



وزارة التعليم العالي والبحث العلمي
جامعة عباس لغرور - خنشلة -
كلية الحقوق والعلوم السياسية



قسم الحقوق

تزوير التوقيع الإلكتروني كجريمة إلكترونية مستحدثة

مذكرة مقدمة ضمن متطلبات نيل شهادة الماستر في الحقوق
تخصص: جنائي وعلوم جنائية

إشراف الأستاذ:

- د. عمراوي خديجة

إعداد الطالبة:

- ديار مريم

لجنة المناقشة

الاسم واللقب	الرتبة العلمية	الجامعة الاصلية	الصفة
هباز سناء	أستاذ محاضر - أ -	جامعة عباس لغرور - خنشلة -	رئيسا
عمراوي خديجة	أستاذ محاضر - أ -	جامعة عباس لغرور - خنشلة -	مشرفا ومقررا
كواشي نجوى	أستاذ محاضر - أ -	جامعة عباس لغرور - خنشلة -	عضوا مناقش

السنة الجامعية: 2025/2024

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

Class of
2025

شكر وتقدير

أتقدم بخالص الشكر وعظيم الامتنان إلى كل من
كان له الأثر الطيب في مسيرتي، وساندني في
كل خطوة بخالص نية ودعاء أو بكلمة طيبة أو
موقف لا يُنسى.

أخص بالشكر أساتذتي الكرام، الذين لم يبخلوا
بعلمهم وتوجيهاتهم، فكانوا نبراسًا أنار لي
الطريق، وزرعوا في نفسي حب الاجتهاد والسعي
نحو الأفضل. جزاكم الله عني خير الجزاء.

ولا يفوتني أن أتوجه بأسمى عبارات التقدير إلى
أخي العزيز، الذي كان سندًا لي في كل الظروف،
دعمه المتواصل وكلماته المشجعة كانت حافزًا
كبيرًا لي للاستمرار وعدم الاستسلام.

كما أتقدم باسمي معاني الشكر والتقدير لابن
خالي الذي ترك بصمة في هذا النجاح العظيم

شكرًا لكم جميعًا من القلب، ونسأل الله أن يوفقنا
وإياكم لكل خير، وأن يجزيكم خير الجزاء على
كل ما قدمتموه.

مع خالص التحية والاحترام،
[مريم]



إِهْدَاء

إلى العزيز الذي حملت اسمه فخراً،
إلى من كلله الله بالهيبة والوقار،
إلى من حصد الأشواك عن دربي وزرع لي الراحة بدلاً منها،
إلى أبي...

لم يحن ظهره ما كان يحمله،
بل انحنى ليحملني، ومن أحلي انحنى..
وكنت أحجب عن نفسي رغباتها،
فكان يكشف عما أشتي الخجبا.
فشكراً لكونك أبي!

وإلى من علمتني الأخلاق قبل أن أعلمها،
إلى الجسر الصاعد بي إلى الجنة،
إلى اليد الخفية التي أزالته عن طريقي العقبات،
ومن ظلت دعواتها تحمل اسمي ليلاً ونهاراً...
أمي، محبوبتي وملهمتي.

وإلى من وهبني الله نعمة وجودهم،
إلى مصدر قوتي، وأرضي الصلبة، وجدار قلبي المتين...
إخوتي وأخواتي،

وإلى من إن ضاقت بي الدنيا وسعت بخطاهم،
وإن سقطت، كانوا أول من رفعوني بكلامهم،
إلى من رافقني بالقلب قبل الدرب،
أصحابي الأحبة...

طويث صفحة من التعب، وسجلت في تاريخي فخراً لا ينسى.
لم أعد أتساءل عن ملامح الوصول، فقد رأيتها في عيوني.
تلاشت غيوم التعب، وابتسم الأفق بعد عتمة الانتظار.
ها هي الخطى التي كانت تتعثر أحياناً،
قد وجدت مستقرها في قمة الإنجاز.
وبين طيات الطريق، تنفست سلاماً، وفرحاً، وامتناناً.



مقدمة

مقدمة:

بالنظر إلى الطفرة الهائلة التي عرفها العالم خلال العقود الأخيرة في مجالي الإعلام والاتصال، بفعل انتشار الحواسيب والهواتف الذكية وتوسع شبكات الإنترنت، باتت البشرية تعيش واقعا افتراضيا موازيا للعالم المادي، بل ويتفوق عليه أحيانا في السرعة والانتشار. فقد أصبحت أغلب التعاملات اليومية، سواء كانت تجارية أو إدارية أو خدمية أو حتى مالية، تتم بشكل إلكتروني لما توفره هذه الوسائل من مرونة وسرعة وتوفير للجهد والتكاليف. بل إن الإدارة الحديثة نفسها اتجهت نحو الرقمنة في إصدار الوثائق واتخاذ القرارات وإبرام العقود، الأمر الذي أفرز ضرورة اعتماد هوية إلكترونية لكل متعامل ضمن هذا الفضاء الرقمي، تضمن إثبات شخصه وتمكن من التحقق من صحة الإجراءات.

وفي هذا السياق، برزت أهمية التوقيع الإلكتروني كوسيلة قانونية لحماية المعاملات الرقمية وضمان مصداقيتها، لما له من دور في تأكيد هوية الأطراف وتثبيت التصرفات القانونية. غير أن هذا التقدم التكنولوجي، ورغم ما يحمله من فرص كبيرة في دعم الاقتصاد وتسهيل المعاملات، إلا أنه فتح الباب أمام أشكال جديدة من الجرائم، أفرزتها الإمكانيات التقنية المتاحة، وفي مقدمتها الجرائم الإلكترونية التي باتت تتطور بوتيرة موازية لتطور الوسائل الرقمية.

ومن بين أخطر تلك الجرائم المستجدة، نجد الاعتداءات على التوقيع الإلكتروني، والتي تأخذ صوراً متعددة كالتقليد أو التزوير أو الاختراق غير المشروع لقواعد البيانات والمنصات الخاصة بالتوقيع. وتتميز هذه الجرائم بالتعقيد الفني، وتتطلب مهارات تقنية عالية، كما تتسم بخطورة كبيرة نظرا لارتباطها المباشر بمصداقية المعاملات القانونية والإدارية، مما يجعلها من أخطر صور الاحتيال الرقمي.

ويزيد من حدة هذه الظاهرة عدم تقيدها بالحدود الجغرافية والسياسية، مما يشكل تحديًا كبيرًا أمام القوانين الوطنية التي غالبًا ما تعجز عن مواكبة تطوراتها السريعة والمتنوعة، سواء من حيث الأساليب أو الأدوات المستخدمة فيها.

وتتجلى خطورة تزوير التوقيع الإلكتروني في كونه يمس صلب الإثبات القانوني للمعاملات، وقد يؤدي إلى أضرار جسيمة تمس الأفراد والدولة على حد سواء، وتهدد سلامة النظام الإداري بأكمله. وتبرز أهمية تناول هذه الجريمة في الوقت الراهن، خصوصًا بعد أن شرعت السلطات العمومية في الجزائر في إطلاق خدمات التوقيع والتصديق الإلكترونيين، في ظل تفعيل التدرجي للقانون رقم 04-15 المنظم لهذه المجالات، بعد أن أقر المشرع الجزائري بالحاجة القانونية للتوقيع الإلكتروني، موازيا في آثاره للتوقيع الخطي التقليدي، رغم الاختلاف الجوهرى في طبيعتهما وآليات استخدامهما.

أهمية دراسة الموضوع :

تكتسي دراسة موضوع تزوير التوقيع الإلكتروني أهمية بالغة في ظل الانتشار الواسع للمعاملات الرقمية، مما يجعل فهم الإطار المفاهيمي للتوقيع الإلكتروني ضرورة أساسية، باعتباره وسيلة إثبات قانونية معترف بها في مختلف الأنظمة، شريطة استيفائه للضوابط التقنية والقانونية التي تكفل حجته أمام الجهات القضائية.

ومن خلال تحليل أركان جريمة تزوير التوقيع الإلكتروني، تتضح معالم هذه الجريمة المستحدثة التي تمس بمصادقية الوثائق الإلكترونية، حيث تقوم على تغيير الحقيقة بنية الإضرار أو تحقيق مصلحة غير مشروعة، مما يستدعي التدقيق في كل من الركن المادي والمعنوي لتوصيف الفعل بدقة قانونية.

كما تُبرز الدراسة أهمية اعتماد آليات إجرائية متخصصة، تعتمد على تقنيات الكشف الرقمي والتحليل الجنائي الإلكتروني، للكشف عن هذا النوع من الجرائم، والتي غالبًا ما

يصعب إثباتها بالطرق التقليدية، مما يتطلب تكوينًا خاصًا للجهات الأمنية والقضائية في التعامل مع الأدلة الرقمية.

وتتجلى أهمية الدراسة كذلك في الوقوف على العقوبات المقررة لهذه الجريمة، والتي تعكس حرص المشرع على حماية الثقة العامة في البيئة الرقمية، وردع كل من تسول له نفسه المساس بأمن المعاملات الإلكترونية، وذلك من خلال عقوبات رادعة تتراوح بين الغرامات والحبس، بل وقد تصل إلى إبطال المعاملات المتحصلة بالتزوير

أسباب اختيار الموضوع:

جاء اختيار موضوع تزوير التوقيع الإلكتروني نتيجة لعدة اعتبارات أكاديمية وعملية، أبرزها:

1. التحول الرقمي الكبير الذي تعرفه مختلف القطاعات، واعتماد التوقيع الإلكتروني كوسيلة أساسية في توثيق العقود والمعاملات، ما يستدعي دراسة المخاطر المرتبطة به، وعلى رأسها التزوير.

2. حداثة الموضوع نسبيًا، باعتباره من المواضيع القانونية المعاصرة التي لا تزال تحتاج إلى مزيد من البحث والتحليل، خاصة في ظل التطور المستمر للتكنولوجيا.

3. قلة الدراسات المتخصصة في هذا النوع من الجرائم الرقمية، رغم أهميته وخطورته، مما يفتح المجال للإسهام في سد هذا الفراغ العلمي.

4. تعقيد إثبات جرائم التزوير الإلكتروني وصعوبة اكتشافها بالطرق التقليدية، ما يفرض البحث في الآليات القانونية والتقنية المناسبة لمواجهتها.

5. الرغبة الشخصية في التعمق في الجرائم المعلوماتية وفهم الجوانب التقنية والقانونية المرتبطة بها، خصوصًا ما يتعلق بالأمن السيبراني وحماية المعاملات الإلكترونية.

الدراسات السابقة :

بالرغم من حداثة موضوع تزوير التوقيع الالكتروني إلا أنا هذا لا يمنع من وجود دراسات سابقة حول هذا الأخير من بينها:

1. براهيم حنان، جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية، أطروحة دكتوراه

علوم، جامعة محمد خيضر، بسكرة، الجزائر، 2015. وقسمت الدراسة إلى فصل تمهيدي وبابين، تمت الإشارة في الفصل التمهيدي إلى تأثير المعلوماتية على الأنظمة القانونية، أما الباب الأول خصص لدراسة الوثيقة المعلوماتية محل التزوير، في حين تناولت الباحثة في الباب الثاني الصيغ التشريعية في تجريم الوثيقة المعلوماتية.

2. شنين صالح، الحماية الجنائية للتجارة الإلكترونية (دراسة مقارنة)، أطروحة دكتوراه في القانون الخاص، جامعة أبو بكر بلقايد، تلمسان، الجزائر، 2013. حيث قدم هذه الدراسة من خلال بابين تحدث في الأول عن الحماية الجنائية الموضوعية للتجارة الإلكترونية من العمومية إلى الخصوصية، أما الباب الثاني فأبرز فيه مدى كفاية الحماية الاجرائية للتجارة الإلكترونية.

3. راضية مشري، جريمة تزوير التوقيع الالكتروني في التشريع الجزائري، جامعة 8 ماي 1945، قالمة، الجزائر، مقال منشور على حوليات جامعة قالمة للعلوم الاجتماعية والانسانية. العدد 20، جوان 2017، قسمت هذه الدراسة تقسيما ثنائيا، تضمن مبحثين رئيسيين، الأول بين التوقيع الالكتروني محل الجريمة، أما المبحث الثاني فتطرق إلى المدى الذي تنطبق فيه جرائم قانون العقوبات على جريمة تزوير التوقيع الالكتروني.

أهداف الدراسة:

يسعى البحث الى تحقيق الاهداف الآتية:

الوقوف على الاطار القانوني والمفاهيمي للتوقيع الالكتروني في التشريع الجزائري.

مدى إمكانية تطبيق النصوص العامة المتعلقة بجريمة التزوير على حالات التوقيع الإلكتروني.

الكشف عن القصور التشريعي الناتج عن غياب نصوص جزائية صريحة تعالج نزوير التوقيع الإلكتروني.

صعوبات البحث:

مما لا شك فيه أن كل عمل أو بحث تعثره بعض الصعوبات أو العراقيل، ولعل أهم الصعوبات التي إلتبسناها خلال بحثنا تكمن في:

-قلة المراجع المتخصصة في الجانب الإجرائي لجريمة تزويرالتوقيع الإلكتروني بحد ذاتها، فيما يقابلها وفرة المراجع المتعلقة بتزوير المحررات بصفة عامة .

-أن الموضوع يحتوي على جانبين مختلفين جانب قانوني وآخر مفاهيمي، حيث لا يمكن دراسة هذا الموضوع من الناحية القانونية فقط بل يجب أيضا التطرق إلى الجانب المفاهيمي له ومدى إمكانية تطبيق الآليات الاجرائية ذات الصلة بالموضوع .

منهج البحث:

للإحاطة بكل ما يتعلق بالموضوع ومحاولة للإجابة على الإشكالية المطروحة اعتمدنا على المناهج الآتية

- **المنهج الوصفي:** وهذا ما تقتضيه دراسة المفاهيم العامة، من خلال ذكر المفاهيم القانونية والفقهية للتوقيع الإلكتروني وبيان خصائصه وكذا أركانه .
- **المنهج التحليلي:** وهذا قصد تحليل آليات واجراءات والحلول التي وضعت لمكافحة جريمة تزوير التوقيع الالكتروني، وتحليلها بشكل من التفصيل ثم بيان الاستنتاجات بشأنها، ومن ثمة تقديم الحلول المناسبة

على ضوء ما توصل إليه الفقه والتشريع والقضاء المقارن.

كما تم الاستئناس بالمنهج المقارن، حيث تعرضنا إلى بيان موقف التشريعات المقارنة سواء اللاتينية

أو الأنجلوساكسونية من جريمة تزوير التوقيع الإلكتروني، وكذا توضيح الإجراءات التي اعتمدها مختلف التشريعات والأنظمة في مواجهة هذه الجريمة. هذا كمحاولة منا لسد الثغرات في النصوص القانونية

اشكالية البحث

بالنظر لأهمية التوقيع الإلكتروني في المعاملات المدنية عموماً والتجارية خصوصاً، وبالأخص فيما يتعلق بموضوع الحماية الجنائية التي أولاها المشرع لهذا الإجراء القانوني ومدى حجبه في الإثبات وعن هذه المشكلة يمكن أن نطرح التساؤل الآتي:

"إلى أي مدى يمكن اعتبار التزوير في التوقيع الإلكتروني جريمة معاقب عليها في ظل غياب نصوص قانونية صريحة في التشريع الجزائري، وما مدى كفاية النصوص العامة لمواجهة هذا النوع من التزوير الرقمي؟"

والذي بدوره انبثقت عنه أسئلة فرعية يمكن ادراجها فيما يلي:

1. ما هو المقصود بالتوقيع الإلكتروني؟ وما أنواعه وشروطه القانونية؟
2. ما هو الإطار القانوني المنظم للتوقيع الإلكتروني في الجزائر؟
3. هل يمكن اعتبار تزوير التوقيع الإلكتروني مشمولاً ضمن جريمة التزوير التقليدية المنصوص عليها في قانون العقوبات؟
4. ما هي التحديات القانونية والقضائية التي تعيق إثبات تزوير التوقيع الإلكتروني؟
5. هل التشريع الجزائري بحاجة إلى نصوص خاصة وصريحة لتجريم تزوير التوقيع الإلكتروني؟

خطة البحث:

قصد الإجابة على إشكالية البحث وتساؤلاته الفرعية، ارتأينا تقسيم الإجابة عليها وفق فصلين:

الفصل الأول: الإطار الموضوعي لجريمة تزوير التوقيع الإلكتروني، كما قسم هذا الفصل الى مبحثين الأول بعنوان ماهية التوقيع الإلكتروني، أما في المبحث الثاني فتم التطرق الى صور التوقيع الالكتروني وحجته، بعدها انتقلنا الى آليات الحماية القانونية للتوقيع الالكتروني، والذي بدوره انقسم الى مبحثين الأول جاء تحت عنوان الإطار الجزائي لجريمة تزوير التوقيع الالكتروني أما فخصص لبيان العقوبات المقررة لمرتكبي هذه الجريمة. وانتهى البحث بخاتمة تم فيها عرض أهم النتائج والتوصيات الخاصة بالموضوع.

الفصل الأول

الإطار الموضوعي لجريمة تزوير

التوقيع الإلكتروني

تمهيد:

مع تطور الوثائق الإلكترونية، برز التوقيع الإلكتروني كوسيلة أساسية لإثبات حجيتها وضمان حياتها القانونية ولتحقيق نفس الوظائف التي يؤديها التوقيع التقليدي، عملت التشريعات الوطنية والدولية على تحديد مفهوم التوقيع الإلكتروني.

وتم تقسيم الفصل الأول الى مبحثين.

المبحث الأول: ماهية التوقيع الإلكتروني.

تضمن المبحث الأول مطلبين أساسيين، تطرق الأول الى (تعريف التوقيع الإلكتروني)، أما الثاني فبين (آلية إنشاء التوقيع الإلكتروني).

المطلب الأول: تعريف التوقيع الإلكتروني.

حظي التوقيع الإلكتروني باهتمام واضح على مختلف التشريعات، مما أدى الى اختلاف التعاريف لهذا الأخير فقها وقانونا، لكن لم نجد أي إشارة إلى التوقيع الإلكتروني في قانون العقوبات الجزائري، لكن وبعد صدور القانون 15/04 الذي يحدد القواعد العامة للتوقيع والتصديق الإلكترونيين عرف التوقيع الإلكتروني، وقبل التطرق إلى التعريف التشريعي، لابد من التطرق إلى التعريف الفهمي.

الفرع الأول: تعريف التوقيع الإلكتروني.

أولا: التعريف الفقهي.

لم يثر تعريف التوقيع الإلكتروني جدلا في الفقه، إذ نجد أن معظم التعريفات الفقهية تدور حول فكرة واحدة، ألا وهي إظهار شكل التوقيع وبيان خصائصه، أما الاختلاف الذي وجد في تعريفاتهم فيكمن في اختلاف الزاوية التي ينظر إليها كل فقيه، فعرف التوقيع الإلكتروني على أنه: "اتباع إجراءات محددة تؤدي في النهاية إلى نتيجة معينة معروفة مقدما، فيكون مجموع هذه الإجراءات هو البديل للتوقيع التقليدي".¹

كما عرف على أنه: "ما يوضع على محرر الكتروني (شريحة الكترونية) ويتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها، ويكون له طابع متميز ومنفرد يسمح بتحديد الشخص الموقع ويميزه عن غيره".²

¹ المرسي، الزهرة محمد. عناصر الدليل الكتابي الإلكتروني التقليدي. دون ناشر، 2001، ص. 92.

² يوسف، أمير فرج. التوقيع الإلكتروني. دار المطبوعات الجامعية، 2008، ص. 14.

وعرف هذا النوع من التوقيعات بأنه: "طريقة اتصال مشفرة على توثيف المعاملات التي تتم عبر الانترنت".¹

وعرفه البعض الآخر بأنه: "ملف رقمي صغير يصدر عن إحدى الهيئات المتخصصة والمستقلة والمعترف بها من طرف الحكومة تماما مثل نظام الشهر العقاري، وفي هذا الملف يتم تخزين الاسم وبعض المعلومات الهامة الأخرى مثل الرقم التسلسلي وتاريخ انتهاء الشهادة ومصدرها".²

ومن خلال ما تم ذكره نستخلص أن الجانب الفقهي ركز على الكيفية التي ينشأ من خلالها التوقيع الإلكتروني كونه مجموعة من الرموز أو الإجراءات (آلية إنشاء التوقيع الإلكتروني)، ومن جهة أخرى على وظائفه ومميزاته من حيث إفادته في إثبات وحجية استعماله وإسناده لشخص معين، وموافقة من خلال توقيعه على ما يتضمنه السند الذي يحمل هذا الأخير.

ثانيا: التعريف التشريعي.

1/- في قانون الأونسيترال النموذجي:

تضمن هذا القانون إطارا عاما يوضح ملامح التوقيع الإلكتروني، لاسيما المادة (07) منه والتي جاء فيها: "إذا كان القانون يشترط وجود توقيع يستوفي ذلك الشرط بالنسبة إلى رسالة البيانات، إذا استخدمت طريقة لتعيين هوية ذلك الشخص والتدليل على موافقة ذلك الشخص على المعلومات الواردة في رسالة البيانات، أو كانت تلك الطريقة جديرة بالتعويل عليها بالقدر المناسب للغرض الذي أنشأت أو أبلغت من أجله رسالة البيانات في ضوء كل الظروف".³

¹ يوسف، أمير فرج. المرجع السابق، ص. 17.

² عجابي، إلياس. الطبيعة القانونية للتوقيع الإلكتروني. جامعة محمد بوضياف، المسيلة، ص. 256.

³ القرار رقم 51-162 المؤرخ في 16 ديسمبر 1996 المتضمن قانون الأونسيترال النموذجي للتجارة الإلكترونية، منشور

على الموقع: <http://www.uncitral.org>

بعدها تم تعريف التوقيع الإلكتروني من خلال قانون الأونيسترال النموذجي للتوقيعات الإلكترونية بنص المادة (02) منه والتي جاء فيها بأنه: "بيانات في شكل الكتروني مدرجة في رسالة البيانات ولبيان موافقة الموقع على المعلومات الواردة في رسالة البيانات".¹

2- في توجيهات الاتحاد الأوروبي:

تضمن التوجيه الأوروبي تعريف التوقيع الإلكتروني بنص المادة (02) منه والتي كان نصها: "التوقيع الإلكتروني يعني معلومة معالجة الكترونياً ترتبط منطقياً بمعلومات أو بيانات الكترونية أخرى كرسالة أو محرر، والتي تصلح وسيلة لتمييز الشخص وتحديد هويته"² كما أضافت المادة نفسها الفقرة الثانية تعريفاً للتوقيع الإلكتروني المتقدم (المؤمن) Advanced electronic signature عل أنه: "عبارة عن توقيع الكتروني يتضمن المتطلبات الآتية:

- مرتبط بشكل فردي (حصري) بصاحب التوقيع.
- قادر على تحديد هوية صاحب التوقيع.
- يتم إنشاؤه بالاعتماد على وسائل تضمن لصاحبها السرية التامة.
- مرتبط بالمعلومات التي تتضمنها الرسالة بكيفية تمكن من كشف أي تغيير يحصل على المعلومات.³

¹ القرار رقم 56-80 المؤرخ في 12 ديسمبر 2001 المتضمن قانون الأونيسترال النموذجي للتوقيعات الإلكترونية، منشور على الموقع: <http://www.uncitral.org/stable/m/-arba.pdf>

² التوجيه الأوروبي الصادر في 13 ديسمبر 1999، (نقلاً عن يوسف، أمير فرج. المرجع السابق، ص 370).

Article 2:

"1-Electronic signature means data is electronic from which are attached to or logically associated with other electronic data and which serve as method of authentication

³ التوجيه الأوروبي الصادر في 13 ديسمبر 1999، (نقلت عن يوسف، أمير فرج. المرجع السابق، ص 370).

Article 2:

" Advanced electronic signature means an electronic signature which meets the following requirements:

a-It is uniquely linked to the signatory.

b-It is capable of identifying the signatory.

3/- في القانون العربي الاسترشادي للإثبات بالطرق الحديثة:

عرف هذا القانون الذي تبنته الجامعة العربية وصادق عليه مجلس الوزراء العدل العرب بموجب القرار رقم 24/د/771 المؤرخ في 27 نوفمبر 2008، التوقيع الإلكتروني في مادته الأولى الفقرة (03) بأنه: " ما يوضع على محرر الكتروني ويتخذ شكل حروف أو أرقام أو إشارات أو غيرها، ويكون له طابع منفرد يسمح بتحديد شخص الموقع ويميزه عن غيره.¹"

4/- في التشريع الجزائري:

اعتد المشرع الجزائري بالتوقيع الإلكتروني لأول مرة بنص المادة 327/2 من القانون المدني، ومن ثم في القانون المتعلق بنظم الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية.²

وصولا إلى تعريف المشرع الجزائري للتوقيع الإلكتروني في قانون خاص بالتوقيع والتصديق الإلكترونيين حصرا، متمثلا في القانون 15-04، الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين.

اعترف المشرع الجزائري بالتوقيع الإلكتروني في القانون المدني في المواد 323 مكرر، 323 مكرر 1، و 327 ونصت المادة 323 مكرر المستحدثة بالقانون رقم 05-10 المؤرخ في 20-07-2005 على ما يلي: " ينتج الإثبات بالكتابة من تسلسل حروف أو أوصات أو أرقام أية علامات أو رموز ذات معنى مفهوم مهما كانت الوسيلة التي تتضمنها أو طرق إرسالها. "

c-t is created using means that the signatory can maintain under his sole control;and.
d-It is linked to the data to which it relates in such a manner that my subsequent change of the data is detectable.

¹ القانون العربي الاسترشادي للإثبات بالتقنيات الحديثة، معتمد بالقرار رقم 24/د/771 المؤرخ في 27 نوفمبر 2008.

² المرسوم التنفيذي رقم 07-162 المؤرخ في 30-05-2007، يعدل ويتمم المرسوم التنفيذي رقم 01-123 المؤرخ في 09-05-2001 .

ونصت المادة (323 مكرر 1) من القانون نفسه على أنه: "يعتبر الإثبات بالكتابة في الشكل الإلكتروني كالأثبات على الورق بشرط امكانية التأكد من هوية الشخص الذي أصدرها وأن تكون معدودة ومحفوظة في ظروف تضمن سلامتها."

أما المرسوم التنفيذي رقم 07-162 لسنة 2007، فقد عرف المشرع الجزائري التوقيع الإلكتروني من خلاله بنص المادة (03) منه التي أقرت: "التوقيع الإلكتروني هو معطى ينجم عن استخدام أسلوب عمل يستجيب للشروط المحددة في المادتين 323 مكرر، 323 مكرر 1".¹

أما تعريف المشرع الجزائري للتوقيع الإلكتروني من خلال القانون رقم (15-04) لسنة 2015 فقد كان بنص المادة (02) التي جاء فيها أن التوقيع الإلكتروني هو: "بيانات في شكل الكتروني، مرفقة أو مرتبطة منطقيا ببيانات إلكترونية أخرى تستعمل كوسيلة توثيق".²

الفرع الثاني: تمييز التوقيع الإلكتروني عن التوقيع التقليدي.

بعد النطرق إلى الإطار المفاهيمي للتوقيع الإلكتروني تبين لنا أن هذا الأخير لا يقوم إلا بعد اعتماد دعامات الكترونية، مما يجعله مميزا عن التوقيع التقليدي الذي يعتمد على الدعامة الورقية، كما أننا نجد أن التوقيع التقليدي محصورا قد يكون في شكل إمضاء أو في البصمة ختما أو إصبعيا باختلاف كل تشريع، على غرار التوقيع الإلكتروني الذي يمكن أن حروفا أو أرقاما أو حتى رموزا أو غيرها كونها تحدد هوية الموقع نقلا يمكن اعتبار التوقيع بالبصمة أو الختم في هذا التوقيع توقيعاً إلكترونياً.³

التوقيع التقليدي تزويره أو تقليده من قبل الغير لا يفرض على صاحبه عند اكتشاف التقليد أو التزوير تغيير شكل توقيعيه، بعكس صاحب التوقيع الإلكتروني، يجب عليه تغيير توقيعيه

¹ المادة 3 من المرسوم التنفيذي رقم 07-162 لسنة 2007.

² القانون رقم 15-04 المؤرخ في 01-02-2015 يحدد القواعد العامة المتعلقة بالوقيع والتصديق الإلكترونيين، الجريدة الرسمية للجمهورية الجزائرية، العدد 06، ص 07.

³ محروك، محمد. "خصوصيات التوقيع الإلكتروني وحجتيه في الإثبات". جامعة القاضي عياض، مراكش، ص. 7.

إن اكتشاف توصل الغير الى المنظومة التي تنشئه، كما أن التوقيع التقليدي لا يحتاج إلى أية وسيلة أخرى تثبت صحته، بينما التوقيع الإلكتروني غير المصدق بشهادة إلكترونية يقع على عاتق صاحبه إثبات موثوقية صاحبه وإثبات المنظومة التي تنشئه¹.

ومنه يمكننا تبين خصائص جريمة تزوير التوقيع الإلكتروني، والتي تتمثل في:

- يعتبر التوقيع الإلكتروني جزءاً من عقد الكتروني أو قرار إداري الكتروني أو أي تصرف آخر فإذا أثبتنا مشروعية المتصرف، أثبتنا معه سلامة وصحة التوقيع الإلكتروني، وبهذا فإن التوقيع الإلكتروني يحقق وظيفة التوقيع الكتابي أو العادي².
- أن يكون التزوير مرتبطاً بشخص واحد يسمح بتعيينه وأن يتم التوقيع من خلال وسائل الكترونية تخضع للسيطرة المباشرة من صاحب التوقيع التي توضح ارتباط هذا الشخص بمضمون التوقيع، وأهدافه وبالتالي فإن التوقيع الإلكتروني يمتاز بالاستقلالية فلا يمكن أن يحمل شخص وآخر ذات التوقيع الإلكتروني³.
- يمتاز التوقيع الإلكتروني بالأمان والسرية التي تحقق من خلاله، حيث لا يمكن لأي شخص مهما كان الاطلاع عليه إلا في حالات القرصنة والاختراق للخصوصية، وهذا ما قام القانون الأردني بتجريمه من خلال قانون الجرائم الإلكترونية، والذي أقرت به المادة 5 من التوجيه الأوروبي بشأن التوقيعات الإلكترونية⁴.

¹ بوكر، رشيدة. "التوقيع الإلكتروني في التشريع الجزائري (دراسة مقارنة)". جامعة عبد الحميد بن باديس، العدد 4، ديسمبر 2016، ص. 69.

² غلاب، عبد الحق. "خصوصية جريمة تزوير التوقيع الإلكتروني في التشريع الجزائري". مجلة الدراسات القانونية والسياسية، جامعة الجزائر 1، المجلد 8، العدد 1، جانفي 2022، ص. 493.

³ غربي، خديجة. التوقيع الإلكتروني. رسالة ماجستير، جامعة قاصدي مرباح، ص. 98.

⁴ نصت المادة 05 من التوجيه الأوروبي بشأن التوقيعات الإلكترونية لعام 1999 التي تنظم الآثار القانونية للتوقيعات الإلكترونية على أنه: "يجب على الدول الأعضاء أن تتأكد من أن التوقيعات الإلكترونية التي تعتمد على شهادات مؤهلة والتي تنشأ بواسطة أداة إنشاء توقيع آمنة، أنها تقي بالمطلوبات القانونية للتوقيع فيما يتصل بالبيانات في شكلها الإلكتروني على النحو نفسه الذي تستوفي به التوقيعات وأن تكون مقبولة كدليل إثبات في الإجراءات القانونية...".

المطلب الثاني: آلية إنشاء التوقيع الإلكتروني

حرص المشرع الجزائري على ضمان صحة التوقيع الإلكتروني بما يكفل له إحداث الأثر القانوني ذاته الذي يرتبه التوقيع التقليدي، وقد تجلّى ذلك من خلال وضع آلية دقيقة وواضحة لإنشاء التوقيع الإلكتروني، تتضمن مجموعة من الإجراءات التي تضمن حمايته وسلامته، وتعكس مدى موثوقية ارتباط معطيات التوقيع بصاحبه، وهو ما يمنحه حجية قانونية في الإثبات، مماثلة تماما لحجية التوقيع الخطي .

وعليه يتعين أن يستجيب التوقيع الإلكتروني لمعطيات إنشائه، ونصت على تلك المعطيات المادة 03 مكرر، الفقرة 4 من المرسوم (07-162) لسنة 2007، حيث عرفت بأنها: "العناصر الخاصة بالموقع مثل الأساليب التقنية التي يستخدمها الموقع نفسه لإنشاء التوقيع".¹

ولقد فصل القانون رقم (04-15) لسنة 2015 في آلية إنشاء التوقيع الإلكتروني من خلال تعريفه لكل من آلية وبيانات إنشاء التوقيع الإلكتروني على أنها: "بيانات فريدة مثل الرموز أو مفاتيح التشفير الخاصة التي يستعملها الموقع لإنشاء التوقيع"، كما عرفت الفقرة (04) من المادة نفسها آلية إنشاء التوقيع الإلكتروني بكونها: "جهاز أو برنامج معلوماتي معد لتطبيق بيانات إنشاء التوقيع الإلكتروني".

ومنه قد أفرد القانون رقم (04-15) لسنة 2015 فصلا كاملا منه حدد من خلاله متطلبات إنشاء التوقيع الإلكتروني بصفة مؤمنة، ومن ثم تحديد المتطلبات الآلية الموثوقة للتحقق من التوقيع الإلكتروني.

¹ المرسوم التنفيذي رقم 162-07 المؤرخ في 30-05-2007 المعدل والمتمم للمرسوم التنفيذي رقم 123_01 الصادر في 09-05-2001.

الفرع الأول: متطلبات آلية إنشاء التوقيع الإلكتروني.

ركزت المادة 10 من القانون (04-15) لسنة 2015 على ضرورة أن تكون آلية إنشاء التوقيع الإلكتروني مؤمنة حيث جاء فيها: "يجب أن تكون آلية إنشاء التوقيع الإلكتروني الموصوف مؤمنة ."

وحددت المادة 11 من هذا القانون المتطلبات التي تضمن لآلية إنشاء التوقيع الإلكتروني أن تكون مؤمنة والتي جاء فيها أن: "الآلية المؤمنة لإنشاء التوقيع الإلكتروني هي آلية إنشاء توقيع الكتروني تتوفر فيها المتطلبات الآتية:

1- يجب أن تضمن بواسطة الوسائل التقنية والإجراءات المناسبة على الأقل ما يأتي:

أ- ألا يمكن عمليا مصادفة البيانات المستخدمة لإنشاء التوقيع الإلكتروني إلا مرة واحدة، وأن يتم ضمان سريتها بكل الوسائل التقنية المتوفرة وقت الاعتماد.

ب- ألا يمكن إيجاد البيانات المستعملة لإنشاء التوقيع الإلكتروني عن طريق الاستنتاج، وأن يكون هذا التوقيع محميا من أي تزوير عن طريق الوسائل التقنية المتوفرة وقت الاعتماد .

ج- أن تكون البيانات المستعملة لإنشاء التوقيع الإلكتروني محمية بصفة موثوقة من طرف الموقع الشرعي من أي استعمال من قبل الآخرين .

2- يجب ألا تعدل البيانات محل التوقيع وأن لا تمنع أن تعرض هذه البيانات على الموقع قبل عملية التوقيع.

الفرع الثاني: متطلبات آلية التحقق من التوقيع الإلكتروني.

نصت المادة 12 من القانون رقم (04-15) لسنة 2015 على أنها: " يجب أن تكون آلية التحقق من التوقيع الإلكتروني الموصوف موثوقة ."

و لخصت المادة 13 من ذات القانون المتطلبات الكفيلة بتحقيق هذه الموثوقية حيث نصت على أن:

" الآلية الموثوقة للتحقق من التوقيع الإلكتروني هي آلية تتوفر فيها المتطلبات الآتية:

1. أن تتوافق البيانات المستعملة للتحقق من التوقيع الإلكتروني مع البيانات المعروضة عند التحقق من التوقيع الإلكتروني.
 2. أن يتم التحقق من التوقيع الإلكتروني بصفة مؤكدة وأن تكون نتيجة هذا التحقق معروضة عرضاً صحيحاً .
 3. أن يكون مضمون البيانات الموقعة إذا اقتضى الأمر محدداً بصفة مؤكدة عند التحقق من التوقيع الإلكتروني.
 4. أن يتم التحقق بصفة مؤكدة من موثوقية وصلاحية شهادة التصديق الإلكتروني المطلوبة عند التحقق من التوقيع الإلكتروني.
 5. أن يتم عرض نتيجة التحقق وهوية الموقع بطريقة واضحة وصريحة.
- ولقد أسندت إجراءات التحقق من هذه الآليات إلى هيئة وطنية مكلفة باعتماد آليات إنشاء التوقيع الإلكتروني والتحقق منها .

الفرع الثالث: شروط التوقيع الإلكتروني.

أثار العديد من القانونيين تساؤلات حول مدى استيفاء التوقيع الإلكتروني للشروط القانونية التي تكسبه حجية كاملة في الإثبات، وقد جاءت الإجابة على هذه التساؤلات من خلال صدور عدة قوانين خاصة بالمعاملات الإلكترونية، هدفت إلى تعزيز الثقة في التوقيع الإلكتروني وتمكينه من أداء الوظيفة ذاتها التي يؤديها التوقيع التقليدي، ووضعه على قدم المساواة معه من حيث القوة القانونية في الإثبات ويهدف هذا الفرع إلى استعراض الشروط القانونية الواجب توافرها في التوقيع الإلكتروني، وذلك في ضوء عدد من القوانين والتشريعات القانونية، وقد انحصرت هذه الشروط في ثلاثة عناصر رئيسية وهي:

أولاً: أن يكون التوقيع مميزاً لصاحبه:

يقصد بهذا الشرط: «أن يدل التوقيع الموجود على المحرر الإلكتروني¹ أنه ينسب إلى شخص معين، فحتى يقوم هذا التوقيع بوظيفته بالإثبات يجب أن يكون دالاً على شخصية صاحبه ومميزاً له عن غيره من الأشخاص»²، وليس فقط الفقه القانوني الذي اشترط هذا الشرط بل أن غالبية القوانين الدولية والوطنية قامت بذلك .

و تنص المادة 2/2 من التوجيه الأوروبي بشأن التوقيعات الإلكترونية لعام 1999 بالنسبة للتوقيع المؤهل "أن يكون مرتبطاً فيها"³، أين اشترط أن يكون التوقيع الإلكتروني يسمح بتحديد شخصية الموقع .

أما تحديد شروط التوقيع الإلكتروني في التشريعات الوطنية، فهناك قوانين لعدة بلدان تطرقت لهذا الموضوع، نذكر منها:

القانون الأردني للمعاملات الإلكترونية لسنة 2001 في المادة 31 منه على أنه: «إذا تبين نتيجة تطبيق إجراءات التوثيق المستخدمة أنها معتمدة أو مقبولة تجارياً أو متفق عليها بين الأطراف، ويعتبر التوقيع الإلكتروني موثقاً إذا اتصف بالآتي:

- متميز بشكل فريد بارتباطه بالشخص صاحب العلاقة .

- كان كافياً للتعريف بشخص صاحبه .

- تم انشاؤه بوسائل خاصة بالشخص وتحت سيطرته .

¹ حسب نص المادة 2 من قانون الأونسيترال بشأن التجارة الإلكترونية يراد بالمحرر الإلكتروني « رسالة البيانات » ويقصد بها « المعلومات التي يتم إنشاؤها أو إرسالها أو استلامها أو تخزينها بوسائل الكترونية أو صوتية أو بوسائل مشابهة »، (نقلاً عن عيسى غسان ربضي- القواعد الخاصة بالتوقيع الإلكتروني - ص 187).

² الحاج علي، ألاء أحمد محمد. التنظيم القانوني لجهات التصديق على التوقيع الإلكتروني. رسالة ماجستير، كلية الدراسات العليا، جامعة النجاح الوطنية، فلسطين، 2013، ص. 49.

³ الفقي، عبد الحليم فؤاد. جريمة تزوير التوقيع الإلكتروني. أطروحة دكتوراه، قسم القانون الجنائي، كلية الحقوق، جامعة القاهرة، ص. 3740.

- ارتبط بالسجل الذي يتعلق به بصورة لا تسمح بإجراء التعديل على القيد بعد توقيعه دون إحداث تغيير في التوقيع»¹.
- و كذلك جاء بالمادة 1/ج من قانون التوقيع الإلكتروني المصري رقم 15 لسنة 2004 حيث نصت على أنه:«... ويكون له طابع منفرد ويسمح بتحديد شخص الموقع ويميزه عن غيره»².
- أما التشريع الجزائري فقد نص القانون رقم (15-04) لسنة 2015 على هذا الشرط فضلا عن شروط أخرى بنص المادة 7 تمثلت في:
- أن ينشأ التوقيع الإلكتروني على أساس شهادة تصديق موثوقة.
- أن يرتبط بالموقع دون سواه .
- أن يكون مصمما بواسطة آلية مؤمنة أو إجراءات قانونية تمكن من التحكم والسيطرة عليه .
- أن يكون مرتبطا بالمعلومات الموجودة بالمستند المعلوماتي، بحيث يمكن اكتشاف التغييرات اللاحقة بهذه المعلومات وعليه فالتوقيع عبارة عن علامة مميزة لشخصية صاحبه محدد هويته ويعرفه تعريفا دقيقا .

ثانيا: سيطرة الموقع على التوقيع:

- يشترط هذا أن يكون صاحب التوقيع منفردا به سواء عند انشائه أو استعماله بأي شكل من الأشكال، حتى لا يستطيع أي شخص فك رموز التوقيع الخاص به أو الدخول عليه ومحاولة التوقيع بدلا عنه.³

¹ البياتي، نادية ياس. التوقيع الإلكتروني عبر الإنترنت ومدى حجية الإثبات. الطبعة الأولى، دار البداية ناشرون وموزعون، الأردن، 2014، ص. 188.

² الفقي، عبد الحليم فؤاد. المرجع السابق، ص 3739.

³ البياتي، نادية ياس. المرجع نفسه، ص 190.

وحتى تتحقق سيطرة الموقع على التوقيع "لا بد من امكانية السيطرة على الوسيط الإلكتروني المتضمن هذا التوقيع، وذلك لضمان أن يكون صاحب التوقيع منفردا به سواء عند التوقيع أو استعماله بأي شكل من الأشكال".¹

وقد أقر أيضا القانون النموذجي للأونسيترال بشأن التوقيعات الإلكترونية هذا الشرط من شروط هذا الأخير، لا سيما المادة 06/3 منه، والتي جاء فيها: «يعتبر التوقيع الإلكتروني موثوقا به لغرض الوفاء بالاشتراط المشار إليه في الفقرة (01) إذا:

- كانت بيانات إنشاء التوقيع خاضعة وقت التوقيع لسيطرة الموقع دون أي شخص آخر.
 - كان أي تغيير في التوقيع الإلكتروني يجري بعد حدوث التوقيع قابلا للاكتشاف.
 - كان الغرض من اشتراط التوقيع قانونا هو تأكيد سلامة المعلومات التي يتعلق بها التوقيع وكان أي تغيير يجري في تلك المعلومات بعد وقت التوقيع قابلا للاكتشاف».²
- ومنه نبين أن المشرع الفرنسي لم يبين شروط التوقيع الإلكتروني صراحة سوى أنه بين أنه إذا كان التوقيع إلكترونيا فيتمثل في استخدام وسيلة آمنة لتحديد هوية الشخص تضمن صلاته بالمستند الذي وضع توقيعه عليه.³

ثالثا: عدم قابلية التوقيع الإلكتروني للتعديل أو التغيير:

أن يرتبط بالسجل المتعلق به ارتباطا ماديا مباشرا، وذلك للتأكد من سلامة الوثيقة من أي تعديل أو تغيير قد يطرأ عليها، وهذا يعني ضرورة ارتباط التوقيع الإلكتروني بمضمون السند بشكل لا يمكن فصله عنه، ولكي يتحقق هذا الأخير لابد من استخدام كفاءات تقنية في

¹ براهيم، حنان. جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية. أطروحة دكتوراه، كلية الحقوق، جامعة بسكرة، 2015، ص. 155.

² قانون الأونسيترال لسنة 2001 بشأن التوقيعات الإلكترونية (نقلا عن معوان، مصطفى. الإثبات في المعاملات الإلكترونية في التشريعات الدولية: التوقيعات والبصمات الإلكترونية. دار الكتاب الحديث، الجزائر، 2010، ص. 91).

³ الربيع، إبراهيم إسماعيل، وعلاء موسى علي نالي. "التوثيق الإلكتروني قرارات التحكيم في التوقيع الإلكتروني: دراسة مقارنة". مجلة المحقق الحلي للعلوم القانونية والسياسية، المجلد 1، 2012، ص. 161.

تأمين محتوى السجل الإلكتروني نذكر منها مفاتيح التشفير سواء كان العام أو الخاص والتي لا يمكن فك تشفيرها إلا بواسطة الشخص حامل المفتاح². إذ يقوم المرسل بتشفير الرسالة بالمفتاح العام، ثم يتم اختصار الرسالة إلى خانات رقمية لها قيمة معينة وفردية لكل رسالة، بعد ذلك يشفر المرسل رسالته بالمفتاح الخاص، مما ينشئ توقيعاً رقمياً مميزاً، ومن ثم ترسل الرسالة للمستقبل الذي يقوم بدوره بعملية معاكسة.¹

¹ الصفدي الطوال، عيبر ميخائيل. النظام القانوني لجهات توثيق التوقيع الإلكتروني. الطبعة الأولى، دار وائل للنشر، 2010، ص. 57.

المبحث الثاني: صور التوقيع الإلكتروني وحجته.

يتخذ التوقيع الإلكتروني أشكالاً وصوراً متعددة تختلف من حيث الإجراءات المتبعة في إنشاء وإثبات حجية التوقيع ونسبته لصاحبه، إذ يعد عامل حجية التوقيع الإلكتروني في الإثبات من أهم المواضيع التي أثّرت من مختلف التشريعات وفي ضوء هذا الطرح سنتناول: صور التوقيع الإلكتروني (كمطلب أول)، وحجته (كمطلب ثاني).

المطلب الأول: صور التوقيع الإلكتروني.

تختلف أشكال وصور التوقيع الإلكتروني سواء من حيث الإجراءات أم من حيث درجة الأمان ومن بين أهم صور التوقيع الإلكتروني نجد: التوقيع الرقمي، التوقيع البيومتري، التوقيع بالقلم الإلكتروني، والتوقيع بالرقم السري.

الفرع الأول: التوقيع الرقمي.

يعتبر أحدث أشكال التوقيع الإلكتروني وأكثرها أماناً نظراً للشروط الفنية والتقنية الخاضع لها، وينشأ التوقيع ويتحقق من صحته باستخدام التشفير (الترميز)، فإذا أراد الموقع إرسال رسالة بيانات عبر البريد الإلكتروني مثلاً فإنه يقوم بإعداد ملخص الرسالة باستخدام برنامج تشفير وباستخدام المفتاح الخاص، وإرسالها للشخص المستلم الذي يستخدم المفتاح العام للتحقق من صحة التوقيع الرقمي، ثم ينشئ المرسل إليه ملخص باستخدام نفس برنامج التشفير ويقارن بين ملخصي الرسالتين، فإذا كانتا متطابقتين فهذا دليل على أن الرسالة وصلت سليمة كما هي، أما إذا تم إحداث تغيير في الرسالة فسيكون ملخص الرسالة الذي أنشأها المستلم مختلفة عن ملخص الرسالة التي أنشأها الموقع.¹

الفرع الثاني: التوقيع البيومتري.

وهذا النوع يعتمد على الخواص الكيميائية والطبيعية للأفراد وتشمل ما يلي:

¹ غلاب، عبد الحق. "خصوصية جريمة تزوير التوقيع الإلكتروني في التشريع الجزائري." مجلة الدراسات القانونية والسياسية، المجلد 8، العدد 1، جامعة الجزائر 1، 2022، ص. 499.

1. البصمة الشخصية (بصمة الأصبع) Finger Printing.
2. بصمة شبكية العين أو مسح العين البشرية Retina Scanning.
3. مستوى ونبرة الصوت Voice Recognition.
4. خواص اليد البشرية Hand Gesmetry.
5. التعرف على الوجه البشري Facial Recognition.
6. التوقيع الشخصي Handwritten Signature¹.

يتميز هذا النوع من التوقيعات بمجموعة خصائص كعدم اعتماده على المفاتيح السرية، وهو ما يساهم في تجاوز العديد من المشكلات المرتبطة بالأرقام والكلمات السرية المعرضة للنسيان والسرقة والتزوير، وهذا لا يعني أنه لا يخلو من المشاكل منها أن صورة التوقيع يتم وضعها على القرص الصلب للحاسب، ومن ثم يمكن مهاجمتها أو نسخها بواسطة القرصنة الإلكترونية باختلاف طرقها، كما أن هذا النوع من التوقيع يحتاج إلى استثمارات ضخمة لتمكين مستخدمي الشبكة الإلكترونية من استخدام الخصائص الذاتية لشخص الموقع في التوقيع الإلكتروني.²

الفرع الثالث: التوقيع بالقلم الإلكتروني.

يتم التوقيع أيضا بواسطة قلم الكتروني يمكنه الكتابة على شاشة الحاسوب عن طريق برنامج معلوماتي يتيح النقاط التوقيع حيث يتلقى البرنامج المثبت على قاعدة بيانات الحاسوب ببيانات المستخدم عن طريق بطاقة التحقيق هوية الكترونية خاصة تحتوي على بيانات كاملة عن هذا الشخص ثم تظهر بعد ذلك تعليمات على شاشة الحاسوب ليتبعها المستخدم، تطلب من المستخدم تحريك القلم على الشاشة وكتابة توقيعه، ويلتقط البرنامج حركة اليد

¹ عبير ميخائيل الصفدي الطوال، المرجع السابق، ص 50.

² يوسف، أمير فرج. المرجع السابق، ص 19.

ويظهر التوقيع مكتوباً على الشاشة¹، والذي يتميز بسمات خاصة من حيث: الحجم، الشكل، الحروف، المنحنيات، الدوائر، الخطوط، النقاط... إضافة إلى تحديد السرعة التي يجري بها وضع التوقيع، لكن ما يعاب على هذا التوقيع أنه يتطلب وجود حاسب آلي ذي مواصفات خاصة، احتوائه على وحدة القلم الإلكتروني والشاشة الحساسة، وهذا لتمكنه من أداء مهمته في التقاط التوقيع من شاشته، والتحقق من مطابقته للتوقيع المحفوظ بذاكرته، بالإضافة إلى مشكلة إثبات العلاقة بين التوقيع والمحرم حيث لا توجد أي تقنية تتيح التأكد من إثبات هذه الرابطة، إذ بإمكان المرسل إليه الاحتفاظ بنسخة من صورة التوقيع مما يؤدي إلى انعدام الثقة والأمان.²

الفرع الرابع: التوقيع بالرقم السري.

من أنواع التوقيع الإلكتروني التوقيع باستعمال البطاقات الممغنطة المقترنة بالرقم السري، والذي يمكن إدراجه ضمن التوقيع الرقمي، والذي يسمح بالتحويل الإلكتروني للأموال والقيام بالعمليات إلكترونية والتي تعتبر كوسيلة وفاء، حيث تعتبر هذه وسيلة وفاء عند تنفيذ الالتزام الوارد على المشتري بدفع الثمن، كما أن هذه البطاقة تحتوي على معالج أو عقل آلي صغير الحجم كما تحتوي على ذاكرة مغناطيسية يسجل عليها بيانات الكترونية خاصة بالعميل يرمز لها باللاتينية P.I.N.³

و تعتبر البطاقة الممغنطة أداة لتسيير المعاملات المصرفية الإلكترونية، وتعد هذه الصورة من أكثر صور التوقيع الإلكتروني شيوعاً وانتشاراً، إذ لا يتطلب جهداً ولا خبرة، ومن أكثر المجالات التي انتشر فيها استعمال هذه البطاقات هو القطاع المصرفي، حيث أصبحت جل البنوك تتوفر على خدمة الصراف الآلي، وتحتوي هذه البطاقات على بيانات خاصة بشخص

¹ لالوش، راضية. أمن التوقيع الإلكتروني. مذكرة ماجستير، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، ص. 45.

² حامدي، بلقايم. إبرام العقل الإلكتروني. أطروحة دكتوراه، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة، 2014-2015، ص. 214.

³ عجابي، إلياس. المرجع السابق، ص 265.

معين ألا وهو صاحب البطاقة أو العميل، وهذه البيانات موجودة على مستوى دائرة إلكترونية مغلقة مثبتة على البطاقة.¹

و لهذه البطاقات أصناف تختلف باختلاف نوع التكنولوجيا المستخدمة في صنعها ولعل أهمها البطاقات المغناطيسية، والبطاقات الذكية.

أولاً: البطاقات المغناطيسية

تُعد البطاقة المغناطيسية من الوسائل التقنية الحديثة المُستخدمة في توثيق الهوية الرقمية وإنشاء التوقيعات الإلكترونية، وهي عبارة عن بطاقة بلاستيكية تحتوي على شريط مغناطيسي أو شريحة إلكترونية تُخزن فيها بيانات مشفرة تتعلق بصاحب البطاقة، كالمعرف الرقمي أو الشهادة الإلكترونية. ويُعتمد عليها في تنفيذ العمليات الرقمية المؤمنة، مثل الدخول إلى المنصات الإلكترونية، أو توقيع الوثائق الرقمية بطريقة تضمن سلامة المعاملة ومصداقيتها. وتُصنف هذه البطاقة ضمن الوسائل الآمنة التي نصّ عليها القانون رقم 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين، باعتبارها أداة لتحديد الهوية وإنشاء توقيع إلكتروني موثوق.²

وقد أخذ التشريع الجزائري بهذه الوسائل في إطار سعيه لمواكبة التطورات التكنولوجية وضمان أمن التعاملات الإلكترونية، حيث نصت المادة 6 من القانون المذكور على أن التوقيع الإلكتروني يكون موثقاً إذا تم إنشاؤه بوسائل آمنة ومؤمنة تقنياً، منها استخدام البطاقة المغناطيسية المدعّمة بشهادة تصديق إلكتروني. وعلى المستوى العملي، تبنت بعض المؤسسات العمومية والمالية الجزائرية هذه الوسائل، لا سيما في مجال الدفع الإلكتروني والتصديق على المعاملات عن بعد، غير أن استخدام هذه البطاقات لا يخلو من التحديات

¹ طمين، سهيلة. *الشكلية في عقود التجارة الإلكترونية*. رسالة ماجستير، جامعة مولود معمري، تيزي وزو، 2011، ص. 58.

² الجزائر. القانون رقم 15-04 المؤرخ في 1 فبراير 2015، المتعلق بالتوقيع والتصديق الإلكترونيين. الجريدة الرسمية للجمهورية الجزائرية، العدد 06، سنة 2015.

الأمنية، كحالات سرقة المعطيات أو استنساخ البطاقة، مما يؤدي إلى تزوير الهوية أو التوقيع الإلكتروني.

وفي هذا السياق، بدأ القضاء الجزائري يتعامل بحذر مع القضايا المتعلقة بالتوقيعات الإلكترونية المزورة الناتجة عن سوء استخدام البطاقة المغناطيسية، حيث تشترط بعض الهيئات القضائية توفر شروط المصادقة الرقمية الكاملة والشهادة الإلكترونية السليمة لقبول التوقيع الإلكتروني كوسيلة إثبات، ما يبرز أهمية تعزيز البنية التشريعية والتقنية لحماية هذه الوسيلة من التزوير والاستغلال.¹

ثانياً: البطاقات الذكية

تُعد البطاقة الذكية من التقنيات الحديثة التي ساهمت في تحسين جودة الخدمات وتبسيط الإجراءات في مختلف القطاعات. وهي بطاقة بلاستيكية تحتوي على شريحة إلكترونية قابلة للبرمجة، تُستخدم لتخزين ومعالجة البيانات بشكل آمن. وتُوظف هذه البطاقات في مجالات متعددة مثل الهوية الوطنية، الخدمات المصرفية، الرعاية الصحية، النقل، والدفع الإلكتروني. وتتميز البطاقة الذكية بقدرتها على حماية المعلومات من التلاعب أو السرقة، إضافة إلى تسهيل عمليات التحقق من الهوية وتوثيق البيانات بدقة وكفاءة.²

لقد أصبح استخدام البطاقات الذكية أمراً أساسياً في إطار التحول الرقمي الذي تسعى إليه العديد من الدول، لا سيما في ظل الاتجاه نحو تقليص المعاملات الورقية وتحقيق الحوكمة الإلكترونية. كما تتيح هذه البطاقات تقنيات متقدمة مثل التشفير، والتوقيع الرقمي، مما يعزز الثقة في المعاملات الإلكترونية، ويقلل من معدلات التزوير.³

¹ معزوز، عبد القادر. "الإثبات الإلكتروني في التشريع الجزائري". مجلة دراسات قانونية، العدد 12، 2021، ص. 88، جامعة الجزائر.

² السعيد، محمد. تقنيات البطاقات الذكية وتطبيقاتها. دار الفكر، 2020، ص 23

³ العتيبي، فهد. "البطاقة الذكية ودورها في تطوير الخدمات الحكومية". مجلة التقنية الحديثة، العدد 15، 2021، ص. 52-45.

إن ما يميز هذا النوع من التوقيع هو الأمان الذي يوفره إلى حد ما، حيث من الصعب الحصول على الرقم السري الذي لا يعلمه إلا صاحب البطاقة، إذ ترسله الجهة المختصة بذلك بمراسلة رسمية، وعليه الاحتفاظ به وعدم إطلاع الغير عليه، وهذا لا يعني خلوه من المخاطر التي تتمثل في التزوير حيث كلما تطورت التقنية في هذا الجانب، كلما تناسبت الأساليب الإجرامية معها، وبالتالي تطور تقنيات التزوير.¹

المطلب الثاني: حجية التوقيع الإلكتروني في مجال الإثبات.

ترتبط حجية التوقيع الإلكتروني استيفائه للشروط اللازمة للاعتداد به كتوقيع كامل، ولهذا بادرت الدول إلى تضمين نصوصها وإعطاء التوقيع الإلكتروني قوة ثبوتية تعادل تلك الممنوحة للتوقيع التقليدي ومنه نقوم بتبيان شروط حجية التوقيع الإلكتروني في التشريع الجزائري مع عرض بعض نصوص التشريعات المختلفة التي نظمت التوقيع الإلكتروني وأقرت بحجيته.

الفرع الأول: شروط حجية التوقيع الإلكتروني في التشريع الجزائري.

لقد ساوى المشرع الجزائري - من خلال القانون المدني الجزائري - في الحجية بين التوقيع الإلكتروني والتوقيع التقليدي، حيث نصت المادة 327/2 من القانون المدني على أنه: «يعتد بالتوقيع الإلكتروني وقفا للشروط المذكورة في المادة 323 مكرر 1»، وتتمثل هذه الشروط في إمكانية التأكد من هوية الشخص الذي أصدر التوقيع وأن يكون هذا التوقيع معدا في ظروف تضمن سلامته .

وبالرجوع إلى القانون (04-15) المتعلق بالتوقيع والتصديق الإلكترونيين، نجد أن المشرع قد ميز بين التوقيع البسيط والتوقيع الإلكتروني الموصوف، حيث أقر صراحة حجية توقيع

¹ براهيم، حنان. المرجع السابق، ص ص 150، 149.

هذا الأخير مساويا بينه وبين التوقيع التقليدي طبقا لنص المادة 08 من ذات القانون¹، كما حددت المادة 07 من نفس القانون الشروط الواجب توافرها حتى يكون التوقيع الإلكتروني موصوفا والتي تتمثل في:

1. أن ينشأ التوقيع على أساس شهادة تصديق الكتروني موصوفة حيث ميز المشرع الجزائري بين شهادة التصديق الإلكتروني البسيطة وشهادة التصديق الإلكتروني الموصوفة وهذا من خلال المادة 2 في فقرتها 7 والمادة 15 .
2. أن يرتبط بالموقع دون سواه ويمكن من تحديد هويته حتى يكون التوقيع الإلكتروني توقيعاً موصوفاً فيطلب أن يميز الشخص موقع المستند الإلكتروني عن غيره.
3. أن يكون التوقيع مصمماً بواسطة آلية مؤمنة خاصة بإنشاء التوقيع الإلكتروني.
4. أن يكون منشأً بواسطة وسائل دعمت التحكم الحصري للموقع وهذا ما أطلق عليها المشرع بيانات إنشاء التوقيع الإلكتروني.
5. أن يكون مرتبطاً بالبيانات الخاصة به، بحيث يمكن الكشف عن التغييرات اللاحقة بها.

الفرع الثاني: حجية التوقيع الإلكتروني في التشريعات المقارنة

أ/ وفقاً لقوانين الأونيسترال:

تنص المادة 6-1 من قانون الأونيسترال بشأن التوقيعات الإلكترونية على أنه: "حيث ما يشترط القانون وجود توقيع من شخص، يعد ذلك شرطاً مستوفياً في رسالة البيانات إذا

¹ نصت المادة 8 من القانون 15/04 على أنه: «يعتبر التوقيع الإلكتروني الموصوف وحده مماثلاً للتوقيع المكتوب، سواء كان لشخص طبيعي أو معنوي.»

استخدم توقيع الكتروني موثوقا به بالقدر المناسب للغرض الذي أنشئت أو بلغت من أجله رسالة البيانات في ضوء كل الظروف بما في ذلك اتفاق ذي صلة.¹

وفقا لهذا النص يعد التوقيع الإلكتروني صالحا لإنشاء الالتزامات حينما يتطلب القانون وجود توقيع على مستند معين، يشترط أن يكون هذا التوقيع الإلكتروني موثق به.²

ب/- وفقا لتوجيهات الاتحاد الأوروبي:

جاء في إصدار سنة 1999 من التوجيه الأوروبي حول التوقيعات الإلكترونية بنص المادة 02 منه جملة من الشروط الواجب توافرها في التوقيع الإلكتروني لإضفاء الحجية القانونية عليها، وهي:

أ- أن يكون التوقيع مرتبط بشخص الموقع وحده.

ب- أن يسمح بتعريف هوية الموقع.

ج- أن يكون مرتبطا بالبيانات

د- أن يكون قد وجد بوسائل تمكن الموقع من إبقائها تحت رقابته.³

ولهذا اعترف التوجيه الأوروبي بالتوقيع الإلكتروني وأضفى عليه الحجية القانونية في الإثبات بشرط أن تتوافر فيه بعض الشروط المحددة.

ج/ وفقا للقانون الفرنسي:

لقد أكد المشرع الفرنسي على حجية التوقيع الإلكتروني في الإثبات، على أن يستوفي الشروط التي حددتها المادة 316/4 من القانون المدني، وأحكام المرسوم رقم 272-2001

¹ ربضي، عيسى غسان. القواعد الخاصة بالتوقيع الإلكتروني. الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2005، ص. 172.

² لجنة الأمم المتحدة للقانون التجاري الدولي (الأونسيترال). قانون الأونسيترال بشأن التوقيعات الإلكترونية. 2001، الفقرة 3 من المادة 6.

³ التوجيه الأوروبي بشأن التوقيعات الإلكترونية لسنة 1999، المادة (02).

المحدد لآليات تطبيق أحكام المادة حيث نصت هذه الأخيرة على أنه: "...وحيثما يكون التوقيع إلكتروني فإنه يكمن في استخدام طريقة موثوقة لتحديد الهوية بما يضمن ارتباطه بالعقد الذي وضع عليه التوقيع"، ويفهم من هذه المادة أنه لكي يؤدي التوقيع الإلكتروني وظيفته في إثبات ما ورد في مضمون العقد، أن يحدد هوية الموقع ويميزه عن غيره، فضلا عن ارتباطه بالعقد على نحو لا يمكن فصله عنه، وأن يعبر عن إرادته في قبوله الالتزام بمضمون العقد.¹

كذلك فقد صدر القانون رقم 23 لسنة 2000 الصادر في 13-مارس-2000 في فرنسا، وعدل نصوص التقنين الفرنسي في شأن الإثبات الكتابي، وأضفى حجية كاملة على التوقيع الإلكتروني تطابق تماما ذات الحجية الخاصة بالتوقيع المكتوب أو التوقيع في صورته التقليدية.²

¹ بوكري، رشيدة. "التوقيع الإلكتروني في التشريع الجزائري (دراسة مقارنة)". مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد 4، ديسمبر 2016، ص. 71.

² الحجازي، عبد الفتاح بيومي، المرجع السابق، ص. 278.

الخلاصة:

يُعد التوقيع الإلكتروني من الوسائل القانونية المستحدثة التي فرضتها التطورات التكنولوجية الحديثة، حيث أصبح يُعتمد عليه بشكل واسع في المعاملات المدنية والتجارية لما يتمتع به من حجية في الإثبات. وبالمقابل، برزت جرائم رقمية جديدة من بينها تزوير التوقيع الإلكتروني، والتي تمس بمصادقية الوثائق الرقمية وسلامة المعاملات.

من الناحية الموضوعية، تقوم جريمة تزوير التوقيع الإلكتروني على إدخال بيانات رقمية مزورة أو التلاعب بتوقيع إلكتروني أصلي أو تقليده دون إذن من صاحبه، مع نية الإضرار أو التزوير، مما يشكل اعتداء على الثقة العامة وسلامة التعاملات الإلكترونية. وتتحقق هذه الجريمة متى تم استخدام التوقيع المزور لإضفاء طابع رسمي أو قانوني على مستند رقمي أو للتلاعب في محتواه.

ورغم أهمية هذا الموضوع، فإن التشريع الجزائري لم ينص صراحة على تجريم تزوير التوقيع الإلكتروني، واكتفى بوضع إطار عام لحجية التوقيع والتصديق الإلكترونيين في القانون 04-15 دون أن يرفق ذلك بأحكام جنائية واضحة لمواجهة الأفعال التي تخلّ بهذا النظام. وعليه، يُضطر القضاء إلى تأويل النصوص العامة المتعلقة بالتزوير التقليدي لتطبيقها على التزوير الإلكتروني، رغم الفوارق الجوهرية بينهما من حيث الوسائل والأدوات. لذلك، تبرز الحاجة إلى نصوص جزائية صريحة ومتكاملة تُجرّم تزوير التوقيع الإلكتروني بشكل واضح، وتحدد أركانه وعقوباته بما يتلاءم مع خصوصية البيئة الرقمية، حماية ثقة الأفراد في المعاملات الإلكترونية وضماناً لاستقرارها القانوني.

الفصل الثاني

آليات الحماية القانونية للتوقيع

الإلكتروني

تمهيد:

تفاديا لخطورة تزوير التوقيع الإلكتروني وجب الإحاطة بالإطار الجزائي لجريمة تزوير التوقيع الإلكتروني من أجل تحقيق الحماية القانونية لهذا الأخير بالرغم من إغفال المشرع عن الحديث بصدد هذه الجريمة بحد ذاتها بل استتبطها من الأحكام تزوير التوقيع التقليدي وبعض من أسس الجرائم الإلكترونية .

المبحث الأول: الإطار الجزائي لجريمة تزوير التوقيع الإلكتروني

اكتسبت الجريمة طابعاً جديداً نتيجة للتطورات الاقتصادية والصناعية التي شهدتها العالم، خاصة مع ظهور الحواسيب وشبكة الإنترنت. وقد أدى ذلك إلى انتقال مفهوم الجريمة من شكله التقليدي المعروف إلى شكل جديد أكثر خطورة يتمثل في الجريمة المعلوماتية. ومن بين هذه الجرائم، يُعد تزوير التوقيع الإلكتروني امتداداً لجرائم التزوير التقليدية، لكنه تطور بفعل تأثير التكنولوجيا الحديثة.

المطلب الأول: أركان جريمة تزوير التوقيع الإلكتروني وأساليب التحري الخاصة.

تقوم جريمة تزوير التوقيع الإلكتروني في ركنها المادي على المحرر المعلوماتي الموقع الكترونياً، ويكون الهدف من التزوير هو تغيير الحقيقة، ولابد من وجود ضرر في مجال التوقيع الإلكتروني كما لابد من توفر القصد الجنائي بالنسبة لهذه الجريمة والذي يمتاز بنوع من الخصوصية.

الفرع الأول: الركن المادي.

يجب الإشارة إلى أن جريمة تزوير التوقيع الإلكتروني من الجرائم التي يدور فعل التزوير المعلوماتي على تغيير الحقيقة في محرر الكتروني بطريقة الغش، مما ينتج عنه مضمون مختلف للمحرر وللمعاملات القانونية القائمة على صحة المعلومات التي توفرها هذه البيانات التي تكون محلاً للغش ويكون من شأنه إحداث ضرر¹، والتوقيع هو توقيع إلكتروني على محرر الكتروني، فتقوم جريمة التزوير في ركنها المادي منه بتغيير الحقيقة في محرر بإحدى الطرق التي نص عليها القانون على نحو يسبب ضرراً للغير.²

¹ إبراهيم، محمد خالد ممدوح. "الحماية الجنائية للتوقيع الإلكتروني في القانون الاتحادي رقم 02 لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات." مجلة الفكر الشرطي، مجلد 23، عدد 88، 2006، ص. 157.

² حفصي، عباس. جرائم التزوير الإلكترونية: دراسة مقارنة. أطروحة دكتوراه، تخصص شريعة وقانون، كلية العلوم الإنسانية والعلوم الإسلامية، جامعة أحمد بن بلة، وهران 1، 2015، ص. 97.

لذلك يقتضي الركن المادي أن نتطرق إلى المحرر المعلوماتي الموقع الكترونيا (فرع1)، ثم فعل تغيير الحقيقة (فرع2).

أولاً: المحرر المعلوماتي الموقع إلكترونياً.

تختلف جريمة تزوير التوقيع الإلكتروني عن تزوير التوقيع التقليدي، ففي الأول يقوم الشخص بالحصول على منظومة التوقيع الإلكتروني الخاصة بشخص آخر بغرض استخدامها في توقيع مستندات إلكترونية، أو وثائق إلكترونية¹، فالوثيقة الموقعة الكترونياً هي الوثيقة الإلكترونية المرفقة أو المتصلة بتوقيع الكتروني²، لذلك يكون التوقيع الإلكتروني سليماً حتى كان مالك منظومة التوقيع قد قام بالتوقيع بواسطتها، وتكمن المشكلة هنا في حصول الشخص على المنظومة بواسطة التجسس الإلكتروني أو غيرها من الطرق الأخرى، وعليه فجريمة تزوير التوقيع الإلكتروني تختلف اختلافاً كلياً أو جزئياً عن تزوير التوقيع التقليدي سواء في طريقة التزوير أو في طريقة الكشف عنها.³

والتوقيع الإلكتروني بشرطه المذكور في المادة 323 مكرر 1 من القانون المدني الجزائري حجة في الإثبات، ومنه يكون المشرع قد اعترف بحجية التوقيع الإلكتروني.

يتمثل الركن المادي لجريمة تزوير التوقيع الإلكتروني في فعل تغيير الحقيقة في توقيع الكتروني وذلك بأي وسيلة كانت، ولعل من أشهر وسائل تزوير التوقيع الإلكتروني استخدام برامج حاسوبية وأنظمة معلوماتية خاصة بذلك، يتم تصميمها على غرار البرامج والأنظمة

¹ المرسوم التنفيذي رقم 16-142. "تعريف الوثيقة الإلكترونية كما ورد في المادة 2: «مجموعة تتألف من محتوى وبنية منطقية وسمات العرض، تسمح بتمثيلها واستغلالها من قبل الشخص عبر نظام إلكتروني». الجريدة الرسمية، 2016.

² عرفها جعفر مشيمش في كتابه، جريمة التزوير، ط 2. منشورات زين الحقوقية، 2011، ص 37 على أنها: «الوسيلة الثانية بعد النطق والكلام للتعبير عن مكنون النفس البشرية، وقد بدا أن هذه الأخيرة بالرسوم والصور المعبرة عن المعاني ثم تطورت إلى الأحرف الحالية التي تتبني منها اللغات المعروفة».

*الدعامة هي: أي وسيلة مادية أيا كان شكلها أو خصائصها المادية، تسمح بإستلام وحفظ واسترجاع الوثيقة الموقعة الكترونياً.

³ حفصي، عباس. المرجع السابق، ص 98.

المشروعة أو محاولة البعض كسر الشيفرة والوصول الى المحرر الالكتروني أو البيانات بغرض استخدامها.¹

وقد يكون التغيير ماديا أو بالتقليد ومعناه المشابهة، أو بالتزيف في الإمضاء أو البصمة أو الكتابة. بما في ذلك الزيادة أو الحذف، وأما بانتحال شخصية الغير أو الحلول محلها، فالتزوير نجد أنه موجود في المعنى والمضمون ومن ذلك اصطناع أحكاما قضائية أو وثائق مما تصدره الإدارات العمومية، وهي مزورة من حيث البيانات أو التوقيع، ويكون التزوير بإحدى الطرق المحددة على سبيل الحصر في نص المادة 216 من قانون العقوبات سواء تعلق الأمر بتزوير التوقيع في المحررات الرسمية أو العرفية، وكان هذا قبل الغائه من القانون. وتبعاً لذلك فإن لم يكن تغيير للحقيقة فلا تزوير، لذلك نجد أنه ينصب على البيانات الجوهرية التي يتضمنها المحرر، وأما البيانات غير الجوهرية التي لا تؤثر فيما أعد المحرر من أجله، لأنه عند إضافة أو تعديل أو تحريف أو إزالة لا يعد من التزوير المعاقب عليه، وذلك لعدم وجود ضرر نتج عنه، وهو ما ينطبق عن تزوير التوقيع الالكتروني.

أما عن طرق التزوير فيشترط أن يقع هذا الأخير بطرق معينة ذكرها القانون على سبيل الحصر، وهي نوعان قد يكون ماديا أو معنويا، فالتزوير المادي هو تغيير الحقيقة بطريقة مادية أي أنها تترك أثرا في المحرر تدركه العين، سواء كانت عين الإنسان العادي أو الفني المختص، أما التزوير المعنوي فهو تغيير الحقيقة بطريقة غير مادية، أي أنها لا تترك أثرا في المحرر تدركه العين، ولذلك كان التزوير المادي أيسر إثباتا من التزوير المعنوي، وبينما يقع التزوير المادي حال انشاء المحرر أو بعد انشاءه، إذا التزوير المعنوي لا يقع إلا حال انشاءه فحسب.²

¹ جبيري، ياسين. "الحماية الجنائية والتوقيع الإلكتروني: دراسة مقارنة." مجلة جامعة الأمير عبد القادر، عدد 1، مجلد 32، 2018، ص. 434.

² عبيد، رؤوف. جرائم التزيف والتزوير. ط. 2016، مكتبة الوفاء القانونية، الإسكندرية، ص ص 135-136.

الفرع الثاني: الركن المعنوي لجريمة تزوير التوقيع الإلكتروني

تعد جريمة التزوير بصفة عامة من الجرائم العمدية التي تتطلب قصدا جنائيا عاما وقصدا جنائيا خاصا، فلا يكفي القصد العام الذي يقوم على علم المتهم بأركان الجريمة، واتجاه إرادته إلى الفعل المكون لها وتحقيق نتيجته، بل تتطلب هذه الجريمة توافر قصد جنائي خاص، يتمثل في نية استعمال المزور فيما زور من أجله، وعلى هذا فإن القصد الجنائي في جريمة التزوير يعرف على نحو غالب لدى الفقه والقضاء بأنه: "تعمد تغيير الحقيقة في محرر تغييرا من شأنه أن يسبب ضرر وبنية استعمال المحرر فيما غيرت من أجله الحقيقة".¹

وانطلاقا مما سبق تبين أنه لا يمكن القياس على جريمة تزوير التوقيع التقليدي، كونه يتنافى ومبدأ الشرعية والنصوص التقليدية، لأن جريمة تزوير التوقيع الإلكتروني جريمة مستحدثة مما استوجب على المشرع العمل على النص على هذه الأخيرة وتجريمها .

المطلب الثاني: الأحكام الإجرائية المساعدة في الكشف عن جرائم التزوير

يقصد بها الوسائل المتعلقة بالجانب الإجرائي أو الشكلي المرتبط بالاجراءات الجزائية التي خولها المشرع للجهات القضائية المختصة اللجوء إليها من أجل كشف جرائم التزوير ومعاينتها والتحقيق فيها، والمتمثلة في أساليب التحري الخاصة، إضافة الى التفتيش الإلكتروني.

¹ صدراتي، وفاء. "آليات الحماية القانونية للتوقيع الإلكتروني من جرائم التزوير الإلكتروني في التشريع الجزائري". مجلة العلوم القانونية والسياسية، مجلد 11، عدد 1، 2020، ص. 592.

الفرع الأول: أساليب التحري الخاصة وشروط تطبيقها

أمام تطور أساليب ارتكاب الجريمة لو تعد الاختصاصات التقليدية كافية لصدّها فكان لابد من إيجاد إجراءات جديدة تتكيف مع التطور الحاصل فاستحدث المشرع أساليب تحري خاصة بمقتضى القانون رقم 06-22 المعدل والمتمم لقانون الإجراءات الجزائية.¹

أولاً: أساليب التحري الخاصة (الترصد الالكتروني)

نصت المادة 15 من القانون 02-24 على امكانية القيام بالترصد الالكتروني بواسطة اعتراض المراسلات، تسجيل الأصوات والتقاط الصور، بالإضافة إلى القيام بالتسرب كأسلوب من نوع آخر .

أ/ - اعتراض المراسلات:

يتم عن طريق وسائل الاتصال السلكية واللاسلكية، نصت عليه المادة 65 مكرر 1\5، فهو بمثابة مراقبة المكالمات والتنصت عليها، فهي وسيلة مراقبة الكترونية إلا أنه اختلف في تحديد طبيعتها، حيث هناك من اعتبرها نوع من التفتيش، واعتبرها آخرون من أنواع ضبط الرسائل في حين ذهب آخرون إلى اعتبارها إجراء من نوع خاص.²

والملاحظ أن المشرع لم يحدد الوسيلة التي يتم بها الاعتراض فلا أهمية إن كانت هذه الوسيلة تقليدية أو حديثة، فهو يشمل كل أنواع الاتصالات لعموم النص .

ومن خلال هذا نجد أن الاعتراض لا يتحقق إلا إذا تعلق الأمر بمراقبة اتصال سلكي أو لا سلكي بين المرسل والمرسل إليه أو على الأقل دون علم أحدهما فقط.³

¹ الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، عدد 84، 24 كانون الأول 2006، ص. 4.

² الخرشة، محمد أمين. مشروعية الصوت والصورة في الإثبات الجنائي: دراسة مقارنة. ط. 1، دار الثقافة للنشر والتوزيع، عمان، 2011، ص. 124.

³ عمارة، فوزي. قاضي التحقيق. أطروحة دكتوراه في العلوم القانونية، كلية الحقوق، جامعة الإخوة منتوري، قسنطينة، الجزائر، 2009-2010، ص. 196.

ب/- تسجيل الأصوات:

نصت عليه المادة 65 مكرر 2\5 قانون الإجراءات الجزائية، ويعني تسجيل الكلام والحديث الذي يدور بين شخصين أو أكثر .

فلا أهمية للغة التي تجرى بها المحادثة، غير أن المقصود هنا الأحاديث السرية على اعتبار أن انتهاكها هو محل التجريم في قانون العقوبات الجزائري، فالتشريعات الجنائية اختلفت في تحديد معيار معين للتمييز بين ما يعد حديثا خاصا وما يعد عاما، وبعضها أخذ بطبيعة المكان الذي يدور فيه الحديث والبعض الآخر أخذ بطبيعة الحديث في حد ذاته.

ج/ التقاط الصور:

يتم هذا الأسلوب باستخدام أجهزة المراقبة المرئية لتحديد مكان الشخص وتصرفاتها دون علمه وضد رغبته، فهو رقابة مرئية بخلاف الوسيطتين السابقتين، نصت عليه المادة 65 مكرر 5 فقرة 2، قانون الإجراءات الجزائية، ويكون ذلك باستعمال كاميرات صغيرة الحجم تساعد على كشف المجرمين إذ تسمح بأخذ الصور المراد الحصول عليها مهما كانت طبيعة المكان المتواجد به المجرم .

د/ التسرب:

يعد تقنية من تقنيات البحث والتحقيق نص عليه المشرع في المادة 65 مكرر 11 الى المادة 65 مكرر 18 من ذات القانون، رغم أنه ليس من وسائل التردد الالكتروني لكنه من أساليب التحري الخاصة التي استحدثها المشرع الجزائري مع سابقتها .

عرف التسرب بأنه عبارة عن: «عملية ميدانية تستخدم أسلوب التحري لجمع الوقائع المادية والأدلة من داخل العملية الإجرامية وكذا الاحتكاك شخصا بالمشتببه بهم والمتهمين، يمتاز بطابع الخطورة كونه يتطلب القيام بمناورات وتصرفات توحى بأن القائم بها مساهم في

الجريمة لكن في الحقيقة يخدعهم ويتحايل عليهم قصد الإطلاع على أسرارهم من الداخل ويجمع ما يستطيع من أدلة الإثبات.¹

أما من الناحية القانونية فعرفته المادة 65 مكرر 1\12 بأنه: «قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف.²

ثانيا: شروط تطبيق أساليب التحري الخاصة

بما أنها تمس بحرمة الحياة الخاصة التي تعد من الحقوق الدستورية³، قيدها المشرع بشروط محددة يجب احترامها ومراعاتها .

1/- الشروط الشكلية:

أ/-لابد من الحصول على إذن مسبق من السيد وكيل الجمهورية أو قاضي التحقيق، والذي يجب أن يكون مكتوبا محددًا بدقة الإجراء الواجب القيام به، وإلا اعتبر باطلا وكذا تحديد هوية ضابط الشرطة القضائية في حالة التسرب .

ب/- أن يكون لمدة أقصاها أربعة أشهر قابلة للتجديد حسب مقتضيات التحري أو التحقيق.

ج/- لا بد على ضابط الشرطة القضائية أن يحرر محضر بذلك يذكر فيه تاريخ وساعة بداية الإجراء والإنتهاء منه يصف أو ينسخ المراسلات أو الصور أو المحادثات المسجلة والمفيدة في إظهار الحقيقة، وهذا المحضر يودع بملف القضية.

¹ زوزو، هدى. "التسرب كأسلوب من أساليب التحري في قانون الإجراءات الجزائية الجزائري". مجلة دفاتر السياسة والقانون، مجلد 6، عدد 11، جامعة محمد خيضر - بسكرة -، الجزائر، جوان 2014، ص. 117

² الأمر رقم 66-155 المؤرخ في 8 يونيو 1966، الذي يتضمن قانون الإجراءات الجزائية المعدل والمتمم.

³ أنظر نص المادة 47 من الدستور، المرسوم الرئاسي رقم: 20-442 المؤرخ في: 30-12-2020، المتضمن التعديل الدستوري، الجريدة الرسمية، ع 82، المؤرخة في: 30-12-2020.

2/- الشروط الموضوعية:

أ/- لا بد أن يكون الهدف منها جمع الأدلة المتعلقة بالجريمة محل الترصد الالكتروني، وتحت مراقبة قاضي التحقيق لكي يكون وفقاً لمقتضيات القانون.

ب/- لا بد أن تكون الجريمة من الجرائم المتعلقة بالتزوير الواردة في القانون 02-24.

ج/- لا بد من تسبب الإذن، حيث يظهر العناصر التي جعلت الجهات المختصة تلجأ الى احداها .

الفرع الثاني: امكانية اللجوء الى التفتيش الالكتروني

منح المشرع في القانون 02-24 إمكانية اللجوء إليه قصد معاينة جريمة أو أكثر من الجرائم المنصوص عليها في هذا القانون لإرتباط التزوير بالمحررات الإلكترونية، كونه كان يعتبر اعتداء خطير على حريات وحقوق الإنسان التي كفلها له الدستور والقانون في كافة النظم القانونية لهذا وجب توضيح المقصود من التفتيش وضوابطه.

أولاً: تعريف التفتيش الالكتروني

تضر الخطورة هذا الإجراء تكفل كل من الفقه والقضاء بمحاولة إعطاء تعريفات للتفتيش منها: "إجراء من اجراءات التحقيق تقوم به سلطة حددها القانون، يستهدف البحث عن الأدلة المادية لجناية أو جنحة تحقق وقوعها في محل خاص يتمتع بالحرمة بغض النظر عن إرادة صاحبه".¹

¹ بيومي الحجازي، عبد الفتاح. المرجع السابق، ص 625.

أما التفتيش الالكتروني فيقصد به: " أحد اجراءات التحقيق تقوم به سلطة مختصة في هذا المجال للدخول الى نظم المعالجة الآلية للبيانات، بما تشمله من مدخلات ومخرجات بحثا عن آثار الجرم التي قد يخلفها الفاعل، كل هذا لتجميع الأدلة ضده وبالتالي نسبة الجرم له"¹ لقد نظم المشرع الجزائري أحكام التفتيش بوجه عام في المواد من 44 الى غاية 47 من قانون الإجراءات الجزائية، ومن المادة 79 الى فاية المادة 86 من ذات القانون، أما التفتيش الالكتروني فقد نص عليه في الفصل الثالث من القانون 04-09 المؤرخ في: 05-أوت - 2009 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها طبقا لنص المادة 05 منه.²

تعد جرائم التزوير واستعمال المزور من الجرائم التي نص المشرع على إمكانية اللجوء إليه طبقا من نص المادة 16 من القانون 02-24، إلا أن المشرع لم يضع تعريف له كما لم ينص على إجراءاته وشروطه بل ركز على محله، وهذا ما يجعلنا نرجع الى القوانين ذات الصلة ألا وهي قانون الإجراءات الجزائية أو القانون 04-09 .

ثانيا: شروط تطبيق التفتيش

يعتبر التفتيش من أخطر اجراءات التحقيق كونه يمس بحرمة الأشخاص وحياتهم الخاصة المحمية قانونيا ودستوريا، لذا أحاطه المشرع بجملة من الشروط والاجراءات يجب اتباعها .

1- أن يكون سبب التفتيش وقوع جريمة من الجرائم الواردة في القانون 02-24

لم يحدد المشرع نوع الجريمة المراد إجراء التفتيش الالكتروني، لكن ومن خلال نص المادة 16 من القانون 02-24 هي جريمة التزوير الالكتروني لما حدد محل التفتيش في

¹ نسيغة، فيصل وعبير بعقيقي. "الإثبات في الجرائم المعلوماتية، أو هو البحث عن الدليل الموجود أو المخزن في شكل إلكتروني." مجلة كلية الحقوق والعلوم السياسية، جامعة الوادي، الجزائر، مجلد 9، عدد 2، جوان 2018، ص. 45.

² الجريدة الرسمية، العدد 47، المؤرخة في 16-أوت-2009.

المعلوماتية أو المعطيات المخزنة فيها، أو منظومة تخزين معلوماتية¹ فالجريمة المقصودة هي جريمة التزوير الالكتروني مادام وسع من مدلول المحرر ليشمل المكتوب الورقي او الالكتروني، كما لم يحدد الوسيلة التي يتم بها التزوير وهذا طبقا لنص المادة 02 من ذات القانون.

وهناك شرط ضمني يكمن في انتساب الجريمة لشخص او عدة أشخاص بغض النظر عن مركزهم القانوني، فلا يعقل إجراء التفتيش الالكتروني دون تحديد الشخص الموجهة إليه التهمة بارتكابه لجريمة التزوير .

2- لا بد من إذن أو أمر بالتفتيش

بما أن التفتيش الالكتروني يمس الحريات الفردية، وبما أنه لا يوجد نص خاص مما يستدعي تطبيق القواعد العامة التي تقتضي بضرورة الحصول على إذن بالتفتيش بغية الدخول إلى النظام المعلوماتي وتفتيشه في حالة قيامه من طرف ضابط الشرطة القضائية، والذي ينبغي أن يحتوي على البيانات الضرورية منها أن يكون مكتوبا، تحديد وصف الجريمة، أن يبين محل التفتيش، وأن يكون موقعا ومؤرخا كما يجب أن يكون إذن التفتيش مسببا .

3- لا بد من حضور القاضي المختص الأمر به

إجراء التفتيش الالكتروني يكون إما من طرف القاضي المختص تلقائيا أو إذا طلبه ضابط الشرطة القضائية، لكن يشترط حضور الأمر به طبقا لنص المادة 16\ 03 من القانون 02-24 دون اشتراط حضور المعني عملية التفتيش الالكتروني، إلا أنه وطبقا لنص المادة 45 في فقرتها الأخيرة من قانون الإجراءات الجزائية فقد استثنى المشرع حضور الأشخاص

¹ بن طالب، ليندا. "التفتيش في الجريمة المعلوماتية." مجلة العلوم القانونية والسياسية، مجلد 8، عدد 16، كلية الحقوق والعلوم السياسية، جامعة الوادي، الجزائر، جوان 2017، ص. 493.

عند القيام به، ويرجع ذلك لإضفاء صفة السرية أثناء جمع الدليل الالكتروني نظرا لكونه ذو طبيعة خاصة فهو سريع الاتلاف والتلاعب فيه حتى عن بعد.¹

وانطلاقا دائما من خصوصية الدليل من حيث صعوبة الوصول إليه كونه مرتبط بمسألة تقنية فإن القائم بعملية التفتيش الالكتروني يشترط فيه العلم والدراسة بتقنية المعلومات، كما يجب أن يرافقه شخصا متخصصا في المعلوماتية لأنها مسألة فنية وهذا ماأكدت عليه المادة 16-03 من ذات القانون، وعليه فبخصوص المشرع الجزائري نجد أنه حدد بوضوح الجهة المختصة سواء في مجال الإذن بوضع ترتيبات المراقبة الالكترونية أو في مجال الدخول بغرض تفتيش منظومة المعلوماتية أو جزء فيها فنجد نص المادة 04-أ من القانون رقم 04-09 الذي ينص على: "إذ يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية المتبني للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته المنصوص عليها بموجب المادة 13 من نفس القانون إذن بالتفتيش لمدة ستة أشهر قابلة للتجديد التي تسمح باللجوء الى المراقبة الالكترونية"²

فيما عدا هذه الحالة الخاصة وبموجب نص المادة 05 من القانون 04-09 "يجوز للسلطات القضائية المختصة وكذلك الشرطة القضائية...الدخول بغرض التفتيش"، إذ يتعين الرجوع الى المادة 37 من قانون الإجراءات الجزائية سواء بالنسبة لوكيل الجمهورية أو قاضي التحقيق بموجب المادة 40، اللذان ينصا على تحديد الاختصاص لكل من وكيل الجمهورية أو قاضي التحقيق في جرائم محددة من نيتها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.³

¹ المادة 04 من القانون رقم 04-09 .

² المواد 37 و 40 من قانون الإجراءات الجزائية من الأمر رقم 66-155 المؤرخ في 23-يونيو-1966 المتضمن قانون الإجراءات الجزائية المعدل والمتمم من القانون 17-07 المؤرخ في 17-03-2017.

³ المادة 47 من قانون الإجراءات الجزائية الجزائري والتي نصت على: "لا يجوز البدء في تفتيش المساكن أو معابنتها قبل الساعة الخامسة (5) صباحا، ولا بعد الساعة الثامنة (8) مساء إلا إذا طلب صاحب المنزل ذلك أو وجهت نداءات من الداخل أو في الأحوال الاستثنائية المقررة قانونا".

أما مدته فهو غير مقيد بآجال محددة، بخلاف التفتيش وفقا للقواعد العامة والمحدد مابين الساعة الخامسة صباحا أو الثامنة مساء كأصل عام تطبيقا لنص المادة 47 من قانون الإجراءات الجزائية⁴، فقد استثناءه المشرع من خلال مضمون المادة 16 من ذات القانون، فقط تكون كافية له، وهذا لخصوصية الدليل كونه سريع التلف أو التعديل مما يستدعي عنصر المباغتة في عملية التفتيش حتى يحقق الغاية من اجرائه .

4-محضر التفتيش في الجرائم الإلكترونية

بعد قيام جهات التحقيق بالتفتيش في البيئة الالكترونية فلا بد أن يترجم مجهودات هذه الآلية في محضر تثبت فيه ماتقرمن اجراءات وما أسفر عن التفتيش من أدلة، وهذا الأخير يجب أن يقوم به شخص متخصص في الحاسوب والأنترنت وكذا إحاطة قاضي التحقيق أو عضو النيابة بهذه المعلومات والمحاضر التي تم تحريرها، مع ذكر اسم من قام بإجراء التفتيش وتاريخ التفتيش وساعاته، وتبيان كل الوقائع والأشخاص التي حضرت مع الحصول على توقيعهم.¹

¹ ترجمان، نسيمه .المرجع السابق، ص 156.

المبحث الثاني: الآليات الوقائية لجريمة تزوير التوقيع الإلكتروني .

يعتبر التوقيع الإلكتروني من بين الجرائم المستحدثة التي لاقت اهتماما واضحا من مختلف التشريعات لكن بالرغم من وضع المشرع للقانون رقم 04-15 إلا أنه لم يجرم هذا الأخير وعليه تم الاعتماد على الآليات الاجرائية لجريمة التزوير وتطبيقها على هذا التوقيع الإلكتروني وجزئية من قانون العقوبات (القسم السابع مكرر).

المطلب الأول: الحماية الالكترونية للتوقيع الإلكتروني من التزوير .

تعتبر مسألة الأمن المعلوماتي من أهم الضمانات والتحديات التي تواجهها وسائل الدفع الإلكتروني لأن في غيابه يعيق اعتماد التجارة الالكترونية على الرغم من المزايا التي توفرها، فهو حماية جميع المعلومات التي يتم التعامل معها والمعالجة من منظمة وغرفة تشغيل أجهزة ووسائل التخزين من السرقة والتزوير والتلف والضياع وكذا الاختراق .

لهذا وجب العمل على إيجاد آليات كفيلة تبعث الثقة والاطمئنان لدى المتعاملين به، مع تحقيق الحماية الضرورية للتوقيع الإلكتروني من أي تحايل أو إختراق، ما جعل المشرع يعتبر عملية التشفير كإجراء إلكتروني تقني لحماية البيانات الالكترونية إضافة الى تنظيم مهام جهة التوثيق الإلكتروني وتحديد مسؤولياتها قصد تحقيق الأمن القانوني للمتعاملين إلكترونيا.¹

الفرع الأول: نظام التشفير

من أفضل التقنيات التي تساعد على حماية البيانات والمعلومات المرسلة عبر الشبكات المفتوحة من أي تعديل أو تغيير غير مرغوب فيه، فتأتي هذه التقنية في مقدمة الوسائل التي توفر الأمن وسرية المعلومات والمعاملات.

¹ صدراتي، وفاء .المرجع السابق، ص 595.

أولاً: المقصود بالتشفير

تناول الفقه تعريفاً للتشفير واعتبره بأنه: "تغيير في البيانات عن طريق تحويلها إلى رموز أو اشارات لمنع الغير من معرفتها أو تعديلها".¹

وهناك من عرفه بأنه: "كل العمليات التي تؤدي بفضل بروتوكولات سرية إلى تحويل معلومات أو إشارات مفهومة (مقروءة)، أو القيام بالعكس وذلك باستخدام برامج مصممة لهذه الغاية".²

أما بالنسبة للتعريف التشريعي فلم يرد تعريف التشفير ضمن القانون رقم 04-15 المتعلق بالتوقيع والتصديق الإلكترونيين، كما وقع ذلك في أغلب التشريعات الأوروبية أو العربية من أن تنظيمه يعد من المسائل الضرورية في ميدان المعاملات الإلكترونية، وإنما نص فقط على أنظمة التشفير في المادة 2 بند 8-9 من القانون 04-15 والتي تتمثل في:

أ/- **مفتاح التشفير الخاص:** هو عبارة عن سلسلة من الأعداد يحوزها حصرياً الموقع فقط، وتستخدم لإنشاء التوقيع الإلكتروني، ويرتبط المفتاح بمفتاح تشفير عمومي.

ب/- **مفتاح التشفير العام:** هو عبارة عن سلسلة من الأعداد تكون موضوعة في متناول الجمهور بهدف تمكينهم من التحقق من الإمضاء الإلكتروني وتدرج في شهادة التصديق الإلكتروني.³

يتضح من التعاريف الواردة على اعتبار التشفير عملية تحويل المعلومات إلى رموز غير مفهومة لمنع الغير من الاطلاع عليها أو فهمها ولهذا تتطوي عملية التشفير أساساً على

¹ ترجمان، نسيم. المرجع السابق، ص 52.

² ترجمان، نسيم. المرجع السابق، ص 52.

³ المادة 2 من القانون رقم 04-15 المتعلق بالتوقيع والتصديق الإلكترونيين.

تحويل النصوص العادية الى نصوص مشفرة ومن المعلوم أن الإنترنت تمثل الوسيلة أكثر استعمالا لتوصيل المعلومات.¹

ثانيا: ضوابط وطرق التشفير

أ/- ضوابط التفتيش:

نص المشرع الجزائري على ضرورة التشفير، كما نص على العمل من أجل الحفاظ على سرية البيانات والمعلومات المشفرة وتتمثل هذه الضوابط في:

1. مشروعية تشفير البيانات والمعلومات والتي يتم تبادلها عن طريق الوسائط الإلكترونية، إذ أقر المشرع الجزائري من خلال القانون 04-15 نصوصا تتناول نظام التشفير، وعرف التشفير الخاص العام وأجاز استخدامه في المراسلات الإلكترونية والتعاملات التجارية الإلكترونية، كما أكد على حماية البيانات المشفرة والعناصر المستخدمة في عملية التشفير وفكها في اعتداء سواء تم ذلك باستخدام عناصر التشفير الخاصة بالتوقيع من غير طرفي العلاقة، أو بسبب استخدام التشفير في ارتكاب جرائم احتيالية.

2. الحق في الحفاظ على سرية البيانات والمعلومات المشفرة: اعتبر المشرع الجزائري من خلال القانون 04-15 من خلال المادتين 42 و 1\11 على البيانات المرسلة بين طرفي العقد عبر الوسائط الإلكترونية هو اعتداء على خصوصية وسرية البيانات والمعلومات المرسلة بين طرفي العلاقة المتوفرة، وبالتالي وجب ضمان سرية البيانات المستخدمة لإنشاء التوقيع الإلكتروني بكل الوسائل التقنية المتوفرة²

¹ حوحو، يمينة. عقد البيع الإلكتروني في القانون الجزائري. دار بلقيس للنشر والتوزيع، دار البيضاء، الطبعة الأولى، 2016، ص. 187.

² عقوني، محمد. "الآليات التقنية والقانونية لحماية التوقيع الإلكتروني". مجلة المفكر، عدد 18، 2019، ص. 304.

كما أقر المشرع الجزائري نصوصا تعاقب كل من يقوم بانتهاك سرية البيانات المشفرة وافشائها سواء من طرف الغير، أو من الطرف مؤدي خدمات التصديق الإلكتروني، أو من طرف الشخص المكلف بالتدقيق.

3. كما نجد أن المشرع الجزائري قد اعتبر النص المشفر من المحررات الالكترونية، وذلك من خلال تحويل تلك الاشارات والرموز الى نصوص مقروءة ومفهومة وتكون حجة على من يخالف ما التزم به طرفا الاتفاق¹

ب/- طرق التشفير:

يمكن تصنيف طرق التشفير الى فئتين رئيسيتين بالنظر الى نوعية المفتاح المستخدم في التشفير:

1- التشفير المتماثل: يقوم هذا النوع على وجود مفتاح متماثل لتشفير المعلومات وفك التشفير، حيث يقوم المرسل بكتابة السند أو الرسالة أو المعلومات وتشفيرها، ثم يزود المرسل إليه بالمفتاح المتماثل لكي يفك تشفير الرسالة ويستعيد صيغتها الأصلية التي كانت عليها قبل عملية التشفير.

من الصعوبات التي تواجه هذا النوع من التشفير هي إيجاد آلية آمنة لنقل المفتاح المتماثل من المرسل الى المرسل إليه، كما أنه على المرسل إليه الذي يتلقى الرسائل من جهات مختلفة أن يحتفظ بعدد من المفاتيح يساوي عدد الرسائل الواردة إليه من الجهات.²

2- التشفير اللامتماثل: يطلق على هذه التقنية التشفير بالمفتاح العمومي وخلافا للتشفير بالمفتاح الخصوصي لا يستعمل المفتاح ذاته من أجل تشفير الرسائل، بحيث يستعمل مفاتيح سريين مختلفين من أجل فك تشفيرها الأول خصوصي يملكه مستخدم معين

¹ عقوني، محمد. المرجع السابق، ص 305.

² أبو شام، حنان عبده علي. "التوقيع الإلكتروني وحجيته في الإثبات." www.ajsp.net، عدد 18، 12 نيسان 2020، ص. 493.

لمستعمل الوسائط الإلكترونية وبقية سريا وخصوصا به، أما الثاني عمومي يوزع إلى المتعاملين الآخرين الذي يود تلقي رسائل مشفرة منه.¹

الفرع الثاني: التصديق الإلكتروني.

تظهر الحاجة إلى طرف أو جهة ثالثة في المعاملات الإلكترونية تلعب دور الوسيط المؤتمن بين المتعاملين في هذه البيئة، فتأكد هوية الأطراف وتحدد أهليتهم للتعاون وتضمن سلامة محتوى البيانات المتداولة من خلال اجراءات موسومة بـ "التصديق الإلكتروني" أولاً: تعريف التصديق الإلكتروني.

يعرف التصديق بأنه: «مجموعة من الأشياء أو العناصر التي تعتمد على الغرض الذي يراد استخدام التوثيق لتحقيقه»² كما يعرف على أنه عملية لتحقيق التأكد والموثوقية في هوية المستخدم باستخدام الأجهزة والكيانات الأخرى من خلال نظم المعلومات والاتصالات³

من خلال ما سبق يمكن تعريف التصديق الإلكتروني على أنه مجموعة من الاجراءات والعمليات الرامية إلى التأكد من هوية صاحب التوقيع الإلكتروني والتأكد على سلامة المحرر الذي يحمل هذا التوقيع بهدف ضمان الأمان والموثوقية حول هذا المحرر الإلكتروني والتوقيع الإلكتروني ويقوم بهذه الإجراءات طرف محايد بين أطراف المعاملات الإلكترونية يطلق عليه اسم مقدم خدمات التصديق الإلكتروني.⁴

فباختلاف التعاريف نجد اختلاف التسمية للتصديق الإلكتروني فهناك من يسميه بالمصادقة ومن يسميه بالتصديق وآخرون بالتوثيق.

¹ صدراتي، وفاء. المرجع السابق، ص 597.

² الشنراقي، حسام محمد نبيل. الجرائم المعلوماتية: دراسة تطبيقية مقارنة على جرائم الاعتداء على التوقيع الإلكتروني. دار الكتب القانونية، دار شتات للنشر والبرمجيات، مصر والإمارات، 2013، ص. 79.

³ العبيدي، أسامة بن غانم. "حجية التوقيع الإلكتروني في الإثبات". المجلة العربية للدراسات الأمنية والتدريب، مجلد 28، عدد 56، جامعة نايف للعلوم الأمنية، 2012، ص. 161.

⁴ الشنراقي، حسام محمد نبيل. المرجع السابق، ص 82.

ونجد أن المشرع الجزائري أطلق عليه اسم التصديق مثل ما جاء به نص القانون رقم 04-15

المتعلق بالتوقيع والتصديق الإلكترونيين حيث عرف سياسة التصديق الإلكتروني بنص المادة 2 الفقرة 15 على أنها مجموع القواعد والإجراءات التنظيمية والتقنية المتعلقة بالتوقيع والتصديق الإلكترونيين.¹

ثانيا: دور الجهات المختصة بإصدار شهادات التصديق الإلكتروني في حماية التوقيع الإلكتروني.

تعددت التعريفات سواء كانت فقهية أم قانونية لجهات التصديق على التوقيع الإلكتروني، ومن أهم هذه التعريفات نورد ما يلي:

عرف جانب من الفقه القانوني مزود خدمات التصديق بأنه: "هيئة عامة أو خاصة تسعى إلى ملء الحاجة الملحة لوجود طرف ثالث موثوق به، يقدم خدمات أمنية في التجارة الإلكترونية من خلال إصدار شهادات تثبت حقيقة معينة متعلقة بموضوع التبادل الإلكتروني، لتوثيق هوية الأشخاص مستخدمي التوقيع الرقمي، وكذلك نسبة المفتاح العام المستخدم إلى صاحبه".²

وعرق قانون الأونسترال النموذجي المتعلق بالتوقيعات الإلكترونية لسنة 2001 جهة التصديق أو مقدم خدمات التصديق بنص المادة 2-e بأنه: "الشخص الذي يصدر الشهادات الإلكترونية، ويمكن أن يقدم خدمات أخرى مرتبطة بالتوقيعات الإلكترونية".³

¹ "المادة 2 من القانون 04-15، المؤرخ في 1-2-2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين." الجريدة الرسمية للجمهورية الجزائرية، العدد 6.

² البياتي، نادية ياس. المرجع السابق، ص 263.

³ الشنراقي، حسام محمد. المرجع السابق، ص 89.

Art2-e: "certification service provider means: a person that issues certificates and my provide other service related to electronic signatures".

أما التوجيه الأوروبي بشأن التوقيعات الإلكترونية فقد عرف مقدم خدمة التصديق بنص المادة 02 الفقرة 11 منه، بأنه: "كل كيان أو شخص طبيعي أو معنوي يقدم شهادات التصديق أو خدمات أخرى لها علاقة بالتوقيعات الإلكترونية".¹

أما المشرع الجزائري فقد تناولها بصفة عرضية في المادة 03 من النرسوم رقم 162-07 لسنة 2007 والتي نصها: "مؤدي خدمات التصديق هو كل شخص في مفهوم المادة 08/08 من القانون رقم 2000-03 المؤرخ في 05-08-2000، يسلم شهادات إلكترونية أو يقدم خدمات أخرى في مجال التوقيع الإلكتروني".²

وبالرجوع إلى المادة 08-08 من القانون السابق الذكر (القانون رقم 162-07) فقد جاء فيها أن: «موفد الخدمة هو كل شخص معنوي أو طبيعي يقدم خدمة مستعملا وسائل المواصلات السلكية واللاسلكية.»

كما تناول المشرع الجزائري تعريف جهات التصديق الإلكتروني أو مؤدي خدمات التصديق في القانون رقم (04-15) لسنة 2015 في الفقرة 12 من المادة 02 والتي نصت على أن: «مؤدي خدمات التصديق هو كل شخص طبيعي أو معنوي يقوم بمنح شهادات تصديق إلكترونية موصوفة، وقد يقدم شهادات أخرى في مجال التصديق الإلكتروني». ³

فمن خلال ما سبق تبين أن الهدف الأساسي في إنشاء جهات مختصة في إصدار شهادات التصديق الإلكتروني في تسهيل مراقبة التعاملات الإلكترونية تكمن في إضفاء ضمانات قانونية تحمي وتحافظ على سلامة التوقيع الإلكتروني مع إصدار شهادة التصديق

¹ التوجيه الأوروبي الصادر في 13 ديسمبر 1999 بشأن التوقيعات الإلكترونية.

Art2-11: "prestataire de service de certification tout entité ou personne physique ou morale qui délivre des certificats ou fournit d'autre service liés aux signatures électroniques".

² المرسوم التنفيذي رقم 162-07 المؤرخ في 30-05-2007 المعدل والمتمم للمرسوم التنفيذي رقم 123-01 الصادر في 09-05-2001، المتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية.

³ القانون رقم 04-15 لسنة 2015، المرجع السابق.

الإلكتروني والتحقق من هوية الشخص الموقع، إضافة إلى إثبات مضمون البيانات الإلكترونية، وإصدار مفاتيح التشفير، نحاول إنجاز ما يلي:

أ- إصدار شهادة التصديق الإلكتروني:

ميز المشرع الجزائري بين الشهادة الإلكترونية البسيطة، والشهادة الإلكترونية الموصوفة فالشهادة الإلكترونية البسيطة تتطلب إجراءات ترتبط بمعطيات ومعلومات تتعلق بالتحقق من توقيع شخص معين وتأكيد هوية هذا الشخص.¹

أما شهادة التصديق الإلكترونية الموصوفة، فإنها ترتبط بإصدار الشهادة النوعية وفق شروط حددها المشرع من بينها أن تتضمن على الخصوص التوقيع الإلكتروني الموصوف.²

ب- التحقق من هوية الشخص الموقع:

تقوم جهات التوثيق الإلكتروني بإصدار شهادة توثيق إلكترونية تقيد التصديق على التوثيق الإلكتروني في تعاقد معين تشهد بموجبها بصحته ونسبته إلى مصدر صدر عنه.

و يوجب التحقق من هوية الموقع من خلال جهة التوثيق، تحديد الأهلية القانونية للمتعاقد، وكذلك التحقق من سلطات هذا الشخص واختصاصاته الوظيفية.³

ج - إثبات مضمون التبادل الإلكتروني:

يقصد بالتبادل الإلكتروني «مجموعة معايير يتم استخدامها في تبادل معلومات العمل وتناقلها بين الشركاء التجاريين من خلال أجهزة الكمبيوتر، وفي تنفيذ صفقات الأعمال بطريقة إلكترونية».⁴

¹ "المادة 3 مكرر من المرسوم التنفيذي 07/162، المؤرخ في 30 ماي 2007." المرجع السابق.

² المادة 7/2 والمادة 2/11 من القانون 04-15. "المرجع السابق."

³ سليمان، محمد مأمون. التحكم الإلكتروني. دار الجامعة الجديدة، الإسكندرية، 2011، ص ص. 250-251.

⁴ العاني، إيمان. البنوك التجارية وتحديات التجارة الإلكترونية. رسالة ماجستير، جامعة منتوري قسنطينة، 2007، ص.

حيث تتولى جهة التوثيق التحقق من مضمون التبادل الإلكتروني بين الأطراف وسلامته وجديته وبعده عن الاحتيال والغش، فضلا عن إثبات وجوده ومضمونه.¹

أما تحديد لحظة إبرام العقد أو ما يسمى بإبرام التصرف القانوني ليس شرطا لصحة هذا التصرف، ومع ذلك فإن تحديد تلك اللحظة يكون ضروريا، إذ أن وقت إبرام العقد يعد هو لحظة بداية لبدء الآثار القانونية.

د - إصدار المفاتيح الإلكترونية:

و تتولى هذه الجهات إصدار المفاتيح الإلكترونية سواء المفتاح الخاص الذي من خلاله يتم تشفير المعاملة الإلكترونية أو المفتاح العام الذي يتم بواسطته فك التشفير، بالإضافة إلى ذلك تقوم هذه الجهة بإصدار التوقيع الرقمي.

المطلب الثاني: العقوبات المقررة لجريمة تزوير التوقيع الإلكتروني.

الفرع الأول: في قانون العقوبات.

لقد تناول المشرع الجزائري الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات واستعمال الإعلام الآلي وذلك في القسم السابع مكرر الذي جاء بعنوان "المساس بأنظمة المعالجة الآلية للمعطيات"، وكيف الأفعال الغير مشروعة على أنها جنح والتي حصرها فيما يلي:

1. جريمة الدخول أو البقاء في المنظومة عن طريق الغش نصت على هذه الجريمة المادة 394 مكرر، من قانون العقوبات الجزائري، على أنه:

يعاقب بالحبس من ستة (6) أشهر إلى سنتين (2) وبغرامة من 60.000 دج إلى 200.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.

تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير معطيات المنظومة.

¹ سليمان، محمد مأمون. المرجع السابق، ص 251.

و إذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة، تكون العقوبة الحبس في سنة (1) إلى ثلاثة (3) سنوات والغرامة من 100.000 دج إلى 300.000 دج.¹

فالدخول غير المرخص به عن طريق الغش للمنظومة المعلوماتية سواء نص الدخول أو البقاء كل أو جزء من المنظومة ويكفي إثبات المحاولة لتطبيق أحكام المادة ولا يشترط لقيام هذه الجريمة إلحاق إضرار بالمنظومة المعلوماتية.²

2. جريمة إدخال المعطيات في منظومة المعالجة الآلية أو ازال أو حذف أو عدل معطيات منظومة المعالجة الآلية عن طريق الغش ونصت على هذه الجريمة المادة 394 مكرر 1 على أنه:

يعاقب بالحبس من سنة (1) إلى ثلاث (3) سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها.³

تقوم هذه الجريمة بمجرد ارتكاب أحد الأفعال المذكورة سابقا بغض النظر عن المجال المستهدف سواء كانت البرامج أو المعطيات أو قاعدة بيانات التوقيع الإلكتروني.

3. جريمة تصميم أو بحث أو تجميع أو توفير أو نشر الاتجار في معطيات مخزنة أو معالجة أو مرسلّة عن طريقة منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم وجريمة حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في القسم السابع مكرر من قانون العقوبات، ويعاقب من قام بتلك الأفعال بالحبس من سنة (1) إلى خمس (5) سنوات

¹ المادة، 394 قانون العقوبات.

² لالوش، راضية. أمن التوقيع الإلكتروني. مذكرة ماجستير، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، دون تاريخ، ص. 165.

³ المادة 394 مكرر، وما يليها.

وبغرامة من 1.000.000 دج إلى 5.000.000 دج، كل مت يقوم عمدا وبطريق الغش الأفعال السابقة الذكر، كما نجد أن المادة 394 مكرر 5 قد نصت على كل من شارك في مجموعة أو في اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في ذات القسم، بحيث يكون هذا التحضير مجسدا بفعل أو عدة أفعال مادية، يعاقب بالعقوبة المقررة للجريمة ذاتها، بالإضافة إلى المادة 394 مكرر 7 التي نصت على تجريم الشروع في الأفعال الآتية الذكر.¹

الفرع الثاني: القانون رقم 04-15 المؤرخ في 11 ربيع الثاني 1436 الموافق لـ 1 فبراير 2015.

و الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكتروني، حيث جاء الباب الرابع منه بعنوان العقوبات أما الفصل الثاني منه جاء بجملة من الأحكام الجزائية التي تضمن تحديد العقوبات بالحبس وبالغرامة المالية فيما يتعلق بالتجاوزات التي يمكن وقوعها ضد أحكام هذا القانون كما أصدر المشرع الجزائري قانون مكافحة الجرائم المعلوماتية المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها القانون رقم 09-04.

¹ المواد 394 مكرر 5 ومايليها (قانون العقوبات الجزائري).

الخلاصة:

تناول هذا الفصل الإشكالية القانونية والإجرائية المرتبطة بجريمة تزوير التوقيع الإلكتروني، باعتبارها من أبرز الجرائم المستحدثة في ظل التحول الرقمي المتسارع. وقد تم التركيز على أوجه القصور التي تعاني منها القواعد الإجرائية التقليدية عند التصدي لهذه الجريمة، نظراً لاعتمادها على مفاهيم مادية لا تتلاءم مع الطبيعة الرقمية للجريمة التي تُرتكب في بيئة افتراضية يصعب فيها تطبيق ذات الآليات الإجرائية المعمول بها في الجرائم العادية.

أبرز الفصل أن التشريعات الوطنية، ومن بينها التشريع الجزائري، حاولت تنظيم مجال التوقيع الإلكتروني من خلال قوانين خاصة، على غرار القانون رقم 04-15، إلا أن هذه النصوص لم تتضمن تجريمًا صريحًا لفعل تزوير التوقيع الإلكتروني كجريمة قائمة بذاتها. وهو ما دفع الجهات القضائية إلى تكييف هذا الفعل ضمن أحكام التزوير التقليدي المنصوص عليها في قانون العقوبات، لا سيما القسم السابع مكرر، رغم ما يطرحه هذا التكييف من إشكالات تتعلق بتحديد الأركان المادية والمعنوية للجريمة في السياق الرقمي، وصعوبة إثباتها بالوسائل التقليدية.

كما بين الفصل توجه العديد من التشريعات المقارنة إلى تطوير قواعد إجرائية خاصة تراعي طبيعة الأدلة الرقمية، من خلال استحداث وسائل جديدة مثل التفتيش الإلكتروني، المراقبة التقنية، واعتراض المراسلات الرقمية. وخلص إلى أن غياب نصوص جزائية واضحة وإجراءات رقمية فعالة يؤدي إلى تقويض جهود ملاحقة الجناة ويُعرض الأمن القانوني الرقمي للخطر.

واختتم الفصل بالتأكيد على أن مجابهة هذه الجريمة تتطلب مقاربة تشريعية شاملة وتعاونًا دوليًا فعالاً، من خلال توحيد الجهود عبر الاتفاقيات الدولية وتعزيز التعاون الأمني والقضائي بين الدول، بما يضمن حماية المعاملات الرقمية ويعزز الثقة في الفضاء السيبراني.

خاتمة

خاتمة:

من خلال ما تم عرضه، يتضح أنه على الرغم من صدور القانون رقم 15/04 المتعلق بالتصديق والتوقيع الإلكتروني، ومصادقة الجزائر على الاتفاقية العربية لمكافحة جرائم الإنترنت، فضلاً عن اعتراف المشرع الجزائري في تعديل القانون المدني لسنة 2005 بصحة الإثبات بواسطة المستندات الإلكترونية الموقعة، إلا أن المشرع لم ينص صراحة على جريمة تزوير التوقيع الإلكتروني

كما لا يمكن تطبيق النصوص المتعلقة بجريمة التزوير التقليدي على هذا النوع من الجرائم نظراً لاختلاف محل الحماية القانونية، إذ أن التوقيع الإلكتروني يختلف في طبيعته ووسائله عن التوقيع التقليدي. وكذلك لا يمكن الاستناد إلى النصوص الخاصة بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، نظراً لاختلاف المصلحة القانونية المحمية فيها عن تلك المتعلقة بتزوير التوقيع الإلكتروني.

ويُضاف إلى ذلك أن مبدأ حظر القياس في القانون الجنائي يمنع التوسع في تفسير النصوص لتشمل هذا النوع من الأفعال، الأمر الذي يبرز الحاجة إلى تدخل تشريعي صريح لمعالجة هذا الفراغ القانوني

ومنه توصلنا الى النتائج التالية مقترنة باقتراحات تساعد من معالجة النقائص التي وجدت نبينها فيما يلي:

أولاً: النتائج

1. تزوير التوقيع الإلكتروني يُعد من الجرائم المستحدثة التي ظهرت نتيجة تطور المعاملات الإلكترونية، وتشكل خطراً حقيقياً على الثقة في الوثائق الرقمية والمعاملات عن بُعد

2. بالرغم من أن القانون رقم 15/04 المتعلق بالتوقيع والتصديق الإلكتروني قد تضمن بعض الأحكام الرامية إلى حماية التوقيع الإلكتروني، إلا أنه لم ينص صراحة على تجريم تزوير هذا التوقيع. مما أحدث فراغا تشريعيا في مواجهة هذا النوع من الجرائم، ونظراً لاختلاف طبيعة هذه الجريمة عن جريمة التزوير التقليدي، وكذلك عن الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، فإن الأمر يقتضي استحداث نص خاص يُجرّم تزوير التوقيع الإلكتروني، سواء من خلال تعديل قانون العقوبات أو بإدراج نص تكميلي ضمن أحكام القانون: 04/15
3. السلطة القضائية اضطرت إلى تكييف تزوير التوقيع الإلكتروني ضمن أحكام التزوير التقليدي المنصوص عليها في قانون العقوبات، خصوصاً القسم السابع مكرر، وهو تكييف لا يخلو من صعوبات عملية وقانونية.
4. الآليات الإجرائية المعتمدة حالياً غير كافية للتعامل مع خصوصية الجريمة الرقمية، لا سيما في ما يتعلق بجمع الأدلة الرقمية وتوثيقها وحمايتها وفق المعايير القانونية.
5. غياب النصوص الخاصة بهذا النوع من الجرائم يعوق فعالية الملاحقة القضائية، ويترك المجال مفتوحاً أمام مرتكبيها للإفلات من العقاب أو إثارة إشكالات قانونية أثناء المتابعة القضائية

ثانياً: التوصيات

1. ضرورة تعديل التشريع الجزائي الجزائي من خلال إدراج نصوص صريحة تُجرّم تزوير التوقيع الإلكتروني كجريمة مستقلة، مع تحديد أركانها وعقوباتها بوضوح
2. وضع إطار إجرائي خاص للتعامل مع الجرائم الرقمية، يشمل إجراءات تفتيش وضبط وتحقيق رقمية تراعي طبيعة الدليل الإلكتروني، مع ضمان حماية الحقوق والحريات الأساسية

3. تكوين قضاة وضباط الشرطة القضائية والمحققين على الخصوصيات التقنية للجرائم الإلكترونية، لا سيما ما يتعلق بالتوقييع الرقمية وأمن نظم المعلومات.

4. تعزيز التعاون الدولي والإقليمي في مجال مكافحة الجرائم الإلكترونية، من خلال الانضمام إلى الاتفاقيات الدولية ذات الصلة، وتفعيل آليات تبادل المعلومات والخبرات.

5. العمل على التوعية القانونية والتقنية لدى المؤسسات والأفراد حول أهمية حماية التوقيع الإلكتروني، والآثار القانونية المترتبة على تزويره، للحد من ارتكاب هذه الجريمة

ومنه نستنتج أنه:

وفي ظل غياب نصوص صريحة تعالج هذا النوع من الجرائم الرقمية، يُثار التساؤل حول مدى إمكانية تطبيق أحكام التزوير التقليدي المنصوص عليها في قانون العقوبات على تزوير التوقيع الإلكتروني، رغم اختلاف الوسائل والأدوات المستخدمة.

تواجه الجهات القضائية صعوبات تقنية وقانونية متعددة، منها ضعف الخبرة الفنية، وغياب إطار تشريعي متخصص، مما يُضعف من فعالية إثبات التزوير الرقمي.

يظهر أن الإطار العام غير كافٍ لمواكبة تطور الجريمة الإلكترونية، مما يستدعي تدخلاً تشريعياً لوضع نصوص واضحة تُجرّم صراحة التزوير في التوقيع الإلكتروني وتحدد العقوبات المناسبة له

سُئِهم الإجابة عن هذه الأسئلة في تحديد مدى كفاءة المنظومة القانونية الحالية في الجزائر في التصدي لهذا النوع المستحدث من التزوير، وتُبرز الحاجة إلى تحديثها بما يتلاءم مع التحديات الرقمية المعاصرة.

قائمة المصادر والمراجع

قائمة المصادر والمراجع:

أولاً: التشريعات والقوانين

1. الجزائر. القانون رقم 04-15 المؤرخ في 1 فبراير 2015، المتعلق بالتوقيع والتصديق الإلكترونيين. الجريدة الرسمية للجمهورية الجزائرية، العدد 06، سنة 2015.
2. المرسوم التنفيذي رقم 07-162 المؤرخ في 30-05-2007، المعدل والمتمم للمرسوم التنفيذي رقم 01-123 المؤرخ في 01-05-2001.
3. القرار رقم 51-162 المؤرخ في 16 ديسمبر 1996 المتضمن قانون الأونسيترال النموذجي للتجارة الإلكترونية .
4. القرار رقم 56-80 المؤرخ في 12 ديسمبر 2001 المتضمن قانون الأونسيترال النموذجي للتوقيعات الإلكترونية .
5. القانون العربي الاسترشادي للإثبات بالتقنيات الحديثة، معتمد بالقرار رقم 24 د/771 المؤرخ في 27 نوفمبر 2008.
6. التوجيه الأوروبي الصادر في 13 ديسمبر 1999 بشأن التوقيعات الإلكترونية .

ثانياً: الكتب

7. البياتي، نادية ياس. التوقيع الإلكتروني عبر الإنترنت ومدى حجية الإثبات. الطبعة الأولى، دار البداية ناشرون وموزعون، الأردن، 2014.
8. السعيد، محمد. تقنيات البطاقات الذكية وتطبيقاتها. دار الفكر، 2020.
9. الشنراقي، حسام محمد نبيل. الجرائم المعلوماتية: دراسة تطبيقية مقارنة على جرائم الاعتداء على التوقيع الإلكتروني. دار الكتب القانونية، دار شتات للنشر والبرمجيات، مصر والإمارات، 2013.

10. العتيبي، فهد. "البطاقة الذكية ودورها في تطوير الخدمات الحكومية." مجلة التقنية الحديثة، العدد 15، 2021، ص. 45-52.
11. المرسي، الزهرة محمد. عناصر الدليل الكتابي الإلكتروني التقليدي. دون ناشر، 2001.
12. ربضي، عيسى غسان. القواعد الخاصة بالتوقيع الإلكتروني. الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2005.
13. سليمان، محمد مأمون. التحكيم الإلكتروني. دار الجامعة الجديدة، الإسكندرية، 2011.
14. محروك، محمد. "خصوصيات التوقيع الإلكتروني وحجته في الإثبات." جامعة القاضي عياض، مراكش.
15. يوسف، أمير فرج. التوقيع الإلكتروني. دار المطبوعات الجامعية، 2008.

ثالثاً: الأطروحات والرسائل الجامعية

16. الحاج علي، ألاء أحمد محمد. التنظيم القانوني لجهات التصديق على التوقيع الإلكتروني. رسالة ماجستير، كلية الدراسات العليا، جامعة النجاح الوطنية، فلسطين، 2013.
17. براهيم، حنان. جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية. أطروحة دكتوراه، كلية الحقوق، جامعة بسكرة، 2015.
18. ترجمان، نسيم. الحماية الجنائية للتوقيع الإلكتروني: دراسة مقارنة. أطروحة دكتوراه، جامعة ابن خلدون، تيارت، 2021.
19. حامدي، بلقايم. إبرام العقد الإلكتروني. أطروحة دكتوراه، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة، 2014-2015.

20. حفصي، عباس. جرائم التزوير الإلكتروني: دراسة مقارنة. أطروحة دكتوراه، تخصص شريعة وقانون، كلية العلوم الإنسانية والعلوم الإسلامية، جامعة أحمد بن بلة، وهران 1 ، 2015.
21. غربي، خديجة. التوقيع الإلكتروني. رسالة ماجستير، جامعة قاصدي مرباح .
22. لالوش، راضية. أمن التوقيع الإلكتروني. مذكرة ماجستير، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو .
23. طمين، سهيلة. الشككية في عقود التجارة الإلكترونية. رسالة ماجستير، جامعة مولود معمري، تيزي وزو، 2011.

رابعاً: المقالات العلمية

24. أبو شام، حنان عبده علي. "التوقيع الإلكتروني وحجته في الإثبات". www.ajsp.net، عدد 18، 12 نيسان 2020، ص 493 .
25. الربيع، إبراهيم إسماعيل، وعلاء موسى علي نالي. "التوثيق الإلكتروني وقرارات التحكيم في التوقيع الإلكتروني: دراسة مقارنة." مجلة المحقق الحلي للعلوم القانونية والسياسية، المجلد 1، 2012، ص 161، بابل، العراق .
26. الصفدي الطوال، عبير ميخائيل. النظام القانوني لجهات توثيق التوقيع الإلكتروني. الطبعة الأولى، دار وائل للنشر، 2010.
27. العاني، إيمان. البنوك التجارية وتحديات التجارة الإلكترونية. رسالة ماجستير، جامعة منتوري قسنطينة، 2007.
28. عقوني، محمد. "الآليات التقنية والقانونية لحماية التوقيع الإلكتروني." مجلة المفكر، عدد 18، 2019، ص 304 .

29. غلاب، عبد الحق. "خصوصية جريمة تزوير التوقيع الإلكتروني في التشريع الجزائري". مجلة الدراسات القانونية والسياسية، جامعة الجزائر 1، المجلد 8، العدد 1، جانفي 2022، ص. 493.
30. معزوز، عبد القادر. "الإثبات الإلكتروني في التشريع الجزائري". مجلة دراسات قانونية، العدد 12، 2021، ص. 88، جامعة الجزائر.
31. نسيم، ترجمان. "الحماية الجنائية للتوقيع الإلكتروني: دراسة مقارنة". مجلة العلوم القانونية والسياسية، مجلد 11، عدد 1، 2020، ص. 592.
32. يوسف، زروق. "حجية التوقيع الإلكتروني في الإثبات: دراسة مقارنة". مجلة الحقوق والعلوم الإنسانية، العدد 6، 2010.

خامسا: المصادر الإلكترونية

33. عجابي، إلياس. "الطبيعة القانونية للتوقيع الإلكتروني ASJP"، 2009. رابط المقال .
34. كرازي، سارة، ولجلط، فواز. "الحجية القانونية للتوقيع الإلكتروني كدليل للإثبات". المجلة الجزائرية للأمن الإنساني، 2021. رابط المقال .
35. ريام، وليد، وقرقور، جلال. "الحجية القانونية للتوقيع الإلكتروني". جامعة محمد البشير الإبراهيمي برج بوعريش، 2024. رابط الرسالة .
36. حميل، نورة. "التصديق الإلكتروني آلية لإضفاء الحجية القانونية على التوقيع الإلكتروني ASJP"، 2022. رابط المقال .
37. بن حاجة، أحمد. "الحجية القانونية للتوقيع الإلكتروني في التشريع الجزائري والمقارن ASJP"، 2016. رابط المقال .

فهرس الموضوعات

فهرس الموضوعات

الشكر والعرفان

الإهداء

1..... مقدمة:

الفصل الأول

الإطار الموضوعي لجريمة تزوير التوقيع الإلكتروني

9..... تمهيد:

10..... المبحث الأول: ماهية التوقيع الإلكتروني.

10..... المطلب الأول: تعريف التوقيع الإلكتروني.

10..... الفرع الأول: تعريف التوقيع الإلكتروني.

16..... المطلب الثاني: آلية إنشاء التوقيع الإلكتروني.

17..... الفرع الأول: متطلبات آلية إنشاء التوقيع الإلكتروني.

17..... الفرع الثاني: متطلبات آلية التحقق من التوقيع الإلكتروني.

18..... الفرع الثالث: شروط التوقيع الإلكتروني.

23..... المبحث الثاني: صور التوقيع الإلكتروني وحجته.

23..... المطلب الأول: صور التوقيع الإلكتروني.

23..... الفرع الأول: التوقيع الرقمي.

23..... الفرع الثاني: التوقيع البيومتري.

24..... الفرع الثالث: التوقيع بالقلم الإلكتروني.

25..... الفرع الرابع: التوقيع بالرقم السري.

المطلب الثاني: حجية التوقيع الالكتروني في مجال الإثبات.	28
الفرع الأول: شروط حجية التوقيع الالكتروني في التشريع الجزائري.	28
الفرع الثاني: حجية التوقيع الإلكتروني في التشريعات المقارنة.	29
الخلاصة:	32

الفصل الثاني

آليات الحماية القانونية للتوقيع الالكتروني

تمهيد:	34
المبحث الأول: الإطار الجزائي لجريمة تزوير التوقيع الالكتروني.	35
المطلب الأول: أركان جريمة تزوير التوقيع الالكتروني وأساليب التحري الخاصة.	35
الفرع الأول: الركن المادي.	35
الفرع الثاني: الركن المعنوي لجريمة تزوير التوقيع الالكتروني.	38
المطلب الثاني: الأحكام الاجرائية المساعدة في الكشف عن جرائم التزوير.	38
الفرع الأول: أساليب التحري الخاصة وشروط تطبيقها.	39
الفرع الثاني: امكانية اللجوء الى التفتيش الالكتروني.	42
المبحث الثاني: الآليات الوقائية لجريمة تزوير التوقيع الالكتروني.	47
المطلب الأول: الحماية الالكترونية للتوقيع الالكتروني من التزوير.	47
الفرع الأول: نظام التشفير.	47
الفرع الثاني: التصديق الإلكتروني.	51
المطلب الثاني: العقوبات المقررة لجريمة تزوير التوقيع الالكتروني.	55
الفرع الأول: في قانون العقوبات.	55

فهرس الموضوعات

الفرع الثاني: القانون رقم 15-04 المؤرخ في 11 ربيع الثاني 1436 الموافق لـ 1 فبراير 2015.....	57
الخلاصة:.....	58
خاتمة:.....	60
قائمة المصادر والمراجع:.....	64

المخلص

أدى التطور التكنولوجي الحديث، إلى جانب الاعتماد المتزايد على شبكة المعلومات، إلى ظهور وسائل وأنماط جديدة للمعاملات، حيث انتقلت من الشكل التقليدي المادي إلى الشكل الإلكتروني، مع اعتماد الحاسب الآلي كأداة رئيسية في إبرام هذه المعاملات. وقد نتج عن هذا التحول ظهور تقنيات حديثة، من أبرزها الكتابة الإلكترونية والتوقيع الإلكتروني، الذي أصبح بديلاً للتوقيع التقليدي في تحديد هوية المتعاقدين والتعبير عن إرادتهم في إبرام العقود، مما شكل صورة رقمية حديثة لتأمين الوثائق الإلكترونية.

وقد ساهمت هذه التقنية في تحسين سرعة ومرونة إجراء المعاملات، خاصة بعد أن أُقرت حجيتها ومطابقتها للتوقيع التقليدي من قبل العديد من التشريعات والمنظمات الدولية. إلا أن هذا التقدم التكنولوجي، ورغم مزاياه، يُعد سلاحاً ذو حدين، حيث أن البيئة الافتراضية التي تعتمد عليها هذه الأنظمة تُعتبر بيئة خصبة لعمليات الاختراق وارتكاب الجرائم المعلوماتية، التي باتت تهدد أمن وسلامة التوقيع الإلكتروني بمختلف أشكاله، مما أثار مخاوف المستخدمين وأضعف ثقتهم في هذه التقنية.

وبهدف حماية هذه المنظومة، تبنت الحكومة الجزائرية جملة من التدابير القانونية من خلال القواعد العامة في قانون العقوبات، لاسيما في الفصل السابع مكرر المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات، والذي يتناول الجرائم التي تمس النظام المعلوماتي، بما في ذلك التوقيع الإلكتروني والتزوير المتعلق به. كما أقر المشرع الجزائري القانون الخاص رقم 04-15 الذي يضع الإطار القانوني العام للتوقيع والتصديق الإلكتروني. ورغم أهمية هذا القانون، إلا أنه يعاني من بعض النقائص، حيث لم يعالج جميع أنواع التعدي على هذه التقنية، كالتزوير والاحتيال، والتي تم تصنيفها كجناح تُترك للقاضي سلطة تقديرية واسعة في الحكم بشأنها، رغم خطورتها.

وعليه، يُستنتج أن هناك حاجة ملحة لإعادة النظر في الإطار القانوني المنظم لهذا النوع من الجرائم، من خلال وضع قواعد أكثر صرامة لردع المجرمين، والحد من الجرائم المعلوماتية، إضافة إلى تشكيل فرق متخصصة للتحقيق والفصل في هذه القضايا وفقاً لدرجة خطورتها.

الكلمات المفتاحية: التوقيع الإلكتروني، الجريمة المعلوماتية، قانون العقوبات، المشرع الجزائري، العقوبة.

Abstract:

Modern technological advancements, coupled with the growing reliance on information networks, have led to the emergence of new methods and patterns in transactions. These transactions have transitioned from traditional physical formats to electronic formats, with computers becoming the primary tool for contract formation and execution. This shift has brought about several innovations, most notably electronic writing and electronic signatures, which have replaced traditional signatures in identifying contracting parties and expressing their intent to enter into agreements, thus forming a modern digital means of securing electronic document.

This technology has significantly enhanced the speed and flexibility of transactions, especially after various international legislations and organizations recognized the legal validity of electronic signatures and their equivalence to traditional ones. However, despite its advantages, this technological progress is a double-edged sword. The virtual environment on which these systems operate is fertile ground for cyberattacks and electronic crimes, which increasingly threaten the integrity and security of electronic signatures in all their forms. These threats have raised concerns among users and diminished their trust in such technologies.

To safeguard this system, the Algerian government has adopted a series of legal measures under the general provisions of the Penal Code, particularly in the amended Chapter Seven, which addresses offenses against automated data processing systems. This includes crimes targeting the information systems related to electronic signatures and their falsification. Furthermore, the Algerian legislator enacted Law No. 15-04, which outlines the general legal framework governing electronic signatures and certifications. Despite the importance of this law, it suffers from several shortcomings, primarily its failure to address all forms of attacks on electronic signatures, such as forgery and fraud. These offenses, despite their seriousness, are still classified as misdemeanors and are left to the broad discretionary power of judges.

Accordingly, there is an urgent need to reconsider the legal framework governing this category of crimes. This includes the establishment of stricter legal provisions to deter cybercriminals, reduce the spread of cybercrime, and create specialized teams tasked with investigating and adjudicating such offenses based on their severity.

Keywords: Electronic Signature, Cybercrime, Penal Code, Algerian Legislator, Sanction.