01 فبراير 2015، الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين. وينص هذا القانون على أن التوقيع الإلكتروني الموثوق (Qualifié) يجب أن يكون مرتبطاً بالموقع بطريقة فريدة، وأن يكون تحت سيطرة الموقع وحده، وأن تمكن أي تغيير لاحق في المحرر من كشفه. كما ينشئ القانون نظاماً للتصديق الإلكتروني، حيث تقوم هيئات مستقلة (مقدمو خدمات التصديق المعتمدون) بإصدار شهادات

¹ IO Krytska, "Digitization of the criminal process: Yesterday, today, tomorrow", Publishing House, "Baltija Publishing 2021, p38.

² حابت آمال، مرجع سابق، ص 88.

رقمية تثبت هوية الأشخاص وتضمن سلامة توقيعاتهم. والالتزام بالحصول على هذه الشهادات واستخدام الوسائل التقنية المعتمدة هو بمثابة درع وقائي يسبق أي معاملة إلكترونية.¹

ب- **قواعد الوقاية في القانون رقم 04-09:** خصص المشرع الجزائري القانون رقم 04-09 المؤرخ في 05 أوت 2009 لوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. ويتضمن هذا القانون نصوصاً وقائية هامة، منها إلزام مزودي خدمة الإنترنت ومشغلي شبكات الاتصالات بالاحتفاظ بسجلات الاتصالات والبيانات المروية لمدة زمنية محددة، ووضع أنظمة أمنية لحماية بيانات عملائهم. كما يلزم القانون المؤسسات التي تستخدم أنظمة معالجة آلية للمعطيات بأن تتخذ تدابير تقنية وتنظيمية كافية لحماية هذه الأنظمة من الاختراق والتلاعب. والإخلال بهذه الالتزامات الوقائية يعرض المسؤولين لعقوبات جنائية، وهذا ما يحفز المؤسسات على الاستثمار في الأمن السيبراني بشكل جدي.²

ج- **عقوبات رادعة كآلية ردع عام:** لا يمكن للوقاية أن تتجح بدون تهديد بعقوبات رادعة تثني أي شخص عن التفكير في ارتكاب جريمة التزوير الإلكتروني. وقد رصد المشرع الجزائري في القسم السابع مكرر من قانون العقوبات (المواد 394 مكرر إلى 394 مكرر 11) عقوبات تصل إلى السجن لمدة تتراوح بين سنتين وعشر سنوات، وغرامات مالية كبيرة تصل إلى ملايين السنت يما، حسب خطورة الفعل وظروفه. كما أجاز للقاضي توقيع عقوبات تكميلية كمنع المدان من ممارسة مهنة معينة، أو إغلاق الموقع الإلكتروني المستعمل في التزوير، أو مصادرة الأجهزة والبرمجيات المستعملة. وهذه العقوبات، إذا طبقت بفعالية، تشكل رادعاً قوياً للمزورين المحتملين.³

ح- **ضرورة مواكبة التشريع للتطور التكنولوجي:** يظل التحدي الأكبر أمام المشرع هو سرعة تطور وسائل التزوير التقنية مقارنة ببطء إجراءات سن القوانين وتعديلها. فعندما يصدر قانون لمكافحة التزوير الإلكتروني، قد تظهر بعده بفترة قصيرة تقنيات جديدة (كالذكاء الاصطناعي التوليدي الذي ينتج مستندات مزورة فائقة الواقعية) لم يأخذ بها القانون. لذلك، يوصي الفقهاء بأن تتضمن التشريعات أحكاماً مرنة تسمح بتوسيع نطاق التجريم عن طريق الإحالة إلى نصوص مرنة أو إلى معايير تقنية يتم تحديثها

¹ القانون رقم 15-04، المتعلق بالتوقيع والتصديق الإلكترونيين.

² المواد 394 مكرر إلى 394 مكرر 11، الأمر رقم 66-156، المتضمن قانون العقوبات.

³ لمواد 394 مكرر 3 إلى 394 مكرر 5 من قانون العقوبات الجزائري.

بقرارات وزارية أو تنظيمية، بدلاً من أن تظل النصوص جامدة تحتاج إلى تعديل تشريعي كل مرة. كما يوصى بإنشاء هيئات وطنية متخصصة تتابع تطور الجريمة الإلكترونية وتقتراح تحديثات دورية للتشريع.¹

ثانياً: الحماية التقنية.

لا يمكن للقانون وحده أن يحمي من التزوير الإلكتروني، بل لا بد من الاستعانة بالتقنيات الحديثة كخط دفاع أول. فالحماية التقنية تتمثل في مجموعة من الأدوات والبرمجيات والإجراءات الهندسية التي تجعل من الصعب جداً على المزور العادي اختراق النظام أو تزوير الوثيقة. وهذه الحماية تبدأ من مرحلة تصميم الأنظمة، وتمتد إلى مرحلة تشغيلها ومراقبتها بشكل مستمر.²

أ- التشفير كآلية أساسية لحماية البيانات: يعتبر التشفير (Cryptography الركنية الأساسية لأمن المعاملات الإلكترونية. فهو يحول البيانات من شكلها المقروء إلى شكل مشفر لا يمكن فهمه إلا بواسطة مفتاح خاص. وفي مجال التوقيع الإلكتروني، يستخدم التشفير غير المتماثل (بمفتاحين: عام وخاص) لتوقيع الوثائق: الموقع يستخدم مفتاحه الخاص لإنشاء توقيع فريد، والمستقبل يستخدم المفتاح العام للتحقق من صحة التوقيع. أي تغيير في الوثيقة بعد توقيعها يؤدي إلى إبطال هذا التوقيع. كما يستخدم التشفير لحماية الوثائق المخزنة (عند التخزين) وأثناء نقلها عبر الشبكات، مما يجعل اعتراضها أو تعديلها شبه مستحيل بدون المفاتيح المناسبة.³

ب- الشهادات الرقمية والبنية التحتية للمفاتيح العمومية (PKI): تعتمد سلامة التوقيع الإلكتروني على نظام متكامل يسمى البنية التحتية للمفاتيح العمومية (Public Key Infrastructure ويتكون هذا النظام من: جهة إصدار الشهادات (Certification Authority التي تتحقق من هوية الأشخاص وتصدر لهم شهادات رقمية، وجهة تسجيل (Registration Authority تتولى قبول الطلبات، ودليل إلكتروني (Directory ينشر الشهادات الصالحة، وقائمة إبطال الشهادات (CRL التي تسجل الشهادات الملغاة. وبموجب هذا النظام، يصبح أي شخص يريد التحقق من توقيع إلكتروني قادراً على

¹ شيماء علوان حسن، مرجع سابق، ص 60.

² S. Bourouis et al., "Recent advances in digital multimedia tampering detection for forensics, analysis", Symmetr, 2020, p 6.

³ S. Singh, R. Kumar, "Image forgery detection: comprehensive review of digital forensics, approaches", Journal of Computational Social Science, 2024, p38.

الرجوع إلى الجهة المصدرة للتأكد من أن الشهادة سليمة ولم يتم إبطالها. وهذا يشكل حماية قوية ضد محاولات انتحال الهوية أو تزوير التوقيعات.¹

ج- **تقنيات كشف التزوير والطب الشرعي الرقمي الاستباقي:** لطالما ارتبط الطب الشرعي الرقمي (Digital Forensics) بكشف الجرائم بعد وقوعها، لكن يمكن توظيف نفس التقنيات بصورة استباقية للوقاية.

فالمؤسسات التي لديها أنظمة مراقبة وتحليل للسلوك (Behavioral Analysis) يمكنها اكتشاف محاولات التزوير قبل اكتمالها. على سبيل المثال، إذا حاول شخص تعديل سجل في قاعدة بيانات باستخدام صلاحيات لا يمتلكها، أو إذا حاول توقيع وثيقة بتوقيع غير مطابق لمعايير النظام، يمكن للنظام أن يسجل هذه المحاولة وينبه المسؤولين، بل قد يمنع العملية برمتها. كما أن تقنيات "البصمة الرقمية" (Hashing) تُستخدم لإنشاء ملخص فريد للوثيقة عند إنشائها، وأي تغيير لاحق يغير هذا الملخص، مما يسمح باكتشاف التزوير بسهولة.²

ح- **تحديات الحماية التقنية وسلاح ذو حدين:** رغم فعالية هذه التقنيات، إلا أنها تواجه تحديات عديدة. أولها: التكلفة العالية لتطبيقها، خاصة على المؤسسات الصغيرة والمتوسطة. ثانيها: الحاجة إلى كوادر بشرية مدربة على تشغيل هذه الأنظمة وصيانتها. ثالثها: أن التقنيات نفسها قد تستخدم لارتكاب الجرائم (مثل استخدام التشفير من قبل المجرمين لإخفاء أدلتهم). رابعها: أن تطور تقنيات القرصنة والتزوير (مثل هجمات "الرجل في الوسط" أو استخدام الذكاء الاصطناعي لنسخ التوقيعات) يتطلب تحديثاً مستمراً لوسائل الحماية. لذلك، لا توجد حماية تقنية مطلقة، لكن الهدف هو رفع مستوى الصعوبة على المزورين إلى درجة تجعل الجريمة غير مجدية اقتصادياً أو تقنياً.³

¹ محمد توفيق بابا، ص 120..

² مباركية، مرجع سابق، ص 134.

³ علي صاحب تقي، مرجع سابق، ص 22.

ثالثاً: دور التوعية والرقابة.

إذا كانت التشريعات والوسائل التقنية تشكل خطوط الدفاع الأولى، فإن العنصر البشري يظل الحلقة الأضعف في أي نظام حماية. فمعظم حوادث التزوير الإلكتروني لا تحدث عن طريق اختراق تقني معقد، بل عن طريق استغلال ثقة المستخدمين أو جهلهم بالإجراءات الأمنية (مثل هجمات الهندسة الاجتماعية). لذلك، تأتي أهمية التوعية والتكوين والرقابة كآليات وقائية لا تقل أهمية عن القوانين والتقنيات.¹

أ- **توعية المستخدمين والمتعاملين مع الأنظمة الرقمية:** يجب أن تشمل حملات التوعية جميع فئات المجتمع: الموظفين في المؤسسات العامة والخاصة، العملاء الذين يجرون معاملات مصرفية إلكترونية، التجار الذين يستخدمون منصات التجارة الإلكترونية، وحتى عامة الناس الذين يستخدمون البريد الإلكتروني والتطبيقات اليومية. وتتناول هذه التوعية مواضيع مثل: كيفية التعرف على رسائل التصدي الاحتيالي (Phishing) التي تحاول الحصول على بيانات الدخول، وأهمية عدم مشاركة المفاتيح الخاصة أو كلمات المرور مع أي شخص، وضرورة التحقق من صحة الشهادات الرقمية للمواقع قبل إدخال بيانات حساسة، وكيفية الإبلاغ عن المشتبه به. ويمكن تنفيذ هذه التوعية عبر وسائل متعددة: دورات تدريبية، نشرات توعوية، فيديوهات قصيرة، حملات على وسائل التواصل الاجتماعي.²

ب- **تكوين الكوادر القانونية والقضائية:** لا يكفي توعية المستخدمين العاديين، بل يجب أيضاً تكوين القضاة والمحامين وأعضاء النيابة العامة وأعوان الضبط القضائي بشكل مستمر في مجال الجرائم الإلكترونية والأدلة الرقمية. فالقاضي غير الملم بأساسيات التوقيع الإلكتروني أو التشفير أو آثار الدليل الرقمي قد يصدر أحكاماً غير صحيحة أو يرفض أدلة رقمية سليمة بحجة عدم فهمها. لذلك، توصي الدراسات بتضمين وحدات دراسية حول الجريمة الإلكترونية في مناهج المعاهد القضائية وكلليات الحقوق، وتنظيم دورات تدريبية متقدمة للقضاة الممارسين، وإنشاء نيابات وقاعات متخصصة في الجرائم المعلوماتية.³

ت- **دور هيئات الرقابة الوطنية:** تلعب هيئات الرقابة دوراً محورياً في الوقاية من التزوير الإلكتروني. ففي الجزائر، هناك عدة هيئات تتدخل في هذا المجال: السلطة الوطنية لحماية المعطيات الشخصية

¹ هشام محمد مهدي صالح، محمد هاني فرحات، مرجع سابق، ص 45.

² شيماء علوان حسن، مرجع سابق، ص 58..

³ حابت أمال، مرجع سابق، ص 88.

(التي تراقب كيفية جمع وتخزين البيانات)، وكالة التصديق الإلكتروني (التي تشرف على نشاط مقدمي خدمات التصديق وتضع معايير الأمان)، ومركز الجزائر للأمن المعلوماتي (المسؤول عن حماية الأنظمة الحكومية الحساسة)، بالإضافة إلى هيئة ضبط البريد والاتصالات السلكية واللاسلكية التي تراقب مزودي الخدمة. وتقوم هذه الهيئات بإجراء تفتيش دوري، وإصدار توصيات، وفرض عقوبات إدارية على المؤسسات التي لا تلتزم بالمعايير الأمنية، مما يخلق بيئة وقائية منظمة.¹

ث- **التعاون بين القطاعين العام والخاص في الرقابة:** لا تستطيع جهات الرقابة الحكومية بمفردها مراقبة كل الأنشطة الرقمية، خصوصاً في القطاع الخاص. لذلك، من الضروري إقامة شراكة بين الحكومة والقطاع الخاص (شركات التكنولوجيا، البنوك، مشغلو الاتصالات) لتبادل المعلومات حول التهديدات الجديدة، وتطوير معايير أمنية مشتركة، والإبلاغ عن حوادث التزوير فور اكتشافها. بعض الدول أنشأت ما يسمى بـ "مراكز الاستجابة للطوارئ الحاسوبية" (CERT) التي تعمل كحلقة وصل بين الجهات الحكومية والخاصة، وتقوم بتنسيق جهود الاستجابة للحوادث ونشر التحذيرات الأمنية. والجزائر تمتلك "CERT-DZ" الذي يضطلع بهذا الدور، لكنه يحتاج إلى دعم أكبر وتفعيل أكثر على مستوى المؤسسات الخاصة.²

ج- **التحديات التي تواجه التوعية والرقابة:** رغم أهميتها، تواجه آليات التوعية والرقابة تحديات عديدة: نقص التمويل المخصص لحمالات التوعية، عدم تعاون بعض المؤسسات الخاصة بحجة السرية التجارية، صعوبة مواكبة التطور السريع للتهديدات، وانتشار ثقافة "الأمن ليس مسؤوليتي" بين المستخدمين. ولتجاوز هذه التحديات، لا بد من إرادة سياسية قوية، وميزانيات كافية، وتكامل الأدوار بين كل الأطراف، وإدراج مفاهيم الأمن الرقمي في المناهج التعليمية منذ المراحل المبكرة. يتبين من خلال ما سبق أن التوعية والرقابة تشكلان ركيزتين أساسيتين في مكافحة التزوير الإلكتروني، فالتوعية تهدف إلى الوقاية ونشر الثقافة الأمنية، بينما تساهم الرقابة في الكشف عن الجرائم وردع مرتكبيها، الأمر الذي يعزز الثقة في المعاملات الإلكترونية ويحمي الأمن المعلوماتي.

¹ حابت أمال، مرجع سابق، ص 89.

² القوانين المنشئة لهيئات الرقابة الجزائرية (القانون 04-09، القانون 04-15، أحكام تنفيذية).

خلاصة الفصل.

يعد التزوير الإلكتروني من الجرائم الخطيرة التي تهدد الثقة في المعاملات الرقمية والوثائق الإلكترونية، مما دفع المشرع إلى وضع قواعد قانونية لتنظيم المسؤولية المترتبة عنه جنائياً ومدنياً، من خلال تحديد الأشخاص المسؤولين عن الجريمة، سواء الفاعل الأصلي أو الشريك أو الشخص المعنوي مع إمكانية مساءلة مزودي خدمات التصديق الإلكتروني، إضافة إلى بيان العقوبات الأصلية والتكميلية والظروف المشددة المقررة لهذه الجريمة.

كما أبرز خصوصية إثبات في جرائم التزوير الإلكتروني، من خلال اعتراف بحجية المحررات الإلكترونية ووسائل الإثبات الرقمية، والتأكيد على أهمية الخبرة التقنية في كشف الجريمة وإثباتها. كما عالج المسؤولية المدنية الناتجة عن التزوير الإلكتروني، مبيناً أركانها والضرر الرقمي وطرق التعويض عنه. كما أكد على ضرورة تعزيز الحماية القانونية والتقنية واعتماد على التوعية والرقابة لمواجهة التزوير الإلكتروني وضمان أمن المعاملات الرقمية وحماية الثقة في البيئة الإلكترونية.

الخاتمة

الخاتمة:

في ختام هذه الدراسة الموسومة بعنوان المسؤولية القانونية للتزوير في المعاملات الرقمية والوثائق الإلكترونية، يتضح أن التطور التكنولوجي أدى إلى انتشار الواسع للمعاملات الرقمية والاعتماد المتزايد على الوثائق الإلكترونية في مختلف المجالات، الأمر الذي ساهم في تسهيل التواصل وإنجاز المعاملات بسرعة ودقة، لكنه في المقابل أفرز صورا جديدة من الجرائم المعلوماتية، وعلى رأسها جريمة التزوير الإلكتروني التي أصبحت تشكل تهديدا حقيقيا لأمن المعلومات والثقة العامة في البيئة الرقمية.

وقد سعت هذه الدراسة إلى بيان الإطار القانوني للمسؤولية المترتبة عن التزوير في المعاملات الرقمية والوثائق الإلكترونية، من خلال توضيح مفهوم التزوير الإلكتروني وصوره المختلفة، وتحليل أركانه، إضافة إلى دراسة المسؤولية الناجمة عنه سواء كانت جزائية أو مدنية، مع إبراز دور التشريع الجزائري في توفير الحماية القانونية للوثائق والمعاملات الرقمية.

من خلال تحليل النصوص القانونية المنظمة للجرائم المعلوماتية والتوقيع والتصديق الإلكتروني، خاصة القانون رقم 04-09 المتعلقة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، والقانون رقم 04-15 المتعلق بالتوقيع والتصديق الإلكترونيين، إضافة إلى القانون رقم 24-02 المتعلق بمكافحة التزوير واستعمال المزور، وقانون العقوبات الجزائري، تبين أن المشرع الجزائري قد حاول مواكبة التطورات التقنية من خلال إقرار حماية قانونية للمحررات الإلكترونية وتجريم مختلف صور التزوير الرقمي.

وبناء على ذلك يمكن القول أن المشرع الجزائري نجح إلى حدّ معتبر في تنظيم المسؤولية القانونية للتزوير في المعاملات الرقمية والوثائق الإلكترونية، غير أن هذا النجاح يبقى نسبيا في ظل التطور السريع للتقنيات الحديثة وتعقد الجرائم الإلكترونية، مما يستوجب تطوير التشريعات وآليات الإثبات الرقمي وتعزيز الكفاءة التقنية والبشرية لضمان حماية أكثر فعالية للمعاملات والوثائق الإلكترونية.

أولا: نتائج الدراسة.

1- يعد التزوير في المعاملات الرقمية من أخطر الجرائم الإلكترونية التي تمس الثقة العامة وأمن المعلومات.

2- اعترف المشرع الجزائري بالمحرر الإلكتروني ومنحه الحجية القانونية متى استوفى الشروط القانونية والتقنية اللازمة.

3- ساهم القانون رقم 04-09 في تنظيم التوقيع والتصديق الإلكترونيين وتعزيز الثقة في البيئة الرقمية.

4- وسّع المشرع الجزائري نطاق التجريم ليشمل صور التزوير الواقعة على الوثائق والبيانات الإلكترونية.

5- تقوم المسؤولية القانونية عن التزوير الإلكتروني على توفر الأركان القانونية للجريمة وما يترتب عنها من أضرار.

6- تواجه الجهات القضائية صعوبات في إثبات جرائم التزوير الإلكتروني بسبب الطابع التقني للأدلة الرقمية.

7- يعتمد كشف جرائم التزوير الإلكتروني على الخبرة الفنية والتقنيات الحديثة في التحليل الرقمي.

8- مازال الحماية القانونية للوثائق الإلكترونية بحاجة إلى تطوير مستمر لمواكبة التطورات التقنية الحديثة.

ثانيا: الاقتراحات.

1- ضرورة تحديث النصوص القانونية المتعلقة بالجرائم الإلكترونية بشكل مستمر لمواكبة التطورات التقنية الحديثة.

2- تعزيز التكوين المتخصص للقضاة وأعوان الضبط القضائي في مجال التحقيق في الجرائم المعلوماتية.

3- إنشاء هيئات ومخابر متخصصة في فحص وتحليل الأدلة الرقمية والكشف عن جرائم التزوير الإلكتروني.

4- تدعيم أنظمة الحماية المعلوماتية والتشفير لضمان سلامة الوثائق والمعاملات الرقمية.

5- نشر الوعي القانوني والتقني لدى الأفراد والمؤسسات حول مخاطر التزوير الإلكتروني ووسائل الوقاية منه.

6- تعزيز التعاون الدولي وتبادل المعلومات والخبرات في مجال مكافحة التزوير الإلكتروني.

7- تطوير آليات الإثبات الرقمي وتوحيد الإجراءات التقنية والقانونية المتعلقة بجمع الأدلة الإلكترونية وحفظها.

8- تشديد الرقابة والعقوبات على الجرائم التي تستهدف قواعد البيانات والوثائق الإلكترونية والأنظمة المعلوماتية.

المصادر والمراجع

قائمة المصادر والمراجع

أولاً: المصادر

1- القوانين:

- قانون رقم 82-04 المؤرخ في 13 فيفري 1982، المتضمن قانون العقوبات. المادة 41،
- قانون رقم 05-02، المؤرخ في 06 فبراير 2005، المعدل والمتمم لأمر رقم 75-59 مؤرخ في 26 سبتمبر 1975، المتضمن القانون التجاري، الجريدة الرسمية، العدد 11، 2005.
- قانون رقم 15-04 المؤرخ في 01 فبراير 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، الجريدة الرسمية، عدد 06، 2015.
- قانون رقم 24-02 المؤرخ في 26 فيفري 2024، يتعلق بمكافحة التزوير واستعمال المزور، الجريدة الرسمية، عدد 15، 2025.
- قانون رقم 5-04 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكتروني في الجزائر.
- قانون رقم 09-04، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، المؤرخ في 05 أوت، 2009، العدد 47، الجريدة الرسمية.
- قوانين المنشئة لهيئات الرقابة الجزائرية (القانون 09-04، القانون 15-04، أحكام تنفيذية).
- قانون رقم 05-10، المتضمن القانون المدني، المؤرخ في 20 جوان 2005 المعدل والمتمم للأمر رقم 75-58 المؤرخ في 26 سبتمبر 1975، العدد 44، الجريدة الرسمية.

- الأوامر:

- الأمر رقم 66-155 المؤرخ في 8 يونيو 1966 المتضمن قانون الإجراءات الجزائية، المعدل والمتمم، الجريدة الرسمية.
- الأمر رقم 66-156 المؤرخ في 8 يونيو 1966 المعدل والمتمم، المتضمن قانون العقوبات الجزائي، المواد 36 مكرر و 37 مكرر، المادة 42، المادة 51، المادة 394 مكرر، مكرر 1، مكرر 2، مكرر 3، مكرر 4، مكرر 5، مكرر 6، الجريدة الرسمية.

ثانياً: كتب:

- أحسن بوسفيعة، الوجيز في القانون الجنائي الخاص (الجرائم ضد الثقة العامة)، دار هومة، الجزائر، 2022.
- أحسن بوسقيعة، الوجيز في القانون الجزائري العام، الطبعة الثامنة عشرة، دار هومة، د. ب. ن، 2019.
- أحسن بوسقيعة، الوجيز في القانون الجنائي العام، الديوان الوطني للأشغال التربوية، الجزائر، 2002.
- أحمد خليفة الملط، الجرائم المعلوماتية، الطبعة 2، دار الفكر الجامعي، الإسكندرية، مصر، 2006.
- بلحاج العربي، أبحاث ومذكرات في قانون والفقہ الإسلامي، ديوان المطبوعات الجامعية، بن عكنون، الجزائر، 1996.
- بوبتر عبد المنعم وبن شيخ وليد، أثر التزوير على التعاقد الإلكتروني، جامعة برج بوعريج، الجزائر، 2022.
- جمال نجيمي، جرائم التزوير في قانون العقوبات الجزائري، دون طبعة، دار هومة، الجزائر، 2013.
- جميل عبد الباقي الصغير، جرائم تزوير المستندات المكتوبة بالحاسب الآلي، دار النهضة العربية، القاهرة، مصر، 2001.
- حابس يوسف زيدات، "مدى استيعاب النصوص التقليدية للسرقة الإلكترونية - دراسة مقارنة"، Rule of Law and Anti-Corruption Center Journal، 2019.
- خالد ممدوح إبراهيم، التزوير في المحررات الإلكترونية، دار الفكر الجامعي، الإسكندرية، مصر، 2008.
- رياض فتح الله بصله، جرائم بطاقة الائتمان، دار الشرق، بيروت، لبنان، 1995.
- سرور أحمد فتحي، الوسيط في قانون العقوبات، القسم الخاص، طبعة 4، دار النهضة العربية، 1991.
- طهاري عبد الله، الحماية الجنائية للمحررات الإلكترونية، جامعة تلمسان، الجزائر، 2016.

- عبد الرحمن عبد الله حميد آل علي، جرائم التزوير المعلوماتي، الطبعة الأولى، دار حائل للطباعة والنشر، سوريا، 2009.
- عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت دراسة عملية في جرائم الحاسوب الآلي والإنترنت، طبعة 1، دار الكتب القانونية، القاهرة، مصر، 2005.
- عبد الله بن سعود محمد السراني، فاعلية الأساليب المستخدمة في إثبات جريمة التزوير الإلكتروني، الطبعة 1، دار جامعة نايف العربية للعلوم الأمنية، المملكة العربية السعودية، 2011.
- عمر بن يونس، المسؤولية الجزائية عن الجرائم المعلوماتية، دار هومة، الجزائر.
- محمد الأمين البشري، التحقيق في الجرائم المستحدثة، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، 2004.
- محمد صلاح وشادي حمادة، البيانات الرقمية في مصر دراسة قانونية تحليلية، مجلة الدراسات القانونية والاقتصادية، 2025.
- ممدوح عبد الحميد عبد المطلب، الجرائم المعلوماتية، دار الكتب القانونية، مصر، 2005.
- مهند فايز الدويكات وحسين محمد الشبلي، صور الاحتيال والتزوير في البطاقات الائتمانية، جامعة نايف العربية للعلوم الأمنية، 2013.
- نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة 3، دار الثقافة للنشر والتوزيع، الأردن، 2010.

ثالثاً: الأطروحات والمذكرات:

– الأطروحات:

- حفصي عباس، جرائم التزوير الإلكتروني، أطروحة مقدمة لنيل شهادة الدكتوراه، كلية العلوم الإنسانية والعلوم السياسية، جامعة وهران، الجزائر، 2014.
- طهاري عبد الله، الحماية الجنائية للمحررات الإلكترونية في التشريع الجزائري، أطروحة دكتوراه، جامعة تلمسان، الجزائر، 2016.
- قارس بوبكر، "المسؤولية المدنية في مجال المعاملات الإلكترونية"، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة باتنة، 2021.

- الهام بن خليفة، الحماية الجنائية للمحررات الإلكترونية من التزوير، أطروحة الدكتوراه، كلية الحقوق والعلوم السياسية، جامعة باتنة، الجزائر، 2016.

- الرسائل ماجستير:

- الجبوري عمر عبد السلام حسين، جريمة التزوير الإلكتروني في التشريع الأردني، رسالة ماجستير، جامعة الشرق الأوسط، الأردن، 2017.
- حفصي عباس، جرائم التزوير الإلكتروني، رسالة دكتوراه جامعة وهران، كلية الحقوق والعلوم السياسية، قسم الحقوق، الجزائر، 2015.
- رسالة دكتوراه، وصف البيانات الرقمية - دراسة تقويمية، المجلة العربية للمعلوماتية وأمن المعلومات، 2021.

- المذكرات ماستر:

- سفيان بن صويلح، مكافحة التزوير واستعمال المزور في ظل القانون 24-02، مذكرة مكملة لمتطلبات نيل شهادة ماستر في قانون، كلية الحقوق، جامعة 08 ماي 1945، قالمة، الجزائر، 2025.
- عبد القادر هوارى، المسؤولية المدنية المترتبة عن المعاملات الرقمية، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة عين تيموشنت.

رابعاً: المقالات العلمية:

- امل خلف الحباشنة، الحماية المعلوماتية للمحاكمة عن بعد، مجلة العلوم الإنسانية والطبيعية، 2022.
- بلخير بلحاج، "حجية التوقيع الإلكتروني في الإثبات (الضوابط والشروط)"، مجلة القانون والعلوم السياسية، كلية الحقوق والعلوم السياسية، المركز الجامعي تندوف، المجلد 3، العدد 2، 2017.
- بن مسعود وبوطيمة، القصد الجنائي في الجرائم المعلوماتية، مجلة جامعة غرداية للعلوم القانونية، الجزائر، 2022.
- الثنيان رياء، جريمة التزوير المعلوماتية - دراسة مقارنة، مجلة البحوث الفقهية والقانونية، العدد 46، السعودية، 2024.

- حابت أمال، "الجريمة المعلوماتية في التشريع الجزائري: بين قانوني 04-15 و 09-04"، مجلة هيروودوت للعلوم الإنسانية والاجتماعية، جامعة مولود معمري، الجزائر، المجلد 7، العدد 25، 2023.
- حسام أحمد كيلاني، "الدليل الرقمي ومعوقات إثبات الجريمة الإلكترونية"، مجلة القانون والقضاء، المجلد 47، العدد 47، أكتوبر 2024.
- رياء بنت عبد الرحمن الثنيان، القصد الجنائي في جريمة التزوير المعلوماتية دراسة مقارنة، مجلة كلية الشريعة والقانون بتفهننا الأشرف، المجلد 29، العدد 9، ديسمبر 2024، جامعة القصيم، المملكة العربية السعودية.
- زهيرة عبوب، المسؤولية المدنية لمقدم خدمات التصديق الإلكتروني، دراسة تحليلية القانون رقم 04-15، مجلة الدراسات القانونية المقارنة، كلية الحقوق والعلوم السياسية، جامعة حسيبة بن بوعلي، الشلف، المجلد 6، العدد 02، 27 ديسمبر 2020.
- شيماء علوان حسن، "الصعوبات القانونية في مكافحة الجريمة الإلكترونية"، مجلة العلوم الإنسانية والطبيعية، 2024.
- طه محمد إبراهيم، السلوك الاتصال وعلاقته بإدراك خصوصية البيانات الرقمية، المجلة العربية لبحوث الإعلام والاتصال، 2023.
- عبد الله بلقاسم، الطبيعة الخاصة لجريمة التزوير في المحررات الإلكترونية، مجلة الدراسات القانونية المقارنة، جامعة التكوين متواصل مركز تيزي وزو، المجلد 06، العدد 02، 2020/12/27.
- علي صاحب تقي، "حماية المستفيد من المخاطر الناشئة عن الدفع الإلكتروني دراسة مقارنة"، مجلة دجلة للعلوم، المجلد 1، العدد 2، 2025.
- غلاب عبد الحق، "خصوصية جريمة تزوير التوقيع الإلكتروني في التشريع الجزائري"، مجلة الدراسات القانونية والسياسية، المجلد 8، العدد 1، 2022.
- فرقد عبود العارضي، جريمة التزوير الإلكتروني-دراسة مقارنة، مجلة الكوفة للعلوم القانونية والسياسية، المجلد 1، العدد 13، د. ب. ن، 2012.
- فوزي عمارة، نبيهة قنفود، الخبرة التقنية في مجال إثبات الجريمة الإلكترونية، مجلة جامعة الأمير عبد القادر للعلوم الإسلامية، قسنطينة، المجلد 36، العدد 2، 13 أكتوبر 2022.

- فيصل نسيغة، عبير بعقيقي، الإثبات في الجرائم المعلوماتية على ضوء القانون 04-09، مجلة العلوم القانونية والسياسية، جامعة محمد خيضر بسكرة، المجلد 9، العدد2، 11 جوان 2018.
- مباركية تقي، فاطمة الزهراء غريبي، "دور الخبرة في إثبات المعاملات الإلكترونية"، مجلة العلوم الإنسانية، جامعة الإخوة منتوري قسنطينة، المجلد 33، العدد 2، 9 ماي 2022.
- محمد الأمين شريط، "السياسة العقابية في جرائم تكنولوجيات الإعلام والاتصال في التشريع الجزائري"، مجلة القانون والمجتمع، جامعة أدرار، العدد 11، 2023.
- محمد توفيق بابا، الإثبات الجنائي بالوسائل العلمية الحديثة، مجلة العلوم الإنسانية والطبيعية، 2025.
- محمد توفيق بابا، الإثبات الجنائي بالوسائل العلمية الحديثة، مجلة العلوم الإنسانية والطبيعية، المجلد6، العدد 9، 1 سبتمبر 2025.
- محمد صلاح وشادي حمادة، البيانات الرقمية - دراسة قانونية تحليلية، مجلة الدراسات القانونية والاقتصادية، مصر، 2025.
- محمد عبد المنعم الزهيري، "التحديات القانونية أمام إثبات الضرر السيبراني في ظل تطور التكنولوجيا"، المجلة القانون، كلية الحقوق، جامعة المنصورة، المجلد25، العدد4، أوت 2025.
- محمد مختار السيد، "المسؤولية المدنية الناشئة عن الضرر الإلكتروني عبر الإنترنت - دراسة تحليلية"، مجلة الإلكترونية الدولية لنشر البحوث القانونية، 25 أبريل 2023، <https://www.reiprj.com/2023-04/articles.htm>، تاريخ الاطلاع 13 ماي 2026.
- مقال: المسؤولية الجنائية عن الجرائم التزوير الإلكتروني، دون طبعة، 1 سبتمبر 2025، د. ب. ن، أطلع بتاريخ 20 أبريل 2026 الساعة 02:30 <https://www.menafayq.com/criminal-responsibility-electronic-forgery-crimes>.
- نوال حاج مخناش، التعاون الدولي ومدى فعاليته في مكافحة جرائم تزوير بطاقات الدفع الإلكتروني، مجلة العلوم القانونية والسياسية، جامعة يحي فارس المدية، المجلد10، العدد01، 28 جانفي 2019.

- نورة مرابط، القصد الجنائي في جريمة التزوير المعلوماتي، مجلة الدراسات الحقوقية، العدد 02، جامعة تيبازة، الجزائر، 2019.
- نوي عبد النور، "مبدأ الموثوقية في ظل القانون 04/15 المتعلق بالتوقيع والتصديق الإلكترونيين"، مجلة صوت القانون، جامعة جيلالي بونعامة، خميس مليانة، المجلد 7، العدد 3، 28 ماي 2021.
- هشام بحوش، الجرائم المتصلة بتكنولوجيا الإعلام والاتصال في ظل التشريع الجزائري، مجلة الحقوق والعلوم السياسية، جامعة سوق أهراس، العدد 7، 2017.
- هشام محمد مهدي صالح، د. محمد هاني فرحات، "الصور المستحدثة للجريمة الإلكترونية"، مجلة العلوم الإنسانية والطبيعية، 2026.
- وصف البيانات الرقمية بمواقع مصادر الوصول الحر (الميتاداتا)، المجلة العربية للمعلوماتية وامن المعلومات، 2021.

خامسا: المراجع الأجنبية:

- S. Bourouis et al., "Recent advances in digital multimedia tampering detection for forensics, analysis", Symmetr, 2020.
- S. Singh, R. Kumar, "Image forgery detection: comprehensive review of digital forensics, approaches", Journal of Computational Social Science, 2024.
- M, Tampubalan, "**Digital face forgery and the role of digital forensic, international**", journal for the semiotics of law, 2024.
- Singh. R. Kamar, "**image forgery detection: comprehensive review of digital forensics approaches**", journal of computational social science, 2024, p15.
- IO Krystka, «Digitization of the criminal process: yesterday, today, tomorrow», publishing House Baltija publishing, 2021, p34.
- G. Varbanova, «**Electronic Documents as Electronic Evidence**», International journal of law changing world, 2025.

سادسا: المواقع الإلكترونية:

- Code pénal français dernière modification,9 juillet 2025
<https://www.legifrance.gouv.fr/codes/article-ic/LEGIARTI000006418753>. ساعة 03:49