جامعة بلحاج بوشعيب عين تموشنت

كلية الحقوق

قسم: الحقوق

الحماية القانونية للتوقيع الالكتروني في التشريع الجزائري

مذكرة مكملة لنيل شهادة الماستر في الحقوق –تخصص: قانون عام

من إعداد الطالبتين:

- صايم اخلاص
- عسكر كوثر

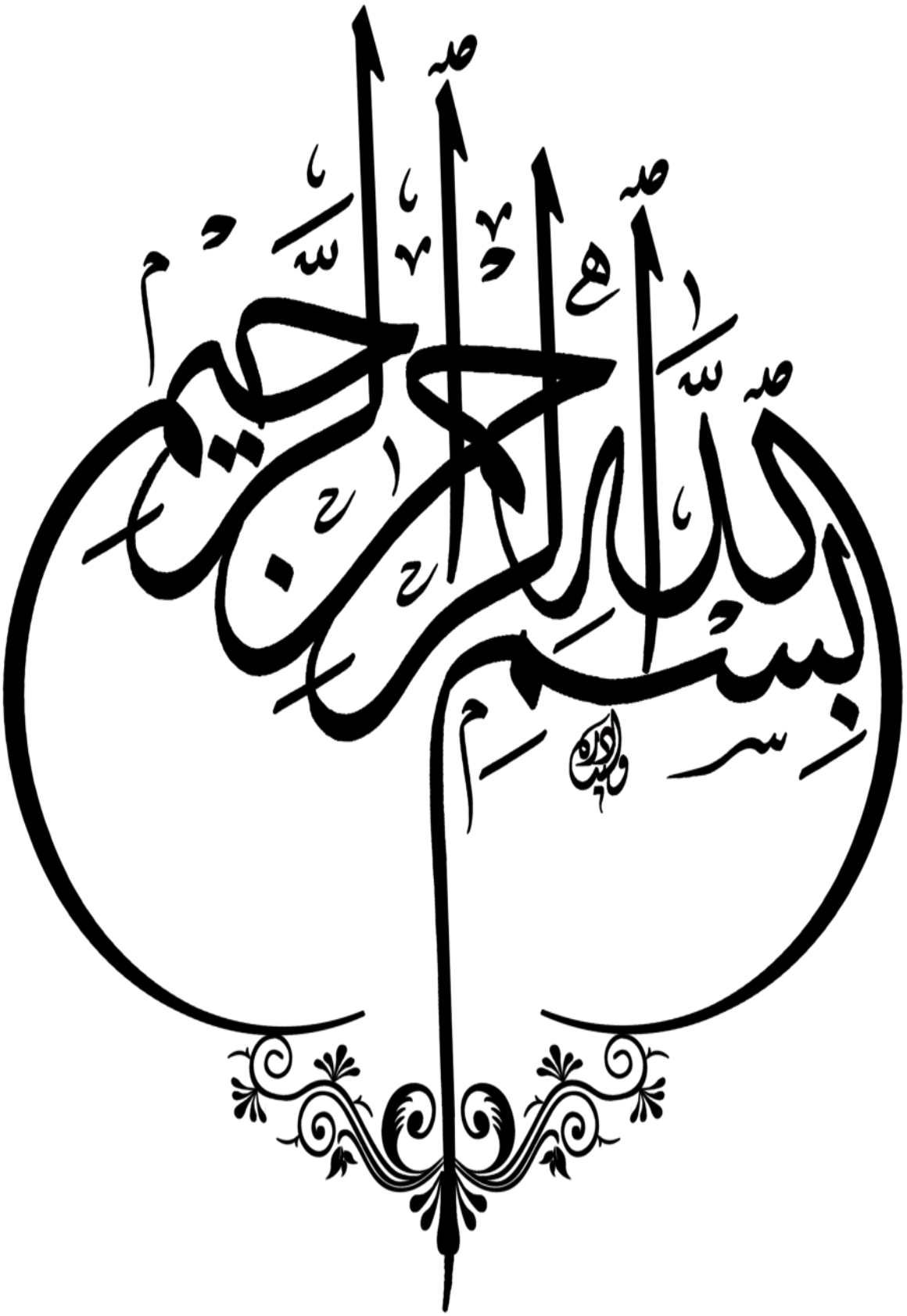
تحت إشراف الدكتور:

- فوحال رياض

لجنة المناقشة:

الرئيس	أ– بوعبسة محمد	أستاذ محاضر –ب–	جامعة عين تموشنت
المشرف	أ–فوحال رياض	أستاذ محاضر – ب –	جامعة عين تموشنت
الممتحن	أ– جغدم بن ذهيبة	أستاذ محاضر –ب–	جامعة عين تموشنت

السنة الجامعية: 2024–2025


بسم الله الرحمن الرحيم

شكر وعرفان

بسم الله الرحمن الرحيم

الحمد لله الذي بنعمته تتم الصالحات وبتوفيقه تتحقق الغايات.

اتقدم بخالص الشكر وعظيم الامتنان إلى أستاذي الفاضل **فوحال رياض** المشرف على هذا العمل لما قدمه لي من دعم متواصل وتوجيهات سديدة طوال فترة إعداد هذه المذكرة لقد كان لخبرته وصيره وملاحظاته العلمية الدقيقة الدور الكبير في إخراج هذا العمل في صورته النهائية، فله مني كل التقدير والاحترام.

ولا يفوتني أن أعبر عن امتناني العميق إلى كل أساتذتي الكرام ما بذلوه من جهد في سبيل تعليمي

كما أخص بالشكر كل من ساهم في إنجاز هذا المشروع من قريب أو بعيد، وأتوجه بتحية تقدير لهم

وأخيرا، أتقدم بأسمى عبارات الشكر والعرفان إلى أسرتي الكريمة. التي كانت ولا تزال السند والداعم الأول لي بفضل دعائهم وتشجيعهم المستمر

جزاكم الله جميعا خير الجزاء

إهـداء

الى من كان تعلوهم زادي وصبرهم دليلي .. ومحبتهم سندي

إلى من علموني معنى الإصرار وكانوا الدافع الأول في كل

.خطوة..

الى والدي العزيزين رمز العطاء والبذل والتضحية أهدي ثمرة جهدي وقطاف سنيني عرفانا وامتنانا لا توفيه الكلمات

إلى إخوتي الأعزاء

رفقاء الرحلة، وسندي وقت الشدة

كنتم العون في كل حين بدعمكم و حبكم لكم من القلب كل التقدير ومن الروح كل الوفاء

وإلى أحبابي الذين لم يبخلوا علي

من قدموا لي الدعم المادي والمعنوي في أوقات الاحتياج إلى من آمنوا بي حين شككت ودافعوني للأمام حين تعرت

أهديكم هذا الإنجاز بامتنان لا يحد ومحبة لا تنطفئ

ولكل من ساندني بكلمة أو ابتسامة، أو دعاء صادق

أنتم جزء من هذا النجاح، فلكم مني أصدق الشكر وأجعله.

اخلاص

إهـداء

إلى كل من علمني حرفا في هذه الدنيا الفانية

إلى أبي الغالي

عرفانا بفضله ووفاء

أهدى ثمرة جهدي هذا إلى أغزو أغلى إنسانة في حياتي التي أثاره دربي بنصائحها ، وكانه بحرا صافيا يجرى بفيض الحب والبسمة إلى من منحتني القوة والعزيمة لمواصلة الدريم وكانت سببا في مواصلة دراستي إلى من علمتني السير والاجتهاد

إلى الغالية على قلبي أمي.

إلى اخوتي واخواتي حفظهم الله

أوجه تحية خاصة وشكر جزيل لكل من ساهم في ثمرة جهدي وأعانني جزاه الله خيرا وجعل عونه في ميزان الحسنات.

إلى كل النفوس الطيبة التي وسعتهم ذاكرتي و لم تسعهم مذكرتي.

إلى أساتذتي الذين لم يبخلوا علينا بالنصائح وبالأخص الأستاذ فوحال رياض

إلى اصدقائي وصديقاتي أتمنى لهم حظ موفق.

كوثر

قائمة المختصرات

ج: جزء

ط: طبعة

ع : عدد

د.د.ن : دون دار النشر

د.س.ن : دون سنة النشر

ج . ر : الجريدة الرسمية

ق : قانون

ص : صفحة

مقدمة

مقدمة

في ظل التحولات العميقة التي أفرزتها الثورة الرقمية، وما رافقها من تطور متسارع في تكنولوجيا الاتصال والمعلومات، أصبح هذا الواقع يشكّل دعامة أساسية للمجتمعات الحديثة، وهو ما انعكس بشكل مباشر على المنظومة القانونية المؤطرة للمعاملات والعلاقات التعاقدية. فقد انتقل التعاقد من شكله التقليدي القائم على التلاقي المادي للإرادات، إلى نمط تعاقدي إلكتروني يتم عبر الوسائط التقنية الحديثة، مما استتبع ظهور إشكالات قانونية جديدة، خاصة في غياب إطار تشريعي واضح ومتكامل في بعض النظم.

وقد ساهم اتساع استخدام شبكة الإنترنت في بروز مفاهيم مستحدثة كالعقود الإلكترونية، والتجارة الإلكترونية، واقتصاد المعرفة، وهو ما فرض على التشريعات المعاصرة ضرورة وضع قواعد قانونية تتماشى مع طبيعة هذه البيئة الرقمية وتحمي المتعاملين فيها. ونتيجة لذلك، تبنّى المشرّع مفاهيم جديدة، منها الكتابة الإلكترونية والمحررات الرقمية، ووسائل الإثبات المستحدثة كالتوقيع الإلكتروني، الذي جاء كبديل للتوقيع التقليدي غير القابل للاستخدام في البيئات الرقمية.

ويعدّ التوقيع الإلكتروني أداة قانونية مستحدثة تؤدي نفس وظيفة التوقيع التقليدي، لكنه يتفوق بقدرته على التكيف مع متطلبات التعاقد عن بعد، ويعكس تحوّلًا في المفاهيم الكلاسيكية للكتابة والإثبات. ونظرًا لسهولة التلاعب بالمحتوى الإلكتروني، برزت الحاجة إلى وسائل تضمن سلامة التوقيع ومصداقيته، من خلال تقنيات تتيح التحقق من هوية الموقع، وهي مهام تضطلع بها جهات معتمدة من قبل السلطات الرسمية لضمان الحجية القانونية للتوقيع الإلكتروني في المعاملات الرقمية.

بناءً على ما سبق، تتجلّى الأهمية القانونية لدراسة نظام التوقيع الإلكتروني في ضوء التوسع الكبير للمعاملات الرقمية، وما نتج عنه من تحديات في مجال الإثبات، خاصة مع تنامي الاعتماد على وسائل الاتصال الحديثة والعقود الإلكترونية. وتبرز هذه الأهمية في ضرورة الوقوف على الطبيعة القانونية للتوقيع الإلكتروني، وبيان قوته الثبوتية ضمن التصرفات القانونية والمعاملات الرقمية، وموقعه ضمن مختلف التشريعات، لا سيما التشريع الجزائري، الذي لا يزال في طور التكيّف مع مقتضيات البيئة الرقمية.

- أهمية الموضوع:

تتجلى أهمية هذا الموضوع في النقاط التالية:

- يُعد التوقيع الإلكتروني من أبرز نتائج التحول الرقمي، كونه بديلاً قانونيًا للتوقيع التقليدي، ويضطلع بدور أساسي في التوثيق والإثبات.
- ظهوره كمستجد تقني يستوجب ضبط مفهومه قانونًا، وبيان أنواعه وشروطه لإضفاء الحجية القانونية على المعاملات الإلكترونية.
- يحظى بأهمية خاصة في التشريع الجزائري، لا سيما في إطار القانون 11-40 المؤرخ في 2001، باعتباره الإطار المرجعي للتوقيع والتصديق الإلكترونيين.
- يُعزز الثقة والأمان في البيئة الرقمية، ويمكّن الأفراد والمؤسسات من الانخراط في التجارة الإلكترونية محليًا ودوليًا.
- يسهم في تقليل التكاليف وتسريع الإجراءات، كما يتمتع بحجية إثبات معادلة للتوقيع الورقي عند استيفاء شروطه القانونية.

- **أهداف الدراسة:**

تهدف هذه الدراسة إلى تحقيق جملة من الأهداف القانونية الأساسية، من أبرزها:

- يهدف هذا البحث إلى تحديد الإطار المفاهيمي للتوقيع الإلكتروني، من خلال الوقوف على ماهيته القانونية، وتبيان خصائصه الجوهرية، وصوره المتعددة، مع توضيح العناصر التي تميّزه عن التوقيع الخطي التقليدي، سواء من ناحية الشكل أو من حيث الوظيفة القانونية التي يؤديها كل منهما.
- كما يسعى إلى إجراء دراسة مقارنة بين التوقيع الإلكتروني والتوقيع التقليدي، للكشف عن نقاط التلاقي والاختلاف بينهما، مع تحليل الثغرات القانونية والصعوبات العملية التي قد تعيق تطبيق النصوص المنظمة لهذا المجال، واقتراح حلول وآليات قانونية مناسبة من شأنها الحد من هذه الإشكالات، لاسيما في ميدان الإثبات بالوسائل الإلكترونية.
- ويتضمن البحث كذلك تسليط الضوء على حجية التوقيع الإلكتروني في مجال الإثبات، من خلال دراسة الشروط القانونية اللازمة لاعتماده كوسيلة إثبات معتبرة في التصرفات والمعاملات الإلكترونية، مع التركيز على القوة الثبوتية التي يمنحها له التشريع الجزائري، وبوجه خاص القانون

رقم 11-40 المتعلق بالتوقيع والتصديق الإلكتروني، ومدى كفاية هذا الإطار القانوني لتحقيق متطلبات الموثوقية وضمان الأمان القانوني في بيئة رقمية متطورة.

- وتكمن أهمية دراسة موضوع التوقيع الإلكتروني وحجيته في الإثبات في اعتبارات متعددة، منها ما يرتبط بالجوانب الذاتية، كتزايد الاعتماد على الوسائط الرقمية في الحياة اليومية، ومنها ما يتصل بالأبعاد الموضوعية، كالحاجة الملحة لتكييف المنظومة القانونية مع مستجدات البيئة الإلكترونية.

- أسباب اختيار الموضوع:

1-الأسباب الموضوعية:

تتجلى الأسباب الموضوعية التي دفعت إلى اختيار هذا الموضوع في عدة اعتبارات أساسية، أبرزها:

- إن مسألة إثبات التوقيع الإلكتروني وما يرتبط بها من حجية قانونية في بيئة الإنترنت تُعد من الإشكالات ذات الأهمية البالغة في ميدان المعاملات الإلكترونية، خاصة مع صدور القانون رقم 11-40 المتعلق بالتوقيع والتصديق الإلكترونيين. غير أن هذا النص، رغم أهميته، جاء في صيغة موجزة لم تتناول بمقاربة شاملة مختلف الجوانب التقنية والقانونية المرتبطة بالتوقيع الإلكتروني، رغم أن شبكة الإنترنت أصبحت تمثل أحد المكونات الأساسية في الواقع العملي، سواء بالنسبة للأفراد أو الكيانات التجارية أو حتى المؤسسات الرسمية والخاصة.

- إن التحول الرقمي المتسارع وتزايد الاعتماد على الوسائل الإلكترونية في إدارة المعاملات قد أديا إلى توسع نطاق استخدام التوقيع الإلكتروني، ما يفرض على الدولة الجزائرية ضرورة مواكبة هذا التطور التكنولوجي، خصوصًا في ظل مساعيها المتواصلة للانضمام إلى منظمة التجارة العالمية. ويستلزم هذا الواقع تكييف الإطار التشريعي الوطني، لا سيما فيما يتعلق بتنظيم التجارة الإلكترونية، من خلال إرساء منظومة قانونية متكاملة وفعالة للتوقيع الإلكتروني تضمن الموازنة بين متطلبات التطور الرقمي وضمانات الحماية القانونية.

- لقد أقر المشرع الجزائري من خلال النصوص القانونية النافذة بصلاحية التوقيع الإلكتروني كوسيلة إثبات معتبرة في مجال المعاملات الرقمية، واعتبره أداة قانونية تمنح الوثيقة قوة ثبوتية ومصداقية تضاهي تلك التي يتمتع بها التوقيع التقليدي اليدوي. غير أن هذه الوسيلة القانونية الحديثة تتميز بخصوصيات تقنية دقيقة وآليات تنفيذية معقدة، مما يستدعي الخوض في تحليل متعمق لطبيعتها

القانونية والتقنية، بهدف تفعيل النصوص المنظمة لها بشكل يضمن الأمن والثقة داخل البيئة الرقمية المتغيرة.

2-الأسباب الذاتية:

أما الأسباب الذاتية لاختيار هذا الموضوع، فتتمثل في قناعة شخصية راسخة بأهمية هذا المجال وحساسيته في المرحلة الراهنة، لكونه يتصل اتصالًا مباشرًا بالتحولات التقنية المعاصرة التي تشهدها المعاملات القانونية، وخاصة الإلكترونية منها. وقد فرضت هذه التحولات ظهور وسائل جديدة للإثبات، يُعد التوقيع الإلكتروني في طليعتها، بوصفه وسيلة حديثة فرضتها مقتضيات العصر الرقمي. وتأتي هذه الدراسة تعبيرًا عن رغبتنا في الإسهام، ولو بشكل متواضع، في إثراء النقاش الأكاديمي القانوني حول هذا الموضوع، الذي يُرتقب أن يكتسي أهمية متزايدة في المستقبل، سواء في الساحة العلمية الجامعية أو في واقع الممارسة العملية، وخاصة في مجال القضاء والمعاملات الإدارية.

الإشكالية:

إذ أن مجمل التشريعات العربية، ومنها التشريع الجزائري، تُواجه قصوراً نسبياً في مواكبة التحولات التكنولوجية، مما أدى إلى ظهور العديد من الإشكالات القانونية، خاصة أمام الجهات القضائية، نتيجة غياب إطار تشريعي دقيق يُنظم حجية التوقيع الإلكتروني في الإثبات بشكل كافٍ وواضح. ورغم إقدام المشرع على استحداث جملة من النصوص القانونية المتعلقة بالمعاملات الإلكترونية، إلا أن هذه المنظومة ما زالت تعاني من نقائص وثغرات، بالنظر إلى حداثتها وطبيعة الموضوع الذي تُنظّمه. وانطلاقاً من هذا الواقع، تُطرح الإشكالية الجوهرية التالية:

ما مدى نجاعة الحماية القانونية التي اقرها المشرع الجزائري للتوقيع الالكتروني في ظل التطورات التكنولوجية المتسارعة؟

وتتفرع عنها التساؤلات الفرعية الآتية:

- ما مدى وضوح الإطار القانوني المنظم للتوقيع الإلكتروني في التشريع الجزائري، وهل يتماشى مع المعايير الدولية ذات الصلة؟
- ما هي الضمانات المدنية والجزائية التي يقرها القانون الجزائري لحماية التوقيع الإلكتروني من التزوير أو الاستعمال غير المشروع؟

- إلى أي مدى تُسهم النصوص القانونية الجزائرية في تعزيز حجية التوقيع الإلكتروني كوسيلة إثبات أمام الجهات القضائية؟

- المنهج المتبع:

نظراً لطبيعة موضوع التوقيع الإلكتروني، وبالاستناد إلى الإشكالية القانونية المطروحة، تم اعتماد منهجين علميين لمعالجة هذه الدراسة، وهما: المنهج التحليلي والمنهج الوصفي، مع إيلاء الأفضلية للمنهج التحليلي، لما يفرضه الموضوع من ضرورة التعمق في دراسة وتحليل النصوص القانونية ذات الصلة. إذ إن الإلمام بمختلف الأبعاد القانونية للتوقيع الإلكتروني يتطلب تحليلًا دقيقًا لمواده وأحكامه، بما يسمح بكشف مضامينه وتحديد مجالات القوة والقصور فيه، وصولًا إلى تقييم علمي موضوعي يساهم في تطوير المنظومة القانونية.

وفي السياق ذاته، تم توظيف المنهج الوصفي، الذي يقوم على تقديم وصف علمي دقيق للظاهرة القانونية محل الدراسة، من خلال تناول الإطار المفاهيمي للتوقيع الإلكتروني وتحديد أسسه النظرية، مما يُمهّد لبناء قاعدة معرفية ضرورية للولوج في التحليل القانوني المتعمق. كما تم الاستعانة بالتشريعات المقارنة، باعتبارها أداة فعّالة لتوسيع نطاق البحث، عبر الاستفادة من التجارب القانونية المتقدمة في مجال التوقيع الإلكتروني، والذي يُعد من التقنيات الحديثة ذات الطابع الديناميكي. ويساعد ذلك في استلهام النماذج الرائدة، بما يسهم في دعم وتطوير الإطار القانوني الوطني، وتكييفه مع متطلبات البيئة الرقمية المتغيرة.

تقسيم الدراسة :

اما عن الخطة فكانت كما يلي :

- **الفصل الأول : الفصل الاول: الإطار المفاهيمي و القانوني للتوقيع الالكتروني**
- **الفصل الثاني : الحماية القانونية للتوقيع الالكتروني في التشريع الجزائري**

الفصل الأول

الإطار المفاهيمي والقانوني للتوقيع الالكتروني

الفصل الاول: الإطار المفاهيمي والقانوني للتوقيع الالكتروني

ان التوقيع أو الإمضاء من الخصائص الشخصية التي يعتمدها الفرد لتمييز نفسه عن غيره، وهو يُعبّر عن إرادته وتحمله للمسؤولية القانونية عمّا يرد في الوثيقة التي يوقع عليها. وبالتالي، فإنّ أي وثيقة تخلو من توقيع ذي صفة قانونية لا يمكن أن تُعتدّ بها قانونًا.

ومع التطورات المتسارعة في مجال تكنولوجيا المعلومات والاتصالات، لا سيما مع الانتشار الواسع لاستخدام الحاسوب، أصبح التعامل الإلكتروني وسيلة معتمدة في مختلف المجالات، مما أدى إلى نشوء شكل جديد من التعاقدات يُعرف بالعقود الإلكترونية، التي تُبرم غالبًا عبر شبكة الإنترنت. ونظرًا للطبيعة الرقمية لهذه العقود، اقتضى الأمر وجود وسيلة إثبات تتلاءم مع بيئتها الإلكترونية، فبرز مفهوم "التوقيع الإلكتروني"، الذي يُعدّ بديلاً عن التوقيع التقليدي في المحررات الإلكترونية. وبناءً عليه، سيتم تناول هذا الفصل من خلال مبحثين رئيسيين:

- **المبحث الأول: ماهية التوقيع الإلكتروني ومزاياه.**
- **المبحث الثاني: القيمة القانونية للتوقيع الإلكتروني وشروط صحته**

المبحث الأول:

ماهية التوقيع الإلكتروني ومزاياه

يُعتبر التوقيع الإلكتروني إحدى الآليات المستحدثة التي أفرزها التطور الرقمي في ميدان المعاملات، وقد أصبح يشكل بديلاً قانونيًا معترفًا به للتوقيع الخطي التقليدي. وتنبع أهميته من الدور القانوني البارز الذي يضطلع به في مجال الإثبات، الأمر الذي يقتضي الوقوف عند طبيعته، وتحديد مفهومه، واستعراض مزاياه القانونية.

المـطلب الأول:

مفهوم التوقيع الالكتروني

ظلّ التوقيع التقليدي يمثل الأداة الأساسية للإثبات في المعاملات المدنية والتجارية، نظراً لما يحظى به من حجية قانونية راسخة. غير أن التحولات التي أفرزتها الثورة الرقمية، ولا سيما مع الانتشار الواسع لاستخدام شبكة الإنترنت، فرضت واقعاً جديداً يقوم على اعتماد الوثائق الإلكترونية كوسيلة للتعامل وإبرام التصرفات القانونية. وقد استتبع هذا التحوّل ظهور حاجة ملحّة إلى اعتماد تواقيع إلكترونية تُؤدي نفس الوظائف القانونية للتوقيع الخطي التقليدي، وتُضفي الحجية القانونية على المعاملات الرقمية.

وفي هذا السياق، جاء التوقيع الإلكتروني كآلية تقنية مستحدثة، تُواكب طبيعة المعاملات الإلكترونية، وتُحقق الغاية ذاتها التي يحققها التوقيع الورقي، والمتمثلة في التوثيق والإثبات وتحديد هوية الموقع والتعبير عن الإرادة. ورغم ما يطرحه هذا النمط من التوقيع من إشكالات قانونية، لاسيما في ظل غياب الدعامة المادية، فقد حظي باهتمام المشرّعين، الذين سارعوا إلى تنظيمه تشريعياً من خلال ضبط مفهومه القانوني، وتحديد شروط صحته وحجيته، بما يضمن حماية الأطراف المتعاملة ويُحقق الأمن القانوني في البيئة الرقمية. وعليه، يتناول هذا المطلب الإطار المفاهيمي للتوقيع الإلكتروني، من خلال التطرق إلى تعريفه، وبيان خصائصه، واستعراض أنواعه، فضلاً عن إبراز أهم تطبيقاته العملية في مجال المعاملات الإلكترونية.

الفرع الاول :

التعريف الفقهي

تنوّعت التعريفات الفقهية للتوقيع الإلكتروني تبعًا لاختلاف الزاوية التي يُنظر منها إلى هذه التقنية القانونية الحديثة، فقد ذهب بعض الفقه إلى تعريفه بأنه: "مجموعة من الوسائل والإجراءات التقنية، التي

تُمكِّن من إنشاء بيانات إلكترونية تحتوي على علامة مميزة لصاحبها، يتم توليدها باستخدام رموز أو أرقام تُشفّر بواسطة خوارزمية تعتمد على زوج من المفاتيح، أحدهما عام والآخر خاص."

غير أن هذا التعريف يركّز بصورة أساسية على التوقيع الرقمي باعتباره أحد أنواع التوقيع الإلكتروني، وذلك بالنظر إلى اعتماده على تقنية التشفير المزدوج. وبالتالي، فإنه لا يُعبّر بصورة شاملة عن باقي صور التوقيعات الإلكترونية الأخرى، التي قد لا تعتمد بالضرورة على آلية التشفير، وإنما تقوم على تقنيات مختلفة تؤدي ذات الوظيفة القانونية، مما يجعل هذا التعريف قاصرًا عن الإحاطة بمفهوم التوقيع الإلكتروني في مجمله[1].

في المقابل، ورد تعريف آخر للتوقيع الإلكتروني يُفيد بأنه: "مجموعة من الإجراءات التقنية التي تتيح التحقق من هوية الشخص الذي صدر عنه التوقيع، وتُعبّر في ذات الوقت عن قبوله والتزامه بمضمون التصرف القانوني المرتبط به". ويُلاحظ أن هذا التعريف قد تبنّى معيار الوظيفة القانونية للتوقيع دون حصره في وسيلة تقنية بعينها، مما يُضفي عليه طابعاً أكثر شمولاً ومرونة، ويُتيح انسحابه على مختلف صور التوقيعات الإلكترونية، أياً كانت الآلية التقنية المعتمدة في إنشائها، طالما أدّت الغرض القانوني المتمثل في تحديد الهوية والتعبير عن الإرادة الملزمة[2].

وقد عُرّف التوقيع الإلكتروني كذلك بأنه: "بيان يُدرج في شكل إلكتروني، قد يتخذ صورة حرف أو رقم أو رمز أو إشارة أو صوت أو شفرة مميزة، يتم إنشاؤه بواسطة وسيلة إلكترونية مؤمّنة، ويرتبط ارتباطًا منطقيًا بالمحتوى الإلكتروني للمحرر، بهدف تحديد هوية الشخص الموقع، والتعبير الصريح عن إرادته في قبول مضمون المستند الموقع عليه.[3]

وبناءً على ما تقدم، يمكن تعريف التوقيع الإلكتروني بأنه:

"يُقصد بالتوقيع الإلكتروني ذلك البيان الإلكتروني الذي يُدمج أو يُرفق منطقياً بمحتوى رسالة معلومات إلكترونية، ويُستعمل بقصد تحديد هوية الشخص الموقع، والتعبير عن إرادته في الالتزام بمضمون تلك الرسالة وما تضمنته من آثار قانونية".

[1]–غربي خديجة، التوقيع الإلكتروني»، مذكرة ماستر، جامعة قاصدي مرباح–ورقلة، الجزائر ،2015، ص 64.

[2]–وسيم شفيق الحجار، *الإثبات الإلكتروني*، بيروت: دار المنشورات الحقوقية، 2002، ص 75

[3]–وسيم شفيق الحجار، المرجع نفسه، ص134.

الفرع الثاني :

تعريف التوقيع حسب المشرع الجزائري

لقد مثّل الانتقال من الكتابة الورقية التقليدية إلى الكتابة الإلكترونية، ومن التوقيع الخطي إلى التوقيع الإلكتروني، تطورًا نوعيًا انعكس إيجابًا على المنظومة التشريعية الجزائرية، خاصة في إطار تحديث قواعد الإثبات المدنية. وقد تجسّد هذا التوجه من خلال التعديل الذي طرأ على القانون المدني بموجب القانون رقم 05-10 المؤرخ في 20 جوان 2005، الذي عدّل وأتمم الأمر رقم 75-58 المؤرخ في 26 سبتمبر 1975 والمتضمن القانون المدني، حيث تم الاعتراف بالوسائل الإلكترونية كوسائل قانونية للإثبات، في انسجام مع متطلبات العصر الرقمي ومقتضيات التعاملات الإلكترونية.[1]

بموجب التعديل التشريعي، تم إدراج المواد 323 مكرر، 323 مكرر 1، و327 ضمن القانون المدني الجزائري، بهدف مواكبة متطلبات الإثبات في البيئة الرقمية. وقد نصّت المادة 323 مكرر على أن الإثبات بالكتابة يمكن أن ينتج من تسلسل حروف أو أوصاف أو أرقام أو أية علامات أو رموز ذات دلالة مفهومة، وذلك بغض النظر عن الوسيلة المستعملة في تضمينها أو طريقة إرسالها، مما يكرّس مبدأ حياد الوسيلة في الإثبات.

أما المادة 323 مكرر 1، فقد أقرت صراحة بحجية الكتابة الإلكترونية، مساوية بذلك بينها وبين الكتابة الورقية من حيث القوة الثبوتية، شريطة إمكانية التحقق من هوية محرّر الوثيقة الإلكترونية، وأن يتم إعدادها وحفظها في ظروف تقنية تضمن سلامتها وعدم قابليتها للتحريف، بما يضمن مصداقيتها أمام القضاء ويُؤمّن الاستقرار في المعاملات الإلكترونية.

أما الفقرة الثانية من المادة 327 من القانون المدني، فقد نصّت صراحة على أنّه" :ويُعتدّ بالتوقيع الإلكتروني وفق الشروط المنصوص عليها في المادة 323 مكرّر من هذا القانون". وهو ما يفيد اعتراف المشرّع بحجية التوقيع الإلكتروني، شريطة استيفائه الشروط القانونية المحددة في المادة

[1]-قانون رقم 10-05 المؤرخ في 20 جويلية 2005، معدل و متمم للأمر رقم 75/58المؤرخ في 26 سبتمبر1975 و المتضمن القانون المدني المعدل و المتمم، و المنشور في الجريدة الرسمية ،عدد44 الصادر في 2005/07/21.

المذكورة، والتي تُعدّ بمثابة الضابط الفني والقانوني المعتمد لاعتماد هذا النوع من التوقيع كوسيلة صحيحة للإثبات في المعاملات المدنية.."[1]

من خلال تحليل النصوص القانونية ذات الصلة، يتبين أن المشرّع الجزائري لم يُقدّم تعريفًا صريحًا ومباشرًا للتوقيع الإلكتروني في التشريع الأصلي، بل اكتفى بتحديد الأركان الشكلية التي تمنح هذا النوع من التوقيع الحجية القانونية، وفي مقدمتها إمكانية التحقق من هوية صاحب التوقيع، إضافة إلى اشتراط أن يتم إعداد التوقيع الإلكتروني وحفظه في إطار يضمن سلامته وأصالته، بما يُؤسّس لشرعيته كوسيلة إثبات مقبولة قانونًا ضمن البيئة الرقمية.

غير أن المشرّع، واستدراكًا لهذا الفراغ، سعى إلى تقنين مفهوم التوقيع الإلكتروني بشكل أوضح من خلال المرسوم التنفيذي رقم 07-162 المعدِّل والمتمِّم للمرسوم التنفيذي رقم 01-123، حيث نصّت المادة 3 منه صراحة على تعريف التوقيع الإلكتروني بكونه:

"معطى ينجم عن استخدام وسيلة إلكترونية، ويكون مرتبطًا مباشرة بتصرف قانوني، وقادراً على تحديد هوية الموقع، ويدل على قبوله لمضمون الوثيقة المرتبطة به".

ويُعدّ هذا التعريف خطوة مهمة نحو تدعيم الإطار القانوني المنظم للمعاملات الإلكترونية، بما ينسجم مع متطلبات الإثبات الحديثة، ويعكس توجّه المشرّع نحو إرساء منظومة قانونية قادرة على مواكبة مستجدات البيئة الرقمية وضمان أمن التعاملات الإلكترونية. [2]

يتّضح من أحكام المادتين 323 مكرر و323 مكرر 1 من الأمر رقم 75-58 المؤرخ في 26 سبتمبر 1975، المتضمّن القانون المدني، أن المشرع الجزائري قد وضع الإطار القانوني الأساسي للاعتداد بالتوقيع الإلكتروني، من خلال تحديد الشروط التي يجب أن تتوافر فيه ليكتسب حجية قانونية في الإثبات. كما نصّت الفقرة الثانية من المادة الثالثة من المرسوم التنفيذي رقم 07-162 المؤرخ في 20 مايو 2007، المتعلّق

[1]-قانون رقم 10-05 المؤرخ في 20 جويلية 2005، معدل و متمم للأمر رقم 75/58المؤرخ في 26 سبتمبر1975 و المتضمن القانون المدني المعدل و المتمم، و المنشور في الجريدة الرسمية ،عدد44 الصادر في 2005/07/21.

[2]-لمرسوم التنفيذي رقم 07/162،المؤرخ في 13جمادى الأول 1428 الموافق ل 30ماي2007، يعدل ويتمم المرسوم التنفيذي رقم 01/123، المؤرخ في 15صفر 1422، الموافق ل09ماي سنة 2001،المتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشيكات بما فيها اللّاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية و اللّاسلكية، الجريدة الرسمية للجمهورية الجزائرية ،عدد 37 الصادرة في 7جوان2007.

بتحديد كيفيات إعداد التوقيع الإلكتروني وتنفيذه ومراقبته، على تعريف التوقيع الإلكتروني المؤمَّن، مبينة خصائصه الجوهرية، حيث ورد فيها:

"يُعد توقيعًا مؤمنًا كل توقيع إلكتروني يستجيب للشروط الآتية:

- أن يكون خاصًا بالموقّع،
- أن يتم إنشاؤه بواسطة وسائل يمكن أن تبقى تحت الرقابة الحصرية للموقّع،
- أن يضمن وجود ارتباط بين التوقيع والمحرر الموقَّع عليه، بما يسمح بكشف أي تعديل لاحق قد يطرأ على هذا المحرر".

ورغم ما سبق، فإن المشرع، وعلى الرغم من محاولته وضع ضوابط تقنية وقانونية لضمان حجية التوقيع الإلكتروني، إلا أنه لم يُعرّف بشكل دقيق ومتكامل مفهوم هذا التوقيع، مكتفيًا بالإشارة إليه باعتباره "معطى" ناتجًا عن استخدام وسيلة تقنية تستجيب لشروط معيّنة، من دون تحديد ماهية هذه الوسيلة أو خصائصها الفنية والتنظيمية بشكل واضح. وهو ما أدّى إلى وجود نوع من الغموض والإبهام في الإطار المفاهيمي للتوقيع الإلكتروني، مما يفتح المجال لاختلاف التأويلات على المستوى العملي والقضائي، لاسيما عند فحص مدى توافر الشروط القانونية في التوقيع الإلكتروني المستخدَم في محررات معيّنة.

وفي هذا السياق، نجد أن المشرع الجزائري قد تناول تعريف التوقيع الإلكتروني بشكل صريح في القانون رقم 15-04 المؤرخ في 1 فبراير 2015، المتعلق بالتوقيع والتصديق الإلكترونيين. وقد ميّز بين نوعين من التوقيعات الإلكترونية، حيث عرّف التوقيع الإلكتروني العادي في المادة الثانية، الفقرة (1) من الباب الأول، الفصل الثاني، بأنه:" كل بيانات إلكترونية تُقدَّم في شكل إلكتروني، وتُرفق أو ترتبط منطقياً ببيانات إلكترونية أخرى، وتُستخدم كوسيلة للإثبات". [1]

ويُظهر هذا التعريف ميلًا إلى اعتماد المفهوم الوظيفي للتوقيع الإلكتروني، من خلال التركيز على دوره في الإثبات، دون الإحاطة الكافية بالجوانب التقنية والتنظيمية التي تضمن أمانه ومصداقيته، وهو ما

[1]-القانون رقم 04/15المؤرخ في1 فبراير 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، جريدة رسمية للجمهورية الجزائرية، عدد 6، الصادرة في 10/02/2015.

يستدعي، من الناحية التشريعية، تدخلاً أو توضيحًا أكبر لضمان فعالية هذا النظام القانوني في بيئة رقمية متطورة ومعقّدة."

نصّت الفقرة (3) من ذات المادة على تعريف "بيانات إنشاء التوقيع الإلكتروني" بأنها: "بيانات فريدة، كالمفاتيح الخاصة أو الرموز المشفّرة، يُخصّ بها الموقّع ويستعملها بغرض إنشاء توقيعه الإلكتروني"، مما يفيد أن هذه البيانات ترتبط بشخص الموقّع ارتباطاً وثيقاً وتُعدّ وسيلة تقنية مميزة لتحديد هويته وضمان نسبة التوقيع إليه.

أما النوع الثاني من التوقيعات الإلكترونية، فيتمثل في التوقيع الإلكتروني الموصوف، والذي عرّفته المادة 7 (ب) بأنه: "التوقيع الإلكتروني الذي تتوفر فيه المتطلبات الآتية"، وهو بذلك يشير إلى نموذج خاص من التوقيع الإلكتروني الذي يستوفي شروطاً قانونية وتقنية محددة تمنحه حجية قانونية معززة، ويُمكن من خلاله تحقيق مزيد من الأمان والثقة في المعاملات الإلكترونية، لا سيما فيما يتعلق بإثبات هوية الموقع وسلامة المعطيات المرتبطة بالتوقيع [1]:

"يتضح من استقراء مجمل الشروط المشار إليها أعلاه أن التوقيع الإلكتروني المعتمد يجب أن يستوفي مجموعة من الضوابط التقنية والقانونية، تتمثل فيما يلي:

-**أولًا:** أن يتم إنشاء التوقيع استنادًا إلى شهادة تصديق إلكتروني صادرة عن جهة معتمدة وموثوقة قانونًا؛

-**ثانيًا:** أن يكون التوقيع مرتبطًا حصريًا بصاحبه، بصورة تمنع الغير من استخدامه أو نسبته إلى شخص آخر؛

-**ثالثًا:** أن يمكّن من التحقق الدقيق من هوية الموقع، بما يعزز الثقة في صحة نسب التوقيع إلى من صدر عنه؛

-**رابعًا:** أن يُنشأ التوقيع باستخدام وسيلة إلكترونية مؤمّنة، معدّة خصيصًا لهذا الغرض، وبما يضمن حمايته من التلاعب أو الانتحال؛

[1]-بلقنيشي حبيب، إثبات التعاقد عبر الأنترنيت (البريد المرئي)-دراسة مقارنة-، رسالة مقدمة لنيل شهادة الدكتوراه في القانون الخاص، كلية الحقوق، جامعة وهران السانيا ،2010/2011، ص 115 .

-**خامسًا:** أن تظل وسائل إنشاء التوقيع تحت السيطرة الحصرية للموقع، دون أن يكون لأي طرف آخر إمكانية النفاذ إليها؛

-**سادسًا:** أن يكون التوقيع مرتبطًا بالبيانات محل التوقيع على نحو وثيق، بحيث يمكن كشف أي تعديل أو تغيير يطرأ عليها بعد التوقيع.

وتجدر الإشارة إلى أن هذه الشروط تتماشى مع ما نصّ عليه التوجيه الأوروبي المتعلق بالتوقيع الإلكتروني، مما يدل على سعي التشريعات المقارنة، ومنها التشريع الجزائري، إلى ضمان حماية فعالة للتوقيع الإلكتروني من خلال توحيد الضوابط والمعايير التقنية والقانونية المعتمدة.

ويُستخلص من ذلك أن المشرع الجزائري لم يُقيّد التوقيع الإلكتروني بشكل جامد أو في قالب تقني محدد، بل تبنى مفهومًا مرنًا يتسم بالشمولية، يسمح باستيعاب مختلف الابتكارات العلمية المستقبلية في هذا المجال، على غرار ما تم اعتماده في تنظيم الكتابة الإلكترونية، بما ينسجم مع الطبيعة المتطورة والمتجددة للتقنيات الرقمية.[1]

يتّضح من خلال نص المادة 2 من القانون الجزائري المتعلق بالتوقيع الإلكتروني، أن هذا الأخير يُعد شكلاً من أشكال البيانات الإلكترونية، يتم إلحاقه أو ربطه بمحتوى إلكتروني آخر، وقد يتخذ شكل رموز، أو إشارات، أو مفاتيح تشفير، يحتفظ بها المُوقّع ويستعملها إما باسمه ولحسابه الخاص، أو نيابةً عن شخص آخر، سواء أكان طبيعيًا أم معنويًا. ويُستفاد من هذا التعريف أن المشرّع الجزائري اعتمد تصورًا تقنيًا للتوقيع الإلكتروني يتلاءم مع طبيعته الرقمية، ويؤدي في ذات الوقت الوظيفة القانونية المنوطة بالتوقيع التقليدي، لا سيما في مجال إثبات صحة التصرفات القانونية. ويُلاحظ أن هذا التوجه لا يخرج عن الإطار العام الذي تبنّته أغلب التشريعات المقارنة، سواء في الأنظمة القانونية العربية أو الغربية، التي أقرّت بخصوصية التوقيع الإلكتروني كوسيلة تقنية ذات طابع قانوني تُمكّن من تحديد هوية المُوقّع وضمان سلامة المحرر الإلكتروني[1]

[1]-السيد عبد القادر جهيدة، شكرون ساسية، مرجع سابق، ص 07.

[3]- فوغالي بسمة، اثبات العقد الالكتروني وحجيته في ظل عالم الانترنت، مذكرة ماجستير في القانون الخاص، جامعة محمد لمين دباغين ، سطيف 2، الجزائر ، 2015، ص 61.

المـــطلب الثاني:

انواع التوقيع الالكتروني و صوره

يتمثل هذا المطلب في انواع التوقيع و صوره:

الفرع الاول:

انواع التوقيع الالكتروني

هناك عدة أنواع من التوقيعات الإلكترونية الشائعة ومنها نذكر ما يلي:

أولاً: تحويل التوقيع الخطي إلى توقيع إلكتروني عبر الماسح الضوئي

يُعتبر إدراج التوقيع اليدوي في المستندات الإلكترونية عن طريق استخدام الماسح الضوئي (Scanner) من صور التوقيع الإلكتروني غير المؤمَّن، حيث يُصار إلى تحويل التوقيع الخطي إلى صورة رقمية يتم إدماجها ضمن الوثيقة الإلكترونية. وعلى الرغم من إمكانية استخدام هذا النوع من التوقيعات في بعض المعاملات، إلا أن حجيته في الإثبات تبقى محل نقاش قانوني، وذلك بسبب قابليته للتلاعب، سواء من خلال النسخ أو التعديل، في ظل غياب وسيلة تقنية تضمن التحقق من صحة التوقيع وهُوية الموقع.

وفي هذا السياق، فإن هذا النوع من التوقيع الإلكتروني، وبحكم عدم استناده إلى آليات تحقق موثوقة أو بنية تحتية للتصديق الإلكتروني، يُعد قاصرًا عن توفير الحماية القانونية الكافية، ولا يُعتد به كدليل إثبات مستقل ما لم يكن جزءًا من نظام إلكتروني آمن يخضع لاعتماد رسمي يضمن سلامة العملية التعاقدية ومطابقة التوقيع لهوية صاحبه وفقًا للضوابط القانونية المعمول بها[1].

ثانياً: التوقيع الإلكتروني عبر بطاقة السحب الآلي والرقم السري

يُعد إدخال الرقم السري المرافق لبطاقة السحب البنكي بمثابة تعبير صريح عن إرادة العميل وموافقته على تنفيذ العملية المصرفية، ويُشكل ذلك صورة من صور التوقيع الإلكتروني المعتمد في المجال البنكي. غير أنّ هذا النمط من التوقيع، نظراً لغياب ارتباطه المباشر بالمحررات الورقية المعتمدة من قبل البنك، لا يُرتب حجية الدليل الكتابي الكامل في الإثبات، إلا إذا تم الاتفاق صراحةً بين الطرفين، أي البنك والعميل،

[1]- السيد عبد القادر جهيدة، شكرون ساسية، مرجع سابق، ص 07.

على منحه هذه الحجية القانونية، بما يجعله في مرتبة التوقيع الخطي طبقاً لأحكام القانون المدني وقواعد الإثبات المعمول بها.

وقد دأبت بعض المؤسسات المصرفية على إدراج شروط تعاقدية ضمن نماذج فتح الحسابات أو عقود تقديم الخدمات البنكية، تنص على منح العمليات المنجزة باستخدام البطاقة البنكية مقرونة بالرقم السري ذات الحجية القانونية الكاملة. الأمر الذي يُضفي على تلك العمليات صفة الدليل الكتابي، شريطة احترامها للضوابط التقنية والإجراءات القانونية المعتمدة لضمان سلامة التوقيع الإلكتروني ومصداقيته.

ثالثاً: التوقيع الإلكتروني عبر الإنترنت وإبرام العقود إلكترونياً

أصبح من الممارسات الشائعة، في ظل التوسع المتنامي للتجارة الإلكترونية، إبرام العقود والالتزامات عن طريق شبكة الإنترنت، حيث يُعبّر المتعاقد عن إرادته الصريحة في القبول بشروط التعاقد من خلال وسيلة إلكترونية محددة، كالنقر على زر "موافق" أو "قبول". ويُعدّ هذا الأسلوب من التعبير عن الإرادة، من الناحية القانونية، بمثابة توقيع إلكتروني منتج لآثاره، متى استوفى الشروط القانونية المنصوص عليها، ولا سيما ما يتعلق بإمكانية التحقق من هوية الطرف المتعاقد، واعتماد وسيلة إلكترونية مؤمنة وموثوقة، وذلك على النحو الذي قرّره القانون رقم 15-04 المؤرخ في 1 فبراير 2015، المتعلق بالتوقيع والتصديق الإلكترونيين[1].

وفي هذا الإطار، باتت المواقع الإلكترونية تتيح للمتعاملين إمكانية تصفّح المنتجات وإتمام عملية الشراء دون حاجة إلى الحضور الفعلي إلى مقر البائع، إذ يتم إبرام العقد إلكترونيًا بمجرد قيام المستهلك بالضغط على زر الموافقة الظاهر على صفحة العرض، وهو ما يُعدّ تصرفًا قانونيًا مُلزِمًا يرتّب آثاره كأي عقد تقليدي.

أما فيما يخص التوقيع البيومتري، فهو يُعدّ أحد الأشكال المتقدمة للتوقيع الإلكتروني، إذ يستند إلى الخصائص البيولوجية أو الفيزيولوجية الفريدة لكل فرد، كالبصمة، أو صورة قزحية العين، أو بصمة الصوت، أو نمط حركة اليد عند التوقيع. ويتم استخدامه عادة عبر قلم إلكتروني مرتبط بجهاز حاسوب، حيث يقوم الشخص بتوقيع رقمي يعكس سماته البيولوجية المميزة، مما يوفر درجة عالية من الأمان والمصداقية، ويُعد وسيلة فعالة للتحقق من الهوية ومنع الإنكار أو الانتحال.

[1]-القانون رقم 15-04، المرجع السابق.

ويعتمد هذا النوع من التوقيع على تسجيل النمط الحركي الخاص بحركات اليد وأصابع المستخدم، وهو نمط يختلف من شخص لآخر ويُعد فريدًا في طبيعته، مما يُقارب مفهوم "البصمة الإلكترونية" التي تقوم على التقنية ذاتها، وتُستخدم للتحقق من هوية الموقع بصورة دقيقة وآمنة.[1]

تعتمد وسائل التوقيع البيومتري على الخصائص الجسدية والفسيولوجية الفريدة التي تميز كل فرد عن غيره، كالبصمات الوراثية (بصمة الإصبع)، أو السمات البيولوجية الدقيقة مثل شبكية العين، أو نبرة الصوت، أو حركة الشفاه، وغيرها من المعالم الشخصية التي يصعب تزويرها أو تقليدها. وفي هذا الإطار، تُستخدم تقنيات متطورة تعتمد على أجهزة إلكترونية متصلة بالحاسوب، كالقلم الرقمي، الذي يمكن من خلاله تسجيل حركات اليد والأصابع، لتكوين نمط مميز يُعرف بالبصمة البيومترية، التي تُعد فريدة وغير قابلة للتكرار من شخص لآخر.

ويُثار في هذا السياق تساؤل جوهري مفاده: هل يمكن اعتماد هذه السمات البيومترية كوسيلة قانونية معترف بها ضمن وسائل التوقيع الإلكتروني؟ من الناحية التقنية، تعتبر هذه الخصائص مؤهلة بامتياز للقيام بوظيفة التوقيع الإلكتروني، نظراً لصعوبة تقليدها وارتفاع درجة أمانها. إلا أن الاعتراف القانوني بها يظل مرهوناً بتوفير منظومة تكنولوجية محكمة تضمن حماية هذه البيانات من أي اختراق أو تلاعب، فضلاً عن ضرورة تبني المشرّع لنصوص قانونية واضحة تقر بحجية هذا النوع من التوقيع في الإثبات، وتُقرّه جهات القضاء ضمن وسائل الإثبات في المعاملات الرقمية.

أما التوقيع الرقمي، فيُعد من أكثر أنواع التوقيعات الإلكترونية تطوراً وأماناً، حيث يقوم على أسس رياضية وتقنية عالية التعقيد، يتم من خلالها تحويل التوقيع أو الوثيقة من شكلها النصي إلى صيغة مشفرة بواسطة معادلات رياضية، لا يمكن فك رموزها إلا باستخدام "مفتاح خاص" لا يمتلكه إلا صاحب التوقيع نفسه. وتُضمن سرية هذا التوقيع من خلال نظام المفاتيح المزدوجة: المفتاح العام والمفتاح الخاص، بحيث لا يمكن لأي طرف ثالث الاطلاع على أو تعديل محتوى الوثيقة إلا وفق شروط محددة.

وتتمثل آلية هذا النظام في أن الشخص الراغب في إبرام عقد عبر الإنترنت يقوم بقراءة محتوى العقد المُرسل إليه من قبل الجهة الأخرى باستخدام المفتاح العام، دون أن يتمكن من تعديله. وفي حال قبوله

[1]–مصطفى يوسف كافي النقود و البنوك الالكترونية ،ص 197

بشروط العقد، يُعيد إرساله موقَّعًا باستخدام مفتاحه الخاص، ما يمنع الجهة المرسلة أو أي طرف آخر من التعديل أو الإنكار، نظراً لعدم امتلاكهم المفتاح الخاص.

ويشترط لتحقيق هذه الآلية وجود جهة ثالثة ذات ثقة وحياد، يُناط بها إصدار شهادات التصديق الإلكتروني، التي تثبت هوية صاحب التوقيع وصحة المفاتيح المستعملة، وتُشرف على منح المفاتيح العامة والخاصة، وفق معايير أمنية معتمدة قانونًا. وتُعد هذه الجهة عنصرًا محوريًا في ضمان موثوقية التوقيع الرقمي وحجيته القانونية، لاسيما في مجال المعاملات التجارية الإلكترونية، حيث تُسهم في ترسيخ الثقة والطمأنينة لدى المتعاملين، وتُعزّز من مصداقية البيئة الرقمية.

لذلك، تبرز الحاجة الملحة لتسريع وتيرة إنشاء هذه الجهات المختصة في إطار تشريعي وتنظيمي محكم، لما لها من أهمية قصوى في التحقق من سلامة وصحة التوقيع الإلكتروني، وضمان أمن التعاملات الإلكترونية واستقرارها القانوني[1]

الفرع الثاني :

صور التوقيع الالكتروني

بدأت معالم عصر المعاملات الإلكترونية تتبلور وتنتشر بصورة متسارعة، لاسيما بعد أن حظيت بالاعتراف القانوني كوسيلة مشروعة للتصرفات القانونية والتعاملات المدنية والتجارية، مما مهّد الطريق أمام اعتمادها كأداة رئيسية في تنظيم العلاقات بين الأفراد والجهات المختلفة. وقد انطلقت فعليًا الخطوات العملية نحو تعميم استخدامها، بالنظر إلى ما توفره من مزايا تقنية وقانونية تسهم في تسهيل المعاملات، وتسريع الإجراءات، وتحقيق الكفاءة والمرونة في الأداء، الأمر الذي يؤهلها لتكون الوسيلة الأساسية للتعامل في المستقبل القريب ضمن مختلف القطاعات[2].

مع التطور المتسارع الذي يشهده قطاع الاتصالات وتكنولوجيا المعلومات، تنوّعت صور وأشكال التوقيع الإلكتروني، تبعًا لاختلاف أساليب إنشائه واعتماد تقنيات إلكترونية مبتكرة تُستخدم في إبرام التصرفات والعقود القانونية عن بعد. وقد أسهم هذا التقدم التقني في بروز أنماط متعددة من التوقيع الإلكتروني، تُجسد في مضمونها تحولًا عميقًا في نمط التعاقد، الذي بات يُمارس عبر وسائط إلكترونية بديلة عن الوسائل التقليدية.

[1]– مصطفى يوسف كافي ، النقود و البنوك الالكترونية ، ص 198

[2]–أمير فرج يوسف، التوقيع الإلكتروني، الطبعة الأولى، مكتبة الوفاء القانونية للنشر، الإسكندرية، 2011، ص 56

ويُعد التوقيع الإلكتروني اليوم من أبرز مظاهر التفاعل القانوني في البيئة الرقمية، لما يتيحه من إمكانيات تقنية وقانونية تواكب التحولات الحديثة وتُسهم في إرساء الثقة في المعاملات الإلكترونية[1].

أدى التطور التكنولوجي، ولا سيما في مجال الاتصال عبر شبكة الإنترنت، إلى ظهور تصرفات قانونية جديدة، أبرزها التجارة الإلكترونية، التي استوجبت اعتماد التوقيع الإلكتروني كبديل فعّال عن التوقيع التقليدي. وقد أجمعت التشريعات والفقه، في مختلف النظم القانونية، على الاعتراف به كوسيلة تمنح الحجية القانونية للمحررات الإلكترونية، شريطة توافر معايير الأمان والموثوقية.

وسيُخصص هذا المبحث لبيان صور التوقيع الإلكتروني وتطبيقاته العملية، وفق تقسيم ثنائي: المطلب الأول يتناول صوره، بينما يعالج الثاني مجالات استخدامه.

وتجدر الإشارة إلى أن أغلب التشريعات لم تضع تعريفاً حصرياً له، مراعاة للتطور المستمر في تقنيات المعلومات، مما يسمح بظهور أشكال متنوعة له، كما هو الحال في التوقيع التقليدي. ويعتمد التوقيع الإلكتروني على تقنيات رقمية تُحوّل بيانات مميزة إلى رموز مشفّرة، تضمن سرية المعاملات، وتثبت هوية الموقع، وسلامة المحتوى، مما يجعله وسيلة موثوقة للإثبات في البيئة الرقمية.[2]

أفرزت التجارة الإلكترونية جملة من الآليات والوسائل المستحدثة في مجال الدفع، لم تكن مألوفة في المعاملات التقليدية، حيث برزت في الواقع العملي وسائل جديدة كبطاقات الائتمان، والنقود الإلكترونية، وغيرها من أدوات الدفع التي تُنجز عبر شبكة الإنترنت. وتتميّز هذه المعاملات بكونها تتم دون تدخل مادي مباشر من الأطراف المتعاقدة، وتعتمد كليًا على الوسائط التقنية. ونظرًا لطبيعتها الرقمية، فإن توثيقها لا يتم إلا من خلال وسائل إثبات إلكترونية حديثة، وعلى رأسها التوقيع الإلكتروني، الذي يُعدّ الأداة القانونية الوحيدة الكفيلة بإضفاء المشروعية والحجية على هذه المعاملات في ظل غياب التوقيع التقليدي.[3]

ومن خلال ما تم ذكره سوف يتم التطرق لصور التوقيع الإلكتروني المؤمن المعروفة حاليا، وكذلك صور التوقيع الإلكتروني البسيطة، على النحو التالي:

[1]–محمد غسان ريضي مرجع سابق، ص 94

[2]–علاء محمد نصيرات، مرجع سابق، ص 31

[3]–فيصل سعيد الغريب، مرجع سابق، ص 235

أولا : التوقيع المؤمن

يقتصر التوقيع المؤمن في الصور التالية:

أولا : التوقيع الرقمي

يُعد التوقيع الرقمي من أبرز صور التوقيع الإلكتروني وأكثرها موثوقية واعتماداً، لما يتميز به من كفاءة تقنية عالية وسرعة في الأداء، مقرونة بدرجة معتبرة من الأمان والثقة في الاستخدام. وقد أضحى يشكّل وسيلة فعالة للإثبات في البيئة الرقمية، نظراً لما يوفره من حماية ضد الاحتيال والتزوير، حيث تُعد احتمالات التلاعب به ضئيلة مقارنة بأنواع التوقيعات الإلكترونية الأخرى، التي قد تكون أكثر عرضة للاختراق أو الغش.

وتحقيقاً للفعالية القانونية المرجوة من هذا النوع من التوقيع، يشترط أن يتم إنشاؤه وتوثيقه من خلال جهات معتمدة رسمياً، ولا سيما تلك المكلفة بتنظيم وضبط المعاملات الإلكترونية، وخاصة في المجال المالي. ويتم اعتماد التوقيع الرقمي ضمن بيئة قانونية وتقنية مؤمنة، تضمن سلامة البيانات المتبادلة، وتكفل مصداقية التعاملات الإلكترونية، مما يمنحه قوة إثباتية معتبرة ضمن الإطار القانوني المنظّم للعقود والتصرفات المبرمة عن بعد[1].

يُعرَّف التوقيع الرقمي، وفقًا للمواصفة القياسية الدولية رقم ISO 7498-2الصادرة عن المنظمة الدولية للمعايير (ISO) سنة 1988، بأنه" :بيان يُضاف إلى وحدة بيانات أخرى، أو هو عملية تحويل لتلك البيانات المشفّرة بطريقة تمكّن المتلقي من التحقق من مصدر البيانات وسلامة مضمونها، وضمان حمايتها من أي تزوير أو تعديل".

ويُستفاد من هذا التعريف أن التوقيع الرقمي يُعد وسيلة تقنية ذات طابع قانوني تهدف إلى توفير الحماية للمراسلات والوثائق الإلكترونية من خلال ضمان سلامة محتواها، والتأكد من نسبتها إلى مصدرها الصحيح، مما يمنع التلاعب أو التحريف أثناء نقل البيانات عبر الوسائط الإلكترونية. [2]

[1]-هاني سليمان الطعيمات حجية الكتابة والتوقيع الإلكترونين في إثبات المعاملات المالية، دراسة فقهية قانونية مقارنة. المجلة الأردنية في الدراسات الإسلامية، المجلد 14، العدد 2، 2018، ص 87

[2]-عاطف عبد الحميد حسن التوقيع الإلكتروني (مفهومه صوره، حجيته في الإثبات، في نطاق المعاملات المدنية)، دار النهضة العربية القاهرة، مصر، 2008، ص 64

يُعرَّف التوقيع الإلكتروني على أنه مجموعة من البيانات الرقمية القصيرة، ترتبط ارتباطًا تقنيًا ومشفّرًا بمحتوى الوثيقة محل التوقيع، بحيث تُتيح التحقق من صحة الوثيقة والتأكد من هوية الشخص الذي قام بالتوقيع عليها، وذلك عبر علاقة رياضية تُنشأ بواسطة تقنيات التشفير، مما يضفي على المحرر الإلكتروني حجية قانونية في الإثبات. [1]

يقوم التوقيع الإلكتروني على تقنية التشفير الرقمي، التي تعتمد بدورها على خوارزميات ومعادلات رياضية معقدة تهدف إلى ضمان سرية البيانات وحمايتها من الاختراق أو التلاعب. وتتم هذه العملية من خلال تحويل محتوى الرسالة الإلكترونية إلى صيغة مشفّرة غير قابلة للقراءة إلا من قبل الشخص المخوّل، أي صاحب التوقيع، مما يضمن خصوصية المحتوى وسلامته. ويُستخدم في هذا السياق نظام تشفير ثنائي المفاتيح، حيث يعمد المرسل إلى استعمال مفتاح خاص لتشفير الرسالة، في حين يقوم المستقبل بفك التشفير باستخدام مفتاح عام متاح له. وفي حال تمكّن المستقبل من فك التشفير وقراءة الرسالة بصيغتها السليمة، فإن ذلك يُعدّ دليلاً على صحة توقيع المرسل.[2]

يعتمد هذا النوع من التوقيع على نظام التشفير المزدوج، المعروف بنظام "المفتاحين"، حيث يُستخدم مفتاحان منفصلان: أحدهما يُخصص للتشفير ويُعرف بالمفتاح الخاص، وهو ما يُستخدم لإنشاء التوقيع الإلكتروني، ويحوزه الموقع وحده دون غيره. وقد عرّف المشرّع الجزائري المفتاح الخاص في الفقرة الثامنة من المادة الثانية من القانون رقم 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين، بأنه: "سلسلة من الأعداد يحوزها حصريًا الموقّع فقط وتُستخدم لإنشاء التوقيع الإلكتروني، وترتبط ارتباطًا وثيقًا بمفتاح تشفير عمومي". [3]

أما المفتاح الثاني فيستخدم لفك التشفير ويسمى المفتاح العام أو مفتاح التشفير العمومي، وعرفه المشرع الجزائري بموجب الفقرة التاسعة من المادة الثانية من القانون 15/04 سالف الذكر بأنه: "سلسلة من الأعداد تكون موضوعة في متناول الجمهور بهدف تمكينهم من التحقق من الإمضاء الإلكتروني، وتدرج في شهادة التصديق الإلكتروني .

[1]-حنان مليكة النظام القانوني للتوقيع الإلكتروني في ضوء قانون التوقيع الإلكتروني السوري، رقم 4، الصادر بتاريخ 25 فيفري 2009، مجلة جامعة دمشق للعلوم الاقتصادية والفكرية، المجلد 26، العدد 2010، ص 42

[2]-مثاني فراح العقد الإلكتروني وسيلة اثبات حديثة في القانون المدني الجزائري، دار الهدى عين المليلة، الجزائر، ص192

[3]-ثروت عبد الحميد، مرجع سابق، ص 63

يُتيح المفتاح العام لأي شخص الاطلاع على رسالة البيانات عبر شبكة الإنترنت دون إمكانية تعديل محتواها، لكونه لا يمتلك المفتاح الخاص اللازم لذلك. وفي حال طابق محتوى الرسالة رغبة المتلقي وأراد الالتزام بها، يقوم بالتوقيع عليها باستخدام مفتاحه الخاص، ثم يعيد إرسال الرسالة مرفقة بتوقيعه في الملف ذاته. وبمجرد وضع التوقيع على المستند أو العقد، تُغلق الرسالة إلكترونيًا بشكل يمنع أي تعديل لاحق من أي طرف، إلا من خلال استخدام المفتاحين الخاصين بكل من الموقّع وصاحب رسالة البيانات.

وتبقى مسألة أساسية لا بد من معالجتها، وهي كيفية تأكد المرسل إليه من أن المفتاح العام الذي تسلمه يعود فعلاً إلى الشخص الذي ينوي التعامل معه. وهنا تبرز الحاجة إلى وجود جهة ثالثة محايدة وموثوقة، تُعنى بالتحقق من هوية مستخدمي هذا النوع من التوقيع، والتأكد من نسب المفتاح العام لصاحبه الحقيقي. وتتولى هذه الجهة إصدار شهادة تصديق إلكتروني تُثبت صحة التوقيع وتؤكد الصلة بين الموقّع وبيانات إنشاء التوقيع، مما يمنح التوقيع الإلكتروني قوته القانونية ويضمن سلامة التعاملات الرقمية.[1]

تعتمد آلية تشغيل نظام التوقيع الرقمي على تحويل بيانات المحرر الإلكتروني إلى صيغة غير قابلة للقراءة، من خلال استخدام خوارزمية حسابية معينة. ويمكن أن يتم ذلك بطريقتين:

التشفير المتماثل: حيث تُستخدم نفس المفتاح لإغلاق (تشفير) وفتح (فك تشفير) بيانات المحرر، ما يعني أن طرفي الاتصال يشتركان في مفتاح واحد سري.

التشفير غير المتماثل (التشفير بالمفتاح المزدوج): في هذا النظام يُستخدم مفتاحان مختلفان، أحدهما لتشفير البيانات (المفتاح العام)، والآخر لفك تشفيرها (المفتاح الخاص)، مما يعزز من مستوى الأمان ويمنع الوصول غير المصرح به إلى البيانات.[2]

1 التشفير المتماثل

الذي يعرف بالتوقيع السيمتري؛ وهو تشفير يعتمد على فكرة رقم سري متبادل بين طرفين ومعلوم لكليهما، ويشتغل في بيئة منعزلة والمثال عليه التلكس والبطاقات البلاستيكية، إذ أن الرقم السري معلوم لدى صاحبه ولد الجهاز فقط [1]

[1]–بوعلام بوزيدي التوقيع الإلكتروني، مجلة البدر، بشار، بدون سنة، ص 108.

[2]–بلقنيشي حبيب، مرجع سابق، ص 124

2 التشفير غير المتماثل

يُعرف هذا النوع من التشفير بالتوقيع اللامتماثل، أو التوقيع الرقمي غير المتماثل، وهو نظام يعتمد على استخدام زوج من المفاتيح: مفتاح عام وآخر خاص. يتيح المفتاح العام لأي شخص إمكانية الاطلاع على محتوى الرسالة عبر شبكة الإنترنت، دون أن يمنحه صلاحية التعديل أو التغيير عليها، مما يضمن سلامة البيانات. في المقابل، يُعد المفتاح الخاص أداة سرية لا يمتلكها إلا صاحب التوقيع الرقمي، ويُستخدم حصريًا لتوقيع الوثائق إلكترونيًا. وتقوم هيئة مختصة بإصدار هذا المفتاح واعتماده، بهدف التحقق من هوية الموقع وضمان مصداقية التوقيع الرقمي. [2]

إن التوقيع الرقمي يُعد وسيلة موثوقة تضمن أعلى مستويات الأمان والثقة في المحررات الإلكترونية، وذلك بالنظر لما يوفره من ارتباط تقني محكم بين التوقيع والمحرر المثبت عليه، على نحو يُعبّر صراحة عن إرادة الموقع في الالتزام بالتصرف القانوني وتقبّل مضمونه. وبذلك، فإنه يستوفي الشروط الشكلية والموضوعية التي يتطلبها القانون للاعتداد بالمحرر كدليل كتابي كامل الحجة.

فضلاً عن ذلك، يكفل التوقيع الرقمي حماية سرية البيانات المتضمنة في الوثائق الإلكترونية، إذ لا يمكن الاطلاع عليها إلا من قبل الشخص المخاطَب بها، وباستخدام المفتاح العام الموافق للمفتاح الخاص الذي تم به التوقيع. ويُعزز من موثوقية هذا النظام وجود هيئة معتمدة مختصة في توثيق المعاملات الإلكترونية، تضطلع بمهمة إصدار الشهادات الإلكترونية التي تتيح التحقق من صحة التوقيع الرقمي وهوية صاحبه، وفقًا للضوابط القانونية المعمول بها. [3]

ورغم المزايا التي يتمتع بها التوقيع الرقمي مقارنة مع غيره من التواقيع الإلكترونية الأخرى، فإنه يمكن أن يؤخذ عليه عدة أوجه سلبية ومنها :

الوجه الأول / احتمال تعرضه للسرقة أو الضياع، فالعميل . على سبيل المثال ملتزم بسرية البطاقات حسب اتفاق البنك وإلا تعرض للمسائلة، فضلا عن ذلك فلو كان توقيعه الإلكتروني الصادر به شهادة موثقة

[1]–علاء محمد نصيرات، مرجع سابق، ص 37

[2]–منصور عز الدين مرجع سابق، ص 74

[3]–رشيدة بوكر التوقيع الإلكتروني في التشريع الجزائري (دراسة مقارنة)، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة عبد الحميد بن باديس، مستغانم العدد الرابع ديسمبر 2016، ص 70

من الجهة المختصة قد تسرب الآخرين فهو مسؤول عن ذلك، طالما لم تتخذ إجراءات الحيطة المنصوص عليها فسيكون الوحيد الذي سرب هذا الرقم للغير.

الوجه الثاني/ وما يعيب كذلك على هذا النوع من التوقيعات أنه لا يعبر عن شخصية صاحبه مثل التوقيع التقليدي، إلا أن ذلك مردود عليه بأن التوقيع الإلكتروني لا يصدر عن جهاز الحاسب الآلي، وإنما يتم من قبل صاحب التوقيع، فالحاسب ما هو إلا مجرد وسيلة في أداء هذا التوقيع تماما كما أن القلم وسيلة للتوقيع التقليدي، ولا إرادة له في إتمام عملية التوقيع.

الوجه الثالث/ وعلى الرغم مما يحققه التوقيع الرقمي من مستويات عالية من الثقة والأمان في ظل التطورات التكنولوجية الراهنة، إلا أن بعض الآراء تُبدي تخوفًا مشروعًا من المخاطر المحتملة الناتجة عن تطور أساليب القرصنة والاحتيال الإلكتروني، والتي قد تصل في بعض الحالات إلى إمكانية اختراق رسالة البيانات من خلال كسر أو كشف المفتاح الخاص، مما يُعرض سرية المعاملة وسلامتها للخطر.. [1]

ثانيا : التوقيع البيو متري

من أبرز التطورات التكنولوجية المعاصرة في مجال إبرام العقود عبر الوسائط الإلكترونية، يبرز نظام التوقيع البيومتري، الذي يُعد وسيلة دقيقة وموثوقة لتوثيق هوية الشخص. وتستند هذه التقنية إلى الخصائص الفيزيولوجية والسلوكية الفريدة لكل فرد، والتي لا يمكن تماثلها أو انتحالها، مما يمنحها قوة إثبات عالية في تحديد هوية الموقّع وضمان سلامة المعاملات الإلكترونية، وفقًا لما تقتضيه الضوابط القانونية المتعلقة بصحة التوقيع وصحة الرضا.[2]

وعليه، فإن التوقيع البيومتري يُؤدي ذات الوظيفة القانونية للتوقيع التقليدي، والمتمثلة في تحديد هوية الشخص الموقّع، متى تم توظيف إحدى الخصائص المميزة له وتخزينها في وسائط رقمية مضغوطة ضمن نظام إلكتروني مُؤمَّن، على نحو لا يستهلك حيزًا كبيرًا من ذاكرة المعالجة المعلوماتية.

وفي هذا الإطار، يُمكن التمييز بين ثلاث فئات رئيسية من الخصائص البيومترية المعتمدة في هذا النوع من التوقيعات:

[1]–غربي خديجة، مرجع سابق، ص 17

[2]–بسعر سمية، بوخشة وردة، التوقيع الإلكتروني ودوره في الإثبات في التشريع الجزائري، مذكرة مكملة لنيل شهادة الماستر في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة محمد الصديق بن يحي، جيجل 2015/2016، ص22.

- **الفئة الأولى:** الخصائص البيولوجية، وتشمل السمات الفيزيولوجية الثابتة لدى الإنسان، مثل الحمض النووي (DNA)، الدم، اللعاب، والرائحة.
- **الفئة الثانية:** الخصائص السلوكية أو الذاتية، والتي تتجلى في أنماط متكررة ومميزة للفرد، كطريقة التوقيع اليدوي، حركات الجسم، ونبرة الصوت.

ويُعتد بهذه الخصائص كوسيلة قانونية للتحقق من الهوية في إطار المعاملات الإلكترونية، متى توافرت فيها معايير الدقة والثبات والخصوصية التي تضمن سلامة التوثيق وعدم قابليته للإنكار أو التزوير.الفئة الثالثة الخصائص الشكلية مثل: بصمة الإصبع، شكل اليد مسح العين البشرية، والتعرف على الوجه البشري.[1]

يسمح جهاز الحاسب الآلي بالتعرف على هذه الخواص عن طريق تخزينها بصورة دقيقة في نظام معين في هذا الجهاز، وعليه فإن توافق تلك الصفات المخزنة من قبل مع ما تم حدثيا من توقيع و ذلك بغرض التحقق من صحة التوقيع الإلكتروني الحديث وأنه مطابق للتوقيع المخزن سابقا .[2]

وعليه فإن آلية عمل هذه التقنية فيتم تطبيقها بواسطة مرحلتين:

المرحلة الأولى: مرحلة التشفير، حيث يتم التقاط المعطيات البيومترية الخاصة بالمستخدم بواسطة أجهزة إلكترونية متطورة مزوّدة بتقنيات دقيقة، ثم تُحوَّل هذه المعطيات إلى صيغة رقمية مشفَّرة وتُخزن في نظام الحاسوب بطريقة تضمن سريتها وحمايتها من أي اختراق أو تعديل.

المرحلة الثانية: مرحلة فك التشفير، ويتم خلالها التقاط نفس المعطيات البيومترية مرة أخرى، باستخدام نفس الوسائل التقنية، وذلك بغرض مقارنتها مع البيانات المشفّرة والمحفوظة سابقًا. فإذا تبيّن أن هناك تطابقًا

[1]– سمير بن حليمة، القصد الجرمي في تزوير التوقيع الإلكتروني، مذكرة مقدمة لنيل شهادة الماستر الاكاديمي، تخصص قانون جنائي، فرع الحقوق كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف المسيلة 2017/2018، ص 14.

[2]–نايف بن ناشي الغنامي التوقيع الإلكتروني وحجيته في الإثبات بالتطبيق على النظام السعودي، بحث منشور بكلية الشريعة والأنظمة، جامعة الطائف 2019، ص 2323

تامًا بين البيانات الجديدة والمخزنة، يُعتدّ بالتوقيع ويُدمج في المعاملة الإلكترونية بصفته وسيلة موثوقة للتصديق على محتواها، وفقًا لمقتضيات الإثبات الإلكتروني.[1]

بعد التوقيع باستخدام الخواص الفيزيائية للشخص من الوسائل الموثوق فيها وذلك عائد لتباين المعطيات الذاتية من انسان آخر، بالإضافة إلى ذلك إمكانياتها من تمييز الشخص وتعيين هويته نظرا لارتباطها به، مما يتيح الاعتداد بها في إقرار التصرفات القانونية المبرمة عبر الوسائل الإلكترونية. [2]

إن التوقيع الديو متري يقوم بوظائف التوقيع التقليدي لأن الخصائص الذاتية لكل شخص من شأنها أن تميزه عن أي شخص آخر، ولذلك فإن هذا التوقيع بعد وسيلة موثوقا بها لتمييز الشخص وتحديد هويته عن طريق تشفيره حتى لا يمكن أن ينتحل شخص آخر شخصية الموقع . [3]

لهذه الصورة العديد من النقائص والثغرات، منها أن صورة التوقيع يتم وضعها على القرص الصلب للحاسب الآلي، ومن ثمة يمكن تحريفها أو نسخها بواسطة الطرق المستعملة في القرصنة الإلكترونية، بالإضافة إلى عدم إمكانية استخدام هذه التقنية مع جميع الحسابات المتوفرة، حيث يحتاج هذا النوع من التوقيع إلى إجراءات مطولة في استخدام الخصائص الذاتية للشخص الموقع مما يكلف مصروفات باهظة على عاتق الموقع[4]، وكذلك فقدان السرية والكفاءة الضامنة لهذه التقنية، نظرا لمحاولة الشركات المصنعة النظم التوقيع البيو متري الاتفاق على طريقة موحدة لهذه التقنية.

غير أن هذه النقائص، وعلى الرغم من أهميتها، لا يجوز أن تُنقص من القيمة القانونية للتوقيع البيومتري في مجال توثيق المعاملات الإلكترونية، إذ يظل هذا الأخير وسيلة فعّالة وموثوقة متى توفرت له البيئة التقنية المناسبة. ويتطلب ذلك اعتماد تقنيات متطورة تضمن سرية المعطيات البيومترية وحمايتها من أي اختراق أو استعمال غير مشروع، إلى جانب إخضاع عملية التوقيع لرقابة جهة تصديق معتمدة قانونًا،

[1]–ايهاب سمير محمد صالح، الإثبات بالمحررات الإلكترونية (دراسة مقارنة)، رسالة لاستكمال متطلبات الحصول على درجة الماجستير في القانون الخاص، كلية الحقوق، جامعة الأزهر، غزة 2015، ص 46

[2]–ا بسعر سمية بوخدشة وردة، مرجع سابق، ص 40

[3]–عيسى غسان ريضي، مرجع سابق، ص 64

[4]–يمينة جوجو، عقد البيع الإلكتروني في القانون الجزائري، الطبعة الأولى، دار بلقيس للنشر، الجزائر 2016، ص 183

تضطلع بمهمة تأمين هذا النوع من التواقيع، وتوفير عناصر الثقة والأمان القانوني اللازمين لاعتماده كوسيلة إثبات معترف بها في المعاملات الرقمية.[1].

ثالثا : التوقيع بالعلم الإلكتروني

تتمثل هذه الطريقة من التوقيع بكتابة التوقيع اليدوي بواسطة قلم إلكتروني خاص على لوحة معدنية حسابية مرتبطة بجهاز الحاسب الآلي، ومن يظهر التوقيع الخطي على شاشة ذلك الجهاز[2]، ويتم تخزين صورة توقيع الشخص بذاكرة الحاسب الآلي، وعندما يرسل مستند إلكتروني موقع بخط يده عن طريق قلم إلكتروني خاص يتم المضاهاة بين التوقيع المرسل والتوقيع المخزن بذاكرة الحاسب[3]، ومن ثم، يتولى برنامج متخصص مهمة التحقق من صحة التوقيع البيومتري في كل مرة يتم فيها إعادة كتابته، وذلك بالاعتماد على تحليل الخصائص الحركية والديناميكية للكتابة، كاتجاه حركة اليد، وأشكال الحروف، والانحناءات، والالتواءات، وغيرها من السمات المميزة للتوقيع الخطي، والتي سبق تخزينها في النظام بشكل مشفّر ودقيق.

ويُعد هذا النوع من التوقيع أكثر موثوقية من التوقيع اليدوي الإلكتروني البسيط، الذي يتم على شاشة جهاز الحاسوب باستخدام قلم إلكتروني عبر لوحة مخصصة لذلك، عند تحرير المحرر الإلكتروني على الواجهة البصرية للجهاز، إذ أن هذا الأخير يفتقر إلى الحد الأدنى من معايير الأمان، ولا يحقق حجية قانونية كافية في مجال الإثبات، لكونه لا يستند إلى خصائص مميزة أو مؤشرات فنية يمكن الاستناد إليها للتثبت من هوية الموقّع أو صحة إرادته.[4].

---

[1]–كوسام أمينة، الشكلية في عقود التجارة الإلكترونية، أطروحة مقدمة لنيل درجة دكتوراه العلوم في العلوم القانونية، كلية الحقوق والعلوم السياسية، جامعة باتنة 2015/2016، ص 62

[2]–عنوش حنان العلاوي عز الدين النظام القانوني للعقد الإلكتروني في التشريع الجزائري، مذكرة تخرج لنيل شهادة الماستر في الحقوق، تخصص القانون العام للأعمال كلية الحقوق والعلوم السياسية، جامعة عبد الرحمن ميرة، بجاية، 2018/552019

[3]–بلقاسم حامدي، إبرام العقد الإلكتروني، أطروحة مقدمة لنيل درجة دكتوراء العلوم في العلوم القانونية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة 2014/2015، ص 214.

[4]–بن سعدي فريدة، وسائل الإثبات الحديثة في القانون المقارن، مذكرة مقدمة لنيل شهادة الماستر في الحقوق، تخصص القانون الخاص الشامل، كلية الحقوق و العلوم السياسية، جامعة عبد الرحمن بجاية 2012/2013، ص 21

تتميّز هذه الطريقة بقدر كبير من المرونة وسهولة الاستخدام، من خلال إمكانية تحويل التوقيع الخطي إلى توقيع إلكتروني يُدمج ضمن المحررات الرقمية. غير أنه، ورغم هذه المزايا، تظل هذه الوسيلة محفوفة بمخاطر تمسّ بمصداقية التوقيع، وقد تفضي إلى زعزعة الثقة في المعاملات الإلكترونية.

ويُعزى ذلك إلى إمكانية احتفاظ المتلقي بصورة التوقيع واستخدامها لاحقًا في إرفاقها بمستندات أو وثائق أخرى، بذات الكيفية التي استُخدم بها التوقيع على المحرر الأصلي. كما أن هذه الطريقة لا توفر ضمانة تقنية للتحقق من هوية الشخص الذي قام بالتوقيع فعليًا، إذ أن حصول أي طرف على نسخة من التوقيع يمكنه من استعمالها بحرية على أي محرر آخر، ثم إعادة إرساله إلى جهات متعددة، دون وجود وسيلة موثوقة للتثبت من أن الموقع هو بالفعل صاحب التوقيع. يريد، وهو ما يؤدي إلى ضعف الثقة في المحررات الموقع عليها إلكترونيا وبالتالي يقلل من حجية التوقيع الإلكتروني[1].

ولكن هناك من يرى أن هذه المشكلة يمكن حلها من خلال طريقتين هما: الأولى تكنولوجيا المفتاح العام القائمة على التشفير، والثانية إيجاد جهة تصديق معتمدة من قبل السلطة التنفيذية يمكن الرجوع إليها للتحقق مقدما من شخصية منشئ التوقيع قبل الشروع في التعامل معه، حيث سيكون لدى هذه الجهة نموذج لهذا التوقيع يعين هوية منشئه مما يؤدي إلى وجود درجة عالية من الثقة والأمان في استعمال العلم الإلكتروني في التوقيع[2].

غير أن هذه الطريقة تواجه العديد من المعوقات، لاسيما ما يتعلق بعنصر الثقة والمصداقية، إذ أنها لا توفر ضمانات كافية للتحقق من هوية الموقّع. ذلك أن المتلقي يمكنه، من الناحية التقنية، الاحتفاظ بصورة التوقيع المثبت على المحرر الإلكتروني المستلم عبر شبكة الإنترنت، من خلال استخدام أجهزة المسح الضوئي (سكانر)، ثم إعادة إدراجه على محررات أو وثائق أخرى دون علم أو تفويض من صاحبه.

وتكمن خطورة هذه الممارسة في غياب الوسائل الفنية والقانونية الكفيلة بالتحقق من أن صاحب التوقيع الأصلي هو من قام فعليًا بإرفاق توقيعه بالمحرر وإرساله، مما يُفقد هذه الوسيلة الضمانات اللازمة للحماية

[1]–غازي حنون خلف عماد فاضل ركاب، وصفي هاشم عبد الكريم القصد الجرمي في تزوير التوقيع الإلكتروني، بحث 3 مؤسسة دفء الأنبياء الثقافية، كلية القانون، جامعة البصرة، 2010، ص 6/7

[2]–ا خالد ممدوح إبراهيم، إبرام العقد الإلكتروني دراسة مقارنة، الطبعة الثانية، دار الفكر الجامعي، الإسكندرية، 2011 ص256

القانونية، ويجعلها عرضة للاستغلال والتزوير. وهو ما ينعكس سلبًا على القوة الثبوتية للتوقيع الإلكتروني في إطار المعاملات الإلكترونية.

وعليه، يُؤخذ على هذه الطريقة افتقارها إلى عنصر الثقة، الأمر الذي يضعف من مصداقية المحررات الإلكترونية الموقعة بهذه الكيفية، ويُقلل من حجية التوقيع الإلكتروني كوسيلة إثبات معترف بها قانونًا.. [1]

رابعا : التوقيع باستخدام البطاقة الممغنطة والرقم السري

يعرف كذلك باسم التوقيع الكودي، وبعد أول شكل أبرزته التقنيات التكنولوجية للتوقيع الإلكتروني وهو الأكثر شيوعا واستعمالا، وهذه الصورة من التوقيعات الإلكترونية ابتكرتها التقنيات التي استعملت من أجل الإسراع في إنجاز المعاملات البنكية[2]، يرتبط هذا النوع من التوقيع الإلكتروني غالبًا باستخدام البطاقات البلاستيكية والبطاقات الممغنطة وغيرها من الوسائط الإلكترونية الحديثة المزودة بذاكرة رقمية. وتيسيرًا لإجراء المعاملات التجارية والحصول على الأموال في أي وقت، عمدت البنوك إلى إصدار بطاقات ائتمان ممغنطة لعملائها، مصحوبة برقم سري لا يعلمه سوى صاحب البطاقة، وتُستخدم هذه البطاقات كوسيلة للإيداع أو سحب النقود أو سداد ثمن السلع والخدمات.

وتتضمن هذه البطاقات بيانات شخصية تتعلق بحاملها (العميل)، تكون محفوظة داخل دائرة إلكترونية مغلقة ومثبتة على البطاقة ذاتها. وعند استعمال البطاقة، يقوم العميل بإدخالها بطريقة صحيحة داخل الجهاز الإلكتروني المخصص لتنفيذ العمليات، ثم يُدخل رقمه السري الخاص، ويُكمل الإجراءات بالضغط على الخيار المناسب لإنهاء العملية.

وتُعد هذه الإجراءات مجتمعة، سواء من حيث إدخال البطاقة أو استعمال الرقم السري، بمثابة تعبير صريح عن إرادة صاحب البطاقة في الالتزام بمضمون العملية التعاقدية، مما يمنحها حجية قانونية ويُرتب آثارها وفقًا لقواعد التعاقد المعتمدة في المعاملات الإلكترونية.[3].

---

[1]–لوصيف عمار الستراتيجيات نظام المدفوعات للقرن الحادي والعشرين، مع الإشارة إلى التجربة الجزائرية، مذكرة مقدمة كجزء من متطلبات نيل شهادة الماجستير في العلوم الاقتصادية، كلية العلوم الاقتصادية وعلوم التسيير قسم العلوم الاقتصادية، جامعة منتوري، قسنطينة 2008/2009، ص 95/96

[2]–محمد غسان ريضي، مرجع سابق، ص 58

[3]–اجحيط حبيبة جهودي مريم النظام القانوني للعقد الإلكتروني (دراسة مقارنة)، مذكرة تخرج لنيل شهادة الماستر في القانون الخاص تخصص القانون الخاص الشامل كلية الحقوق والعلوم السياسية، جامعة عبد الرحمن ميرة بجاية 96 18/06/2013

وتُعد هذه الصورة من التوقيع في شكله الإلكتروني من أكثر الأشكال شيوعًا وانتشارًا لدى عامة الأفراد، نظرًا لما تمتاز به من بساطة وسهولة في الاستخدام، إذ لا تتطلب خبرة تقنية متقدمة أو إجراءات معقدة. كما يمكن لأي شخص استعمالها دون الحاجة إلى توفره على جهاز حاسوب، أو حتى دون الاتصال بشبكة الإنترنت، مما يجعلها وسيلة عملية وميسرة لإبرام المعاملات الإلكترونية اليومية..[1]

وفي الأخير يمكن استخدام هذه البطاقة في شبكة الأنترنيت عن طريق بطاقات الائتمان المعروضة عالياء مثل Visa Mastercard. America :، يتم عمل هذه البطاقات بنظامين هما: نظام OFF-LINEو نظامON-LINE ، حيث يعين الصاحب البطاقة رقم سري خاص يستخدمه كتوقيع الكتروني في عمليات الدفع الإلكتروني، [2]ووجوبا الإشارة هنا إلى عملية تشغير الرقم السري عند استخدامه في عمليات الدفع عبر الأنترنيت، مما يحيل دون معرفته حتى ولو تم اعتراضه

وتتميز هذه الصورة من التوقيع الإلكتروني، فضلاً عن سهولتها وبساطتها، بدرجة معتبرة من الثقة والأمان، إذ إن إتمام التصرف القانوني لا يتم إلا من خلال اقتران إدخال البطاقة في الجهاز المخصص بذلك بإدخال الرقم السري الخاص بالعميل في الخانة الظاهرة على شاشة الجهاز، مما يُعد ضمانة لحماية العملية وتأكيد هوية المستخدم.

غير أن البعض يُبدي تحفظًا بشأن مدى موثوقية وأمان هذه الوسيلة، ويُشير إلى أنها قد تنطوي على مخاطر في بعض الحالات، من بينها:

الحالة الأولى: ضياع البطاقة أو سرقتها من قبل الغير، بحيث يتمكن هذا الأخير من الحصول على الرقم السري المقترن بها، مما يتيح له إجراء عمليات دون تفويض.

والرد على ذلك، أن احتمال وقوع الغير على البطاقة والرقم السري معًا يُعد من الفرضيات النادرة، ولا يُتصور تحققه إلا في حال وجود إهمال جسيم من جانب صاحب البطاقة. كما أن هذه الحالة قابلة للتدارك قانونًا وفعليًا، من خلال إشعار البنك المختص فورًا بفقدان البطاقة، ليقوم بإيقاف صلاحيتها وتعليق التعامل بها إلى حين إصدار بطاقة جديدة أو العثور على البطاقة المفقودة.

---

[1]–طمين سهيلة، مرجع سابق، ص 59

[2]–محمد محروك خصوصيات التوقيع الإلكتروني وحجيته في الإثبات، مجلة جامعة القاضي عياض، مراكش، بدون سنة،ص114

الحالة الثانية: حدوث خلل تقني أثناء تنفيذ عملية التحويل النقدي، مما قد يترتب عليه بقاء آثار تلك العملية معلقة على النظام المرتبط بالبطاقة، كما أن الرسالة الإلكترونية الحاملة للبيانات المالية قد تتعرض أثناء انتقالها عبر شبكة الإنترنت إلى مؤثرات خارجية، قد تؤدي إلى تغيير محتواها أو تعطيل وصولها إلى الجهة المستفيدة.

وعليه، فإن معالجة هذه الإشكالات تستلزم تطوير البنية التقنية وتفعيل أنظمة الحماية والرقابة الإلكترونية، بما يضمن سلامة المعاملات ويُعزز الثقة في استخدام هذه الصورة من التوقيع الإلكتروني ضمن الإطار القانوني المنظم لها.[1]

الفرع الثاني:

صور التوقيع البسيط

تتعدد صور التوقيع الإلكتروني البسيط، غير أنها تتفق جميعًا في خاصية أساسية تتمثل في أن التقنيات المعتمدة في إنشائها لا تتضمن أدوات تكنولوجية مخصصة لتأمين التوقيع أو حمايته من التلاعب والاحتيال. وتمتاز هذه الصور بكونها سهلة الاستخدام ومنخفضة التكلفة، مما يجعلها مناسبة للمعاملات ذات الأهمية المحدودة، سواء من حيث القيمة المالية أو من حيث طبيعة المعلومات المتضمنة فيها.

وتجدر الإشارة إلى أن بعض صور هذا النوع من التوقيع قد أصبحت شائعة الاستعمال لتقاربها في الوظيفة التي تؤديها، باعتبارها تحقق الحد الأدنى من متطلبات التوقيع الإلكتروني. وسنعرض فيما يلي صورتين من أبرز هذه الصور، بالنظر إلى انتشار استخدامهما وتوافقهما مع الوظائف الأساسية للتوقيع الإلكتروني.

أولا: التوقيع باستخدام الصور الرقمية للتوقيع الكتابي

يتمثل هذا النوع في أن يقوم شخصا بتوقيع مستند ورقي، ثم يقوم بإعادة صورة رقمية الكترونية لذلك التوقيع عن طريق جهاز الماسح الصوتي (scanner)، ويتم تخزين تلك الصور في الحاسوب الموقع الغرض استخدامها بعد ذلك.

[1]–طمين سهيلة، مرجع سابق، ص 59

ورغم ما يتميز به التوقيع الإلكتروني البسيط من سهولة في الاستعمال وانخفاض في التكاليف، إلا أن ذلك لا يحجب ما يعتريه من ثغرات جوهرية، لاسيما فيما يتعلق بانعدام عنصري الأمان والثقة. إذ يُمكن للغير الحصول على صورة ضوئية لتوقيع الشخص بوسائل متعددة، سواء من خلال تصوير التوقيع أو نسخه من مستند سابق، الأمر الذي يفتح المجال أمام إمكانيات التزوير أو التلاعب بالتوقيع الكتابي وتحويله إلى صيغة إلكترونية دون علم صاحبه.

كما أن استخدام هذه النسخ من قبل الطرف الآخر قد يؤدي إلى التشكيك في صحة التوقيع، ويثير الريبة بشأن قدرة هذه الوسيلة على تحديد هوية الموقّع بشكل دقيق وموثوق، مما يُضعف من حجيتها القانونية ويحد من فاعليتها كوسيلة إثبات في المعاملات الإلكترونية.[1].

ثانيا: التوقيع بكتابة الاسم في نهاية المحرر الإلكتروني

يُعد هذا النوع من التوقيع من أبسط صور التوقيع الإلكتروني، حيث يقوم الشخص بإدراج اسمه إلكترونيًا في نهاية المستند باستخدام لوحة المفاتيح، سواء بكتابة اسمه الكامل أو اختصارًا له، وتُعد هذه الكتابة بمثابة توقيع يُنسب إليه، باعتبارها تشكّل جزءًا من هويته الرقمية.

وتتعدد الأشكال التي يُعتمد فيها هذا النوع من التوقيع، ومن أبرزها: رسائل البريد الإلكتروني، الصفحات الإلكترونية (Web pages)، أو الملفات النصية بصيغ مختلفة، لاسيما ملفات "Word" وغيرها من الوثائق الرقمية، وذلك بحسب طبيعة المعاملة أو المستند محل التوقيع.[2]

المبحث الثاني:

النظام القانوني للتوقيع الالكتروني

يُعدّ التوقيع الإلكتروني من الآليات القانونية المستحدثة التي أفرزتها البيئة الرقمية، وقد أولته العديد من التشريعات الحديثة أهمية خاصة في مجال الإثبات، لاسيما في المعاملات الإلكترونية. وتجدر الإشارة إلى أن معظم التشريعات المقارنة لا تُقرّ بحجية الكتابة في الإثبات ما لم تكن ممهورة بتوقيع، خلافًا للتوجيه الأوروبي الذي اعتمد تعريفًا دقيقًا للتوقيع الإلكتروني، وبيّن آثاره القانونية، كما أقر بصراحة إمكانية استعماله

[1]–زروق يوسف، حجية وسائل الإثبات الحديثة، رسالة مقدمة لنيل شهادة دكتوراه في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد تلمسان، 2012/2013، ص 256

[2]–محمد محمد سادات، نفس المرجع، ص 52.

من قبل الأشخاص المعنويين، ما يُفضي إلى صحة التصرفات القانونية متى تم التوقيع عليها إلكترونيًا بطريقة صحيحة ومطابقة للمعايير التقنية والقانونية المعتمدة.

وعليه، فإن الاعتراف القانوني بالتوقيع الإلكتروني لا يُعدّ مجرد امتياز تقني، بل يشكّل ضمانة أساسية لحماية المعاملات الرقمية وتعزيز الثقة في الوسائط الإلكترونية، ما يجعله من العناصر الجوهرية التي يقوم عليها نظام الإثبات في العصر الرقمي.

المطلب الأول:

أهمية التوقيع الإلكتروني ووظائفه

في إطار الحديث عن التوقيع الإلكتروني، وبعد إبراز مكانته المتنامية في المعاملات الرقمية، يبرز من الأهمية بمكان التطرق إلى الأبعاد القانونية التي يُضفيها هذا التوقيع على المحررات الإلكترونية، وهو ما يشكّل محور الفرع الأول المتعلق بالأهمية القانونية للتوقيع الإلكتروني.

الفرع الأول:

الأهمية القانونية للتوقيع الإلكتروني

يُعدّ التوقيع أحد المبادئ الأساسية في مجال الإثبات، وشرطاً جوهرياً لتوثيق المستندات، سواء تعلّق الأمر بالمراسلات العادية أو الإلكترونية، على اختلاف طبيعتها ووسائطها، داخل المؤسسة أو في تعاملاتها الخارجية، سواء على المستوى الداخلي للدولة أو في علاقاتها مع الخارج. ويُشكّل هذا التوجه استجابة لحاجات التجارة الإلكترونية، ويُسهم في تيسير المعاملات التجارية للأطراف الراغبة في إبرام علاقات تعاقدية عبر شبكة الإنترنت[1].

وفي هذا السياق، تتضح نية المشرّع في إبراز أهمية التوقيع الإلكتروني من حيث ما يتمتع به من ضمانات تتعلق بالسرية والحماية، مما يُمكّن من توسيع نطاق استخدامه في مختلف القطاعات. وتكمن إحدى أبرز وظائفه في توفير الوقت والجهد لكل من المواطن والموظف، من خلال تسهيل الإجراءات الإدارية والقانونية، خاصة في المنازعات التي تنشأ بين الأفراد أو بين الشركات، كما يُعزّز التوقيع الإلكتروني من

[1]–اياد محمد ، عارف عطا سده، مدى حجية المحررات الالكترونية في الاثبات، دراسة مقارنة، رسالة ماجستير في القانون الخاص، جامعة النجاح الوطنية ، نابلس ، فلسطين ، 2009، ص68–69.

فعالية التواصل بين المواطن والإدارة، ويرفع من كفاءة العمل الإداري من خلال إمكانية اعتماده على مختلف النماذج والمستندات والطلبات الرسمية.

وبالنظر إلى ما يوفره من مرونة، فإن التوقيع الإلكتروني يُغني المواطن عن التنقل إلى الإدارات والهيئات الحكومية لقضاء معاملاته، كما هو الحال في بعض الدول النامية، على خلاف الدول المتقدمة التي أصبحت فيها معظم المعاملات تُنجز عن بُعد، ولا يُطلب الحضور الشخصي إلا في حالات استثنائية تتعلق بالهوية أو بشروط محددة[1].

أما فيما يتعلق باعتماد التوقيع الإلكتروني ضمن الإجراءات القانونية والقضائية في المنازعات، فإن الأمر يخضع لتقدير القاضي، الذي يستند في قناعته إلى مدى موثوقية الجهاز أو النظام الذي أُنجز التوقيع من خلاله. ويأخذ القاضي بعين الاعتبار مختلف العناصر الفنية المرتبطة بسرّية المعالجة وحماية البيانات وآليات الإرسال والحفظ، فضلاً عن كفاءة الجهات أو الأشخاص القائمين على تنظيم وضبط هذه العملية التقنية ذات الطبيعة القانونية.

في ظل التقدم التكنولوجي المتسارع، أصبح من الضروري تقييم مدى كفاءة التوقيع الإلكتروني كوسيلة قانونية يُعتد بها في مختلف المعاملات، وبيان مدى قابليته للاعتماد عليه في الإثبات، سواء في المجال الإداري أو التجاري أو القضائي. فكل هذه التحولات تحتم على الجهات المعنية، من مشرّع وقضاء، الوقوف على جدارة هذا النظام التقني وقدرته على تحقيق الأهداف المرجوة[2].

وفي هذا السياق، يساهم التوقيع الإلكتروني في فتح آفاق جديدة للتواصل بين المواطن والإدارة، بما من شأنه القضاء على العديد من العراقيل التي تعيق فعالية العمل الإداري، وتحقيق درجة عالية من الشفافية، وصولاً إلى ترسيخ مفهوم الحكومة الإلكترونية التي تطمح إليها المجتمعات الحديثة، في سبيل تحسين نوعية الخدمة العمومية المقدمة للمواطن، باعتباره الطرف الرئيسي المتعامل يومياً مع الإدارة في شتى مناحي حياته، سعياً نحو تسهيل معاملاته وتحسين ظروف معيشته. كما أن توسيع نطاق استخدام التوقيع الإلكتروني من شأنه رفع مستوى الكفاءة الإدارية، وذلك من خلال تسريع وتيرة العمل الإداري، وتقليص

[1]–اياد محمد ، عارف عطا سده، المرجع السابق ، ص69.

[2]–عبد الحميد ثروت ، المرجع السابق، 408.

تكاليفه، وتحقيق جودته، فضلاً عن تعزيز رضا المواطن، من خلال تقديم خدمة عمومية أكثر جودة وفعالية، ترتكز على أدوات رقمية موثوقة[1].

أما من حيث إمكانية اعتماد التوقيع الإلكتروني في جميع أنواع المستندات ونماذج الطلبات الإدارية، فإن ذلك من شأنه إرساء مفهوم "الهوية الرقمية" لكل مواطن، مما يسهم في تعزيز الوعي القانوني والتقني لديه، ويكرّس ثقافة التعامل الرقمي، وهو ما ينعكس إيجاباً على ازدهار التجارة الإلكترونية. فقد بات من الملاحظ أن العديد من رواد الأعمال، من خلال استغلالهم للبيئة الرقمية، تمكنوا من تأسيس شركات افتراضية كبرى تحقق أرباحاً ضخمة، دون الحاجة إلى مقرات مادية ضخمة، وهو ما يبرز الأهمية البالغة للتوقيع الإلكتروني، باعتباره أداة تضمن سلامة العمليات التجارية الإلكترونية، وتضفي عليها الطابع الرسمي والقانوني[2].

ومن ثمّ، فإن التوقيع الإلكتروني يشكل ركيزة أساسية لإتمام مختلف المعاملات الإلكترونية، سواء تعلّق الأمر بعقود البيع، أو التصدير والاستيراد، أو المعاملات البنكية، أو حجز تذاكر السفر والفنادق، وغير ذلك من التصرفات القانونية التي تتم عبر الوسائط الإلكترونية، والتي تستند إلى محررات إلكترونية موقعة توقيعاً إلكترونياً، مما يحقق فاعلية أكبر في تبادل البيانات والمعلومات بين المواطن والمؤسسات، ويوفر في الوقت ذاته الكثير من التكاليف المرتبطة بالورق والطباعة والطلبات اليدوية[3].

الفرع الثاني:

وظائف التوقيع الإلكتروني

يؤدي التوقيع، سواء كان تقليديًا أو إلكترونيًا، دورًا جوهريًا في النظام القانوني، إذ يُعد وسيلة لإثبات صدور المحرر عن شخص معين، وتعبيرًا عن إرادته بالالتزام بمضمونه. وإذا كان التوقيع الخطي التقليدي يضطلع بوظائف أساسية، لا سيما في تحديد هوية الموقع والتعبير عن رضاه بمحتوى المحرر، فإن التوقيع الإلكتروني، بخصائصه التقنية، أضاف إلى تلك الوظائف وظيفة جديدة بالغة الأهمية، تتمثل في ضمان

[1]–مليسا حمود، الحجية القانونية للعقد الإلكتروني في التشريع الجزائري، مجلة العلوم الإنسانية، مجلّد 32 ، جامعة الاخوة منتوري ، قسنطينة ، الجزائر ، 2021، ص 499.

[2]–الربيع سعدي، حجية التوقيع الإلكتروني في التشريع الجزائري ، أطروحة ماجستير في القانون الخاص، جامعة باتنة، 2017، ص52.

[3]–مليسا حمود، المرجع السابق ، ص 499.

سلامة المحرر الإلكتروني من أي تعديل أو تلاعب بعد التوقيع، ما يعزز الثقة في التعاملات الرقمية ويؤمن الأطراف من المخاطر المرتبطة بها.

وفي ضوء ذلك، يمكن حصر الوظائف الرئيسة للتوقيع الإلكتروني في ثلاث وظائف أساسية، وهي:

1 –تحديد هوية الشخص الذي صدر عنه التوقيع الإلكتروني: تُعد وظيفة تحديد هوية الموقع من أبرز الوظائف التي يؤديها التوقيع الإلكتروني، تمامًا كما هو الحال في التوقيع التقليدي. إذ لا يمكن الاعتداد بالتوقيع الإلكتروني قانونًا إلا إذا أمكن إسناده إلى شخص معين على نحو لا يترك مجالًا للشك في هوية صاحبه. فالتوقيع الإلكتروني الذي لا يُمكِّن من تحديد هوية الموقع بدقة، لا يُعتد به ولا يُرتب أثرًا في الإثبات[1].

ولتحقيق هذه الوظيفة، يعتمد التوقيع الإلكتروني على تقنيات معلوماتية متقدمة، كالمفاتيح السرية والخاصة، مما يجعله أكثر أمانًا من التوقيع التقليدي، الذي يمكن تقليده أو تزويره بسهولة نسبية. فبفضل الخوارزميات المعقدة التي تحكم إنشاء التوقيع الإلكتروني، يكون من شبه المستحيل انتحال هوية الموقع أو استخدام توقيعه من طرف آخر، دون تفويض أو سلطة.

2 –التعبير عن إرادة الموقع: من المبادئ المستقرة في الفقه والقضاء أن التوقيع – سواء كان تقليديًا أو إلكترونيًا – يُعد دلالة قانونية على انصراف إرادة الموقع إلى الالتزام بمضمون المحرر. فالتوقيع على محرر، ورقيًا كان أو إلكترونيًا، يُشكّل قرينة قانونية على أن الشخص الذي وقّع عليه قد قرأ محتواه، ووافق على ما ورد فيه من التزامات، ما لم يثبت العكس صراحة[2].

وبالرجوع إلى قواعد الإثبات، لا يُمكن لمن نُسب إليه توقيع في محرر قانوني أن ينكر مضمونه، ما لم يُنكر صراحة الخط أو الإمضاء أو الختم أو البصمة المنسوبة إليه. وينسحب هذا الحكم على المحررات

[1]–فيصل سعد الغريب ، التوقيع الالكتروني وحجيته في الاثبات ، المنظمة العربية للتنمية الإدارية ، بحوث ودراسات، لبنان، 2005،ص98.

[2]–نور خالد عبد المحسن عبد الرزاق، حجية المحررات والتوقيع الالكتروني في الاثبات عبر شبكة الانترنت ، رسالة دكتوراه في الحقوق، جامعة عين شمس ، مصر، 2009، ص61.

الإلكترونية، إذ يُعد التوقيع الإلكتروني قرينة على رضا الموقع والتزامه، ما لم يطعن صراحة في صحة التوقيع أو نسبته إليه[1].

3 -الحفاظ على سلامة مضمون المحرر الإلكتروني: يتميّز التوقيع الإلكتروني، لا سيما التوقيع الرقمي القائم على تقنيات التشفير غير المتماثل، بقدرته الفائقة على ضمان سلامة المحرر الإلكتروني ومنع التعديل عليه بعد التوقيع. وتتحقق هذه الوظيفة التقنية من خلال إنشاء ما يُعرف بـ"البصمة الإلكترونية" للمحرر، والتي تُنتَج بواسطة خوارزميات رياضية تُعرف بـ"دوال التمويه" أو "اقترانات التجزئة."

تُعد هذه البصمة الإلكترونية نسخة مشفّرة ومضغوطة من محتوى المحرر، لا يمكن قراءتها أو فهمها إلا باستخدام المفتاح المناسب الذي يتطابق مع المفتاح المستخدم عند إنشاء التوقيع. وبهذا الشكل، تضمن هذه التقنية عدم وقوع أي تعديل على المحرر بعد التوقيع، وفي حال حدوث أي تغيير، يُصبح التوقيع الإلكتروني غير صالح، مما يوفر دليلًا قاطعًا على التلاعب بالمحتوى. وعليه، فإن وظيفة سلامة المحرر الإلكتروني تُعد من أهم الضمانات التي يُوفرها التوقيع الإلكتروني، وتُؤسّس لثقة قانونية وتقنية في البيئة الرقمية، وتُحقق الحماية الضرورية للمتعاملين عبر الوسائط الإلكترونية[2].

المطلب الثاني :

شروط صحة التوقيع الالكتروني

في مستهل الأمر، تجدر الإشارة إلى أن المشرّع الجزائري قد حدّد شروط التوقيع الإلكتروني المضمون (المؤمَّن) بموجب المرسوم التنفيذي رقم 07-162، حيث نصّت المادة 3 مكرر منه على ثلاثة شروط أساسية يجب توافرها، وهي على النحو الآتي:

- **الشرط الأول:** أن يكون التوقيع الإلكتروني خاصًا بالشخص الموقع، أي مرتبطًا به على نحو لا يُمكن فصله عنه.
- **الشرط الثاني:** أن يتم إنشاء التوقيع باستخدام وسائل يُمكن لصاحب التوقيع الاحتفاظ بها تحت سيطرته الحصرية، بما يضمن سرية المعطيات وسلامتها.

[1]-أبو غرابي غازي، فياض القضاة، حجية التوقيع الإلكتروني ، دراسة في التشريع الاردني، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 20، العدد 1، سوريا، 2004، ص175.

[2]- Eric. A. CAPRIOLI sécurité et confiance dans le commerce électronique, sécurité numérique et autorité de certification, J.C.P Ed G 1998, P58.

- **الشرط الثالث:** أن يكون التوقيع مرتبطًا بالفعل أو التصرف القانوني المراد توثيقه، ارتباطًا يتيح الكشف عن أي تعديل لاحق قد يطرأ عليه.

وفي المقابل، نصّ القانون رقم 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين على شروط إضافية يُشترط توافرها حتى يُمنح التوقيع الإلكتروني صفة "الموثوقية"، حيث استعمل المشرّع في هذا السياق مصطلح "التوقيع الإلكتروني الموصوف" بدلًا من مصطلح "المؤمن"، وذلك بموجب المادة 7 من القانون المذكور، التي حدّدت الشروط القانونية الواجب توفرها في التوقيع حتى يُعتد به كوسيلة موثوقة لإثبات التصرفات والمعاملات الإلكترونية. أما التوقيع الإلكتروني الموصوف هو التوقيع الإلكتروني الذي تتوفر فيه المتطلبات الآتية[1]:

- أن ينشأ على أساس شهادة تصديق الكتروني موصوفة.
- أن يرتبط بالموقع دون سواه.
- أن يمكن من تحديد هوية الموقع.
- أن يكون مصمما بواسطة آلية مؤمنة خاصة بإنشاء التوقيع الإلكتروني.
- أن يكون منشأ بواسطة وسائل تكون تحت التحكم الحصري للموقع.
- أن يكون مرتبطا بالبيانات الخاصة به، بحيث يمكن الكشف عن التغييرات اللاحقة بهذه البيانات. من خلال هاتين المادتين اللتين تعرض فيهما المشرع الجزائري لجملة من الشروط، ارتأينا أن نقسمهما إلى شروط شكلية وأخرى موضوعية سنتناولها في المطلبين التاليين:[2]

الفرع الاول :

الشروط الشكلية

سنتناول في هذا الموضع شرطًا شكليًا لا يقل أهمية عن باقي الشروط الموضوعية المتعلقة بالتوقيع الإلكتروني، بل يُعد من بين الشروط الجوهرية والأساسية لقيامه، ويتمثل في شهادة التصديق الإلكتروني، التي يُنظر إليها، في كثير من الفقه، على أنها بطاقة هوية إلكترونية لما تضطلع به من دور محوري في التحقق من هوية صاحب التوقيع الإلكتروني ونسبته إليه على وجه اليقين.

[1]-القانون رقم 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين، المرجع السابق.

[2]-بلحاج بلخير، مداخلة بعنوان حجية التوقيع الإلكتروني في الإثبات الملتقى الوطني حول الإطار القانوني للتوقيع والتصديق الإلكتروني في الجزائر 2016، ص2

ولا يقتصر دور شهادة التصديق الإلكتروني على تأكيد الهوية، بل يتعداه إلى ضمان سلامة التوقيع الإلكتروني ذاته، وبالتالي سلامة بيانات المحرر الإلكتروني وعدم تعرّضها للتغيير أو العبث، وهو ما يُعزز عنصري الثقة والأمان في المعاملات الإلكترونية الجارية عبر شبكة الإنترنت.

ومما لا شك فيه، أن توافر الثقة والأمان يُعد من أهم الضمانات التي يجب أن تتسم بها التصرفات والمعاملات الإلكترونية، ما استدعى ضرورة تدخل طرف ثالث محايد وموثوق، يُسند إليه اختصاص إصدار شهادات التصديق، وحماية المعلومات المضمّنة فيها والتأكد من صحتها.

وفي هذا الإطار، برزت آلية جهات التصديق والتوثيق الإلكتروني، بوصفها من أبرز الأدوات التقنية والقانونية المعتمدة في هذا المجال، حيث تتولى هذه الجهات، وفقًا لما يُسند إليها من صلاحيات قانونية، مهام إصدار شهادات المصادقة، وتأكيد الهوية الرقمية، وضمان أمن وسلامة المعاملات الإلكترونية من خلال منظومة موثوقة للتوقيع الرقمي. خلق بيئة الكترونية آمنة للتعامل عبر الأنترنت

-جهات التصديق الإلكتروني

تعتبر عملية التصديق الإلكتروني من أهم الضمانات القانونية الفعالة في تحقيق الثقة والائتمان بين المتعاملين بمجال التبادلات التجارية الإلكترونية، وذلك نظرا لمخلف الإشكالات التي تثيرها البيئة الرقمية من صعوبة التأكد من صحة التوقيع الإلكتروني، لذلك كان من الضروري أن توكل مثل هذه المهمة إلى طرف ثالث محايد عن المتعاقدين يطلق عليه مؤدي خدمات التصديق، الذي يعمل على التحقق من انتساب التوقيعات الإلكترونية إلى أصحابها، إلى جانب تنظيم إطار قانوني يحدد مسؤولية هذا الطرف المحايد في حالة حدوث أي إخلال، وذلك من باب تعزيز الثقة في نفوس المتعاملين بالتوقيعات الإلكترونية لتوثيق مختلف معاملاتهم عبر شبكة الاتصالات الإلكترونية ...

-السلطة الوطنية للتصديق الإلكتروني نصّ المشرّع الجزائري في المادة 16 من القانون رقم 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين، على إنشاء السلطة الوطنية للتصديق الإلكتروني، باعتبارها هيئة إدارية رئيسية، تتمتع بالشخصية المعنوية والاستقلال المالي، وتخضع لوصاية الوزير الأول. وقد أُشير إليها في صلب النص التشريعي تحت تسمية "السلطة".

وبموجب المادة 2 من المرسوم التنفيذي رقم 07-162، تم تحديد مقر السلطة الوطنية للتصديق الإلكتروني بمدينة الجزائر، مع إمكانية نقله إلى أي موقع آخر داخل التراب الوطني، وفق ما تقتضيه ضرورات التنظيم أو متطلبات المصلحة العامة في المرسوم رقم 16-134[1]

[1]-مرسوم تنفيذي رقم 16-134 مؤرخ في 17 رجب 1437 الموافق ل 25 أفريل 2016 ، يحدد تنظيم المصالح التقنية والإدارية للسلطة الوطنية للتصديق الإلكتروني وسيرها ومهامها، ج ر ع 26 صادرة بتاريخ 28 أفريل 2016

تكلف السلطة الوطنية بترقية استعمال التوقيع والتصديق الإلكترونيين وتطويرهما وضمان موثوقية استعمالهما، وتتولى هذه السلطة جملة من المهام بمقتضى المادة 18 من القانون 15-04[1]

نصّ المشرّع الجزائري في المادة 16 من القانون رقم 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين على إنشاء السلطة الوطنية للتصديق الإلكتروني، بصفتها هيئة إدارية عليا، تتمتع بالشخصية المعنوية والاستقلال المالي، وتخضع لوصاية الوزير الأول، ويُشار إليها في النص التشريعي بمصطلح "السلطة".

وبموجب المادة 2 من المرسوم التنفيذي رقم 07-162، تم تعيين مدينة الجزائر كمقر رسمي للسلطة الوطنية للتصديق الإلكتروني، مع جواز نقل مقرها إلى أي جهة أخرى داخل الإقليم الوطني، حسب ما تقتضيه متطلبات المصلحة العامة أو ضرورات التنظيم الإداري..[2]

-السلطة الحكومية للتصديق الإلكتروني

نص المشرع الجزائري في القانون رقم 15-04 في المادة 26 منه على أنه: تنشأ لدى الوزير المكلف بالبريد وتكنولوجيا الإعلام والاتصال سلطة حكومية للتصديق الإلكتروني تتمتع بالاستقلال المالي والشخصية المعنوية

كلّف المشرع الجزائري، بموجب المادة 28 من القانون رقم 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين، السلطة الحكومية المختصة بمهام متابعة ومراقبة نشاط التصديق الإلكتروني الممارس من قبل الأطراف الثالثة الموثوقة، لفائدة المتدخلين في القطاع الحكومي.

وقد حددت هذه المادة جملة من المهام الرقابية والتنظيمية المسندة إلى هذه السلطة، والتي تهدف إلى ضمان التزام الجهات المعنية بالمعايير القانونية والتقنية المعتمدة، بما يكرّس موثوقية عمليات التصديق الإلكتروني داخل الأطر الإدارية والحكومية.[3].

-السلطة الاقتصادية للتصديق الإلكتروني

نصّت المادة 29 من القانون رقم 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين على أن السلطة المكلفة بضبط البريد والمواصلات السلكية واللاسلكية تُعد السلطة الاقتصادية المختصة في مجال التوقيع الإلكتروني.

وبموجب المادة 30 من نفس القانون، أوكلت إلى هذه السلطة مهمة رئيسية تتمثل في متابعة ومراقبة مقدمي خدمات التصديق الإلكتروني الذين يُوفرون خدمات التوقيع والتصديق الإلكتروني لفائدة الجمهور.

[1]-أنظر المادة 18 من القانون رقم 15-04

[2]-أنظر المادتين 19 و 23 من القانون 15-04

[3]-أنظر المادة 28 من نفس القانون

وتمارس هذه السلطة مهامها من خلال جملة من الصلاحيات والوظائف الرقابية والتنظيمية المنصوص عليها قانونًا.

كما تلتزم السلطة الاقتصادية للتصديق الإلكتروني، في إطار قيامها بمهامها، بإبلاغ النيابة العامة بكل فعل يكتسي طابعًا جزائيًا يتم اكتشافه أثناء ممارسة اختصاصاتها، وذلك تعزيزًا لحماية المعاملات الإلكترونية وضمانًا لسلامتها القانونية.[1].

أما فيما يتعلق بالقرارات الصادرة عن السلطة الاقتصادية للتصديق الإلكتروني، فإنها تكون قابلة للطعن فيها أمام السلطة ذاتها خلال أجل أقصاه شهر واحد من تاريخ تبليغ القرار.

كما يجوز الطعن في هذه القرارات أمام مجلس الدولة، وذلك في نفس الأجل، أي خلال شهر واحد من تاريخ التبليغ. ويُضاف إلى ذلك أن هذا الطعن لا يترتب عليه أثر موقف، ما لم يُنص على خلاف ذلك صراحة بموجب قرار قضائي.[2]

-دور مؤدي خدمات التصديق الإلكتروني

إن الغاية الرئيسية من إنشاء جهة مختصة بالتصديق على التوقيع الإلكتروني هو إصدار شهادات التصديق الإلكتروني وتحقق المرسل إليه من هوية المرسل، وحتى تؤدي هذه الجهة الأهداف المرجوة منها فإنه يقع على عاتقها عدة مهام نذكر منها:

-تزويد المتعاقدين بشهادة تصديق الكترونية

من أهم الصلاحيات التي تتمتع بها جهات التصديق الإلكتروني، والتي أُنشئت من أجلها أساسًا، هي تزويد المتعاملين في مجال المعاملات الإلكترونية والتعاقد عن بُعد عبر شبكة الإنترنت بشهادات التصديق الإلكتروني. فهذه الشهادات تُعد أداة لتأكيد هوية صاحب الرسالة الإلكترونية (الموقّع)، وذلك بالاستناد إلى إجراءات تصديق معتمدة تُبيّن تاريخ التوقيع، وطبيعة عمل صاحبه، والتراخيص المخوّلة له، ومدى صلاحية توقيعه.

ويكمن الغرض الرئيسي من لجوء الأفراد إلى هذه الجهات في تعزيز الثقة، والأمان، والسرية في مراسلاتهم وتوقيعاتهم الإلكترونية، مما يشجع الغير على إبرام العقود معهم بعد التأكد من هويتهم وجدية إرادتهم في التعاقد.[3].

---

[1]-أنظر المادة 30 من القانون رقم 15-04

[2]-أنظر المادتين 31 و 32 من القانون رقم 15-04

[3]-كريمة زايدي، النظام القانوني لجهات التصديق الإلكتروني، مذكرة تكميلية لنيل شهادة الماستر، تخصص قانون أعمال كلية الحقوق والعلوم السياسية، جامعة العربي بن مهيدي، أم البواقي، 2015/2016، ص 20

نصّ المشرع الجزائري في المادة 41 من القانون رقم 15-04 على أن مقدم خدمات التصديق الإلكتروني يُكلف بمهام تسجيل وإصدار وتسليم شهادات التصديق الإلكتروني. كما أوجبت الفقرة الثانية من المادة 44 من نفس القانون على مقدم خدمات التصديق الإلكتروني منح شهادة التصديق لكل شخص يتقدم بطلبها، ما دامت مستوفية للشروط القانونية.

وبالتالي، فإن عبء إصدار شهادة التصديق الإلكتروني يقع على عاتق الجهة المقدمة للخدمة، وذلك وفقًا للشروط المنصوص عليها قانونًا والمتفق عليها مع الشخص المعني، وفي الآجال المحددة لتاريخ تقديم الطلب.[1].

-التحقق من هوية المتعاقد

يتمثل الالتزام الرئيسي لجهات التصديق الإلكتروني في قيامها بالتحقق من هوية شخص الموقع حيث تقوم بإصدار شهادة تصديق الكتروني تفيد التصديق على التوقيع الإلكتروني في صفقة معينة تشهد بموجبها بصحته ونسبته إلى من صدر عنه، فإذا قام أحد الأطراف بوضع توقيعه الإلكتروني على رسالة البيانات الإلكترونية وضمنت جهة محايدة صحتها، فإن ذلك يؤكد على صدور التوقيع من صاحبه[2].

تنص الفقرة الثانية من المادة 44 من القانون الجزائري رقم 15-04 على أن مقدم خدمات التصديق الإلكتروني ملزم بمنح شهادة أو أكثر لكل شخص يتقدم بطلب بذلك، وذلك بعد التحقق من هويته، وكذا التحقق من صفاته الخاصة عند الاقتضاء. كما يُلزم القانون مقدم الخدمة بإنشاء سجل يُدوّن فيه هوية وصفة الممثل القانوني للشخص المعنوي الذي يستعمل التوقيع الإلكتروني المرتبط بشهادة التصديق الإلكتروني المعنية، بما يتيح إمكانية تحديد هوية الشخص الطبيعي في كل مرة يتم فيها استخدام ذلك التوقيع الإلكتروني.[3].

-إصدار المفاتيح الإلكترونية

في إطار تعزيز الثقة وتأمين المبادلات في مجال التجارة الإلكترونية عبر شبكة الإنترنت، تم اعتماد مجموعة من الأساليب والتقنيات تهدف إلى حماية محتوى الرسائل الإلكترونية. وتتمثل هذه الأساليب في تحويل النص المرفق بالرسالة إلى رموز أو إشارات أو أرقام غير قابلة للقراءة أو الفهم من طرف الغير، إلا بعد إعادتها إلى صيغتها الأصلية من خلال عملية فك التشفير.

---

[1]-زهيرة كيسي النظام القانوني لجهات التوثيق (التصديق) الإلكتروني، مجلة دفاتر السياسة والقانون، المركز الجامعي بتمنراست، الجزائر، العدد السابع، جوان 2012، ص 216

[2]-إيمان مأمون أحمد سليمان إبرام العقد الإلكتروني وإثباته الجوانب القانونية لعقد التجارة الإلكترونية)، دار الجامعة الجديدة للنشر الإسكندرية، مصر، 2008، ص 314

[3]-كريمة زايدي، مرجع سابق، ص 21.

ولا يمكن فك هذا التشفير إلا باستعمال مفاتيح خاصة بذلك، إما المفتاح الخاص الذي يُستخدم في تشفير المعاملة الإلكترونية ويكون حصرًا بيد صاحب التوقيع، أو المفتاح العام الذي يُستعمل لفك هذا التشفير.

وتعتمد هذه المفاتيح على معايير محددة لتشفير البيانات، بما يضمن سريتها، ويحول دون كشف محتواها أو الاطلاع عليها من قبل أطراف غير مخوّلة..[1]

-تحديد وقت إبرام العقد الإلكتروني:

تحديد وقت إبرام العقد ليس شرطا ضروريا لصحة العقد، لكن يعتبر بداية لتنفيذ ما ترتب على العقد من آثار، وعلى ذلك إذا نظرنا إلى التاريخ المدون بالرسالة الإلكترونية فنجده لا يقدم أي ضمان إذ بإمكان المستخدم أن يغير الزمن المدون بحاسوبه، بل المشكلة تزداد تعقيدا في تحديد زمان انعقاد العقد عند تعدد أطرافه المتواجدين في أكثر من دولة، لأن مختلف الحواسيب التي ستقوم بالاتصال ستحلي أزمنة مختلفة[2]، لذا فإن زمن تحديد إبرام العقد يتعين أن يتم من خلال جهات التصديق والتي تعمل على تحديد تاريخ واحد لإبرام العقد الإلكتروني.

-التزام جهات التوثيق الإلكتروني بالسرية

يُعد الالتزام بالحفاظ على السرية من أخطر وأهم الالتزامات التي تقع على عاتق جهات التصديق الإلكتروني، إذ يمثل أحد أبرز الواجبات التي قد تُرتب مسؤوليتها تجاه صاحب الشهادة الإلكترونية، سواء من حيث المسؤولية المدنية أو الجزائية.

ويكتسي هذا الالتزام أهمية بالغة في تعزيز الثقة بين الأطراف المتعاملة بالوسائط الإلكترونية، لاسيما أن معظم هذه المعاملات تتم بين أشخاص لا تجمعهم معرفة سابقة ولا لقاء مباشر، مما يجعل من ضمانات السرية شرطًا جوهريًا لإقدام الأفراد على إبرام العقود وإتمام الصفقات عبر الإنترنت.

ويقصد بالسرية، في هذا السياق، وجوب حماية البيانات ذات الطابع الشخصي التي يقدمها صاحب الطلب إلى الجهة المختصة بإصدار شهادة التصديق الإلكتروني. وبالتالي، فإن التزام مقدم خدمة التصديق باحترام خصوصية هذه البيانات يضفي على العملية مزيدًا من الحماية والثقة، ويضمن أمن التعاملات الإلكترونية.[3].

حيث ألزم المشرع الجزائري مؤدي خدمات التصديق الإلكتروني بالحفاظ على سرية البيانات والمعلومات المتعلقة بشهادة التصديق الإلكتروني الممنوحة، وذلك من خلال المادة 42 من القانون 15- 04.

-إثبات مضمون التبادل الإلكتروني

---

[1]-ليندة بلحارث، مرجع سابق، ص 865

[2]-إيمان مأمون أحمد سليمان، مرجع سابق، ص 316.

[3]-إلياس ناصيف العقد الإلكتروني في القانون المقارن، الطبعة الأولى منشورات الحلبي الحقوقية، لبنان، 2009 ، ص282

يؤدي مزودو خدمات التصديق الإلكتروني إثبات مضمون التعاقد الإلكتروني بين أطرافه وضمان سلامته وجديته وأن لا للاحتيال والغش فيه، وذلك بواسطة تتبع مختلف المواقع التجارية للتحقق من وجودها الفعلي ومدى مصداقيتها، وفي حالة ما إذا تبينوا أنها غير حقيقية قاموا بتوجيه إنذار للمتعامل وأكثر من ذلك فإنه يمكنه طلب المساعدة من خدمات التصديق الإلكتروني للتحقق والتأكد من أمر الشركة التي سيتم التعاقد معها[1]...

-ضرورة الحصول على ترخيص من الجهة المختصة قبل ممارسة عملها:

في الواقع، لا يجوز لهيئات التصديق الإلكتروني ممارسة نشاطها إلا بناءً على ترخيص مسبق تصدره السلطة المختصة في الدولة لهذا الكيان القانوني. وبالرجوع إلى التشريع الجزائري، يتبيّن أنه قبل صدور القانون رقم 15-04، كانت سلطة ضبط البريد والمواصلات السلكية واللاسلكية هي الجهة المخولة بمنح الترخيص لمزاولة خدمات التصديق الإلكتروني، وذلك تطبيقًا لأحكام المادة 2 من المرسوم التنفيذي رقم 07-162 المذكور سابقًا.[2].

وفقًا للمادة 33 من القانون رقم 15-04، فإن مزاولة نشاط تقديم خدمات التصديق الإلكتروني مشروط بالحصول على ترخيص مسبق تصدره السلطة الاقتصادية للتصديق الإلكتروني، وذلك بعد استيفاء طالب الترخيص لجملة من الشروط القانونية المحددة. ويُمنح هذا الترخيص لمدة سنة واحدة قابلة للتجديد مرة واحدة فقط.

وبعد منح الترخيص، تخضع الجهة المصرح لها لنوع من الرقابة تمارسها السلطة المختصة، وهو ما يُسهم في ترسيخ الثقة وتعزيز الأمان لدى المستفيدين من خدمات التصديق الإلكتروني.

ورغم أن نشاط التصديق الإلكتروني يُعد من الأنشطة ذات الطابع التجاري، إلا أنه لا يُمارس في إطار مبدأ حرية التجارة بصورة مطلقة، بل يبقى خاضعًا لضوابط تنظيمية صارمة تفرضها خصوصيته وحساسيته..[3]

الفرع الثاني :

الشروط الموضوعية

التوقيع الإلكتروني يتوفر على شروط يعتد بها في البيئة القانونية ويعطي الثقة بين الأفراد في تعاملاتهم، ويتمتع بحجية قانونية في إثبات تلك التصرفات القانونية تحديدا في مجال التجارة الإلكترونية فقد اعترفت

---

[1]-ليندة بلحارث، مرجع سابق، ص 865

[2]-رحمان يوسف، سلطات التصديق الإلكتروني في التشريع الجزائري طبقا للقانون 15-04 دراسة مقارنة، مجلة الدراسات القانونية والسياسية، جامعة تلمسان، الجزائر، ص 174

[3]-رضوان قرواش، مرجع سابق، ص 417.

مختلف التشريعات المتعلقة بالمعاملات الإلكترونية بحجية التوقيع الإلكتروني، إلا أنه استلزمت في التوقيع الإلكتروني حتى يتمتع بهذه الحجية ويقوم بخدمته في الإثبات ينبغي أن تتوفر فيه مجموعة من الشروط الموضوعية التي تجعل منه توقيعا موثوقا به ومحميا، والمتمثلة في:

- **أن يرتبط بالموقع دون سواه:**

نظرًا لخصوصية البيئة الافتراضية التي تتم فيها المعاملات الإلكترونية، حيث يغيب الحضور المادي للأطراف، ولا يمكن التعرف على هوية الشخص الموقع بطريقة تقليدية عبر حضوره الفعلي وتوقيعه الخطي، فقد أصبح الارتباط بين التوقيع الإلكتروني وصاحبه مسألة تقنية بحتة، تتطلب استخدام وسائل تكنولوجية متقدمة تضمن تأمين عملية التوقيع والتحقق من هوية الموقع.

ويُقصد بهذا الشرط أن يُبيَّن على وجه الدقة هوية الموقع من خلال توقيعه الإلكتروني، وأن تكون وسيلة إنشاء هذا التوقيع تحت السيطرة الحصرية للموقع دون غيره، بما يعني أن بيانات إنشاء التوقيع الإلكتروني تكون خاصة ومميزة له، ولا يمكن إصدار توقيع مطابق لشخص آخر، حفاظًا على طابعه الشخصي والفردي.

وتأكيدًا على هذا المعنى، نصت الفقرة الثانية من المادة 2 من القانون رقم 15-04 على أن الموقع هو "كل شخص طبيعي يحوز بيانات إنشاء التوقيع الإلكتروني ويتصرف بها لحسابه الخاص، أو لحساب شخص طبيعي أو معنوي يمثله، ويترتب على توفر هذا الشرط في التوقيع الإلكتروني أن يُعتبر وسيلة لإظهار نية الموقع في الالتزام بمضمون الوثيقة الموقع عليها، كما يُعد قرينة على قبوله لمحتواها. ويشترط كذلك أن يكون التوقيع مميزًا وخاصًا بصاحبه بحيث يُتيح التحقق من هويته بشكل يقيني، ويمنع أي التباس أو خلط مع توقيع شخص آخر[1].

تُعد إمكانية تحديد هوية الموقع من العناصر الأساسية في مجال المعاملات الإلكترونية، لما لها من أهمية في تحديد هوية الطرف المُبرِم للعقد، وبالتالي ضمان الوفاء بالالتزامات العقدية المترتبة عليه. غير أنه لا يكفي التحقق من الهوية فحسب، بل يجب كذلك التأكد من أهلية الشخص الذي يصدر عنه التوقيع الإلكتروني، إذ لا يجوز منح توقيع إلكتروني لشخص عديم الأهلية.

وعليه، يُشترط في الشخص الذي يُقدم على استخدام التوقيع الإلكتروني أن يكون كامل الأهلية القانونية، باعتبار أن هذا التصرف يُرتب التزامات قانونية قد تكون جسيمة، ولا يُمكن ترتيبها على شخص

[1]-رضوان قرواش، مرجع سابق، ص 417.

يفتقر إلى الأهلية اللازمة. ولهذا، تتولى جهة إصدار التوقيع الإلكتروني التحقق من أهلية طالب التوقيع قبل منحه الشهادة الإلكترونية.

ويُضرب مثال على ذلك باستخدام الرقم السري لبطاقة الصراف الآلي، حيث يُدخل حامل البطاقة رقمه السري، وتقوم الأجهزة بالتعرف عليه والتحقق من صحة البيانات المدخلة، مما يُعد قرينة على هوية الشخص واستعماله المشروع للبطاقة، وهي إجراءات تُشكّل في مجملها عملية مصادقة إلكترونية تُضفي المصداقية على التوقيع الإلكتروني.

وقد أكد المشرع الجزائري هذا المبدأ في الفقرة الأولى من المادة 323 من القانون المدني، حيث أشار إلى أهمية الأهلية في صحة الالتزامات القانونية، مما ينطبق أيضًا على استخدام التوقيع الإلكتروني كوسيلة لإثبات الإرادة والالتزام على أنه شرط إمكانية التأكد من هوية الموقع التي أصدرها، وكنا المادة 03 مكرر من المرسوم 07/162 التي نقضي بأن التوقيع الإلكتروني يفي بالمتطلبات الآتية:

- يكون خاص بالموقع، ويتم إشارة بوسائل يمكن أن يحاط بها الموقع تحت مراقبته الحصرية يضمن مع الفعل المربط به صلة بحيث يكون كل تعديل لاحق تعمل للكشف عنه.
- نجد أنه يشترط في التوقيع الإلكتروني أن يكون قادرا على تحديد هوية الشخص الموقع وتمييزه عن غيره، وهذا الشرط يحققه التوقيع الإلكتروني لأنه يتميز بقدرة تقنية تعتمد على أرقام سرية خاصة لا يعرفها الا الموقع الذي اختارها لينال بها على هويته ويعبر بواسطتها عن رضاء بمضمون المحرر الإلكتروني. [1]
- تتمثل الغاية الأساسية من التوقيع الإلكتروني في تحقيق ذات الوظيفة القانونية للتوقيع التقليدي، وهي تحديد هوية الموقع، وتأكيد نسبة الوثيقة إليه، وتحميله المسؤولية القانونية عن مضمونها. وقد أقر المشرع بإمكانية الاعتماد على التوقيع الإلكتروني كوسيلة إثبات، شريطة أن يُمكن من التعرف على هوية الموقع والتحقق من نسبة التوقيع إليه، بما لا يترك مجالاً للشك في صلة التوقيع بصاحبه.
- ويُثار إشكال في حالة ما إذا تم التوقيع نيابةً عن شخص آخر، كما في حالة الولي أو الوصي أو الوكيل أو الممثل القانوني لشخص معنوي، حيث يشترط في هذه الحالات أن يُوقّع الشخص المفوض باسمه الشخصي، مع بيان صفته ومصدر سلطته في التوقيع، فلا يجوز له التوقيع باسم القاصر أو الموكل أو الشخص المعنوي بطريقة توحي بأنه هو صاحب التوقيع الأصلي، إلا إذا تم ذلك برضى مسبق وبشكل صريح، وباستخدام وسائل توثيق معتمدة، كأن يكون التوقيع مصممًا بواسطة آلية آمنة ومخصصة لإنشاء التوقيع الإلكتروني.

[1]–ليندة بلحارث، مرجع سابق، ص 865

- ويُتيح التوقيع الإلكتروني العديد من الوسائل التقنية التي تمكّن الشخص من توقيع الوثيقة إلكترونيًا، بما يُثبت التزامه بمضمونها. وقد يتجسد ذلك في تثبيت صورة موقعة رقميًا محفوظة إلكترونيًا، أو بطباعة اسم المرسل في نهاية الرسائل الإلكترونية، أو باستخدام رمز سري أو شفرة شخصية، كما هو الحال في أوامر الدفع ببطاقات الائتمان أو الصراف الآلي.
- وقد حرص المشرع الجزائري على ضمان صحة التوقيع الإلكتروني وسلامته، حتى يُنتج آثاره القانونية شأنه في ذلك شأن التوقيع التقليدي، وذلك من خلال وضع معايير دقيقة لإنشاء التوقيع الإلكتروني، تضمن أمنه وسلامته وتؤكد ارتباط بياناته بالشخص المعني. كما يُعتد قانونًا بكل علامة إلكترونية ترتبط ارتباطًا وثيقًا بالموقع وتدل على هويته، ما دام التوقيع قد أُنشئ بوسائل موثوقة، ولصاحب التوقيع حرية اختيار الوسيلة التي تعكس هويته بشكل واضح لا لبس فيه.[1].
- فقد نصت المادة 03 مكرر فقرة 4 من المرسوم 07-162 على المعطيات التي تستجيب لإنشائه حيث عرفها بأنها : العناصر الخاصة بالموقع مثل الأساليب التقنية التي يستخدمها الموقع نفسه لإنشاء التوقيع ، فالقانون 15/04 قد فصل في آلية إنشاء التوقيع الإلكتروني وذلك من خلال تعريفه لكل من آلية وبيانات إنشاء التوقيع الإلكتروني في المادة 02 منه على أنها : بيانات فريدة مثل الرموز أو مفاتيح التشفير الخاصة التي يستعملها الموقع لإنشاء التوقيع، وكذلك عرفت الفقرة 4 من المادة نفسها آلية إنشاء التوقيع الإلكتروني بكونها : " جهاز أو برنامج معلوماتي معد لتطبيق بيانات إنشاء التوقيع الإلكتروني[2].
- فأقر القانون 15/04 فصلا كاملا للتفصيل في إجراءات إنشاء التوقيع الإلكتروني وآليات ووسائل التحقق منه وحدد من خلاله متطلبات إنشاء هذا التوقيع بصفة مؤمنة، ومن بعد تحديد متطلبات آلية موثوقة وذلك للتحقق من التوقيع الإلكتروني، فحجية التوقيع الإلكتروني مرتبطة بالطريقة المعتمدة لإثباته؛ أي متطلبات لآلية الإنشاء ومتطلبات لآلية التحقق.

-متطلبات آلية إنشاء التوقيع الإلكتروني

يقصد باليات إنشاء التوقيع الإشارة إلى المفتاح السري أو الرموز أو العناصر الأخرى التي تستعمل في عملية إنشاء التوقيع الإلكتروني لتوفير صلة مأمونة بين التوقيع الإلكتروني الناتج والشخص الموقع[3].

---

[1]-أبو عرابي غازي القضاة فياض، حجية التوقيع الإلكتروني (دراسة في التشريع الأردني)، مجلة جامعة دمشق للعلوم الإقتصادية والقانونية، المجلد 20 ، العدد الأول، ص 166.

[2]-خالد ممدوح إبراهيم، مرجع سابق، ص 46.

[3]-إبراهيم سيد أحمد، قانون التجارة الإلكتروني والتوقيع الإلكتروني وقانون الملكية الفكرية والأدبية، دون طبعة، الدار. 322 الجامعية، مصر، 2005، ص

فأكدت المادة 10 من القانون 15-04 لسنة 2015 على ضرورة أن تكون آلية إنشاء التوقيع الإلكتروني مؤمنة بنصها: يجب أن تكون آلية إنشاء التوقيع الإلكتروني الموصوفة مؤمنة، حيث وضع المشرع الجزائري مجموعة من المتطلبات التي تضمن لآلية إنشاء التوقيع الإلكتروني أن تكون مؤمنة، فقد حددها في المادة 11 من هذا القانون.

والتي نصت على أن [1]الآلية المؤمنة لإنشاء التوقيع الإلكتروني هي آلية إنشاء توقيع إلكتروني تتوفر فيها المتطلبات الآتية:

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

ا ألا يمكن عمليا مصادقة البيانات المستخدمة لإنشاء التوقيع الإلكتروني إلا مرة واحدة، وأن يتم ضمان سريتها بكل الوسائل التقنية 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 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 أن لا تعدل البيانات محل التوقيع وأن لا تمنع أن تعرض هذه البيانات على الموقع قبل عملية التوقيع.

فنستنتج من هذه المتطلبات التي وضعها المشرع الجزائري اشتراطه السرية بيانات إنشاء التوقيع الإلكتروني، وهذا ما يمكن أن يكون ضمانة لحفظها من أخطار التزوير أو التحريف أو استعمالها من قبل شخص آخر ليس صاحب التوقيع[2].

فالمشرع الجزائري استنبط هذه المتطلبات من التشريع الفرنسي والذي اشترط بدوره سرية معطيات. إنشاء التوقيع الإلكتروني في نص المادة 13 من المرسوم رقم 2001-272 المؤرخ في 30/03/2001.[3]

-متطلبات آلية التحقق من التوقيع الإلكتروني

تقوم آلية التحقق بإصدار تقرير يُبيّن مدى صحة التوقيع الإلكتروني من عدمه، وذلك من خلال الاعتماد على قاعدة بيانات تحتوي على إحصائيات ومعطيات خاصة بالطرف الموقع. وتتمثل عملية التحقق في فك

---

[1]-أمين، التوقيع الإلكتروني وحجيته في الإثبات، رسالة مقدمة لاستكمال متطلبات الحصول على شهادة ماستر أكاديمي في تخصص قانون الأعمال، كلية الحقوق والعلوم السياسية، جامعة الشادلي بن جديد، الطارف 2018/2019،ص28.

[2]-ياسمينة كواشي الحماية الجنائية للتوقيع والتصديق الإلكترونيين في ظل القانون مذكرة مكملة لنيل شهادة ماستر في تخصص قانون جنائي للأعمال كلية الحقوق والعلوم السياسية جامعة العربي بن مهيدي أم البواقي، 2016/2017،ص12

[3]-يمينة حوحو، مرجع سابق، ص 179

الرموز المشفّرة للتوقيع الإلكتروني، ثم مقارنتها مع المعلومات والإحصائيات المحفوظة مسبقًا في قاعدة البيانات.

وبناءً على نتيجة هذه المقارنة، يتم إصدار تقرير يُحدد مدى تطابق التوقيع مع البيانات الأصلية، ثم يُرسل هذا التقرير إلى برنامج الكمبيوتر المعني، الذي يتولى بدوره تأكيد صحة التوقيع أو عدمها..[1]

اشترط المشرع الجزائري نفس المتطلبات المتعلقة بموثوقية آلية التحقق من التوقيع الإلكتروني، كما هو الحال بالنسبة لآلية إنشائه، وذلك بهدف ضمان مصداقية وسلامة التوقيع الإلكتروني.

فقد نصت المادة 12 من القانون رقم 15-04 على ضرورة أن تكون آلية التحقق من التوقيع الإلكتروني الموصوف موثوقة.

ولتوضيح ما يُقصد بموثوقية هذه الآلية، جاءت المادة 13 من ذات القانون لتُحدد الشروط والمتطلبات التي يجب توفرها في آلية التحقق، حيث نصت على أن:

"الآلية الموثوقة للتحقق من التوقيع الإلكتروني هي كل آلية تتوفر فيها مجموعة من المتطلبات المحددة، والتي تضمن فعاليتها في التحقق من صحة التوقيع الإلكتروني ومطابقته للمعايير القانونية والتقنية المعتمدة.".

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 عرضا صحيحا.

3-أن يكون مضمون البيانات الموقعة، إذا اقتضى الأمر محددا 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 وصحيحة.

تخلص أن المشرع الجزائري قد أوكل إجراءات التحقق من تطبيق الآلية المؤمنة لإنشاء التوقيع الإلكتروني، والآلية المؤمنة للتحقق منه مع المتطلبات التي جاءت في المادتين 11 و 13 السالف ذكرهما إلى هيئة وطنية مكلفة باعتماد آليات إنشاء التوقيع الإلكتروني والتحقق منه[2].

---

[1]-فيصل سعيد الغريب، مرجع سابق، ص 22

[2]-ياسمينة كواشي، مرجع سابق، ص 13

-أن يكون منشأ بواسطة وسائل تكون تحت التحكم الحصري للموقع

لكي يتمتع التوقيع الإلكتروني بحجية قانونية في الإثبات، يجب أن يتم إنشاؤه باستخدام وسائل تكون خاضعة بالكامل لسيطرة الموقع وحده، بحيث لا يُمكن لأي شخص آخر الاطلاع على رموزه أو فك تشفيره أو استخدامه، سواء أثناء إنشائه أو عند استعماله.

ويعني ذلك أن يتم إنشاء التوقيع الإلكتروني بوسائل تقنية تتيح للموقع الاحتفاظ به والتحكم فيه بصورة حصرية، بما يضمن سريته ويحول دون أي تدخل أو استخدام غير مشروع من قبل الغير.[1]

فيتضح من هذا الشرط أنه يستوجب لتمتع التوقيع الإلكتروني الموصوف بالحجية في الإثبات أن يتم إنشاؤه بوسائل تحت سيطرة الموقع، لكن إذا الموقع فقد سيطرته وتحكمه لأي سبب كان فإن بيانات التوقيع تفقد طابعها السري بحيث يعلمها كل الأشخاص، مما يجعل التوقيع الإلكتروني بعد حجيته في الإثبات لأن تمييزه الهوية الموقع وتحديد شخصيته يكون مشكوك فيه.[2]

أي يجب أن تكون أداء إنشاء التوقيع الإلكتروني تحت سيطرة الموقع كاملة، وذلك سواء بالنسبة لإنشائه أو وسيلة استعماله وقت التوقيع، وأن يكون الموقع هو نفسه من قلم بإنشاء التوقيع الإلكتروني وبطريقته الخاصة وتحت سيطرته[3].

أن يكون مرتبطا بالبيانات الخاصة به

يُعد التحقق من سلامة مضمون المستند الإلكتروني شرطًا جوهريًا لضمان الثقة والأمان في المعاملات الإلكترونية، لا سيما في ظل غياب العلاقات أو التعاملات المسبقة بين الأطراف، ومع ما تفرضه الوسائط التكنولوجية الحديثة من مخاطر محتملة.

ولتحقيق هذه الثقة، لا بد من وجود بيئة إلكترونية مؤمّنة، خاصة في مجال التجارة الإلكترونية، حيث لا يقتصر الأمر على التأكد من هوية الموقع وموافقته الصريحة على مضمون المحرر الإلكتروني، بل يتعين كذلك التحقق من عدم تعرض التوقيع الإلكتروني أو محتوى المستند لأي تغيير أو تلاعب أو تعديل لاحق.

يُشترط، لاعتداد التوقيع الإلكتروني كوسيلة إثبات قانونية، أن يكون البرنامج أو النظام المستخدم في إنشائه والتحقق منه قادراً على كشف أي تعديل أو تغيير لاحق، سواء تعلق ذلك بالتوقيع ذاته أو بمحتوى المستند الإلكتروني المرتبط به.

---

[1]-سعيد السيد قنديل التوقيع الإلكتروني، دار الجامعة الجديدة، الإسكندرية، 2006، ص 61

[2]-زروق يوسف، مرجع سابق، ص 62.

[3]-زياد خليف العنزي، المشكلات القانونية لعقود التجارة الإلكترونية، الطبعة الأولى، دار وائل للنشر، الأردن، 502010. 49 ص

ففي حال وقوع أي تعديل لم يتم رصده من قبل النظام المعتمد، فإن التوقيع الإلكتروني يفقد قيمته القانونية، ولا يُعتد به كدليل أمام الجهات القضائية أو الإدارية.

وعليه، فإن سلامة التوقيع الإلكتروني لا تتحقق إلا إذا اقترنت بإمكانية التأكد من عدم تغييره أو التلاعب به، وهو ما يُعد شرطًا جوهريًا لضمان حجية التوقيع في الإثبات، وترسيخ الثقة في المعاملات الإلكترونية..[1].

فالموقع يضع توقيعه في الغالب في نهاية المحرر الإلكتروني بحيث يسحب التوقيع على كافة البيانات الواردة بالمحرر، ولكن هذا لا يمنع من أن يوضع التوقيع في أي مكان من المحرر إذا اتفق الأطراف على ذلك مع إلزامية أن يكون التوقيع متصلا اتصالا ماديا ومباشرا بالمحرر المكتوب[2].

يتطلب تحقيق الأمان والثقة في التوقيع الإلكتروني أن يتم تحرير الوثيقة الإلكترونية والتوقيع عليها باستخدام وسائل ونظم تقنية تضمن سلامة محتواها، وتحافظ على صحتها، وتمكّن من كشف أي تعديل أو تغيير قد يطرأ عليها بعد التوقيع.

كما يشترط أن تكون هناك علاقة وثيقة وواضحة بين الصفحة الموقّع عليها وسائر صفحات المحرر الإلكتروني، إذ إن وضع التوقيع على المستند هو ما يمنحه القوة القانونية والحجية في الإثبات، طالما يُعبّر التوقيع بشكل صريح عن إقرار الموقع بمضمون الوثيقة، والتزامه بما ورد فيها.[3]

فالمحرر الإلكتروني قد يتعرض للتغيير أثناء عملية نقله من المرسل إلى المرسل إليه، وهذا التعبير قد يكون سببنه عمل من الوسائل الفنية أو تدخل الغير أو من المرسل إليه[4].

عند النظر في تقنية التوقيع الرقمي، التي تقوم على نظام التشفير باستخدام مفتاحين: أحدهما عام والآخر خاص، يتضح أن هذه التقنية تضمن مستوى عالٍ من الأمان، حيث لا يمكن الاطلاع على محتوى المحرر الإلكتروني إلا من قبل الشخص الذي يحوز المفتاح الخاص. ويُحوَّل التوقيع الإلكتروني في هذه الحالة إلى صيغة رياضية مشفّرة لا يمكن فهمها أو فك شفرتها إلا باستخدام ذلك المفتاح الخاص.

ويُعد هذا الأسلوب ضمانًا لعدم إمكانية فصل التوقيع عن المحرر أو تعديله إلا من طرف صاحب التوقيع نفسه. ويُستخلص من ذلك شرط جوهري، مفاده أن أي تغيير في المحرر الإلكتروني لا يمكن أن يتم دون المساس بالمحرر ذاته، ما لم يكن مصحوبًا بإعادة التوقيع، الأمر الذي يضمن عدم الوصول إلى

---

[1]–محمد مرسي زهرة مدى حجية التوقيع الإلكتروني في الإثبات، رسالة دكتوراه جامعة عين شمس، فبراير 1994،.260ص

[2]–خالد مصطفى فهمي، مرجع سابق، ص 34

[3]–ا عبد الحميد ثروت، مرجع سابق، ص 38

[4]–عيسى غسان ريضي، مرجع سابق، ص 177.

المحتوى أو تعديله دون علم الموقع. ولا يهدف هذا الشرط إلى حماية التوقيع الإلكتروني فحسب، بل يمتد أيضًا إلى حماية المحرر الإلكتروني بكامله، بما يعزز من قوته وحجيته القانونية.[1].

يمكن، من الناحية التقنية، فصل التوقيع عن السند الإلكتروني، ويرجع ذلك إلى طبيعة الوسائل والتقنيات المعتمدة في تأمين المحررات الإلكترونية. ومن بين أبرز هذه التقنيات المستخدمة لضمان استقرار وأمان الاتصال، تقنية التشفير الثنائي المعتمدة على زوج من المفاتيح: أحدهما عام والآخر خاص.

وتكمن فعالية هذه التقنية في أن مضمون رسالة البيانات يُرسل في شكل رموز أو إشارات مشفّرة لا يمكن قراءتها أو فهمها إلا باستخدام المفتاح الخاص، الذي يقوم بتحويل النص المشفر إلى صيغته الأصلية، بما يُتيح قراءته وفهمه بشكل واضح ودقيق.

وهذا يعزز من حماية محتوى المحرر الإلكتروني، ويضمن سريته وسلامته من أي اختراق أو تعديل غير مشروع..[2]

يمكن كشف أي تعديل أو تغيير قد يطرأ على التوقيع الإلكتروني من خلال استخدام تقنية التشفير الثنائي المعتمدة على المفتاحين العام والخاص، أو عن طريق الاستعانة بجهة التصديق الإلكتروني وشهادة التصديق التي تصدرها، أو عبر أي وسيلة تقنية مماثلة تحقق ذات الغرض.

فإذا توفرت في التوقيع الإلكتروني الشروط المشار إليها سابقًا، فإنه يُعتد به قانونًا ويتمتع بالحجية الكاملة في الإثبات أمام الجهات القضائية، وذلك في إطار المعاملات المدنية والتجارية.

ارتباط التوقيع الإلكتروني بالمحرر ارتباطا وثيقا

ويقصد بهذا الشرط أن يكون لصاحب التوقيع الإلكتروني بيانات وشفرة خاصة به عن باقي الموقعين، لأنه عندما تصدر بيانات إنشاء التوقيع لشخص ما فمن غير الممكن أن يتم إصدار نفس التوقيع لشخص آخر غيره[3]. أي وجوب أن يتصل التوقيع بالمحرر الإلكتروني الذي يرغب الموقع بقبول مضمونه بشكل مباشر بحيث لا يمكن الفصل بينهما بأية طريقة أو إجراء أي تعديل أو تبديل في بيانات المحرر بعد توقيعه إلكترونيا إلا إذا تم تغيير التوقيع الإلكتروني نفسه[4].

يشترط للاعتداد بالتوقيع الإلكتروني كوسيلة إثبات أن يكون مرتبطًا ارتباطًا وثيقًا بالمحرر المكتوب، بحيث يُشكل دليلًا قاطعًا على إقرار الموقع بمضمون المستند.

---

[1]–يوسف أحمد النوافلة، مرجع سابق، ص 87.

[2]–آمنة بومجو، الإثبات في عقود التجارة الإلكترونية، مذكرة تكميلية لنيل شهادة الماستر، تخصص قانون أعمال، كلية الحقوق و العلوم والسياسية،جامعة العربي بن مهيدي. ام البواقي.2016/2015.ص62.

[3]–عزولة طيموش، علاوات فريدة، مرجع سابق، ص 19.

[4]–ناهد فتحى الحموري، مرجع سابق، ص ...87

فعلى سبيل المثال، يعتمد التوقيع الرقمي على نظام التشفير الثنائي القائم على مفتاحين: أحدهما عام والآخر خاص، حيث يُستخدم أحد المفتاحين للوصول إلى المحرر، بينما يُستخدم الآخر للتحقق من صحة التوقيع.
ولا يمكن لأي طرف الاطلاع على مضمون المستند أو تعديله إلا إذا كان بحوزته المفتاح الخاص، وهو ما يجعل التوقيع والمحرر مرتبطين ارتباطًا لا يقبل الفصل أو التلاعب، إلا من قبل صاحب المحرر ذاته.
وبالتالي، فإن أي تعديل في محتوى المحرر يستوجب التمكن من الوصول إلى التوقيع الإلكتروني ذاته، وهو أمر شديد التعقيد، ما يضمن حماية المستند وسلامة التوقيع.،[1] لأن هذه الرموز لا يمكن معرفة فحواها دون استخدام مفتاح التشفير الخاص الذي يحول النص المشفر إلى الوضع الأصلي بحيث يتم قراءته بشكل واضح، ومنه فإن المحرر الإلكتروني على نحو لا يمكن فصله أو تعديله من الغير، فهذا الشرط جاء الحماية المحرر الإلكتروني من التغيير والتحريف وليس الحماية التوقيع الإلكتروني فقط، بحيث أنه لو تم التبديل في إحداهما يصبح غير قابل للإثبات لأنه تعرض للتغيير مما يؤدي إلى زعزعة سلامته وبالتالي فإنه يفقد حجبته في الإثبات.
فالارتباط بالمستند لا يخول لصاحب التوقيع بتعديله إلا خلال مدة زمنية، ومن ثم إطلاع كافة الأطراف الذين تربطهم علاقات قانونية بهدف المحافظة على جميع حقوقهم لأن هذا الشرط يحمي أطراف العقد وذلك من خلال إجراءات عديدة قبل الشروع بأي تعبير على التوقيع كاختيار جهة إصدار التوقيع برغبته في القيام بمثل هذا الإجراء، بعد ذلك تقوم تلك الهيئة بإجراء ما يلزم للتأكد ذلك أن الرموز الناتجة عن التوقيع الإلكتروني لا يمكن فهم مضمونها أو فك تشفيرها إلا من خلال استخدام المفتاح الخاص، الذي يعيد النص المشفر إلى حالته الأصلية ليُصبح قابلاً للقراءة بشكل واضح. وبناءً عليه، فإن المحرر الإلكتروني يكون محصّنًا ضد التعديل أو الفصل عنه من قبل الغير، إذ لا يمكن المساس به إلا من طرف صاحب التوقيع ذاته.

ويُعد هذا الشرط وسيلة لحماية مضمون المحرر الإلكتروني من أي تغيير أو تحريف، وليس فقط لحماية التوقيع الإلكتروني، حيث إن أي تعديل في أحدهما يؤدي إلى الإخلال بوحدة الوثيقة، ويترتب عنه فقدانها لقيمتها القانونية كوسيلة إثبات، نظرًا لعدم سلامتها، ما يُضعف حجيتها أمام القضاء.
كما أن الارتباط بين التوقيع والمحرر لا يتيح لصاحب التوقيع إجراء أي تعديل بعد توقيعه إلا في حدود زمنية محددة، وخلال هذه الفترة يجب إعلام جميع الأطراف المرتبطين بالمعاملة القانونية بالتعديلات، حفاظًا على حقوقهم ومراكزهم القانونية.

[1]–موسى شالي، مرجع سابق، ص14.

ويُحقق هذا الشرط حماية فعالة لأطراف العقد من خلال سلسلة من الإجراءات المسبقة، تبدأ باختيار الموقع لجهة إصدار التوقيع الإلكتروني بإرادته، ثم تقوم هذه الجهة باتخاذ كافة التدابير اللازمة للتحقق من صحة التصرفات التي تمت باستخدام التوقيع السابق، مع الحفاظ عليه لمدة زمنية محددة، إلى جانب التوقيع الجديد، لضمان سلامة المعاملات واستمرارية الحجية القانونية. ،[1] وأي تصرف يبرم بعد إصدار التوقيع الجديد بالتوقيع القديم لا يعترف به، ذلك لأن التوقيع القديم قد تم إيقافه فأدرج ذلك من قبل جهة توثيق التواقيع التي تصدر كل فترة نشرة خاصة بالتواقيع التي تم إيقاف اعتمادها.[2]

ومادام الأمر كذلك فإن التوقيع الإلكتروني يوفي شروط التوقيع العادي إذا تم وفقا لإجراءات خاصة بإنشائه، ووضع التوقيع على المحرر هو الذي يمنحه الأثر والحجية القانونية لأداء وظيفته طالما أنه يدل دلالة واضحة على إقرار الموقع بمضمون المحرر.[3]

[1]–طرافي ياسمين منصوري ،ياسمين، مرجع سابق، ص 25

[2]–أسماء أحمد كريمة عاشور، مرجع سابق، ص 69

[3]–مصطفى هنشور وسيمة النظام القانوني للتوقيع الإلكتروني في التشريع الجزائري، مجلة الحقوق والعلوم السياسية، العدد 24، المجلد الثاني، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس مستغانم، دون سنة، ص414.

خلاصة الفصل الاول

وفي الختام، يُشكل التوقيع الإلكتروني إحدى أبرز الوسائل القانونية الحديثة التي أفرزها التطور التكنولوجي في ميدان المعاملات الإلكترونية، وقد اكتسب مكانته بوصفه بديلاً فعالًا للتوقيع التقليدي، من حيث حجيته في الإثبات وصلاحيته في توثيق التصرفات القانونية. كما أنّ تأصيل مفهومه يقتضي الإحاطة بجوانبه التقنية والقانونية، بالنظر إلى طبيعته الرقمية وخصوصيته في الإنشاء والتوثيق. وقد بيّنت التشريعات، ومن بينها القانون الجزائري، الشروط القانونية التي تمنحه القوة الثبوتية، لاسيما من حيث التعريف، والتمييز بين أنواعه، وضمانات مصداقيته. وتبرز أهمية هذا التأصيل في ضبط الإطار المفاهيمي الذي يُمكّن من توحيد الفهم القانوني للتوقيع الإلكتروني، وتهيئة بيئة قانونية آمنة وموثوقة للمعاملات الرقمية.

الفصل الثاني:

الحماية الجزائية للتوقيع الالكتروني في التشريع الجزائري

الحماية الجزائية للتوقيع الالكتروني في التشريع الجزائري

يعد التوقيع الالكتروني من أهم الوسائل المناسبة للمعاملات الالكترونية والتجارة الالكترونية خاصة حيث يساهم في تثبيت المعاملات وخلق الثقة عند الأطراف ويزيد على التعاقد الالكتروني مما يدفع إلى زيادة حجم تبادلات التجارة الالكترونية مما يجعله مفتوحا للاعتداءات وبذلك أصبح من الضروري التحقق من المعلومات الواردة في العقد الكتروني لتحديد أطراف العقد من حيث سلامة وأمن المعاملات مما يتطلب آليات قانونية تحمى هذه المعاملات بين الأطراف المتعاقدة وهذا ما يتطلب تدخل طرف ثالث موثوق للتحقق من المعلومات، حيث تم إنشاء منظمات متخصصة تسمى جهات التصديق التي تقوم بخدمة التصديق الالكتروني كطرف محايد حيث تقوم بإصدار شهادات تحتوي قاعدة بيانات الكترونية وقد تم اعتماد الشهادة من قبل جهات التصديق المختصة طبقا لأحكام التشريعات الوطنية التي تنظم مهامها والتزاماتها والمسؤولية المترتبة في حالة مخالفة هذه الأحكام إلى جانب هذا وجب على المشرع الجزائري تحديد الجرائم المتعلقة بالتوقيع الالكتروني وتحديد العقوبات المتعلقة بها لحمايتها جنائيا. لذلك، من خلال ما تقدم سنعالج في هذا الفصل كل من الحماية المدنية للتوقيع الالكتروني في التشريع الجزائري كمبحث أول والحماية الجنائية للتوقيع الالكتروني في التشريع الجزائري كمبحث ثاني كما يلي.

المبحث الأول:

الحماية المدنية للتوقيع الالكتروني في التشريع الجزائري

نظرا للدور المهم الذي يلعبه مقدم خدمة التصديق الالكتروني وخطورة التبعات المترتبة على ذلك، فقد قررت معظم التشريعات تحديد الالتزامات المفروضة عليه بغض النظر عما إذا كانت هذه الالتزامات اتجاه حامل الشهادة أم لا، إلى أي مدى يتحمل مقدمو خدمات الشهادات الالكترونية المسؤولية إذا كان الشخص الذي تربطه علاقة تعاقدية معه أو الطرف الثالث الذي يعتمد على الشهادة الصادرة منه ومن نفسه في حال تبين أن المعلومات الواردة في هذه الشهادات غير صحيحة وعليه يتم توضيح صحة مقدم خدمة التصديق الالكتروني والتأكيد على التزامات كل جهة والمسؤولية المرتبة على الإخلال بهذه الالتزامات وكذا تبيان القيمة القانونية للتوقيع الالكتروني في التشريع الجزائري فلأي مدى أصبح له حجية قانونية في الإثبات وبذلك ارتأينا إلى تقسيم هذا المبحث إلى مطلبين المسؤولية المدنية وأثارها على التوقيع الالكتروني (المطلب الأول) والقيمة القانونية للتوقيع الالكتروني في التشريع الجزائري (مطلب الثاني).

المطلب الأول :

المسؤولية المدنية وأثارها على التوقيع الالكتروني

مع التطور المتسارع للمعاملات الإلكترونية، أضحى من الضروري وجود جهات موثوقة تُعنى بضمان صحة التوقيعات الرقمية وسلامة التبادلات الإلكترونية، وهو ما أدى إلى استحداث ما يُعرف بجهات التصديق الإلكتروني، التي أسند إليها المشرّع دورًا محوريًا في تأمين الثقة في البيئة الرقمية. ونظرًا للطبيعة الدقيقة والحساسة للمهام المنوطة بهذه الجهات، فإن إخلالها بالالتزامات القانونية الملقاة على عاتقها قد يُفضي إلى إلحاق أضرار بالأطراف المتعاملة معها، مما يستوجب بحث مدى قيام مسؤوليتها المدنية.

وتأسيسًا على ما سبق، يُعالج هذا المطلب أحكام المسؤولية المدنية المترتبة على جهة التصديق الإلكتروني عند إخلالها بالتزاماتها، حيث نقسّمه إلى فرعين: نتناول في الفرع الأول المقصود بالمسؤولية المدنية وجهة التصديق، في حين نخصص الفرع الثاني لبيان التزامات هذه الجهة والأساس القانوني لمسؤوليتها المدنية الناتجة عن الإخلال بتلك الالتزامات.

الفرع الأول :

المسؤولية المدنية لجهة التصديق الالكتروني

يراد عموما بالمسؤولية الجزاء الذي يترتب على الشخص عند إخلاله بقاعدة من قواعد السلوك ، ويختلف هذا الجزاء باختلاف نوع القاعدة المخل بها ، وقد يتعلق الأمر بقاعدة جزائية فتكون المسؤولية

جزائية ، ويتمثل هذا الجزاء في العقوبة (الحبس أو الغرامة مثلا) ، وقد تكون القاعدة المخل بها مدنية فتكون المسؤولية مدنية ، ويتمثل الجزاء حينئذ في الالتزام بالتعويض ، والجدير بالذكر إلى أنه إضافة إلى الخلط الذي كان موجودا قديما بين المسؤولية المدنية والمسؤولية الجزائية ، فقد تجتمع هاتان المسؤوليتان في فعل واحد مما يستوجب التمييز بينهما. [1] حيث نتناول مفهوم المسؤولية المدنية أولا ثم التصديق الالكتروني.

أولا : تعريف المسؤولية المدنية

تُبنى المسؤولية المدنية على وضع قانوني يقوم فيه شخص بإخلال بالتزام قانوني، يؤدي إلى إلحاق ضرر بالغير يمس بذمته المالية. وتُعرَّف بأنها التزام قانوني يقع على عاتق المسؤول بتعويض الضرر الناتج عن الإخلال بالتزامه، سواء كان التزاماً تعاقدياً أو تقصيرياً. ويكمن جوهرها في إلزام المسؤول بإصلاح الضرر الذي أصاب الغير، عبر إزالته أو تعويضه تعويضاً نقدياً يعادل حجم الضرر.

وتُعد هذه المسؤولية ذات طبيعة قانونية، لكونها ترتب أثراً قانونياً مباشراً يتمثل في التزام المدين بالتعويض، ويُكفل تنفيذ هذا الالتزام عن طريق الجزاء القانوني. كما تُعد مسؤولية مدنية لأنها تستهدف معالجة الضرر الواقع على الغير، لا من خلال العقاب، بل عبر إعادة الوضع إلى ما كان عليه قدر الإمكان، أو تعويض المتضرر بمبلغ مالي يعادل الضرر الحاصل، تحقيقاً للعدالة وحماية للمراكز القانونية للأفراد. [2]

أما عن الأساس القانوني للمسؤولية المدنية : الجزء 124 ق ج : " كل عمل اية كان يرتكبه الفرد عن خطئه ويسبب ضررا للغير يلزم من كان السبب في وقوعه بالتعويض "فيما يتعلق بنص المادة فقد اعتبرت الأساس القانوني للمسؤولية المدنية المتمثل في الخطأ والضرر والعلاقة السببية وأعني بذلك:

أ/- الخطأ:

لم يحدد المشرع للجزائري تعريف الخطأ لما فيه من الدقة والصعوبة، ولكن الرأي الراجح فقها الخطأ " هو الانحراف عن سلوك الرجل المعتاد مع إدراك الشخص لذلك، وبعبارة أخرى هي الإخلال القانوني الذي يفرض على كل شخص عدم الإضرار بالغير وأن يراعي في سلوكه الحيطة والتبصر يضر بغيره ، وهذا

[1]- فيلالي علي ، الالتزامات : الفعل المستحق للتعويض ، موفم للنشر ، الجزائر ، الطبعة 03 ، 2015 ، ص06 .

[2]- مقلاتي مونة ، مطبوعة بيداغوجية حول الأسس الجديدة للمسؤولية المدنية ، جامعة 8 ماي 1945 ، قالمة ، 2019 ، ص05 .

الالتزام هو التزام ببذل عناية وليس بتحقيق نتيجة وبالتالي إذا انحرف عن هذا السلوك مخطئا واستلزم ذلك قيام مسؤوليته [1].

ثانيا: شهادة التصديق الالكتروني :

لشهادة التصديق الالكتروني دورا مهما في تأمين وسلامة المعاملات الالكترونية ، كون هذه الأخيرة قد أثارت إشكالات أدت إلى تدخل التشريعات وأقرت ما يسمى بشهادة التصديق الالكتروني باعتبارها وثيقة متضمنة على بيانات شخصية من صاحب التوقيع والحل في وجود نزاع ما.

ستكون شهادة التصديق ضمانا لعدم إنكار أي من الأطراف توقيع الوثيقة المبعوثة عبر وسيلة الكترونية ، ودلالة واضحة ونابضة بالحياة على أن الموقع ملك المفتاح الشفوي الخاص ، وبالتالي هو من وقع عليها فمن أبعد ما تكون عنه ديان هذه الشهادات ومن ثم تكون ضمانة هامة وأكيدة للأشخاص الذين يريدون التعامل معه ، وتضمن تحقق الوظائف هامة وهي السرية والسلامة والموثوقية ، وعليه نعالج تعريف شهادة التصديق الالكتروني والبيانات الواجب توافرها في شهادة التصديق الالكتروني وأنواع شهادة التصديق الالكتروني، كما أخذت شهادة التصديق الإلكتروني تسميات كثيرة أدت إلية اختلاف التعاكس سواء على مستوى التشريعات أو الفقه القانوني، ومع ذلك متفقون على المفهوم العام منها ، وبالتالي سنتعامل مع التعريف الفقهي للشهادة التصديق الإلكتروني و ثم التعريف التشريعي للشهادة التصديق الإلكتروني.

أ- التعريف التشريعي لشهادة التصديق الالكتروني

لقد حاول العديد من الفقهاء وضع التعريف لشهادة التصديق الالكتروني وذلك نظرا لأهمية هذه الأخيرة في تأكيد هوية أطراف هذه المعاملة ، وعرفت شهادة التصديق عدة تعاريف من قبل الفقهاء ، حاولوا من خلالها بيان مفهوم شهادة التصديق .

فقد عرفها غانى جابر السعدي :" هي الشهادات التي يصدرها مقدموا خدمات التصديق الالكتروني المرخص لهم من قبل الجهات المسؤولة في الدولة ، لنشهد بان التوقيع الالكتروني هو توقيع صحيح ينسب إلى من أصدره ، ويستوفى الشروط والضوابط المطلوبة فيه باعتباره دليل إثبات يعول عليه"[2]

[1]- محمد المهدي بكراوي ، جامعي مليكة ، يوم دراسي حول الاتجاهات الحديثة في نظرية المسؤولية المدنية ، كلية الحقوق والعلوم السياسية ، قسم الحقوق ، جامعة ادرار ، الجزائر ، 2013 ، ص27 .

[2]- محمد صبري السعدي ، الواضع في شرح القانون المدني « النظرية العامة للالتزامات – مصادر الالتزام – العقد والإرادة المنفردة ،دار الهدى ، الجزائر ، 2019 ، ص317 .

كما عرفها محمد أمين الرومي أنها :" صك أمان صادر عن جهة مختصة يفيد صحة وضمان المعاملة الالكترونية ، وذلك من حيث صحة البيانات ومضمون المعاملة وأطرافها" [1] .

كما عُرفت الشهادة الإلكترونية من قبل جانب من الفقه بأنها: "سجل إلكتروني يصدر عن جهة توثيق معتمدة، يتضمن بيانات تتعلق بهوية الشخص الحامل له، والجهة التي أصدرت هذا السجل، وتاريخ صلاحيته، إلى جانب المفتاح العام الخاص بذلك الشخص". وتُعد هذه الشهادة بمثابة هوية رقمية يصدرها طرف محايد، بهدف التعرّف على الشخص المعني، والمصادقة على توقيعه الإلكتروني، وكذا على المعاملات التي يُبرمها عبر شبكة الإنترنت [2].

حاولت التعريفات الفقهية السابقة لشهادة التصديق الالكتروني أن تبرر جوانب معينة من الوظائف التي تقدمها هذه الشهادة ، والتي من أهمها التحقق من هوية الشخص المتعاقد فيها وأهليته وسلطاته القانونية لإبرام التصرفات القانونية .

أما عن التعريف التشريعي لشهادة التصديق الالكتروني

عرف المشرع الجزائري شهادة التصديق الإلكتروني في القانون 04/15 بأنها وثيقة رقمية تثبت ارتباط توقيع إلكتروني بشخص معين، بغرض التحقق من هويته وصحة البيانات الموقعة. وقد اعتمد على المعيار الوظيفي الذي يربط الموقّع بمفتاحه العام لضمان مصداقية التوقيع ومنع أي تلاعب في البيانات. كما استخدم تعبير "تحرى التوقيع" بدلًا من "تفحص التوقيع" تأكيدًا على الدقة والبحث المعمق في إثبات صحة التوقيع وهوية صاحبه. [3]

كما نضيف هنا أن المشرع الجزائري ميز بين شهادة التصديق الالكترونية البسيطة والموصوفة، فشهادة التصديق الالكترونية البسيطة وفقا لفترة 07 من المادة 02 السالفة هي وثيقة الكترونية تثبت الصلة بين بيانات التحقق من التوقيع الالكتروني والموقع، أما شهادة التصديق الالكتروني الموصوف، وفقا للمادة 15 تتمثل في شهادة التصديق الالكتروني التي يصدرها الطرف الثالث الموثوق ومؤدي خدمات التصديق الالكتروني للموقع دون سواء. [4]

---

[1]– غانى جابر السعدي وآخرون، النظام القانوني لشهادة التوثيق الالكتروني، مجلة المحقق المحلي للعلوم القانونية والسياسية، العدد 02 ، 2017 ، ص 587 .

[2]– محمد أمين الرومية، التعاقد عبر الانترنت، دار المطبوعات الجامعية، الإسكندرية، الطبعة الأولى، 2004 ، ص43 .

[3] مباركي ياسين ، بن زعزع وليد، المرجع السابق، ص 37 .

[4] جودي أمينة ، المرجع السابق ، ص35 .

هنا نرى أن المشرع الجزائري ميز بين نوعين الشهادة التصديق حسب طريقة إصدارهما إلا أن الواقع العملي يبين وجود أنواع أخرى من شهادات التصديق والمتمثلة فيما يلي :

– **شهادة التصديق تاريخ الإصدار** : يوثق تاريخ ووقت إصدار التوقيع الرقمي حيث يقوم صاحب الرسالة بعد التوقيع عليها بإرسالها إلى جهة التصديق التي تقوم بتسجيل التاريخ عليها وتوقيعها من جهتها ثم تعيدها إلى مرسلها . [1]

– **شهادة الإذن** : بمقتضاها يتم تقديم معلومات إضافية عن صاحبها ، مثل عمله ومؤهلاته والترخيصات التي يملكها ومكان إقامة الشخص وعمره ، وفيما إذا كان الشخص عضوا في إحدى المنظمات أو النقابات المهنية كنقابة المحامين. [2]

– **شهادة البيانات أو الإثبات** : هي التي تثبت صحة واقعة معينة وقت وقوعها ، وغالبية التشريعات ترى أن للشهادات الالكترونية التي تصدرها هيئات التصديق الأجنبية لها نفس الحجية في الإثبات المقررة لنظيرتها الوطنية أي أن المقصد من ذلك هو إتاحة مستوى مكافئا يمكن التعويل عليه [3].

من هنا نستشف من التعاريف السابقة لتعريف شهادة التصديق أنها تنصب كلها في محور واحد مفاده أن شهادة التصديق عبارة عن وثيقة الكترونية تصدر جهة محايدة تتضمن مجموعة من البيانات ، تتضمن وظيفتها الأساسية في إثبات هوية الموقع ، والتوثيق من صحة التوقيع الالكتروني ونسبته إلى من صدر عنه ، والتأكد من صحة البيانات التي تتضمنها المعاملة الالكترونية ، مما يساهم على تلاشي مخاطر إبرام العقد الالكتروني . [4]

ج– البيانات الواجب توافرها في شهادة التصديق الالكتروني

إن الاعتداء بشهادة التصديق الالكتروني وحتى تكون لها القيمة القانونية التي تكسبها الحجية الكاملة في الإثبات حيث يعول عليها المتعامل الالكتروني لتحديد هوية المتعامل الأخر ، لابد من توافر

[1] مباركي ياسين ، بن زعزع وليد ، المرجع السابق، ص39 .

[2] بلقاسم حامدي ، إبرام العقد الالكتروني ، أطروحة دكتوراه في العالم القانونية تخصص قانون أعمال ، كلية الحقوق والعلوم السياسية ، جامعة الحاج لخضر ، باتنة ، 2014 ، ص257

[3] مباركي ياسين ، بن زعزع وليد ، نفس المرجع ، ص40 .

[4] Lisant de belle fonds et A . Holland , pratique du droit de l’informatique ,4 éme éd ,Delmas ,paris ,1998 ,p127,

البيانات التي اشترط القانون توافرها نظرا لأهمية هذه البيانات وجوهريتها ، من هذا المنطلق نتطرق إلى بيانات شهادة التصديق الالكتروني في التشريع الجزائري .[1]

د- بيانات شهادة التصديق الالكتروني في التشريع الالكتروني

تطرق المشرّع الجزائري في الفقرة الرابعة من المادة 15 من القانون رقم 15-04 المتعلق بالتوقيع والتصديق الإلكتروني، إلى تحديد البيانات الإلزامية التي يجب أن تتوفر في شهادة التصديق الإلكتروني الموصوفة، حيث عرّفها بأنها شهادة تصديق إلكتروني تستوفي مجموعة من المتطلبات الشكلية والموضوعية، من أهمها:

- أن تُمنح حصرياً لصاحب التوقيع دون غيره؛
- أن تتضمن بشكل صريح ما يُفيد أنها صادرة بصفة "شهادة تصديق إلكتروني موصوفة"؛
- تحديد هوية الطرف الثالث الموثوق أو مقدم خدمات التصديق الإلكتروني المرخص له بإصدار الشهادة، مع ذكر الدولة التي يُقيم فيها؛
- ذكر اسم الموقع أو اسمه المستعار الذي يسمح بالتعرف على هويته؛
- إمكانية تضمين صفة مهنية أو وظيفية للموقّع، بحسب الغرض من استخدام الشهادة؛
- إدراج البيانات التقنية الخاصة بالتحقق من التوقيع الإلكتروني، والتي يجب أن تتطابق مع بيانات إنشاء التوقيع الإلكتروني؛
- بيان تاريخ بدء وانتهاء صلاحية الشهادة بوضوح؛
- تحديد رمز تعريفي خاص بالشهادة؛
- التوقيع الإلكتروني الموصوف لمقدم خدمات التصديق الإلكتروني أو للطرف الثالث الموثوق الذي يصدر الشهادة؛
- تحديد نطاق استعمال الشهادة عند الاقتضاء؛
- بيان حدود القيمة المالية للمعاملات التي يُمكن استعمال الشهادة من أجلها، عند الاقتضاء.

تُشكل هذه العناصر مجتمعة الإطار القانوني الذي يمنح شهادة التصديق الإلكتروني الموصوفة حجيتها القانونية، ويضمن سلامة استخدامها في البيئة الرقمية وفقاً لمقتضيات الأمان والثقة التي تتطلبها المعاملات الإلكترونية.[2]

---

[1] مباركي ياسين ، بن زعزع وليد ، نفس المرجع ، ص 40 .

[2]- مباركي ياسين ، بن زعزع وليد ، المرجع السابق ، ص41 .

2- السلطات المختصة بإصدار شهادة التصديق الالكتروني

إن الهدف من وجود هذه السلطات هو تدعيم الثقة بين المتعاقدين بما يحقق الثقة والأمان خاصة في مجال المعاملات المصرفية والالكترونية وإمكانية إثبات هذه المعاملات والتعاقدات ، سواء من طرف البنوك أو العملاء لذا فان السلطة الوطنية للتصديق الالكتروني هي عبارة عن سلطة وطنية إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي تنشأ لدى الوزير الأول ، أما السلطة الحكومية فهي تنشأ لدى الوزير المكلف بالبريد وتكنولوجيا الإعلام والاتصال سلطة حكومية للتصديق الالكتروني تتمتع بالاستقلال المالي والشخصية المعنوية ، وأيضا السلطة الاقتصادية فهي مكلفة بمتابعة ومراقبة مؤدي الخدمات. [1]

أ- **السلطة الوطنية للتصديق الالكتروني** : لقد بينت المادة 19 من القانون 04/15 >المتعلق بالتوقيع والتصديق الالكترونيين تنظيم السلطة الوطنية للتصديق الالكتروني ، حيث تتكون من مجلس السلطة ، ورئيس ، ومصالح تقنية وإدارية برئاسة المدير العام ، وعلى هذا الأساس سنبرز كيفية تسيير مجلس السلطة ، ومهام المدير العام ، ثم نبين بالتفصيل المصالح التقنية والإدارية للسلطة العامة. [2]

أ - **مجلس السلطة:**يتكون المجلس من خمسة أعضاء، يُعيَّنون من قبل رئيس الجمهورية، بشرط أن يتمتعوا بكفاءة في القانون وتكنولوجيا الإعلام والاتصال. يمكنهم الاستعانة بخبرات إضافية، وتُحدد عهدتهم بأربع سنوات قابلة للتجديد مرة واحدة. تُتخذ القرارات بالأغلبية، وفي حال تعادل الأصوات يُرجَّح صوت الرئيس. يُمنع على الأعضاء تولي وظائف أخرى أو الانخراط في الإشهار حفاظاً على مبدأ الحياد.

2- المدير العام:

يُعينه رئيس الجمهورية باقتراح من الوزير الأول، ويتولى تسيير الجوانب الإدارية والتقنية للسلطة. يرفع الدراسات والمقترحات للمجلس، ويشرف على تنفيذ السياسات، كما يمارس سلطة إدارية على الموظفين ويؤدي دور همزة وصل بين المجلس والمصالح التقنية[3].

3- المصالح التقنية والإدارية للسلطة الوطنية : من خلال المادة 07 من المرسوم التنفيذي 16-134 السالف الذكر يمكن تقسيم هذا المصالح إلى ثلاثة دوائر أساسية وهي :

---

[1]- جودي أمينة ، المرجع السابق ، ص39-38 .

[2]- عروة فتيحة ، وسائل التبادل المصرفي في القانون الجزائري أطروحة دكتوراه في العلوم ، تخصص قانون أعمال ، كلية الحقوق ، جامعة الجزائر 01 ، 2016، ص 219 .

[3]- مباركي ياسين ، بن زعزع وليد ، نفس المرجع ، ص 46 .

-**الدائرة التقنية:** يرأسها رئيس دائرة، وتُعنى أساساً بالمسائل الفنية المرتبطة بنظامي التصديق والتوقيع الإلكتروني، سواء في الإطار الداخلي، من حيث الإشراف على الجوانب التقنية لضمان سلامة العمليات الإلكترونية، أو على الصعيد الدولي، من خلال إبداء الرأي الفني بشأن اتفاقيات الاعتراف المتبادل المبرمة مع هيئات التصديق الأجنبية، بما يضمن توافقها مع المعايير المعتمدة والمعايير الدولية ذات الصلة. [1]

- **دائرة أمن البني التحتية** : وفقًا لأحكام المادة 09 من المرسوم التنفيذي رقم 16-134، تُحدد مهام المصلحة المعنية في تنفيذ السياسة الأمنية الخاصة بالسلطة الوطنية. وتُقسَّم هذه المهام إلى مصلحتين رئيسيتين:

مصلحة الأمن المادي، وهي الجهة المكلفة بضمان أمن وسلامة المنشآت والمرافق التابعة للسلطة الوطنية من كافة الأخطار والتهديدات ذات الطابع المادي.

- **مصلحة الأمن المعلوماتي،** وتتولى تنفيذ السياسة الخاصة بالأمن المعلوماتي المعتمدة من قبل السلطة الوطنية، بما في ذلك حماية نظم المعلومات والبيانات الرقمية من أي اختراق أو تهديد إلكتروني، وذلك في إطار احترام التشريعات والتنظيمات السارية.

- **دائرة الإدارة العامة والشؤون القانونية** : تتجلى مهمة هذه الدائرة في وظيفتين أساسيتين: تتمثل الأولى في توفير الموارد البشرية اللازمة لتسيير عمل السلطة الوطنية، وهي منوطة بمصلحة الإدارة العامة؛ أما الثانية، فتتعلق بإبداء الرأي القانوني في مختلف المسائل المرتبطة بالتوقيع والتصديق الإلكترونيين، وتُسند إلى مصلحة الشؤون القانونية.

وقد أوجب المرسوم التنفيذي رقم 16-134، لا سيما في مادته 11، على المدير العام إعداد نظام داخلي ينظم سير المصالح التقنية والإدارية، مع ضرورة نشره داخليًا. ويجب أن يتضمن هذا النظام الأحكام المتعلقة بشروط التوظيف، وحقوق وواجبات الموظفين، وكذا كيفيات التدرج الوظيفي، والنظام التأديبي، وكل ما يرتبط بتنظيم وعمل السلطة الوطنية للتصديق الإلكتروني.

د- مهام السلطة الوطنية للتصديق الالكتروني : لقد حدد القانون رقم 04/15 السالف الذكر بصفة عامة مهام السلطة الوطنية للتصديق الالكتروني في المادة 18 منه ، حيث أسند السلطة مهمة عامة من خلال

[1]- جبايلي صبرينة ، النظام القانوني للسلطة الوطنية للتصديق الكتروني ، مجلة العلوم الإنسانية ، جامعة الإخوة منتوري قسنطينة ، المجلد أ ، العدد 48 ، ديسمبر 2017 ، ص 491-490 .

الفقرة الأولى من نفس المادة وتتمثل في ترقية استعمال التوقيع والتصديق الالكترونيين وضمان موثوقية استعمالهما ، وفي فقرة موالية أسند لها بعض المهام الخاصة التي تتكفل بها هذه السلطة وهي : [1].

تتولى السلطة الوطنية للتصديق الإلكتروني إعداد السياسات التنظيمية والتقنية ذات الصلة، بالتنسيق مع الدوائر المختصة، قبل عرضها على المجلس ثم إحالتها إلى الهيئة المعنية بالموافقة لتصبح نافذة. كما تراجع سياسات التصديق الصادرة عن السلطتين الحكومية والاقتصادية[2]، وتخضعها للتقييم الفني والأمني ثم اعتمادها. على الصعيد الدولي، تُبرم اتفاقيات اعتراف متبادل تمنح الحجية القانونية للتوقيعات الأجنبية. وتساهم مصلحة الشؤون القانونية في اقتراح مشاريع تشريعات تتعلق بالتصديق الإلكتروني ورفعها إلى الوزير الأول، في حين تبقى عمليات التدقيق من صلاحية هيئة حكومية تُحدد بموجب مرسوم لاحق.[3].

ب- السلطة الحكومية للتصديق الالكتروني : من خلال اطلاعنا على نصوص القانون 04/15 والمرسوم التنفيذي رقم 16-135 السالف ذكرها يتبين لنا أن المشرع الجزائري قد حدد بوجه الدقة تنظيمها أولا وكذا مهامها ثانيا .

1- تنظيم السلطة الحكومية للتصديق الالكتروني : من خلال الاطلاع على الأحكام المنظمة للسلطة الحكومية للتصديق الالكتروني ، نجد أنها تؤطر العملية على مستوى القطاعات الحكومية والإدارية والسلطات الوطنية المختصة ، وتمتد في ذلك على الطرف الثالث الموثوق الذي يقدم خدماته في مجال التصديق الالكتروني للهيئات المذكورة ، وهو ما يبين أنه في المرحلة الحالية على الأقل لا يمكن للوزارات مثلا أن تقدم شهادات تصديق على توقيع موظفيها وأعوانها مباشرة بل لابد أن توجد أطراف ثالثة معتمدة تقدم خدمة التصديق الالكتروني .

لكن بالرجوع إلى القانون 03/15 المؤرخ في أول فبراير 2015 الذي يتعلق بعصرنة العدالة في الفصل الثاني القسم الثاني منه المواد من 04 إلى 08 منه ، حدد كيفية التصديق الالكتروني وصاحب التوقيع تثبت عن طريق شهادة الكترونية موصوفة تصدرها وزارة العدل ، أي أن الوزارة هي التي تصدر شهادة التصديق دون المرور على الطرف الثالث الموثوق ، وهو ما يطرح السؤال بالنسبة للنص القانوني المعتمد عليه في ذلك خصوصا أن القانونيين صدرا بتاريخ واحد ، أم أن مفهوم الطرف الثالث يدخل في إطاره أيضا الوزارات

[1]- أزرو محمد رضا ، التوقيع الالكتروني كوسيلة من وسائل الإثبات ، رسالة تخرج مقدمة لنيل شهادة الماجستير ، تخصص قانون خاص ، كلية الحقوق ، جامعة أبو بكر بلقايد تلمسان 2007 ص 132 .

[2]- أرزو محمد رضا ، نفس المرجع ، ص 133 .

[3]- جبايلي صبرينة ، نفس المرجع ، ص 493 .

وهو ما يحدث تداخل في أحكام القانون خصوصا أن السلطة الحكومية هي التي تراقب عمل الطرف الثالث أي أنها من المفترض أن تراقب عمل الوزارة فيما يتعلق بشهادة التصديق الالكتروني. [1]

تُعد السلطة الحكومية للتصديق الإلكتروني هيئة تابعة لوزارة البريد وتكنولوجيات الإعلام والاتصال، وتتمتع بالشخصية المعنوية والاستقلال المالي. من أبرز مهامها متابعة ومراقبة نشاط التصديق الإلكتروني في القطاع الحكومي، اعتماد سياسات التصديق، نشر شهادات المفتاح العمومي، حفظ الشهادات المنتهية، وتوفير بيانات دورية للسلطة المختصة. كما تضمن تسيير المبادلات الإلكترونية بين الإدارات، خاصة في إطار رقمنة الوثائق والخدمات الإدارية.

– القيام بعملية التدقيق على مستوى الطرف الثالث الموثوق ، عن طريق الهيئة الحكومية المكلفة بالتدقيق طبقا لسياسية التصديق الالكتروني [2].

تجدر الاشارة أنه حسب بيان مشترك للسلطتين نشرته وكالة الأنباء الجزائرية بتاريخ 09 جوان 2021 مفاده أن السلطة الحكومية للتصديق الالكترونية حازت على أختام التصديق على المطابقة لمرجعيات واب ترست فورسي أو واب ترست بي ار أس أل وكذا واب فوركود ساينينغ لصالحها ولصالح السلطة الوطنية للتصديق الالكتروني ، كما أفاد البيان أن السلطة الحكومية للتصديق الالكتروني حازت شهر مارس 2021م وهي ذكرى تبقى في تاريخ التصديق الالكتروني في الجزائر ، على أختام التصديق على ترست فوركود ساينينغ لصالحها ولصالح السلطة الوطنية للتصديق الالكتروني [3].

ختم البيان المشترك إلى أنه بفضل خبرتها وفرقها المعتمدة التخصصات المكونة من شباب متحصلين على شهادات ، تسمح السلطة الحكومية للتصديق الالكتروني بتأمين التواصل عبر الخط وتسيير ألاف الهويات الالكترونية وجعل مسارات التوثيق والتشفير آلية [4].

ج– السلطة الاقتصادية للتصديق الالكتروني :

تُعد السلطة الاقتصادية للتصديق الإلكتروني هيئة تابعة لسلطة ضبط البريد والمواصلات، وتُكلّف بعدّة مهام أساسية تتعلق بتنظيم ومراقبة خدمات التصديق الإلكتروني. فهي مسؤولة عن إعداد دفتر الشروط الذي يحدد كيفيات تقديم هذه الخدمات، كما تتابع نشاط المتعاملين الذين يوفّرون خدمات التصديق

[1]– جودي أمينة ، نفس المرجع ، ص 40 .

[2]– أزرو محمد رضا ، نفس المرجع ، ص 137 .

[3]– جمال ديلمي ، أثار التصديق الالكتروني، أطروحة لنيل شهادة الدكتوراه في العلوم ، تخصص قانون أعمال ، كلية الحقوق والعلوم السياسية ، جامعة مولود معمري تيزي وزو ، 2022 –2023 ، ص 27–28 .

[4] جمال ديلمي ، المرجع نفسه ، ص 30،29 .

الإلكتروني لفائدة المواطنين، وتسهر على اتخاذ التدابير اللازمة لضمان استمرارية هذه الخدمات في حال حدوث أي عجز.

وتعمل هذه السلطة أيضًا على التحقق من مدى تطابق طالبي التراخيص مع سياسة التصديق الإلكتروني، وتسهر على تأمين المعاملات الإلكترونية من خلال ضمان هوية الشخص القائم بالمعاملة، بما يمنع انتحال الهوية. كما تكفل سرية المعلومات عبر تقنيات التشفير، وتمنع نقل بيانات التوقيع الإلكتروني الخاصة بالمواطن الجزائري إلى خارج التراب الوطني.

وقد تناول المشرّع الجزائري أحكام السلطة الاقتصادية للتصديق الإلكتروني في القسم الثالث من الفصل الثاني من الباب الثالث من القانون رقم 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين، لاسيما في المادتين 29 و30. وبموجب هذا القانون، تتولى السلطة الاقتصادية مراقبة ومتابعة مقدّمي خدمات التصديق الإلكتروني العموميين، كما تتكفل بإبلاغ النيابة العامة بكل فعل يكتسي طابعًا جزائيًا قد تُعاينه أثناء أدائها لمهامها. [1].

الفرع الثاني :

التزامات مقدمي خدمات التصديق والمسؤولية الناشئة عن ذلك

حيث تتناول العناصر المهمة في الفرع وهي كما يلي :

أولا : التزامات مقدمي خدمات التصديق الالكتروني

في إطار تأدية خدمات التصديق الالكتروني هناك مجموعة من الالتزامات التي تقع على مؤدي هذا النشاط تتمثل فيما يلي :

1-التزام جهة التصديق بإصدار شهادة تصديق الالكترونية :

يُعد الالتزام الأساسي الواقع على عاتق مقدم خدمة التصديق الإلكتروني هو إصدار شهادة مصادقة إلكترونية لصالح المعني بالأمر، بحيث تتوفر فيها جميع شروط السلامة اللازمة، بما يعزز الثقة في المعاملة الإلكترونية. وتتمثل وظيفة هذه الشهادة في التأكيد على هوية مرسل الرسالة الإلكترونية (الموقّع) وصحة التوقيع الإلكتروني المستخدم.

ويُعتبر هذا الالتزام من قبَل جهات التصديق التزامًا بتحقيق نتيجة، تتجسد في إصدار شهادة تصديق إلكترونية مستوفية لكافة البيانات الأساسية المطلوبة. وبناءً عليه، تلتزم جهة التصديق بالتحقق من صحة

[1] أزرو محمد رضا ، مرجع نفسه ، ص 138-139 .

المعلومات المقدمة من الأفراد طالبي الشهادات، والتثبت من صفاتهم المميزة قبل المصادقة عليها وإدراجها في الشهادة.

ويمثل هذا النوع من الالتزامات أحد أصعب وأدق المهام الموكلة إلى جهات التصديق الإلكتروني، نظرًا لما يتطلبه من كفاءات بشرية وتقنية متخصصة، قادرة على فحص البيانات والتحقق من أهلية الأشخاص المعنيين بالتوثيق. ويجب على مقدم الخدمة أن يضمن صحة المعلومات الواردة في الشهادات، بالاستناد إلى الوثائق الرسمية المقدّمة من العملاء.

ويشمل هذا التحقق مطابقة بيانات إنشاء التوقيع مع بيانات التحقق منه، وذلك من خلال فحص مستندات رسمية مثل بطاقة التعريف الوطنية أو جواز السفر، والتي يمكن الحصول عليها بوسائل متعددة، سواء عبر الاتصال المباشر، أو الوسائل الإلكترونية، أو من خلال البريد الموصى عليه. [1]

2- التزام جهة التصديق الالكترونية بالسرية : يعتبر هذا الالتزام من أخطر الالتزامات الملقاة على عائق الجهة المختصة ، إذ تلزم المادة 42 من القانون 04/15 المتعلق بالتوقيع والتصديق الالكترونيين مؤدي خدمات التصديق الالكتروني بالحفاظ على سرية البيانات والمعلومات المتعلقة بشهادة التصديق الالكترونية لإضفاء الحماية والثقة والأمان في التعامل ، خاصة وأن معظم المعاملات الالكترونية تتم بين أشخاص لا يلتقون بعضهم البعض .

3- التزامات تبعية لمؤدي خدمات التصديق الالكتروني : إن توقف مقدمي خدمات التصديق الالكتروني عن نشاطها لأسباب إرادية يلزمها إعلام سلطة المختصة مانحة الترخيص حيث أوجبت المادة 58 من القانون 04/15 الذي يحدد القواعد المتعلقة بالتوقيع والتصديق الالكترونيين مؤدي خدمات التصديق يتعيّن على مقدم خدمات التصديق الإلكتروني إعلام السلطة الاقتصادية للتصديق الإلكتروني، ضمن الآجال المحددة في سياسة التصديق المعتمدة من طرف هذه السلطة، برغبته في التوقف عن مزاولة نشاطه المتعلق بتقديم خدمات التصديق الإلكتروني، أو عند قيامه بأي تصرف قد يترتب عليه هذا التوقف. وفي هذه الحالة، يلتزم مقدم الخدمة بالتقيد بأحكام سياسة التصديق الخاصة بالسلطة الاقتصادية، لا سيما تلك المتعلقة بضمان استمرارية الخدمة. ويترتب على وقف النشاط سحب الترخيص الممنوح له[2].

[1]- مباركي ياسين ، بن زعزع وليد ، المرجع السابق ، ص 54 .

[2]- لينده بلحارث ، النظام القانوني لمزودي خدمات التصديق الالكتروني في القانون الجزائري محلة العلوم القانونية والسياسية، جامعة محند أولحاج البويرة ، المجلد 09 ، العدد 03 ، 2018 ، ص 869 .

كمل تضيف المادة 59 من قانون 04/15 المتعلق بالتوقيع والتصديق الالكترونيين على أنه يتوجب على مقدم خدمات التصديق الإلكتروني، في حال توقفه عن النشاط لأسباب خارجة عن إرادته، إشعار السلطة الاقتصادية للتصديق الإلكتروني بذلك فورًا. وتقوم هذه الأخيرة، بعد دراسة المبررات المقدمة وتقدير وجاهتها، باتخاذ قرار بإلغاء شهادة التصديق الموصوفة الصادرة عنه.

ثانيا : مسؤولية مقدمي خدمات التصديق الالكتروني

ان القانون 04/15 المتعلق بالتوقيع والتصديق الالكترونيين مسؤولية مؤدي خدمات التصديق الالكتروني في الباب الثالث الفصل الثالث القسم الثاني تحت عنوان مسؤولية مؤدي خدمات التصديق الالكترونية وصاحب الشهادة في المواد 53 إلى 57 .

تقوم مسؤولية مؤدي خدمات التصديق الالكتروني عند إخلاله بأحد الالتزامات المفروضة عليه سواء في مواجهة صاحب الشهادة الذي تعاقد معها أو الغير عند إبرام عقود وصفقاته التجارية بالطرق الالكترونية [1].

بالرجوع إلى نص المادة 53 من القانون 04/15 المتعلق بالتوقيع والتصديق الالكترونيين فان مؤدي خدمات التصديق الالكتروني يكون مسؤولا عن الضرر الذي يلحق بأي هيئة أو شخص طبيعي أو معنوي الذي يتعاقد معه أو اتجاه أي شخص اعتمد بصورة معقولة على الشهادة المصدرة ، وذلك في الحالات الآتية:

– تُعد جهة التصديق الإلكتروني مسؤولة عن صحة جميع المعلومات المدرجة في شهادة التصديق الإلكتروني الموصوفة، وذلك في التاريخ الذي تم فيه إصدار الشهادة، كما تتحمل مسؤولية التأكد من تضمين جميع البيانات الإلزامية المنصوص عليها قانونًا ضمن هذه الشهادة.

–كما تلتزم الجهة المانحة لشهادة التصديق الإلكتروني، عند إصدارها، بالتحقق من أن الشخص المحدد هويته في الشهادة يمتلك بشكل حصري بيانات إنشاء التوقيع، وأن هذه البيانات تتطابق مع بيانات التحقق من التوقيع المدرجة أو المعتمدة في شهادة التصديق الإلكتروني الموصوفة.

– التأكد من إمكانية استعمال بيانات إنشاء التوقيع والتحقق منه بصفة متكاملة إلا في حالة ما إذا قدم مؤدي خدمات التصديق الالكتروني ما يثبت أنه لم يرتكب أي إهمال .

يتضح من نص المادة 53 من القانون 04/15 المتعلق بالتوقيع والتصديق الالكترونيين أنه لا تقوم مسؤولية مقدم خدمات التصديق الإلكتروني إلا في حال كان اعتماد الغير على شهادة التصديق اعتمادًا معقولًا. ويُلزَم مقدم الخدمة بممارسة عناية معقولة لضمان دقة واكتمال جميع البيانات الجوهرية ذات الصلة

[1]– مباركي ياسين ، بن زعزع وليد ، المرجع السابق ، ص 55 .

بالشهادة، سواء المدرجة فيها أو المرتبطة بها، وذلك طوال مدة صلاحيتها. ويُقصد بالعناية المعقولة تلك العناية المعتادة التي يُفترض بمقدم خدمات التصديق الإلكتروني ممارستها وفقًا للأصول المهنية المعتمدة في مجال إصدار شهادات التصديق الإلكتروني والتوقيعات الإلكترونية[1] .

من جهة نص المشرع الجزائري على حالة أخرى تقوم فيها مسؤولية مؤدي خدمات التصديق الالكتروني من خلال نص المادة 54 من القانون 04/15 المتعلق بالتوقيع والتصديق الالكترونيين يُسأل مقدم خدمات التصديق الإلكتروني عن الضرر الناتج عن عدم إلغاء شهادة التصديق الإلكتروني في الوقت المناسب، إذا ترتب على ذلك ضرر لهيئة أو لشخص طبيعي أو معنوي قام بالاعتماد على تلك الشهادة، ما لم يُثبت مقدم الخدمة أنه لم يرتكب أي خطأ أو إهمال في هذا الشأن. [2]

المطلب الثاني :

حجية شهادة التصديق الالكتروني في الإثبات

تُعد شهادة التصديق الإلكتروني وسيلة قانونية لإثبات وجود التزام أو عقد إلكتروني مبرم بين طرفين، شريطة أن تكون مطابقة للشروط القانونية المنصوص عليها في التشريع المنظّم لها، دون أن يطرأ عليها أي تعديل أو تدليس يفقدها حجيتها أمام الجهات القضائية، خاصة عند الاستناد إليها للمطالبة بالحقوق التي تتضمنها. وقد ميّز المشرع الجزائري بين نوعين من شهادات التصديق، وهما: شهادة التصديق الإلكتروني الوطنية، وهي التي تصدر عن مقدم خدمات معتمد داخل التراب الوطني، وشهادة التصديق الإلكتروني الأجنبية، وهي التي تُنشأ في دول أجنبية أو من قبل مزوّد خدمات أجنبي يمارس نشاطه داخل الجزائر. وقد منح المشرع لكل منهما حجية قانونية تتيح الاستناد إليهما في إثبات المعاملات الإلكترونية، وفقًا لما تقرّره النصوص القانونية ذات الصلة. ، وعليه سنتطرق إلى حجية شهادة التصديق الالكتروني الوطنية في (الفرع الأول) ، وحجية شهادة التصديق الالكتروني الأجنبية في (الفرع الثاني) .

الفرع الأول :

حجية التوقيع الالكتروني البسيط

في خضم المعطيات المالية من عدم تنصيب الأجهزة المتعلقة بالتوقيع والتصديق الالكترونيين على المستوى الوطني ، فان جل التوقيعات التي ستتواجد هي توقيعات الكترونية بسيطة إلا أنه لا يمكن

[1]– درار نسيمة ، التوثيق الرقمي ومسؤولية سلطات المصادقة الالكترونية في القانون الجزائري 04/15 ، مجلة الأستاذ الباحث للدراسات القانونية والسياسية ، المجلد 02 ، العدد 9 ، 2018 ص 861 .

[2]–المادة 54 من القانون 04/15 المتعلق بالتوقيع والتصديق الالكترونيين.

تجاهلها بل لابد من الأخذ بها تطبيقا لنص المادة 9 من القانون رقم 15-04 المحدد للقواعد العامة للتوقيع والتصديق الالكترونيين ، إذ أكدت على انه لا يمكن تجريد التوقيع الالكتروني من فعاليته القانونية أو رفضه كدليل أمام القضاء بسبب شكله الالكتروني أو أنه لا يعتمد على شهادة التصديق الالكتروني الموصوف أو أنه لم يتم إنشاؤه بواسطة آلية مؤمنة لإنشاء التوقيع الالكتروني .

وقد سبقتها المادة 323 مكرر من التقنين المدني[1] بنصها يُعد الإثبات بالشكل الإلكتروني مكافئًا للإثبات بالكتابة الورقية، وقد كرّس المشرع هذا التوجه من خلال اعتماد مبدأين أساسيين واردين في القانون التوجيهي للجنة الأمم المتحدة للقانون التجاري الدولي (الأونسيترال)، وهما: مبدأ التعادل الوظيفي بين المحررات الإلكترونية والمحررات الورقية، ومبدأ الحياد التقني في ما يتعلق بالتوقيع الإلكتروني. ويقضي المبدأ الأول بوجوب عدم التمييز، من حيث الحجية القانونية، بين التوقيع الإلكتروني والتوقيع التقليدي، متى توافرت في الأول شروط الأمان والوظائف الجوهرية للتوقيع، بحيث يُعتد بهما على قدم المساواة دون تفضيل أحدهما على الآخر. أما المبدأ الثاني، المتعلق بالحياد التقني، فينص على ضرورة عدم حصر التشريعات الوطنية في اعتماد تقنية أو وسيلة إلكترونية واحدة لإتمام التوقيع الإلكتروني، بل ينبغي أن تبقى التشريعات مفتوحة أمام مختلف الآليات والتقنيات، شريطة أن تضمن مستوى كافيًا من الأمان، ويمكن إثباته، دون تمييز مسبق أو تقييد غير مبرر. [2]

ورغم سهولة المبدأين من حيث المفهوم النظري ، إلا انه قد تطرح مسائل عدة في الموضوع و خاصة في ظل تشريعنا الحالي الذي نظم الموضوع بصفة عامة دون تحديد لبعض التفاصيل ، ولعل من أهم المسائل التي تطرح : مسالة عبء إثبات مدى توافر الشروط المطلوبة للاعتداد بالتوقيع الالكترونية والمحددة في التشريع لكي يؤدي الوظائف المتوخاة منه ، فعلى من يقع عبء إثبات توفر هذه الشروط ، ومدى سلطة القاضي في الأخذ بالتوقيع الالكتروني من عدمه. [3]

ان تحديد الطرف المكلّف بالإثبات أولى خطوات تنظيم قواعد الإثبات، إذ يتوقف الفصل في العديد من الدعاوى على معرفة من يتحمل عبء الإثبات من الخصمين. ويُعد من المبادئ الأساسية في هذا المجال أن البيّنة على من ادّعى، حيث يُكلّف بالإثبات من يدّعي خلاف الأصل أو الظاهر أو ما هو ثابت

---

[1]-المادة 323 مكرر من التقنين المدني.

[2]- عبد الرزاق أحمد السهوري ، الوسيط في شرح القانون المدني ، منشأة المعارف ، الجزء الثاني ، الإسكندرية ، 2004 ، ص57 .

[3]- تنص المادة 323 من القانون المدني الجزائري انه على الدائن إثبات الالتزام وعلى المدين إثبات التخلص منه .

قانونًا أو واقعًا. ويقع عبء الإثبات على عاتق المدعي، سواء كان دائنًا أو مدنيًا أو حتى مدعى عليه إذا ادّعى أمرًا يخالف الأصل. في المقابل، فإن من يتمسك بما هو ثابت أصلًا أو ظاهرًا أو قانونًا لا يُطالب بتقديم الدليل، إذ لا يُلزم بالإثبات إلا من ينازع في ذلك الثابت. [1]

من الثابت في مجال المعلوماتية أن طرق إصدار، وتخزين، ونقل الكتابة والتوقيع الإلكترونيين لا تخلو من مخاطر تقنية، ما يستدعي اتخاذ جملة من الاحتياطات لضمان سلامتها ومنع اعتراضها أو التلاعب بمحتواها. وبناءً عليه، فإن عبء الإثبات يقع على من يتمسك بالمحرر الإلكتروني ويحتج بمضمونه، إذ يتعين عليه إثبات أن الأنظمة والتقنيات المستخدمة في إصدار ونقل وتخزين ذلك المحرر تستوفي شروط الأمان التي يفرضها القانون للاعتداد به.

وعليه، ففي حال أنكر من نُسب إليه التوقيع الإلكتروني صحته، فإن عبء الإثبات ينتقل إلى من يدعي صدور التوقيع عنه، ويُطالب بإثبات أن التوقيع مستوفٍ لجميع الشروط القانونية والفنية التي تجعله صحيحًا. ويشمل ذلك إثبات أن التقنية المستعملة تُحدد هوية الموقّع بشكل حصري ودقيق، وأن التوقيع يعبر عن إرادته الحرة والواضحة دون لبس أو قصور تقني، مع ضمان سلامة المحرر من أي تعديل بعد التوقيع عليه، وتمكين كشف أي تغيير قد يطرأ عليه لاحقًا.

وفي حال تحقق كل هذه الشروط، يُعتد بالمحرر الإلكتروني وتوقيعه، وتمنح له حجية مطلقة في الإثبات، وذلك وفقًا لأحكام المادة 327 من القانون المدني [2].

في حال تعذّر إثبات التصرف القانوني بالكتابة الرسمية أو العرفية، يثور التساؤل حول إمكانية اعتبار المحرر غير الكامل بمثابة بدء ثبوت بالكتابة، وهو ما سيتم معالجته في النقطة الموالية. وقد نصت الفقرة الأولى من المادة 335 من القانون المدني الجزائري على أنه" :يجوز الإثبات بالشهادة فيما كان يجب إثباته بالكتابة إذا وُجد مبدأ ثبوت بالكتابة"، وهو ذات المبدأ الذي تقرره المادة 62 من قانون الإثبات المصري، والمادة 1347 من التقنين المدني الفرنسي.

ويُفهم من هذه النصوص أن كل كتابة تصدر عن الخصم، ويكون من شأنها أن تجعل وجود التصرف المدعى به قريب الاحتمال، تُعدّ بدء ثبوت بالكتابة. ويتضح من الفقرة المذكورة أن نطاق هذا المبدأ يقتصر

[1]– عبد الرزاق السهوري ، المرجع السابق ، ص 63 .

[2]– هني بوطيبة جمال ، حجية التوقيع الالكتروني في الإثبات في التشريع الجزائري ، مذكرة ماستر ، كلية الحقوق والعلوم السياسية ، جامعة عبد الحميد بن باديس ، مستغانم 2021 ، ص 67 .

على الحالات التي يُشترط فيها الإثبات بالكتابة أصلاً، أي تلك المتعلقة بمصدر الحق، كما هو الشأن في الحالات المنصوص عليها في المادتين 333 و334 من القانون المدني الجزائري.

وعليه، يشترط لقيام بدء الثبوت بالكتابة توافر عنصرين أساسيين: أن تصدر الكتابة عن الخصم، وأن تكون كافية في حد ذاتها لجعل وقوع التصرف المدعى به قريب الاحتمال، دون أن ترقى إلى مرتبة الدليل الكتابي الكامل.

فالركن الأول لبدء الثبوت بالكتابة هو الكتابة ، وعليه تستبعد الأعمال المادية ، ايجابية كانت أم سلبية، ولو كانت ثابتة بالشهادة و القرائن ، أي أنه لا بد من توافر محرر مكتوب ، غير أنه لا يرقى بذاته إلى مرتبة الدليل الكامل، لعدم اشتماله على الشروط الخاصة التي يتطلبها المشرع في كتابة الورقة العرفية ، كما لو كانت الورقة العرفية غير موقعة ، متى كان مصدرها معروف كان تكون جاءت ضمن مراسلات الخصم ، وتأخذ كلمة " كتابة " بمفهومها الواسع ، بحيث تشمل كل كتابة أيا كان نوعها دفاتر تجارية ، مذكرات خاصة ، رسائل ، كشف حساب [1].

يمثّل الركن الثاني لمبدأ الثبوت بالكتابة ضرورة صدور الكتابة عن الخصم أو عن من ينوب عنه قانونًا، سواء كان صدورها ماديًا بخط يده أو بتوقيعه، أو معنويًا من خلال إملائه لمضمونها، أو تمسكه بمحتواها كما في حال المخالصات الصادرة عن مدينه، أو إذا كانت أقواله مدوّنة في محررات رسمية لا يعتريها شك.

أما الركن الثالث، فيتعلق بكون تلك الكتابة تجعل الواقعة محل الادعاء قريبة الاحتمال، أي أن ترجّح حصولها لا أن تكتفي بإمكان وقوعها فقط. وتُعد مسألة قرب الاحتمال من مسائل الواقع التي تندرج ضمن السلطة التقديرية لقاضي الموضوع، ولا تخضع لرقابة المحكمة العليا.

ومن ثم، فإن مبدأ الثبوت بالكتابة لا يكفي بذاته لإثبات التصرف القانوني أو مضمونه، وإنما يُجيز استخدام وسائل إثبات أخرى لم تكن مقبولة في الأصل، كالشهادة والقرائن. كما أن قبول القاضي للكتابة كمبدأ ثبوت لا يحول دون سلطته في تقدير قيمة باقي الأدلة المعروضة أمامه، لاستكمال وتعزيز هذا الإثبات. فإذا اقتنعت المحكمة بالأدلة المقدّمة، فإن مبدأ الثبوت بالكتابة يرقى إلى مستوى الكتابة الكاملة من حيث قوتها الثبوتية.. [2]

و تطبيقا لتلك الأركان على المحرر الإلكتروني للقول بمبدأ الثبوت بالكتابة :

---

[1]–هني بوطيبة جمال ، المرجع نفسه ، ص 68 .

[2]– هني بوطيبة جمال ، نفس السابق ، ص 68 .

فأول ركن المتعلق بالكتابة الصادرة من الخصم في المحرر الالكتروني يخضع لجملة من الشروط لا بد من تحققها ، وإلا استبعد المحرر على أساس عدم اعتباره كتابة أصلا ، أي أن القاضي يتطرق ابتداء لمدى توافر شروط المادة 323 مكرر 1 ، فيما إذا كانت الكتابة قد أعدت ، و خزنت ، و نقلت في ظروف تضمن سلامتها مع إمكانية تحديد مصدرها ، ثم يتحقق من صدورها من الخصم ويتحقق من احتمال المدعي به .

فلو قدم محرر الكتروني وجد في حاسب خصمه "ب " مكتوب في نظام(Microsoft World) و محمي باستعمال خاصية الحماية التي يوفرها هذا النظام ، باستعمال رقم سري يمنع تغيير مضمون المحرر الذي مفاده أدائه الدين المتجاوز مبلغ 100.000 دينار جزائري ، مع تبيان تاريخ الوفاء ، فهذا رغم أن كل الشروط يظهر أنها متوافرة من كتابة وصدورها من الخصم و قرب احتمال الوفاء ، إلا أنه بالتدقيق في مدى توافر شروط الكتابة نجدها غير متوافرة فخاصية الحماية التي يوفرها النظام باستعمال رقم سري لمنع تغيير مضمون المحرر ، غير آمنة فيمكن اختراق الرقم السري وتحوير مضمون المحرر دون أن يترك ذلك أثرا على المحرر وعليه يجب التصريح بانعدام الكتابة هنا ، وبالتالي عدم النظر في الشروط الأخرى وبالنتيجة استبعاد ذلك المستند الالكتروني من الإثبات. [1]

الفرع الثاني:

حجية التوقيع الالكتروني الموصوف

نصت المادة 8 من القانون 15-04 أن التوقيع الإلكتروني[2] الموصوف يُعتبر التوقيع الإلكتروني الموصوف معادلًا في حجيته للتوقيع الخطي، إذ لا يتطلب إثبات الشروط العامة المتعلقة بنسبة التوقيع إلى صاحبه أو بمدى سيطرته على منظومة إنشائه، طالما قدّم الموقع شهادة التصديق الإلكتروني. فهذه الشهادة تُضفي على التوقيع الإلكتروني صفة الوثوق، من خلال ربطه بشخص الموقع وبياناته الشخصية، مع إمكانية كشف أي تعديل أو تغيير قد يطرأ على المحرر الإلكتروني. وبناءً على ذلك، نتناول حجية التوقيع الإلكتروني الموصوف من خلال النقاط التالية:

1- حجية التوقيع الالكتروني لإثبات مضمون المحرر الالكتروني

تطبيقا لمبدأ التعادل الوظيفي بين المحررات الالكترونية والتقليدية مع مرعاة الخصوصية التي يتمتع بها كل من الشكلين ، وعلى اعتبار أن المحررات الالكترونية تأخذ حكم المحررات التقليدية العرفية،

[1]- هني بوطيبة جمال ، نفس المرجع ، ص 69 .

[2]المادة 8 من القانون 15-04.

يتضح من نص المادة 327 المذكورة أعلاه : بالطبع، إليك إعادة الصياغة القانونية للفقرة بأسلوب واضح ومحكم:

تُعد المحررات العرفية دليلًا كاملًا في الإثبات وتتمتع بحجية مطلقة، غير أن هذه الحجية تظل مرتبطة باعتراف الخصم بصحة التوقيع أو خط اليد أو بصمة الإصبع المنسوبة إليه، أو بإنكاره لها، أو بتصريح الوارث أو الخلف بشأن علمه أو جهله بما نُسب إلى السلف. وتنطبق ذات الأحكام على المحررات الإلكترونية، إذ تمنح حجية مطلقة في الإثبات، ما لم يتم إنكار التوقيع الإلكتروني المرفق بها، ففي هذه الحالة يُعاد النظر في قوتها الثبوتية تبعًا لما يُقدم من أدلة.

وعليه نستنتج أن للمحرر حجية من حيث صدوره ممن وقعه ، وحجية من حيث صحة ما ورد به من مضمون ووقائع ، فمسألة حجية المحرر العرفي التقليدي أو الالكتروني من حيث صدوره ممن وقع عليه وطبقا لنصوص القانون المدني المتعلقة بالإثبات فالمحرر العرفي لا يكون حجة إلا إذا لم ينكره الشخص المنسوب إليه إنكارا صحيحا ، أي انه متوقف على اعتراف من وقعه بصحة هذا التوقيع بعدم إنكاره ، فان اعترف بها أو أكدت كان المحرر العرفي ذو حجية مطلقة بين أطرافه لا يجوز إثبات عكس ما ورد فيه إلا بالكتابة ، إما إن أنكر من نسب إليه المحرر ، أو نفى الوارث أو الخلف علمه بذلك قبل مناقشة موضوع المحرر العرفي فهنا يفقد المحرر حجيته مؤقتا في الإثبات إلى غاية الفصل في أمر الإنكار أو الادعاء بالجهالة ، ويمكن في كل الأحوال دفع كل ذي مصلحة بأن المحرر المحتج به مزور ، أما عن حجية المحرر الالكتروني من حيث مضمونه بعد ثبوت توقيعه من الشخص المنسوب إليه سواء باعترافه به أو لثبوت ذلك بعد الإنكار ، كان للمحرر الالكتروني حجيته من حيث مضمونه ، على أن ثبوت نسبة التوقيع للموقع أو الخط له لا يمنع من الطعن في مضمون المحرر نفسه ، مثلا لو كان مضمون المحرر يتعلق بعقد بيع بين شخصين وأن البائع قبض الثمن وأن المشتري تسلم المبيع فان هذه البيانات يفترض جديتها وحقيقتها وأن ذكرها في المحرر قرينة على صحتها ، ولصاحب التوقيع أن يثبت صوريتها أو أنه لم يقبض الثمن ، لكن لا يجور إثبات ذلك إلا بالكتابة تطبيقا لقاعدة. [1]

لا يجوز الطعن في حجية الكتابة إلا بمحرر كتابي مماثل، فلا يكفي مجرد الإنكار لنقضها، بل يتحمّل من يدعي خلاف ما ورد فيها عبء إثبات ذلك. وبناءً عليه، فإن المحرر الإلكتروني يُعد دليلًا كاملاً ذا حجية مطلقة من حيث نسبته إلى الموقع وصحة مضمونه، ما لم يُطعن فيه بإحدى الطرق القانونية المعتمدة للطعن في المحررات، والتي سنحاول التطرق إليها لاحقًا.

[1]– محمد قاسم ، أصول الإثبات في المواد المدنية والتجارية ، منشورات الحلبي الحقوقية ، 2003 ، ص 17–16 .

2- طرق الطعن في المحررات العرفية

أ-الدفع بالإنكار أو الجهالة :

يجوز لمن نُسب إليه توقيع أو احتُج عليه بسند أن يُنكر صراحة ما ورد فيه، وبموجب هذا الإنكار ينتقل عبء الإثبات إلى الخصم الآخر، الذي يتعيّن عليه، وفقًا للقواعد العامة في الإثبات، إثبات صحة التوقيع ونسبته إلى المنكر. ويشترط في هذا الإنكار أن يكون صريحًا وواضحًا، وأن يُقدَّم قبل الخوض في موضوع الدعوى. كما يجب أن يكون المحرر محل النزاع منتجًا في الدعوى، أي ذا صلة مباشرة ومؤثرة في الفصل في النزاع القائم بين الخصوم.[1]

يُلاحظ أن مبدأ مضاهاة الخطوط يُتصوَّر تطبيقه فقط على المحررات التقليدية، حيث يتم التوقيع أو الكتابة بخط اليد، ما يسمح بإبراز السمات الخاصة لصاحب الخط أو التوقيع، ويُسهل بالتالي التحقق من التطابق بين نمط الكتابة أو التوقيع في مختلف الوثائق الصادرة عن نفس الشخص، حتى في حال محاولته تغيير شكلهما. أما في المحررات الإلكترونية، فإن الأمر يختلف، إذ إن نمط الكتابة والتوقيع يخضع لآليات رقمية لا تعكس الخصائص الشخصية للمرسل، ما يجعل مضاهاة الخطوط غير ممكنة عمليًا، إلا في حالات استثنائية تتعلق بمستخرجات ورقية، مثل رسائل التلكس أو الفاكس.

وبناءً على ذلك، تبرز الحاجة إلى تدخل تشريعي ينظم هذه المسألة بدقة ويضع إطارًا قانونيًا ملائمًا لتسهيل تطبيق النصوص، وضمان فعاليتها، بما يتيح الاستفادة من الإمكانيات التي توفرها التكنولوجيا الحديثة، لاسيما في مجال المعاملات والاستثمارات التجارية، دون إثارة الشك أو الحيرة في كيفية التحقق من نسبة المحرر الإلكتروني إلى من يُنسب إليه، خاصة عند إنكاره له. [2]

انطلاقًا مما سبق، يمكن بحث مدى إمكانية الإنكار في المحررات الإلكترونية في حال اعتماد نظام متكامل. ويُقصد بالنظام المتكامل، اعتماد منظومة مؤمّنة لإنشاء التوقيع الإلكتروني تستوفي شروط الأمان والمطابقة القانونية. وفي هذا الإطار، يُناط بالهيئة الوطنية المختصة باعتماد آليات إنشاء التوقيع الإلكتروني والتحقق منها، التأكد من مدى مطابقة هذه الآلية للشروط المنصوص عليها في المادة 11 من القانون رقم 15-04، والمتعلقة بخصائص الآلية المؤمّنة لإنشاء التوقيع الإلكتروني.

---

[1]- نصت على ذلك المادة 327 من القانون المدني الجزائري وكذلك المواد 164 وما يليها من قانون الإجراءات المدنية والإدارية .

[2]- المادتين 11 من القانون 15-04 المتعلق بالتوقيع والتصديق الالكترونيين .

ويُضاف إلى ذلك، ضرورة حصول الموقع على شهادة تصديق إلكتروني من طرف معتمد، تثبت صحة التوقيع وتمكّن من التحقق من هوية الموقع. ويُستند في التأكد من اعتماد هذا النظام المتكامل إلى البيانات الإلزامية الواجب توفرها في شهادة التصديق الإلكتروني، والتي تم التطرق إليها سابقًا، لما لها من دور في ترسيخ الثقة بالمحرر الإلكتروني وصحة نسبته إلى صاحب ، وبذلك نكون أمام وهو ما اصطلح عليه المشرع الجزائري بالتوقيع الالكتروني الموصوف ، إذ أنه يتم عن طريق مفتاح سري خاص تقع مسؤولية سوء استخدامه على حامله ، بالإضافة إلى أن فك الشفرة يكون بالمفتاح المقابل ، مع الإشارة أن لكل زبون مفتاح خاص وأن لكل رسالة أو محرر الكتروني بصمة خاصة وفريدة ، وكل ذلك يثبت أن الموقع الكترونيا يكون قد تعامل مع المستند الالكتروني فعلا ، وعليه يسهل التحقق من مدى جدية الدفع بإنكار توقيعه لكل هذا لا يعني أن الموقع في حالة حدوث خطأ معين في المنظومة المعلوماتية يبقى عاجزا عن إثبات عدم مهر المحرر بتوقيعه ، أو عدم صحة المحرر المدعي به بل له اللجوء إلى الدفع بتزوير المحرر المقدم وتزوير المحرر الإلكتروني له خصائصه لمجرد إثبات صحة التوقيع الإلكتروني بتوافر أركانه و شروطه تصبح مسألة التزوير مستبعدة كونه كما أوضحنا سابقا فمن وظائف التوقيع الإلكتروني حفظ سلامة المحرر من أي تعديل أو تغيير، و يجعل ذلك قرينة قاطعة على صحة ما جاء فيها، وعليه فيتصور الدفع بالتزوير بأن يدفع باستخدام التقنية المتعلقة به من قبل الغير بإهماله مثلا، أو أن يكون قد سلمه للغير على أساس أحد عقود الأمانة.

المبحث الثاني:

الحماية الجزائية للتوقيع الالكتروني

ان التقدم في الحيازة والزيادة نتج عنه التقدم التكنولوجي في جميع الميادين سواء تجارة الكترونية ...، سوف نتطرق في هذا المبحث إلى مفهوم أنواع وأهداف الجريمة المعلوماتية (المطلب الأول)، وتحديد طبيعتها القانونية وخصائصها وأركانها المطلب الثاني).

المطلب الاول:

الاطار العام للجريمة المعلوماتية

تعددت تعريفات الجريمة المعلوماتية وتباينت فيما بينها ضيقا واتساعا وقد أسفر ذلك على تعذر إيجاد فهم مشترك لظاهرة الجريمة المعلوماتية، وما سيتبع ذلك للوصول إلى إيجاد الحلول المناسبة لمواجهتها.

الفرع الأول :

ماهية الجريمة المعلوماتية

مع دخول الحاسوب والانترنت إلى مجتمعاتنا وفي كافة جوانب حياتنا بدأ يظهر نوع جديد من الجرائم تسمى الجرائم المعلوماتية وبالتالي أصبح هناك حاجة لتعريف هذه الجرائم والتوعية حولها، حيث سنقوم بتعريفها قانونيا وفقهيا.

أولا: التعريف الفقهي

قدّم الفقهاء والباحثون مجموعة واسعة من التعريفات التي تختلف فيما بينها تبعًا لاختلاف المدارس الفقهية والانتماءات الفكرية التي يستند إليها كل اتجاه، إضافةً إلى تنوع المعايير المعتمدة في بناء هذه التعريفات. وقد تم حصر أبرز هذه التعريفات بهدف الإلمام بمختلف الرؤى الفقهية المتعلقة بالموضوع.

ومن بين هذه التعريفات، نجد تلك التي تركز على الوسيلة المستعملة في ارتكاب الجريمة، حيث ينطلق أصحابها من كون الجريمة المعلوماتية تتحقق متى تم استخدام الحاسوب كوسيلة رئيسية في تنفيذ الفعل الإجرامي. ومن أبرز هذه التعريفات، ما ذهب إليه الأستاذ "جون فورستر" الذي عرّفها بأنها: "فعل إجرامي يُرتكب باستخدام الكمبيوتر كأداة رئيسية"، في حين عرّفها "تادمان" بأنها: "جميع أشكال السلوك غير المشروع التي تُرتكب بواسطة الحاسب الآلي"[1].

يشير جانب من الفقه، إلى جانب بعض الهيئات المتخصصة، إلى أن التعريفات المتعلقة بالجريمة المعلوماتية تأخذ في الاعتبار، جزئياً، الخصائص المعرفية والتقنية لمرتكبها. وفي هذا الإطار، عرّفت وزارة العدل الأمريكية، استناداً إلى دراسة أعدها معهد "ستانفورد للأبحاث" وتضمنها دليلها الصادر سنة 1979، الجريمة المعلوماتية بأنها: "كل فعل إجرامي يُرتكب من طرف شخص يمتلك معرفة فنية بالحاسوب تُمكنه من تنفيذه".

وفي ذات الاتجاه، يرى الأستاذ دافيد تومن أن الجريمة المعلوماتية تتمثل في: "كل جريمة يتطلب ارتكابها توفر معرفة تقنية بالحاسوب لدى الفاعل. .[2]

ثانيا: التعريف القانوني

نصّ المشرّع الجزائري على تعريف الجريمة المعلوماتية في المادة 02، الفقرة (أ) من القانون رقم 09-04 المؤرخ في 05 أوت 2009، المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات

[1]– هدى قشقوش، جرائم الحاسب الالكتروني في التشريع المقارن، دار النهضة العربية ، القاهرة، 1992، ص120.

[2]–هشام محمد فريد رستم، العقوبات ومخاطر جرائم المعلوماتية، دار النهضة العربية ، القاهرة، 2000 ، ص 20

الإعلام والاتصال ومكافحتها، حيث اعتبرها تلك الجرائم التي تمسّ بأنظمة المعالجة الآلية للمعطيات، كما هو محدد في قانون العقوبات، أو أي فعل إجرامي آخر يُرتكب أو يُسهل ارتكابه بواسطة منظومة معلوماتية أو نظام للاتصالات الإلكترونية.

وبالاستناد إلى هذا التعريف، وإلى مختلف التعريفات الفقهية المقترحة في هذا المجال، يمكن تقديم تعريف جامع للجريمة المعلوماتية، يأخذ في الحسبان أبعادها التقنية والقانونية، على النحو الآتي:

"الجريمة المعلوماتية هي كل فعل مجرَّم قانوناً يتم باستخدام الحاسوب أو شبكات الاتصالات أو أي وسيلة إلكترونية، سواء باعتبارها أداة لتنفيذ الجريمة أو موضوعاً لها، ويقع هذا الفعل ضمن بيئة رقمية أو إلكترونية تمكّن من ارتكابه أو تسهّله."

ويُظهر هذا التعريف الطبيعة المزدوجة للجريمة المعلوماتية، بوصفها جريمة تنشأ في بيئة افتراضية، وتستهدف المعطيات أو الأنظمة المعلوماتية، أو تُستغل فيها هذه الوسائل لارتكاب جرائم تقليدية بأدوات غير تقليدية. [1]

الفرع الثاني:

خصائص وأنواع الجريمة الالكترونية

سوف نتناول في الفرع أولا الخصائص، ثم الأصناف أو الأنواع .

أولا: خصائص الجريمة المعلوماتية

تتميز الجريمة المعلوماتية بصفة عامة عن الجريمة التقليدية في عدة نواحي، سواء كان هذا التميز في السمات العامة لها أو في الباعث على تنفيذها أو في طريقة هذا التنفيذ ومن أهم خصائصها:

أ- صعوبة اكتشاف الجريمة المعلوماتية؟

تُصنّف الجرائم المرتبطة باستخدام الإنترنت على أنها جرائم خفية ومستترة في غالب الأحيان، إذ قد تُرتكب دون أن يلاحظها الضحية، حتى أثناء تواجده الفعلي على الشبكة. ويرجع ذلك إلى امتلاك الجاني قدرات تقنية عالية تمكّنه من تنفيذ أفعاله الإجرامية بدقة واحترافية. ومن أبرز صور هذه الجرائم: إرسال

[1]-عمار حشمان,الجريمة المعلوماتية في التشريع الجزائري.مذكرة لاستكمال متطلبات شهادة الماستر المهني الطور الثاني .كلية العلوم الاقتصادية و العلوم التجارية و علوم التسيير ،ادارة التحقيقات الاقتصادية و المالية ،جامعة قاصدي مرباح،ورقلة،2019،ص4.

الفيروسات، سرقة الأموال أو البيانات الشخصية، إتلاف المعطيات، التجسس، وسرقة المكالمات، وغيرها من الأفعال التي تتم في البيئة الرقمية وتُلحق أضرارًا بالغة دون ترك آثار واضحة فورًا.[1]

كما أن وسيلة تنفيذها تتميز في أغلب الأحيان بالطابع التقني الذي يضفي عليها الكثير من التعقيد بالإضافة إلى الأحجام عن التبليغ عنها في حالة اكتشافها لخشية المجنى عليهم فقدان عملاتهم فضلا عن إمكانية تدمير المعلومات التي يمكن أن تستخدم كدليل إثبات في مدة تقل عن الثانية.[2]

ب – صعوبة إثبات الجريمة المعلوماتية.

تُرتكب الجريمة المعلوماتية في بيئة غير تقليدية، خارج إطار الواقع المادي المحسوس، حيث تقوم أركانها ضمن نطاق الحاسوب وشبكة الإنترنت، ما يُعقّد مهمة سلطات الأمن وأجهزة التحقيق والملاحقة. ونظرًا للطابع التقني البحت لارتكاب هذه الجرائم، فإن اكتشافها والتعامل معها يتطلبان نفس المستوى من الكفاءة التقنية. وبالتالي، فإن التحقيق فيها يستلزم اتباع أساليب خاصة ومناهج تقنية دقيقة، وهو ما لا يتوافر بالقدر الكافي لدى الجهات الأمنية والقضائية في كثير من الأنظمة، بسبب محدودية المعرفة التقنية لدى هذه الجهات.

ويُبرز هذا الواقع الحاجة الماسّة إلى تخصص تقني فعّال داخل المنظومتين الأمنية والقضائية، من أجل مواجهة هذا النمط المتطور من الإجرام الرقمي، خاصة وأن القوانين التقليدية لم تَعُد كافية لمجابهة الجرائم المعلوماتية، في ظل التسارع الكبير للتطورات التكنولوجية واتساع نطاق استخدام الإنترنت.[3]

ج– أسلوب ارتكاب الجريمة المعلوماتية.

تبرز الجرائم المعلوماتية بصورة أكثر وضوحا في أسلوب ارتكابها وطريقتها، فإذا كانت الجريمة التقليدية تتطلب نوعا من الأسلوب العضلي الذي قد يكون في صورة الخلع أو الكسر كما هو الحال في جريمة السرقة.[4]

د– الجريمة المعلوماتية تتم عادة بتعاون أكثر من شخص.

تتميّز الجريمة المعلوماتية في الغالب بكونها جريمة جماعية تُرتكب بتنسيق بين أكثر من شخص بهدف الإضرار بالجهة المجني عليها. وغالبًا ما يتولى تنفيذها شخص ذو خبرة تقنية عالية في مجال

[1]–محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام الغير مشروع لشبكة الانترنت، دارالنهضة العربية، القاهرة،د ت ، ص32.

[2]–نهلا عبد القادر المومني، الجرائم المعلوماتية،ط2،دارالثقافة للنشر والتوزيع، ص56.

[3]–محمد عبيد الكعبي، المرجع السابق ، ص40.

[4]–نهلا عبد القادر المومني، المرجع السابق، ص56.

الحاسوب والإنترنت، يُكلف بالشق الفني للعملية الإجرامية، مثل اختراق الأنظمة أو زرع البرمجيات الخبيثة. ويُسانده في ذلك شخص آخر من داخل محيط المؤسسة أو من خارجها، يتولى توفير التغطية اللازمة لعملية التلاعب، وضمان تحويل المكاسب غير المشروعة الناتجة عن الجريمة لصالح الجناة، مما يُضفي على هذا النوع من الجرائم طابعًا منظمًا ومعقّدًا يصعب كشفه دون توافر إمكانيات تقنية وتحقيقية متقدمة.[1]

ذ- خصوصية مجرمي المعلوماتية.

يُطلق على مرتكب الجريمة المعلوماتية وصف "المجرم الإلكتروني" أو "المجرم المعلوماتي"، وهو يختلف في صفاته وخصائصه عن المجرم التقليدي الذي يقترف الجرائم الكلاسيكية. ففي حين أن الجرائم التقليدية لا تستلزم بالضرورة مستوى معرفيًا أو علميًا معينًا لدى مرتكبها، فإن الجريمة المعلوماتية تُعد في جوهرها جريمة تقنية وفنية، تتطلب قدرًا من الإلمام بتكنولوجيا المعلومات.

وعليه، فإن المجرم المعلوماتي غالبًا ما يكون من ذوي الاختصاص أو التأهيل التقني في مجال المعلوماتية، أو على الأقل يمتلك حدًا أدنى من المعرفة والمهارة في استخدام الحاسوب والتعامل مع الإنترنت، ما يُمكنه من تنفيذ الأفعال الإجرامية داخل البيئة الرقمية بكفاءة وسرية..[2]

هـ- الجريمة المعلوماتية جريمة عابرة للحدود.

بعد ظهور شبكات المعلومات لم يعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة، فالمقدرة التي تتمتع بها الحواسيب وشبكاتها في نقل كميات كبيرة من المعلومات وتبادلها بين أنظمة يفصل بينها آلاف الأميال قد أدت إلى نتيجة مؤداها أن أماكن متعددة في دول مختلفة قد تتأثر بالجريمة المعلوماتية الواحدة في آن واحد.[3]

ثانيا :أنواع الجريمة المعلوماتية: فهناك عدة أصناف من الجريمة الالكترونية نذكر منها:

1-الجرائم التي تقع على الأشخاص: هي الجرائم التي تنال بالاعتداء أو تهدد بالخطر الحقوق ذات الطابع الشخصي البحث أي الحقوق اللصيقة بالشخص والتي تعتبر من بين المقومات الشخصية وتخرج عن دائرة التعامل الاقتصادي، ومن أهم هذه الحقوق الحق في الحياة والحق في سلامة الجسم وفي الحرية والحق في صيانة الشرف.[4]

---

[1]-محمد عبيد الكعبي، المرجع السابق ، ص42.

[2]-نهلا عبد القادر المومني، المرجع السابق، ص57-58.

[3]عمار حشمان، الجريمة المعلوماتية في التشريع الجزائري ، المرجع السابق، ص 12.

[4]-عمار حشمان، الجريمة المعلوماتية في التشريع الجزائري ، المرجع السابق، ص 05.

أ-الجريمة انتحال الشخصية: هي جريمة قديمة جدا تتمثل صورها في الكثير من الجرائم التي ترتكب بالطرق التقليدية، إلا أنه ومع انتشار شبكة الانترنت فقد أخذ هذا النوع شكلا جديدا وهي انتحال شخصية الفرد على الشبكة الالكترونية واستغلالها أسوء استغلال وذلك بأخذ البيانات الشخصية كالعنوان وتاريخ الميلاد ورقم الضمان الاجتماعي وما شابهها من أجل الحصول على بطاقات ائتمانية وغيره، ومن خلال هذه المعلومات يستطيع المحرم إخفاء شخصيته الحقيقية والتصرف بحرية تحت اسم مستعار، وغالبا ما يتحصل المنتحل على تلك المعلومات عن طريق الكم الهائل من الإعلانات التي تزدحم بها شبكة الانترنت.[1]

ب - جريمة المضايقة والملاحقة: وهو نوع حديث من الجرائم المتزايدة باستمرار مع كل إضفاء وتحديث يطال برامج الحوارات المتبادلة والدردشة، وهي عبارة عن مساحات معروفة في الفضاء الالكتروني تتيح لمستخدميها الاشتراك في محادثات بين بعضهم البعض.

وجرائم الملاحقة تشمل رسائل تهديد وتخويف ومضايقة وقد شبه القضاة هذه الجريمة خارج الشبكات بجرائم التهديد العلني، ولا تتطلب الجريمة المرتكبة عبر الإنترنت أي اتصال مادي بين المجرم والضحية مما يدل أن لها تأثيرات سلبية نفسية فهي لا تؤدي إلى أي تصرفات عنف مادية .[2]

ب-جرائم التغرير والاستدراج: هي من أشهر جرائم الانترنت ومن أكثرها انتشارا خاصة بين أواسط صغار السن ومن مستخدمى الشبكة، وهي تقوم على عنصر الإمام حيث يوهم المجرمون ضحاياهم برغبتهم في تكوين علاقة صداقة أو زواج على الانترنت والجريمة المعلوماتية التي قد تتطور إلى لقاء مادي بين الطرفين، وهذه الجرائم لا تعرف الحدود ولا يمكن حصرها، وهي دون حدود سياسية أو اجتماعية اذ يستطيع كل مراسل عبر الشبكة ارتكابها بكل سهولة وكذلك يقع ضحيتها أي مستخدم حسن النية .[3]

د- جرائم التشهير وتشويه السمعة: مع انتشار الشائعات والأخبار الكاذبة التي تطول وتمس رموز الشعوب سواء كانت تلك الرموز فكرية أو سياسية أو حتى دينية، وقد ظهرت على شبكة الانترنت بعض المواقع والتي جندت نفسها لهدف واحد هو خدمة تلك الشائعات والأخبار الكاذبة وذلك بهدف تشهير وتشويه سمعة تلك الرموز، وكذلك لتسميم أفكار الناس أو محاولة ابتزاز بعض الأشخاص بنشر الشائعات عنهم. وأبرز وسائل

---

[1]-منير محمد الجنبيهي ،ممدوح محمد الجنبيهي، جرائم الانترنت و الحاسب الآلي، ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، 2005، ص42-43.

[2]-محمد أمين أحمد الشوابكة جرائم الحاسوب الأولى والإنترنت دار الثقافة للنشر والتوزيع، الطبعة الأولى، عمان، 2004، ص 45

[3]-عبد الكريم شيباني الحماية الإجرائية والموضوعية للجريمة المعلوماتية، مذكرة لنيل شهادة ماستر، كلية الحقوق والعلوم السياسية، جامعة الطاهر مولاي، سعيدة ، 2016-2015، ص 19.

ارتكاب هذه الجريمة إنشاء مواقع على الشبكة تحتوي المعلومات المطلوب إدراجها ونشرها أو إرسالها عبر المواقع الالكترونية، ومن أمثلتها إرسال الصور الغير اللائقة أو معلومات غير صحيحة.[1]

هـ-الجرائم المخلة بالأخلاق والآداب العامة: ظرًا للطبيعة العالمية لشبكة الإنترنت، التي تتيح الوصول إليها دون قيود جغرافية، فإن المحتوى المعروض عبرها قد يُعد مشروعًا في بعض الدول، بينما يُعتبر جريمة يعاقب عليها القانون في دول أخرى، تبعًا لاختلاف المعايير الأخلاقية والتشريعية. ومن بين هذه الجرائم ما يتعلق بالأفعال المخلة بالآداب والأخلاق العامة، وعلى وجه الخصوص التحريض على استغلال القُصّر في أنشطة جنسية غير مشروعة، أو السعي إلى إفسادهم باستخدام الوسائل الإلكترونية، كالدعوة إلى الانخراط في أعمال فاحشة أو نشر صورهم ومعلوماتهم الشخصية، أو تصويرهم ضمن محتوى إباحي.

وتُعد الأعمال الإباحية من أكثر الجرائم الإلكترونية رواجًا وانتشارًا حاليًا، خاصة في بعض الدول العربية، والأوروبية، والآسيوية. وتشمل هذه الجرائم جميع الأشكال التي تمس الآداب العامة، سواء كانت صورًا، مقاطع فيديو، محادثات نصيّة، أو حتى نشر أرقام هاتفية لأغراض غير مشروعة. وقد ساهمت سهولة استخدام الإنترنت وغياب الحواجز الرقابية في جعل هذه المواد في متناول الجميع، ما يفرض تحديات قانونية وأخلاقية جسيمة على المجتمعات والأنظمة القضائية..[2]

2-الجرائم التي تقع على الأموال: هي جرائم الاعتداء على الأموال والتي تهدد الحقوق ذات القيمة المانية ويدخل في نطاق هاته الحقوق الحق ذو قيمة اقتصادية.

فإذا كان موضوع الاعتداء على الأموال في نطاق ما ينصب على الحاسب الآلي ذاته وما يرتبط به من أسلاك وما يتصل به من ملحقات لأنه هنا لا يثير أي صعوبة في تطبيق النصوص الجزائية التقليدية كون الأمر يتعلق بمال عادي منقول، أما إذا وقع الاعتداء على ما يتعلق بفن الحاسب الآلي من برمجيات ونظم فإن النصوص التشريعية التقليدية قاصرة عن حمايتها لما لهذا المجال من طابع خاص غير تقليدي . [3]

أ-جرائم صناعة ونشر الفيروسات: يُعد الفيروس برنامجًا حاسوبيًا شأنه شأن باقي البرامج الأخرى المثبتة على جهاز الحاسوب، غير أنه يُصمَّم بطريقة خبيثة تمكّنه من التأثير على باقي البرامج والملفات المخزّنة في الجهاز. وقد يقوم الفيروس بنسخ نفسه داخل هذه البرامج، أو بالتسبب في تعطيلها أو حذفها كليًا، مما يؤدي إلى إعاقة أداء النظام وإتلاف البيانات، وفي أحيان كثيرة إلى توقف الجهاز عن العمل بشكل كامل.

---

[1]-منير محمد الجنبيهي ،ممدوح محمد الجنبيهي، المرجع السابق، ص34.

[2]-محمد أمين أحمد الشوابكة المرجع السابق، ص 114

[3]-محمد امين احمد التوابلة المرجع السابق، ص 136.

وأما عن مبدأ عملها فيتحدد طبقا لأسلوب تصميمها، فقد تبدأ بالعمل بمجرد فتح الرسالة الموجودة بها، وقد تبدأ بمجرد تشغيل البرنامج الموجودة عليه، وتعتبر هذه الصناعة من أهم جرائم الانترنت وأكثرها اتساعا وانتشار، ويعود تاريخ الفيروسات لأول مرة في أربعينيات القرن الماضي حين تحدث عنها العالم الرياضي فون نيو مان على صعيد الحاسب الآلي دون الانترنت، ومن أشهرها فيروس رسائل الحب فيروس الدودة الحمراء، وقد أحدث هذا الأخير أعطالا في أكثر من ربع مليون جهاز كمبيوتر في أقل من9 ساعات عام2001.[1]

ب- جرائم الاختراقات: الاختراق هو عبارة عن عملية دخول غير مصرح به إلى أجهزة الغير والشبكات الالكترونية، ويتم هذا الاختراق بواسطة برامج متطورة يستخدمها كل من يملك الخبرة وله القدرة على تخطي أي إجراءات أو أنظمة حماية اتخذت الحماية تلك الحاسبات أو الشبكات.

وتختلف أسباب الاختراق باختلاف أهداف المخترق، فمنهم من يخترق أجهزة البعض أو مواقعهم المجرد الفضول والبعض الآخر لسرقتها، وهذا هو السبب الأبرز الذي يدفع المخترقين إلى الدخول إلى مواقع الحواسيب الأخرى لسرقة معلوماتهم التي قد يكونون قد عرضوها مقابل مبلغ مالي للاطلاع عليها.

وقد يكون السبب تبديل أو تحريف أو تعطيل المعلومات في أجهزة الغير، وهو أخطر أنواع الاختراق ومن أبرز ضحايا الاختراق فهي مواقع الانترنت التي يقوم المخترقون بتحريف تصاميمها ومعلوماتها وهذه العملية تسمى تغيير وجه الموقع .[2]

ج- جريمة تعطيل الأجهزة والشبكات: يطال التعطيل أجهزة الحاسب الآلي عبر برابحها، كما قد يؤدي تعطيل البرامج إلى أعطال فنية تقع على القطع الالكترونية للجهاز والهدف من التعطيل منع الحواسيب والشبكات من تأدية عملها دون أن تتم عملية اختراق فعلية لتلك الأجهزة وتتم عملية تعطيل الأجهزة عن طريق إرسال عدد هائل من الرسائل بطرق فنية معينة إلى الأجهزة أو الشبكات المراد تعطلها وهو الأمر الذي يعيقها عن تأدية عملها .[3]

د-جريمة النصب والاحتيال: أصبح التعاقد عبر الانترنت حاجة وضرورة نظرا لسرعة وسهولة التعامل عبرها، لكن هذه الميزة ما لبثت أن شابتها سلبيات عديدة هي عبارة عن أفعال إجرامية تعرف النصب والاحتيال ومن بينها:

---

[1]-منير محمد الحنبيهي، ممدوح محمد الحنبيهي المرجع السابق، ص 36.

[2]-منير محمد الجنبيهي ممدوح محمد الجنيهي، المرجع نفسه، ص 37.

[3]-عبد الكريم شيباني، المرجع السابق، ص23.

- خرق التعاملات عبر طرق احتيال جديدة تم ابتكارها، وكذلك زادت من وقوع جرائم النصب التي لا يزال يقع فيها عدد كبير من مستخدمي الانترنت.
- إما المظهر الأبرز للاحتيال فهو سرقة معلومات البطاقات الائتمانية واستخدام هذه المعلومات السرقة المبالغ الموجودة داخل حسابات الضحايا، ومرتكبو الجرائم عبر تلك الوسائل يسهل هروبهم وتواريهم لذلك من الصعب جدا ملاحقتهم والقبض عليهم.

المطلب الثاني:

مكافحة الجرائم المتعلقة بالتوقيع الالكتروني في التشريع الجزائري

ان المشرع أخذ على عاتقه حماية المعاملات الالكترونية وذلك من خلال حماية قانونية سواء كانت وقائية أو إجرائية و هذا ما سنحاول التطرق اليه في هذا المطلب، حيث تعددت صور الاعتداءات على التوقيع الالكتروني وهي كالتالي:

الفرع الأول :

الجرائم المتعلقة بالتوقيع الالكتروني والعقوبات المقررة لها

تنص المادة 214/1 من قانون العقوبات الجزائري على أنه: "يعاقب بالسجن المؤبد كل قاض أو موظف أو قائم بوظيفة عمومية ارتكب تزويرا في المحررات العمومية أو الرسمية أثناء تأدية وظيفته.

1- إما بوضع توقيعات مزورة."

و نصت المادة 216/1 من نفس القانون على أنه: "يعاقب بالسجن المؤقت من عشر (10) سنوات إلى عشرين سنة وبغرامة من 1.000.000 دج إلى 2.000.000 دج. كل شخص عدا من عينتهم المادة 215 ارتكب تزويرا في محررات رسمية أو عمومية.

2-إما بتقليد أو بتزييف الكتابة أو التوقيع."

ومن خلال نص المادتين يتضح أن الركن المادي لهذه الجريمة هو تقليد وتزوير التوقيع، بحيث يتخذ الجاني سلوك إيجابي وهو الاعتداء على التوقيع بتقليده وإيجاد صورة طبق الأصل له أو تزويره جزئيا أو كليا.[1]

[1]-رحال بومدين،سعداني نورة ،الحماية الجنائية للتوقيع الالكتروني وفق القانون الجزائري 15_04،قسم الحقوق ،كلية الحقوق و العلوم السياسية ،جامعة طاهري محمد،بشار ، د ت ، ص252.

ويهدف المشرع من وراء المعاقبة على تزوير التوقيع أو المحرر الإلكتروني (شهادة التصديق حماية الثقة المفترضة في هذا التوقيع أو هذا المحرر من العدوان الواقع عليهما باعتبارهما وسيلتي إعلان عن الإرادة.[1]

جدير بالإشارة أن الشهادات المصادق عليها من مؤدي خدمات التصديق الإلكتروني تعتبر وسيلة لاعتماد التوقيعات الإلكترونية. كما يترتب على الشهادات آثارا قانونية تتمثل في إنشاء الالتزامات وإثبات الحقوق بالنسبة الطرفي العقد في التجارة الإلكترونية في حالة اعتماد التوقيع الإلكتروني بينهما. ولذلك فإن تزوير أو تقليد شهادات التصديق على التوقيع الإلكتروني يعادل في خطورته تزوير أو تقليد التوقيع الإلكتروني ذاته .[2]

أما الأستاذان "منير محمد الجنبي" و"ممدوح محمد الجنبي ينفيان عملية تقليد التوقيع الإلكتروني، لأنه حسب رأييهما لا يمكن تقليده، ولكن يمكن استعماله دون علم ورضا صاحبه باعتباره يتم بواسطة منظومة الكترونية تتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها، فيما يقرآن بإمكانية تزوير التوقيع التقليدي عن طريق التقليد مما يعني أن التوقيع المقلد لا يمكن أن يكون بذات التوقيع الأصلي وبالتالي لا يمكن أن يكون متماثلا معه.[3]

وتتم عملية تقليد أو تزوير التوقيع الإلكتروني باستخدام برامج حاسوبية أو أنظمة معلوماتية مخصصة لذلك على غرار البرامج والأنظمة المصممة لكسر الشفرة والوصول إلى الأرقام الخاصة بالتوقيع الإلكتروني. والقيام بنسخها، وإعادة نسخها بعد ذلك .[4]

أما فيما يتعلق بالركن المعنوي فالأكيد أن هذه الجريمة تعتبر من الجرائم العمدية التي تستلزم توافر القصد الجنائي العام المتمثل في عنصريه العلم والإرادة. ويتحقق العلم بإدراك الجاني بفعل تغيير بيانات التوقيع الإلكتروني بذاته أو شهادات التصديق المنشأة له بالتقليد أو التزوير، وهذا العلم مفترض فلا يدفع مسؤوليته عن ذلك بجهله، أضف إلى ذلك يجب أن نتجه إرادة الجاني للقيام بهذا الفعل المجرم قانونا، ولذلك

---

[1]–ثروت عبد الحميد، التوقيع الالكتروني (ماهيته، مخاطره، وكيفية مواجهته، مدى حجيته في الاثبات)، دار الجامعة الجديدة ، الإسكندرية، مصر ، 2007،ص47.

[2]–امين اعزان، الحماية الجزائية للتجارة الالكترونية، أطروحة دكتوراه، جامعة عين شمس ، د ت ، ص245.

[3]–رحال بومدين، سعداني نورة ،المرجع السابق ، ص252.

[4]محمد الشهاوي، شرح قانون التوقيع الالكتروني رقم 15 لسنة 2004، ط1، دار النهضة العربية، القاهرة، مصر، 2010،ص194.

فإن عدم علم الجاني أنه يغير الحقيقة في بيانات التوقيع الإلكتروني تجعله يتمتع بحماية قانونية لانتفاء القصد الجنائي لديه.

يضاف إلى القصد الجنائي العام القصد الجنائي الخاص حيث لا تقوم جريمة التزوير إلا بتوافر نية استعمال التوقيع المزور فيما زور من أجله. [1]

مع التنويه أن استعمال التوقيع المزور يعتبر جريمة مستقلة عن جريمة التزوير، لأن جريمة التزوير تقوم وأن لم يستعمل الجاني هذا التوقيع المزور.

ثانياً: جريمة الإدلاء بإقرارات كاذبة للحصول على شهادة تصديق إلكترونية موصوفة

وفقًا للمادة 66 من القانون رقم 15-04، يُعاقب بالحبس من 3 أشهر إلى 3 سنوات وبغرامة من 20,000 إلى 200,000 دينار جزائري، أو بإحدى هاتين العقوبتين، كل من يقدم معلومات كاذبة للحصول على شهادة تصديق إلكترونية موصوفة[2].

أركان الجريمة:

- **الركن المادي** :يتحقق عند تقديم بيانات غير صحيحة إلى مقدم خدمات التصديق الإلكتروني.
- **الركن المعنوي** :يتطلب توافر القصد الجنائي العام، أي العلم والإرادة في تقديم المعلومات الكاذبة.

ثالثاً: جريمة استخدام شهادة التصديق الإلكتروني الموصوفة لغير الأغراض المخصصة لها

تنص المادة 74 من القانون ذاته على معاقبة كل من يستخدم شهادته الإلكترونية لأغراض غير تلك المخصصة لها بغرامة تتراوح بين 2,000 و200,000 دينار جزائري.[3]

أما عن أركان الجريمة:

- **الركن المادي** :يتحقق عند استخدام الشهادة الإلكترونية في غير الأغراض المخصصة لها.
- **الركن المعنوي** :يتطلب العلم بتجاوز حدود الاستخدام المسموح به والإرادة في ارتكاب هذا الفعل.

[1]-ثروت عبد الحميد، المرجع السابق،ص47.

[2]-إبراهيم بن سطم بن خلف العنزي، التوقيع الالكتروني وحمايته الجنائية، رسالة دكتوراه ، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، 2009، ص111.

[3]-رحال بومدين، سعداني نورة ،المرجع السابق ، ص240.

يُعفى مقدم خدمات التصديق الإلكتروني من المسؤولية عن الأضرار الناتجة عن هذا الاستخدام غير المشروع.

كما ان المشرع عمل على حماية البيانات الشخصية:

تُعد البيانات الشخصية معلومات تتعلق بالفرد وتُستخدم لتحديد هويته، مثل الاسم والعنوان ورقم الهاتف.

صور الاعتداءات على البيانات الشخصية:

أ-جريمة إفشاء سرية البيانات الإلكترونية:

بحسب المادة 70 من القانون رقم 15-04، يُعاقب مقدم خدمات التصديق الإلكتروني الذي يخل بسرية البيانات بالحبس من 3 أشهر إلى سنتين وبغرامة من 200,000 إلى 1,000,000 دينار جزائري، أو بإحدى هاتين العقوبتين.

- **الركن المادي** :يتحقق عند إفشاء البيانات السرية المتعلقة بشهادات التصديق الإلكتروني.
- **الركن المعنوي** :يتطلب العلم بأن هذا الفعل يمثل انتهاكًا للالتزامات القانونية والإرادة في ارتكابه.

ب-جريمة جمع البيانات الشخصية دون موافقة صريحة:

تنص المادة 71 من القانون ذاته على معاقبة مقدم خدمات التصديق الإلكتروني [1]الذي يجمع بيانات شخصية دون موافقة صريحة من المعني بالأمر بالحبس من 6 أشهر إلى 3 سنوات وبغرامة من 200,000 إلى 1,000,000 دينار جزائري، أو بإحدى هاتين العقوبتين.

- **الركن المادي** :يتحقق عند جمع أو استخدام البيانات الشخصية دون موافقة صريحة من صاحبها.
- **الركن المعنوي** :يتطلب العلم بأن هذا الفعل مخالف للواجبات القانونية والإرادة في ارتكابه.

الفرع الثاني:

المتابعة الجزائية لجرائم التوقيع الالكتروني

نظرا لطبيعة الخاصة للجريمة الإلكترونية وما نتج عنها من تساؤلات وتناقضات حول استجابة هذه الجريمة للقواعد الإجرائية التقليدية وبالأخص ما يثار حول قواعد الاختصاص القضائي في الجريمة

[1]-براهمي حنان، جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية ، أطروحة دكتوراه، جامعة محمد خيضر، بسكرة ، الجزائر، 2014-2015، ص155.

المعلوماتية، وكذا المساعدة القضائية الدولية في مجال الإلكترونية وهذا ما سنتطرق اليه في هذا الفرع في عدة عناصر.

أولا: الاختصاص القضائي في الجريمة الالكترونية

حيث نتناول فيه الاختصاص القضائي والمحلي .

1-اختصاص النيابة العامة في تحريك الدعوى العمومية في مجال جرائم الإلكترونية في التشريع الجزائري

يتعين التأكيد هنا بأن الأمر لا يخرج عن نطاق المادة الأولى من قانون الإجراءات الجزائية وفق استثناءات عندها هذا القانون نصه، كما سوف ترى ومن الواضح أيضا إن دور النيابة العامة كما رسمته المادة 29 من قانون الإجراءات الجزائية الجزائري وكذا المادة 36 يكون قد توسع في ظل المستحدثات والتطور الحاصل في مجال الجرائم المنظمة والجرائم عارة الحدود والجرائم الإلكترونية على الأخص سارع المشرع الجزائري بتعديل قانون الإجراءات الجزائية تماشيا مع التطور المعلوماتي الذي لحق بالجريمة، محاولة منه الحد من انتشارها، وذلك في إطار المكافحة الإجرائية لهذا النوع من الإجرام، حيث أنه بتعديلي 01/09 و 04/14 وضع قواعد وأحكام خاصة السلطة المتابعة والاختصاص، العرض منها هو مواجهتها، حيث نصت المادة 329 من قانون الإجراءات الجزائية في فقرتها الأخيرة على جواز تمديد الاختصاص المحلي للمحكمة ليشمل اختصاص محاكم أخرى عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة والجرائم الماسة بأنظمة المعالجة الآلية المعطيات.

ومما يتعين الإشارة إليه أن تحريك الدعوى العمومية في جرائم الانترنت وتقديم الشكاوى بشأنها من قبل المتضررين بات محل اهتمام الهيئات الدولية فالإضافة إلى القرارات الصادرة عن الأمم المتحدة بخصوص الجرائم المتصلة بالكمبيوتر في توصيات المؤتمر الخامس عشر للجمعية الدولية القانون العقوبات الذي عقد سنة 1994 بالبرازيل بشأن جرائم الكمبيوتر، والذي أبرز الوجود المركز العالمي للشكاوي الخاصة بجرائم الأنترنت، حيث يعتبر هذا المركز من أهم المؤسسات التي ظهرت إلى الوجود في مجال مجابهة جرائم الأنترنت الذي تأسس في الولايات المتحدة الأمريكية سنة 1999 .

ومن هذا يتضح أن اختصاص النيابة العامة توسع مجاله ليمتد ويغطي نطاقات أخرى لم لكن مرخصة لها من قبل، إذ أن المادة 37 من ق اج ج. بعد تعديله بموجب القانون رقم 04/14 المؤرخ في 10 نوفمبر 2004 وبعد أن كان اختصاص المحلي لوكيل الجمهورية محصورا في المجالات التالية:

- بمكان وقوع الجريمة .

- بمحل إقامة أحد الأشخاص المشتبه في مساعدتهم في الجريمة بالمكان الذي تم في دائرته القبض على أحد الأشخاص المشار لهم ولو لسبب آخر
- فانه نص على تعديد الاختصاص المحلي لوكيل الجمهورية إلى دائرة اختصاص محاكم أخرى في ابشار جرائم المخدرات والجريمة المنظمة والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات والجرائم تبيض الأموال والإرهاب والجرائم المتعلقة بقوانين الصرف وذلك عن طريق التنظيم[1] .

كما جاء في نص المادة 17 ق ا ج ج وبصدور المرسوم التنفيذي رقم 06/348 المؤرخ في 5 أكتوبر 2006 المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق[2] ليكون بذلك قد شمل الاختصاص المحلي للنيابة العامة كل ربوع الوطني في ما يخص الجرائم المعلوماتية، علما أن المحاكم التي تم تمديد اختصاصها أصطلح على تسميتها في التشريع الجزائري بالأقطاب أو محكمة القطب .

والنيابة مجال اختصاص واسع جدا في إطار البحث والتحري عن الجرائم الإلكترونية ومنح الإذن بالتفتيش والقيام باعتراض المراسلات وتسجيل الأصوات والنقاط الصور كما هو منصوص عليه في المادة 65 مكرر 5 من ق اج ج وسوف يأتي شرحه، وهذا بالإضافة إلى استعمال التقنيات المخزنة وكذا حجز هذه المعطيات هذا فضلا عن اتخاذ التدابير الملائمة والتحفظية في إطار المساعدات الدولية المتبادلة في مجال الجريمة المعلوماتية .

2- الاختصاص المحلي القاضي التحقيق في جرائم الإلكترونية

من المعلوم أن المشرع الجزائري سار بوتيرة متسارعة على خطى التشريعات العالمية في إطار مواكبة التطور الحاصل في مضمار القانون المجابهة التطور الحاصل في مجال الإجرام بصورة الحديثة لا سيما ما تعلق بالجريمة المنظمة والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات[3]، وفي هذا الاتجاه جاء تعديل قانون الإجراءات الجزائية بموجب القانون رقم 04/014 المؤرخ في 10/11/2004 ومس التعديل المادة 40 من قانون أ ج ج لتصبح كما يلي :

[1]-زليخة زيدان، الجريمة الالكترونية في التشريع الالكتروني الجزائري والدولي، دار الهدى للطباعة والنشر والتوزيع، عين مليلة، الجزائر ، 2011،ص111.

[2]-المرسوم التنفيذي رقم 06/343 المؤرخ في 115/10/2006 المتضمن تمديد الاختصاص المحلي البعض المحاكم ووكلاء الجمهورية قضاة التحقيق.

[3]-زبيجة زيدان، المرجع السابق، من 113 و 114

يتحدد اختصاص قاضي التحقيق محليا بمكان وقوع الجريمة أو محل إقامة أحد الأشخاص المشتبه في مساهمتهم في اقترافها أو بمحل القبض على أحد هؤلاء الأشخاص حتى ولو كان هذا القبض قد حصل لسبب آخر[1] .

يجوز تمديد الاختصاص المحلي القاضي التحقيق إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم، في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبيض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف

ومن الملاحظ أن تمديد اختصاص المحلي القاضي التحقيق مشمولا كما هو الشأن بالنسبة النيابة العامة بأحكام المرسوم التنفيذي رقم 06/348 المؤرخ في 05/10/2006 وقد حددت المادة الأولى من المرسوم المشار له مجال الاختصاص المحلي المحدد في النطاق الأقطاب القضائية المحددة في المواد 5432 من نفس المرسوم في الجرائم المذكورة سابقا وما بهمنا في الموضوع هو ما يتعلق بالجرائم الماسة بأنظمة المعالجة الآلية المعطيات .

3- الصلاحيات المكانية للضبطية للشرطة القضائية في الجرائم المعلوماتية

من الواضح أن المشرع الجزائري يكون قد سارع إلى تدارك النقص وسد الفراغ القائم بخصوص مجلات التحقيق الابتدائي إثر التطور الذي عرفته الجريمة لاسيما بأشكالها الحديثة كما هو الحال في الجرائم الإلكترونية لذلك جاءت تعديلات قانون الإجراءات الجزائية المتعاقبة لاسيما التعديل الذي جاء به القانون 06/22 المؤرخ في 20/12/2006 والذي مند من صلاحيات الضبطية القضائية ووسع دائرة اختصاصها ودعمه في ذلك القانون رقم 09/04 المؤرخ في 05/08/2009 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بالتكنولوجيات الإعلام والاتصال ومكافحتها كما سوف ترى.[2]

اناط القانون الجزائري بالضبطية القضائية مهمة البحث والتحري عن الجرائم المحددة في قانون العقوبات تماشيا مع المبدأ الدستوري المتعارف عليه " لا جريمة ولا عقوبة إلا بنص [3]، وذلك في مرحلة أولية قبل أن يباشر بشأنها التحقيق القضائي، ويتضح من نص المادة 12 قانون اج ج أن مناط البحث عن الجرائم بالنسبة للضبطية القضائية ينحصر في جمع الأدلة والبحث عن مرتكبي تلك الجرائم فإذا ما ابتدأ

[1]-المادة 40 من ق ا ج ج المعدل بموجب القانون رقم 04-014 المؤرخ في 10-11-2004.

[2]-زبيجة زيدانن المرجع السابق، ص155.

[3]-المادة 46 من الدستور 1990.

التحقيق القضائي تقلص دورها، لينحصر في تنفيذ طلبات جهات التحقيق الفضائي وانجاز ما توجه إليهم من طلبات ويدير وكيل الجمهورية إدارة الضبط القضائي.

كما نصت عليه المدة 185 مكرر من قانون اج ج في إطار الصلاحيات المحددة بنص المادة 36 من قانون (ج ج وكل ذلك تحت إشراف النائب العام وتحت رقابة غرفة الإتهام بدائرة اختصاص المجلس التابعين له، وفقا لأحكام المادة 206 من قانون الإجراءات الجزائية.

والمعلوم أن ضباط الشرطة القضائية نوعان : ويتمثل النوع الأول في هم الذين يتمتعون بإختصاص عام ويختصون بإجراءات الاستدلال بشأن للجرائم المنصوص عليها في قانون العقوبات، أما النوع الثاني فهم ذو الاختصاص النوعي المحدود بخصوص نوع معين من الجرائم حددها القانون على سبيل الحصر

أما ما يهمنا في الموضوع هو دور الضبطية ومجال اختصاصها فيما يتعلق بالجرائم. المعلوماتية، وعليه فإن الاختصاص الإقليمي الضباط الشرطة القضائية في مجال الجرائم المعلوماتية[1]، حسب ما نصت عليه المادة 16 قاح بالقول :" يمارس ضباط الشرطة القضائية اختصاصهم المحلي في الحدود التي يباشرون ضمتها وظائفهم المعتادة . [2]

إلا أنه يجوز لهم – في حالة الاستعجال – أن يباشروا مهمتهم في كافة دائرة اختصاص المجلس القضائي الملحقين به، وكذلك في كافة الإقليم الوطني إذا طلب منهم ذلك من القاضي المختصين قانونا

غير أنه يتعلق ببعث ومعاينة جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات والجرائم تبيض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف، يمتد اختصاص ضباط الشرطة القضائية إلى كامل التراب الوطني

ثانيا: أساليب التحري والتحقيق والاثبات في الجريمة الالكترونية.

الجريمة الإلكترونية تمتاز بخصائص وعناصر تميزها عن الجرائم التقليدية المنصوص عليها في القوانين، فأن قواعد هذه القوانين تبدو قاصرة إزاء ملاحقة مرتكب الجريمة الإلكترونية وهذا ما يبرز كثمر واقع مسألة صعوبة جمع الاستدلالات و الأدلة في جريمة المعلوماتية وأيضا تطبيق الإجراءات الجنائية التقليدية، وعلى هذا الأساس .

1-أساليب التحري والتحقيق في الجريمة الإلكترونية

[1]-زبيجة زيدان، المرجع السابق ، ص166-177.

[2]-المادة 16 من قانون الإجراءات الجزائية الجزائري.

لم يعرف المشرع الجزائري عن القواعد العامة المنصوص عليها في قانون الإجراءات الجزائية لكنه أرسى قواعد جديدة ذات طبيعة خاصة كان من اللازم أن تلد مع التطور الحاصل في حقل الجريمة الإلكترونية الظاهرة حديثة وبهذا الصدد جاه القانون رقم 09/04 المؤرخ في 2009/08/05المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها ومنها ما نصت عليه المادة 03 منه مما تتطلبه مستلزمات التحريات والتحقيقات الفضائية كما سيأتي ذكره.

أ- مراقبة الإتصالات الإليكترونية .

نص القانون رقم 09/04 المؤرخ في 05/08/2009 والمتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها في المادة 03 منه على ما يلي مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والإتصالات يمكن المقتضيات حماية النظام العام أو المستلزمات التحريات أو التحقيقات القضائية الجارية وفها للقواعد المنصوص عليها في قانون الإجراءات الجزائية في هذا القانون وضع الرتيبات تقنية المراقبة الإتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام باجرءات التفتيش والحجز داخل منظومة الإلكترونية .[1]

ومن الواضح أو المراقبة الإتصالات عندها القانون على سبيل الاستثناء وفي حالات محددة حصرها في المادة 04 من القانون المشار له وهي :

- الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة .
- في حالة توفر معلومات عن احتمال إعتداء على منظومة معلوماتية على نحو يهدد النظام العالم أو الدفاع الوطني أو المؤسسات الدولة أو الاقتصاد الوطني
- المقتضيات التحريات والتحقيقات الفضائية. يكون من الصعب الوصول إلى نتيجة لهم الأبحاث جارية ويكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإليكترونية
- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.[2]

والملاحظ أن المشرع ونظرا لما يترتب عن تطبيق هذه التدابير ميدانيا من مساس بحرية الحياة الخاصة وخصوصيتها وهي مقدمة ومحمية دستوريا، كما أثير لها سابقا فإنه ربط القيام بها بشرط الحصول على إذن مكتوب من السلطة القضائية المختصة .

[1] المادة 03 من القانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة لتكنولوجيا الاعلام والاتصال ومكافحتها.

[2] المادة 04 من القانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة لتكنولوجيا الاعلام والاتصال ومكافحتها.

ومن المعلوم أن الرسالة الإلكترونية ذات طابع خاص لكنها لا تختلف عن الرسالة الورقية من حيث حفظها أو الاستغناء عنها وإعمالها، ولكن ما يتميز الرسالة الإلكترونية اله .

يمكن الوصول إليها عن طريق صناديق البريد الخاصة أو الملفات المحفوظة الرجوع إلى سلة المهملات ومن أجل التحقيق الذي يجري بغرض ضبط المرسلات الإلكترونية فإنه يستلزم الولوج إلى البريد الالكتروني (Email)[1]، وبعد تحديد صندوق البريد للملهم المشكو منه يتمحور العمل حول ثلاث (3) عناصر وهي : الوارد (IN) الصادر (OUT)، الحفظ وسلة المهملات (TRASH) .

فينك يمكن مراجعة قائمة الرسائل التي وصلت إلى المشكو منه في الوارد والعكس بالنسبة المراسلة منه على القائمة الصادرة وكذا الشأن بالنسبة للرسائل المحفوظة أو المهملة غير أن ما يجب تأكيده هذا هو أن المشرع ونظرا الحساسية الموضوع والذي يعد مرتبطا بقدر كبير بذاتية الأشخاص فقد جعل تدابير وإجراءات التحقيق تحت طائلة المسؤولية الجزائية عندما نص في المادة 4 من القانون 09/04 فترة (2) والأخيرة على أن الترتيبات التقنية الموضوعية للأعراض المنصوص عليها في الفقرة (1) من نفس المادة موجهة حصريا للتجميع وتسجيل محليات ذات صلة بالوقاية من الأفعال الإرهابية والاعتداءات على أمن الدولة ومكافحتها وذلك تحت طائلة العقوبات المنصوص عليها في القانون العقوبات بالنسبة للمساس بالحرية الخاصة للغير[2] وهذا ما نص عليه الدستور الجزائري في المادة 39 من بالقول: " بسرية المراسلات و الإتصالات الخاصة بكل اشكالها مضمونة .[3]

وكذلك تم ضمان هذا المبدأ في الإعلان العالمي لحقوق الانسان الصادر عن الجمعية العامة للأمم المتحدة في 10-12-1948 في المادة 12 على :" انه لا يجوز ان يتعرض احد لتدخل تعسفي في حياته الخاصة او مراسلاته و لكل شخص الحق في الحماية القانونية ضد هذا التدخل.[4]

ب- تفتيش المنظومة المعلوماتية .

تصل القانون 09/04 في المادة 15 منه على أنه يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية الدخول بغرض التفتيش ولو عن بعد إلى :

- منظومة معلوماتية أو جزء منها وكذا المعطيات الإلكترونية المخزنة فيها .

---

[1]-البريد الالكتروني : و هو ارسال واستقبال الرسائل الالكترونية عن طريق شبكة الانترنت، عن الأستاذ زبيجة زيدان، المرجع السابق، ص128.

[2]-زبيجة زيدان، المرجع السابق، ص128و 129.

[3]-المادة 39 من الدستور الجزائري بسنة 1996.

[4]-المادة 12 من الإعلان العالمي لحقوق الانسان الصادر عن الجمعية العامة للأمم المتحدة في 10-12-1948.

- منظومة الإلكترونية.

يلاحظ إذن بأن التفتيش في الوضعيات المشار لها يأخذ متمنين فهو إما أن يكون عملا من أعمال التحقيق تقوم به السلطات القضائية المخلصة وإما يكون من أعمال الاستدلال يقوم به ضباط الشرطة القضائية بناء على أمر تصدره السلطة المختصة في كلتا الحالتين فإن المستهدف هنا هو جهاز الكمبيوتر (الحاسوب بمكوناته المادية والمعنوية والحاسوب كما هو معروف يتكون من مكونات مادية، وهي مجموعة وحدات لكل منها وظيفة معينة وهي متصلة ببعضها في شكل نظام متكامل منها وحدات الادخال ومهمتها استقبال البيانات الإلكترونية والغير المعالجة ولها مهام أيضا داخل جهاز الحاسوب فهي تمر إلى الوحدات الذاكرة للمعالجة أو التخزين ووحدة الذاكرة هي التي تقوم بتخزين البرامج والمعلومات وبما تحتويه من ذاكرة رئيسته وعشوائية وذاكرة القراءة ثم وحدة الحاسب والمنطق، أما وحدة الإخراج فتحتوي على أجهزة الشاشة والطابعة ومشغلات الأقراص، أما المكونات المعنوية للجهاز الكمبيوتر والتي تسمى أيضا بالكيانات المنطقية وهي مجموعة البرامج والوثائق المتعلقة بتشغيل وحدة معالجة البيانات.

ومما سبق يمكن القول بأن التفتيش وعند ما يستهدف الكيانات المادية للحاسوب لا يشكل أي عائق إذ أنه من السهولة بمكان ضبط الأجهزة وحجزها أو إتلافها وإنما الإشكال بلور عند ما ينصب التفتيش على المكونات الكمبيوتر المعنوية أو المنطقية كالبرامج وقواعد البيانات ذلك أن التفتيش عن هذه البيانات يتطلب الكشف عن الرقم السري (CODE) المرور إلى الملفات وكذا الكلمات السر أو الشفرات أو ترميز البيانات.[1]

3- إجراء الحجز داخل المنظومة المعلوماتية

تجدر الإشارة إلى القول بأن حجز الأشياء المادية كالمعدات والأوراق والمستندات بعد شيئا سهلا وغير مثير الآية إشكاليات في نظر القانون، غير أنه ليس من السهل أبدا توقيع الحجز داخل منظومة معلوماتية ذلك أن المعلمات في الأصل شيء معنوي .

وقد اختلفت التشريعات العالمية حول إمكانية حجز الكيانات الغير المادية المخزنة في برامج وذاكرة الحاسوب .

و عليه فقد اعتبر البعض أنه لا يسرع ضبطها إلا بعد تحويلها إلى كيان مادي كطباعتها عبارة عن نبضات الالكترونية ممغنطة، ورأى اتجاه أخر أن المعلومات في حالتها لا تقبل التملك ولا يمكن أم يكون محلا للإعتداء ولا محلا للملكية الفكرية[2].

[1]-زبيجة زيدان، المرجع السابق، ص131.

[2]-هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية ، المرجع السابق، ص596

غير أن المشرع الجزائري وقبل صدور القانون 19/04 كان قد أضفى حماية قانونية القواعد البيانات بموجب الأمر رقم 003/05 المؤرخ في 19/07/2003 المتعلق بحقوق المؤلف والحقوق المجاورة له، واعتبر قواعد البيانات من المصنفات المحمية .

وفي إطار الحماية البيئة الجنائية لحقوق المؤلف وطبقا الأحكام المواد 145/146 من الأمر 05-03 – يتولى ضباط الشرطة القضائية أو الأعوان المخلفون التابعون للديوان الوطني الحقوق المؤلف والحقوق المجاورة له ، معاينة المساس بحقوق المؤلف كما يتولون بصفة تحفظية حجز دعائم المصنفات ووضعها تحت حراسة الديوان، وتفصل الجهة القضائية في طلب الحجز التحفظي خلال 03 أيام من تاريخ إخطارها .

وعلى الوجه العموم فأن المشرع الجزائري انجاز إلى الاتجاه القاتل بإمكانية حجز المعلومة طبقا للأحكام المادة 16 من القانون 09/04 حيث يمكن حجز المنظومة الإلكترونية برمتها إذا كان ضروريا والمصلحة التحقيق وذلك بعد نسخها على دعامة مادية كطبعها على الورق أو حيطها على الشاشة وضبط الإدلة عن طريق الحجز المعطيات أو البيانات يجري وفقا لمقتضيات قانون الإجراءات الجزائية ، بالإضافة إلى التدابير أخرى منها المصادر للأجهزة والبرامج والوسائل المستخدمة مع إغلاق الموقع الجريمة قد نص عليها القانون العقوبات في مادته 394 مكررة ،وقد نصت المادة 84 من أ ج ج على ضوابط المتعلقة بالأدلة منها :

- الإطلاع على المستندات المبحوث عنها وذلك مقول القاضي التحقيق أو ضابط الشرطة القضائية الذي أنابه عنه فقط .
- الاحترام التام لمقتضيات وضرورات التحقيق وعلى الأخص ضمان سر المهنة وحقوق الدفاع.
- وعلى الفور يتم فرز الأشياء المضبوطة ووضعها في أحرار مختومة حيث لا يتم فتحها إلا بحضور الملهم مصحوبا بمحامية حسب المادة 84 ف أ ج ج .[1]

4- التزامات مقدمي الخدمات في مساعدة السلطات

بموجب المادة 10 من القانون 09/04 الزمن مقدمي الخدمات بتقديم المساعدة للسلطات المكلفة بالتحريات القضائية والتفتيش، كما الزمتهم أيضا يكتمان السر بخصوص العمليات التي ينجزونها يطلب المحققين وما تحصل عن ذلك من المعلومات، وذلك تحت طائلة العقوبات التي يقررها القانون في حالة إنشاء أسرار التحقيق، ويطلق على مقدمي الخدمات في مجال الانترنت التسمية الوسائط في خدمة الأنترنت ويمكن دورهم في تمكين مستخدم الأنترنت من الدخول إلى الشبكة والإطلاع عليها عما يبحث عنه، وقد عرفت المادة الأولى الفقرة الثالثة من الإتفاقية الأوروبية لمكافحة جرائم الإلكترونية التي تم إقرارها في

[1]- المادة 10 من القانون 09/04

بودابست لسنة 2001 :" عرفت مزودي الخدمات بأنهم كل شخص طبيعي أو معنوي يقوم بتزويد المستخدمين بالخدمات التي تمكن وتسهل الاتصالات بين أجهزة الكمبيوتر وكذلك كل من يتولى معالجة العمليات المخزنة نيابة عن المزود الخدمة .[1]

لعل هذه هي أهم إجراءات البحث والتحري في الجريمة الإلكترونية التي تطرقنا إليها بشكل مختصر لأنه لا يسعنا التفصيل فيها كلها التي تطرقنا إليها بشكل مختصر لأنه لا يسعنا التفصيل فيها كلها وذلك لتعددها، علما أن ما قدمناه في هذا المطلب كانت عبارة عن الإجراءات جاءت في القانون 04:09 سابق الذكر

يضاف إلى ذلك ما نصت عليه المادة 65 مكرر 5 من قانون الإجراءات الجزائية المتمثلة في مايلي:

-**اعتراض المراسلات التي يتم عن طريق وسائل الاتصال السلكية واللاسلكية :** والتي يتم عن طريق وسائل الإتصال السلكية واللاسلكية وذلك بواسطة ترتيبات تقنية يتم وضعها دون موافقة المعينين، ومن أجل التصنت والنقاط وبنت بت وتسجيل الكلام المتفوه به بصفة سرية من أجل تحصيل الدليل .

-**اعتراض البريد الإلكتروني :** باعتباره نظام التراسل باستخدام شبكات الحاسب يستخدم كمستودع لحفظ المستندات. والأوراق والمراسلات التي تتم معالجتها رقميا، حيث يتم اعتراضه إلا بإذن من وكيل الجمهورية في إطار التحري والتحقيق الإبتدائي.

- **التقاط الصور :** ويندرج ذلك تحت طائفة الترتيبات التقنية التي تهدف إلى النقاط الصور الشخص أو لعدة أشخاص يتواجدون في مكان خاص ودون الأماكن العامة حسب المادة 65 من ق اج ج .

-**إجراءات التسرب:** يعتبر هذا الإجراء مستحنا في مجال التحريات والتحقيقات وقد نعم عليه المشرع في المائة 65 مكررة من ق اج ج ، وكنك في المادة 65 مكرر 11 بموجب التعديل بالقانون رقم 06/22 المؤرخ في 20/12/2006، ويقصد به قيام ضباط أو عون الشرطة القضائية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة باهامهم أنه فاعل معهم أو شريك لهم[2] .

ثالثا : اساليب الإثبات في الجريمة المعلوماتية

يعتمد ضبط الجريمة وإثباتها في المقام الأول على جمع الأدلة التي حددها المشرع واعترف لها بالقيمة القانونية، وتتمثل وسائل الإثبات الرئيسية في الجريمة الإلكترونية في المعاينة والخبرة وهذا ما أخذت به معظم التشريعات الدول، أما التفتيش فقد أدرجه المشرع الجزائري بموجب القانون 09/04 كأسلوب التحري والتحقيق أكثر منه كأسلوب الإثبات أما الأساليب الأخرى المتمثلة في إجراءات الاستجواب والمواجهة وسماع الشهود

[1]-زبيجة زيدان، مرجع نفسه، ص153.

[2]-زبيجة زيدان، المرجع السابق، ص157.

علم التطرق إليها على أساسها أنها إجراءات خاصة بالأفراد والتم في مواجهة البشر وليست فنية كما هو الحال بالنسبة للأسلوب المعاينة والخيرة، بالإضافة إلى تطرقنا إلى دليل آخر مستحدث يتناسب مع الطبيعة الخاصة للجريمة الإلكترونية وهو اعتماد الدليل التقني أو الإلكتروني في إثبات، وهذا ما سوف نتطرق في الفروع الآتية :

المعاينة أهمية بالغة في قبلة المعاينة وفي اقتناع المحكمة في كثير من القضايا، إلا أنه يمكن القول أن السلطات المختصة التي تقوم بإجراءات المعاينة أو التي تتكفل بها تواجهها صعوبات في بعض الأحيان، كون أن الجرائم الالكترونية لا تختلف اثارها مادية وقد تطول الفترة الزمنية بين وقوع الجريمة واكتشافها مما يعرض الآثار الناجمة عنها إلى المحور أو التلف أو العبث بها [1]:

وحتى يكون للمعاينة في الجرائم المتعلقة بشبكة الانترنت قائدة في كشف الحقيقة عنها و عن مرتكبيها ينبغي مراعاة عدة قواعد وإرشادات فنية أبرزها ما يلي :

- تصوير الكمبيوتر وما قد يتصل به من أجهزة بدقة تامة .
- ملاحظة والثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام ...
- التحفظ على المحتويات سلة المهملات
- التحفظ على المستندات الإدخال والمخرجات الورقية الكمبيوتر ذات صلة بالجريمة لرفع البسمات والتي قد توجد بها[2] .
- قصر مباشرة المعاينة على فئة معنية من الباحثين والمحققين الذين تتوافر لديهم الكفاءة العلمية والخبرة الفنية في مجال الكمبيوتر والشبكات والنظم المعلوماتية[3] .

وما هو جدير بالذكر أن المعاينة قد تكون العمل في بعض أنواع الجرائم الإلكترونية والتحقق المعاينة لابد من وجود مسرح جريمة وهذا ما يصعب تحديده وصعوبة الحفاظ على الآثار المادية أن وجدت، وتكون عقبة الأساسية أمام المعاينة في الجريمة الإلكترونية عندما ترتكب داخل الفضاء المعلوماتي، فالمحقق بتعامل مع نبضات الكتر ومغناطسية وبيانات مخزنة في نظام المعلوماتي.

[1]–هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية ، المرجع السابق، ص59 .

[2]–هشام رستم، قانون العقوبات والمخاطر تقنية معلومات، المرجع السابق، ص126–127.

[3] Taylor ,R, computer crime, criminal investigation edited, « by Charles Swanson ,N, chamelin and L. Teritto hill,inc.5 edition,1992,p450.

ولذلك تقتضي المعاينة جهات قضائية مختصة بها مؤهلة وتمتع بالخبرة في مجال هذه التقنية، حيث يقوم المحققين بالإطلاع على مختلف الوثائق المحفوظة والمراسلات الإلكترونية المرتكبة في الجريمة وفك الشفرات واقتفاء أثر الإتصلات الإليكترونية من جهاز الحاسب الخاص بالجاني وكذا الخاص بالضحية، حيث تستخدم كل من الإجراءات كدليل وكإثبات للجريمة المعلوماتية، ومن أمثلة فائدة المعاينة التي أتت بنتيجة ، وهو ما قامت به الشرطة الفرنسية في مداهمة منزل شخص كان يستغل الأطفال عن طريق الأنترنت ونشر صور إباحية فتمت المعاينة وثم القبض على الجاني وحجز مختلف الأجهزة المتصلة بالإنترنت الخاصة بجهازه، ما يمكن قوله ان المعاينة تحتاج إلى الضبطية قضائية مؤهلة لهذه التقنية مع التوصية في إعادة النظر في التشريع الذي ينظمها وهذا الأمر أضحى ضرورة لابد منها من أجل فتح المجال العمل الإستدلالي[1] .

2- إعتماد الخبرة في الإثبات الجريمة المعلوماتية

- تعريف الخبرة

يقصد بالخبرة – بصفة عامة المهارة المكتسبة في تخصص معين سواء بحكم العمل في ذلك التخصص لمدة زمنية طويلة أو نتيجة دراسات خاصة تلقاها أو نتيجة الإثنين معا أي العمل والدراسة ، ومن هنا يطلق على ذوي هذه المهارات "بالخبراء " .[2]

والخبرة هي الوسيلة من الوسائل الإثبات التي تهدف إلى الكشف بعض الدلائل أو الأدلة أو تحديد مدلولها بالإستعانة بالمعلومات العلمية والتي لا تتوفر سواء لدى المحقق أو القاضي، فهي بحث مسائل مادية أو فنية يصعب على المحقق أن يثبت طريقة فيها ويعجز عن جمع الأدلة بالنسبة لها بالوسائل الأخرى للإثبات، وتكمن أهمية الخبرة في أنها تنير الطريق لجهة التحقيق والقضاء ولسائر السلطات المختصة بالدعوى الجزائية لتحقيق العدالة في المجال الجزائي، لذا فقد اهتم المشرع الجزائري بالإستعانة بالخبراء لجهات التحقيق، وأجاز للمحكمة تعيين الخبراء سواء من تلقاء نفسها أو بناء على طلب الخصوم. [3]

- تعريف الخبير

[1]–محمد أمين الرومي، جرائم الكمبيوتر وانترنت دار المطبوعات الجامعية، الإسكندرية، سنة 2003 ص 139.

[2]–خالد الممنوح إبراهيم، المرجع السابق، ص 283

[3]–رشيدة بوكر، المرجع السابق، ص 424

الخبير هو شخص مختص فنيا في مجالات مختلفة ومتنوعة سواء كانت فنية أو علمية أو غيرها من المجالات الأخرى، ويستطيع بما له من معلومات وخبرة إبداء الرأي في أمر من الأمور المتعلقة بالقضية والتي تحتاج إلى الخبرة فنية. [1]

وتجدر الإشارة في هذا الإطار، أن بعض الفقه يرى أنه لا يشترط في الخبير المنتدب أن يكون متخرجا من معاهد أو الجامعات المتخصصة في دراسات الحاسوب والأنترنت بل يكفي اكتسابه مهارة موهبة إستعمال الحاسوب والأنترنت و التعامل مع تقنية المعلومات .[2]

- أهمية الخبرة في مجال الجريمة الإلكترونية .

تكتسب الخبرة الفنية في جريمة الإلكترونية أهمية بالغة نظرا لأن الحاسبات وشبكات الإتصال بينها على أنواع ونماذج متعددة كذلك فأن العلوم والتقنيات المتصلة بها تنتمي إلى تخصصات علمية وفنية دقيقة ومتنوعة والتطورات في مجالها سريعة ومتلاحقة لدرجة قد يعصب معها على المتخصص تتبعها وإستعابها [3]، والاستعانة بخبير فني في المسائل الفنية البحثة خاصة في مجال الجرائم الإلكترونية فهو أمر وجوبي، لأن الأمر يتعلق بمسائل معقدة ومحل الجريمة فيها غير مادي ولا يكشف عن غموضها إلا متخصص وعلى درجة كبيرة من التميز.

و كما أن عملية تجميع الدليل الرقمي تعد من أصعب الأمور التي تواجه الخبير التقني في مجال الجريمة الإلكترونية ، لذلك كان لزاما عليه إتباع خطوات وأساليب علمية تتناسب مع البيئة التي يتواجد بها هذا النوع من الدليل[4] .

وبدا من المعلوم أن هناك حاجة دائمة إلى خبراء وفنيين عند وقوع الجريمة المعلوماتية وأن نجاح الاستدلالات وأعمال التحقيق في هذه الجرائم يكون مرتهنا بكفاءة وتخصص هؤلاء الخبراء، وهذا ما يدعو إلى ضرورة تأهيل رجال الضبط وسلطات التحقيق في الجرائم الإلكترونية لنجاح تحقيق في مثل هذه الجرائم، ونظرا لأن الجريمة الإلكترونية لها خصوصيتها فإن الخبير المعلوماتي قد يكون من أولئك الجناة الذين سبق لهم إرتكاب مثل هذه الجرائم وتم تكوينهم وإعادة تأهيلهم كأفراد موطنين صالحين في المجتمع[5] .

---

[1]-عائشة بن قارة مصطفى ، حجبة الدليل الإليكتروني في مجال الإثبات الجنائي دراسة مقارنة رسالة ماجستير، كلية الحقوق جامعة الإسكندرية، سنة 2009، ص 88 و 89

[2]-رشيدة بوكر ، المرجع السابق، ص 426 و 427

[3]على عدنان الفيل، المرجع السابق ، ص 26 و 27

[4]هشام محمد فريد رستم ، الجوانب الإجرائية للجرائم الإلكترونية ، مكتبة الآلات الحديثة، الطبعة 1، 1994 ص 42-143

[5]خيرت محرز، التحقيق في الجرائم الحاسب الآلي، دار الكتاب الحديث للطباعة والتوزيع، القاهرة، مصر، 2012، ص 96.

- مدى حجية تقرير الخبير التقني

يحرر الخبير لدى إنتهاء أعمال الخبرة تقريرا يجب أن يشتمل على وصف ما قام به من أعمال ونتائجها، وطبقا للمادة 221 من قانون . ج. ج تكون هذه التقارير مجرد استدلالات الإنارة القاضي، ولذلك يكون رأي الخبير يعطي دائما بصفة إستشارية ولا يقيده فهو ليس بحكم وليس له قيمة قضائية أكثر من شهادة شهود، فيجوز للقاضي أن يأخذ بالخبرة أو يطرحها و أن يفاضل بين تقارير الخبراء ويأخذ بما يرتاح إليه، حيث أن كل ما يتعلق بالدعوى يجب أن ينتهي عند قاضي الموضوع لكي يتولى الفصل فيه والكلمة الأخيرة ترجع لمحكمة الموضوع وهذا الأمر يسري على الناتج من الخبرة في إطار تكنولوجيا المعلومات، حيث يظل القاضي هو الخبير الأعلى[1].

3- اعتماد الدليل التقني في الإثبات

أ- تعريف الدليل التقني

والدليل الرقمي أو الإليكتروني أو الرقمي هو عبارة عن : " كل البيانات التي يمكن أن إعدادها أو تخزينها في شكل رقمي في الحاسوب"، ويمكن تعريف البيانات الرقمية بأنها مجموعة الأرقام التي تمثل مختلف المعلومات بما فيها النصوص المكتوبة، الرسومات الخرائط الصوت والصورة، أو أنه الدليل المأخوذ من أجهزة الكمبيوتر وهو يكون في شكل نبضات كهرومغناطسية، ممكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة، وهي مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات أو الأشكال من أجل تقديمه أمام أجهزة تطبيق القانون[2] .

وما هو جدير بالذكر أن هناك فرق بين الدليل التقني وبرامج الحاسب الآلي يكمن في الوظيفة التي يؤديها كل واحد منهما، فهذا الأخير له دور في القيام بمختلف العمليات التي يحتويها النظام المعلوماتي عند إعطاء الأوامر بالقيام بذلك، أما الدليل التقني فله أهمية كبرى ودور أساسي في معرفة كيفية حدوث جرائم الإلكترونية بهدف إثباتها ونسبتها إلى مرتكبيها.[3]

ب- تقدير القاضي الجزائي للدليل التقني

[1] رشيدة بوكر ، المرجع السابق، ص 429.

[2] رشيدة بوكر ، المرجع السابق، ص 382.

[3] عائشة قارة مصطفى، المرجع السابق، ص31.

إذا توافرت في الدليل التقني الشروط العامة لما يمكن أن يتمثل أساسا لإنبعاث الثقة فيه، فإنه قد يبدو من غير المعقول أن يعيد القاضي تقييم هذا الدليل وذلك لأن قيمة الدليل تقوم على أسس علمية دقيقة، وبالتالي فلا حرية للقاضي في مناقشة الحقائق العلمية الثابتة .

رغم أن هنالك إمكانية التشكيك في سلامة الدليل التقني بسبب قابلية للعبث إلا أن تلك مسألة فنية لا يمكن للقاضي أن يقطع في شأنها برأي حاسم خاصة إذا توافرت في الدليل التقني الشروط الخاصة بسلامته من العبث والخطأ، ورغم ذلك تبقى مسألة الأدلة العلمية والفنية في الإثبات راجعة الى السلطة التقديرية للقاضي لأنه يبقى المسيطر حقيقة وباستطاعته تفسير الشك الصالح المتهم. [1]

ج- حجية الدليل الإليكتروني في الإثبات

إن الخصوصية الجريمة الإلكترونية والتي تتميز بالطابع الفني دفع المشرع الجزائري بأن يبادر في مواكبة التطور القانوني على المستوى الدولي وتماشيا مع التطور التكنولوجي بتمهيد للطريق أمام إستخلاص الدليل الإليكتروني في القانون رقم 09/04 في المادة 06 منه[2]، مراعيا بذلك الإعمال بالقواعد العامة التي من الضروري توافرها في الدليل الإليكتروني وهي مبدأ المشروعية، بمعنى أنه لا يكون مستخلصا بطريقة مخالفة لأحكام القانون ولا مبادئ دستورية خاصة ما تعلق منها بحماية الحريات الأساسية .

ومما هو مستقر عليه فإن القاضي الجزائري ملزم بفحص الدليل الإليكتروني لكي يتواصل إلى تشكيل قناعة إنطلاقا من عرض هذا الدليل على مناقشة الأطراف، وهو ما نصت عليه المواد 212 و 234 من قانون ا . ج. ج. [3]

وبذلك يتضح لنا الدليل التقني له حجية في الإثبات وذلك بما يتميز به من موضوعية وكفاءة، ومحكم وفق قواعد علمية عملية حسابية قاطعة لا تقبل التأويل مما يقوي يقينيته، ويساعد القاضي من التقليل من الأخطاء القضائية و الإقتراب إلى العدالة بخطوات أوسع، والتوصل إلى درجة أكبر نحو الحقيقة[4] .

والإستدلال على ذلك نلاحظ إن الفقه الفرنسي يتناول حجية الدليل التقني في المواد الجزائية ضمن مسألة قبول الأدلة الناشئة عن الأدلة الناشئة عن الآلة أو الأدلة العلمية مثل: الردارات الأجهزة السنيمائية، أجهزة التصوير ، أشرطة التسجيل، أجهزة التنصت .[1]

---

[1] رشيدة بوكر ، المرجع السابق،ص 507

[2] –المادة 06 من القانون رقم 09/04 والتي تنص : على حجز المعطيات الإلكترونية وذلك بإفراغها أو نسخها على دعامة تخزين إليكترونية قابلة للحجز الوضع في أحراز."

[3] –زبيجة ، زيدان، المرجع السابق، ص 173.

[4] –بوكر رشيدة ، المرجع السابق، ص 497.

مع تطور الدليل التقني، تعزز الدور الذي يلعبه الإثبات العلمي في المجال الجزائي، ورافق ذلك تزايد أهمية الخبراء في تقديم آرائهم الفنية المتخصصة. فقد أسهمت التكنولوجيا الحديثة في توفير وسائل دقيقة لجمع الأدلة، ما مكّن العلم من المساهمة في إنتاج دليل قد يحوز قوة إثباتية يصعب دحضها. وبذلك، يُطرح تساؤل حول مدى تقلص دور القاضي الجزائي في تقدير هذا النوع من الأدلة، لا سيما في ظل ضعف الوعي الإلكتروني لدى بعض القضاة. ورغم ذلك، تظل الحاجة إلى الدليل التقني ضرورية، نظرًا لانسجامه مع طبيعة الجريمة الإلكترونية ومع التقدم التكنولوجي المتسارع، الأمر الذي يفرض عدم الاكتفاء بمضمون الدليل فقط، بل يستوجب تطوير الإجراءات المرتبطة بالحصول عليه، مع التأكيد على مشروعيتها وخلوّها من العيوب والتلاعب. ويكتسب الدليل الإلكتروني قوة حجية معتبرة في الإثبات، خاصة في الأنظمة القانونية التي تتبنى مبدأ حرية الإثبات وتمنح القاضي سلطة تقديرية، كما هو الحال في التشريع الجزائري[2] .

[1]–هلالي عبد الإله أحمد حجية المخرجات الكمبيوترية في المواد الجزائية ، الطبيعة الثانية ، دار النهضة العربية، القاهرة ، مصر، 2008، ص 42 و 43.

[2]–رشيدة بوكر ، المرجع السابق، ص 498.

خلاصة الفصل الثاني:

يتناول هذا الفصل الحماية القانونية التي منحها المشرع للتوقيع الإلكتروني من النواحي القانونية سواء المدنية والجزائية باعتباره أحد الأدوات الأساسية في المعاملات الإلكترونية الحديثة. على الصعيد المدني، يضمن القانون اعتبار التوقيع الإلكتروني ذا حجية في الإثبات، بشرط التزامه بالمعايير القانونية والفنية التي تضمن موثوقيته، ويحدد المسؤولية المدنية في حالات التزوير أو انتحال الهوية، مما يتيح للمتضرر الحق في المطالبة بالتعويض عن الأضرار الناتجة عن إساءة استخدام التوقيع الإلكتروني. من الجانب الجزائي، يعاقب المشرع الأفعال التي تؤثر على صحة وسلامة التوقيع الإلكتروني، مثل التزوير المعلوماتي أو استخدام توقيع شخص آخر بدون إذن، مع فرض عقوبات جزائية تتراوح بين الحبس والغرامة، تبعًا لخطورة الجريمة. كما يُسمح بتحريك الدعوى العمومية في هذه الجرائم، بالإضافة إلى إمكانية رفع دعوى مدنية للمطالبة بالتعويض. تهدف هذه الحماية المتكاملة إلى تعزيز الثقة في البيئة الرقمية وضمان الأمان القانوني للمعاملات الإلكترونية.

الخاتـمـــة

الخاتمة

وفي ختام هذا الفصل المتواضع توصلنا الى مجموعة من النتائج والنقائص هي:

-يُعد التوقيع الإلكتروني من القضايا القانونية المعاصرة ذات الطابع الحيوي، بالنظر إلى ما تشهده المعاملات الإلكترونية من توسع وانتشار على المستوى الإداري والتجاري، ما يفرض ضرورة توفير إطار قانوني يضمن شرعيتها ومصداقيتها، ويواكب مستجدات التكنولوجيا الرقمية.

,- من الناحية القانونية، يُعرّف التوقيع الإلكتروني على أنه وسيلة قانونية لإثبات التصرفات والتعهدات الإرادية، ويُعترف به بموجب أحكام القانون رقم 15-04 المتعلق بالتوقيع والتوثيق الإلكترونيين، شريطة استيفائه لجملة من المتطلبات التقنية والقانونية التي تضمن أمن الوثيقة وسلامتها، وعدم إمكانية تعديلها بعد التوقيع.

- تنقسم أنواع التوقيع الإلكتروني إلى نوعين رئيسيين: التوقيع الإلكتروني البسيط الذي يعتمد على وسائل تعريف أولية، والتوقيع الإلكتروني المتقدم الذي يقوم على تقنيات تشفير دقيقة تتيح التحقق من الهوية الرقمية وضمان عدم التلاعب.

- يُشترط لصحة التوقيع الإلكتروني توافر رضا الموقع، وقدرته على تحديد هويته الرقمية بوسائل موثوقة، مع ضمان عدم قابلية محتوى المستند للتغيير بعد توقيعه، إضافة إلى الربط الوثيق بين التوقيع والمستند بطريقة تحول دون التحريف.

يوفر الإطار القانوني الجزائري حماية مدنية وجزائية للتوقيع الإلكتروني. فمن الناحية المدنية، يُعد التوقيع وسيلة إثبات معترف بها قانونًا، وتترتب عنه مسؤوليات في حال وقوع تزوير أو انتحال هوية. أما من الناحية الجزائية، فقد جرم المشرع بعض الأفعال، على غرار التزوير المعلوماتي أو استخدام توقيع دون إذن، وقرنها بعقوبات تراوحت بين الغرامة والحبس، تبعًا لخطورة الفعل المرتكب.

- رغم الاعتراف القانوني الصريح بالتوقيع الإلكتروني، إلا أن التطبيق العملي لهذه النصوص لا يزال محدودًا، وهو ما يرجع إلى ضعف الوعي الرقمي، وتردد العديد من الفاعلين في الانخراط الفعلي في منظومة التوقيع الإلكتروني.

- كما أن الحماية المدنية المقررة للتوقيع الإلكتروني لا تزال قاصرة عن معالجة مختلف الإشكالات والنزاعات الممكنة، في حين أن الحماية الجزائية اتسمت بالحذر، واقتصرت على صور تقليدية من الجرائم دون التوسع في مواجهة التهديدات الرقمية المستحدثة.

- ولا تزال الخبرة التقنية هي الفيصل في التحقق من صحة التوقيع الإلكتروني وكشف التزوير، مما يستوجب تأهيل الجهات المختصة فنيًا وتقنيًا للقيام بهذه المهمة بكفاءة.

الاقتراحات التوصيات:

1- تطوير الإطار التشريعي: يتعين على المشرّع العمل على تحديث النصوص القانونية المنظمة للتوقيع الإلكتروني، بما يضمن إدراج أحكام تفصيلية تتعلق بآليات الحماية المدنية والجزائية، وذلك لتعزيز الضمانات القانونية الممنوحة للأطراف المتعاملة في البيئة الرقمية.

2- توسيع نطاق التجريم: يُوصى بتعديل النصوص الجزائية لتشمل كافة الأفعال غير المشروعة المرتبطة بالتوقيع الإلكتروني، بما في ذلك الاختراق السيبراني، التحايل المعلوماتي، وانتحال الهوية الرقمية، وذلك تماشياً مع تزايد التهديدات في الفضاء الإلكتروني.

3- تعزيز التكوين القضائي والتقني: من الضروري تنظيم دورات تكوينية لفائدة القضاة ومساعدي القضاء، تُمكنهم من الإلمام بالجوانب التقنية للتوقيع الإلكتروني، بما يضمن التعامل المهني مع الأدلة الرقمية وتقدير حجيتها القانونية.

4- سد الثغرات القانونية: ينبغي مراجعة وتطوير المنظومة التشريعية الحالية لضمان شمولها لجميع أوجه الحماية القانونية المرتبطة بالتوقيع الإلكتروني، سواء من الناحية المدنية أو الجنائية، مع مراعاة المستجدات التكنولوجية المتسارعة والتحديات الناشئة في المجال الرقمي.

5- اعتماد تقنيات تحقق متقدمة: يُستحسن تبنّي آليات فنية متطورة لضمان سلامة ومصداقية التوقيع الإلكتروني، تشمل تقنيات التوثيق الرقمي المتقدم، أنظمة كشف التلاعب والتزوير، بالإضافة إلى سن معايير تنظيمية واضحة لمزودي خدمات التصديق الإلكتروني.

6- نشر الوعي وتكثيف التكوين: يُوصى بإعداد برامج تكوينية وتحسيسية موجهة إلى مختلف الفاعلين، من قضاة، وعمال في القطاع القضائي، ومزودي خدمات التصديق الإلكتروني، فضلاً

عن المستخدمين النهائيين، بهدف تعزيز الثقافة القانونية والتقنية المتعلقة بالتوقيع الإلكتروني، وتشجيع استعماله الآمن والفعال في المعاملات الرقمية.

قائمة المراجع والمصادر

قائمة المراجع والمصادر

I-المصادر

أولا: القوانين

- قانون رقم 10-05 المؤرخ في 20 جويلية 2005، معدل و متمم للأمر رقم 75/58المؤرخ في 26 سبتمبر1975 و المتضمن القانون المدني المعدل و المتمم، و المنشور في الجريدة الرسمية ،عدد44 الصادر في 2005/07/21.

- القانون رقم 04/15المؤرخ في1 فبراير 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، جريدة رسمية للجمهورية الجزائرية، عدد 6، الصادرة في .2015/02/10

القانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة لتكنولوجيا الاعلام والاتصال ومكافحتها.

ثانيا: المراسيم:

-المرسوم التنفيذي رقم 07/162،المؤرخ في 13جمادى الأول 1428 الموافق ل 30ماي2007، يعدل ويتمم المرسوم التنفيذي رقم 01/123، المؤرخ في 15صفر 1422، الموافق ل09ماي سنة 2001،المتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشيكات بما فيها اللّاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية و اللّاسلكية، الجريدة الرسمية للجمهورية الجزائرية ،عدد 37 الصادرة في 7جوان2007.

-المرسوم 230/2000 حول التوقيع الالكتروني المؤرخ 14 مارس 2000، ج ر 62، ص 3 968

-مرسوم تنفيذي رقم 16-134 مؤرخ في 17 رجب 1437 الموافق ل 25 أفريل 2016 ، يحدد تنظيم المصالح التقنية والإدارية للسلطة الوطنية للتصديق الإلكتروني وسيرها ومهامها، ج ر ع 26 صادرة بتاريخ 28 أفريل 2016

- المرسوم التنفيذي رقم 06/343 المؤرخ في 115/10/2006 المتضمن تمديد الاختصاص المحلي البعض المحاكم ووكلاء الجمهورية قضاة التحقيق.

II -المراجع

1-باللغة العربية

أولا: الكتب

أ-الكتب العامة

- إلياس ناصيف، العقد الإلكتروني في القانون المقارن، منشورات الحلبي الحقوقية، 2009.
- أمين أعزان، الحماية الجزائية للتجارة الإلكترونية، أطروحة دكتوراه، جامعة عين شمس، د.ت.
- إيمان مأمون أحمد سليمان، إبرام العقد الإلكتروني وإثباته، دار الجامعة الجديدة، 2008.
- خالد ممدوح إبراهيم، إبرام العقد الإلكتروني: دراسة مقارنة، دار الفكر الجامعي، 2011.
- خيرت محرز، التحقيق في جرائم الحاسب الآلي، دار الكتاب الحديث، 2012.
- زليخة زيدان، الجريمة الإلكترونية في التشريع الجزائري والدولي، دار الهدى، 2011.
- زياد خليف العنزي، المشكلات القانونية لعقود التجارة الإلكترونية، دار وائل، 2010.
- عبد الرزاق أحمد السنهوري، الوسيط في شرح القانون المدني، منشأة المعارف، 2004.
- غازي حنون خلف، وآخرون، القصد الجرمي في تزوير التوقيع الإلكتروني، جامعة البصرة، 2010.
- فيلالي علي، الالتزامات: الفعل المستحق للتعويض، موفم للنشر، 2015.
- مثاني فراح، العقد الإلكتروني وسيلة إثبات حديثة في القانون المدني الجزائري، دار الهدى، 2013/2012.
- محمد أمين الرومي، جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية، 2003.
- محمد أمين الرومية، التعاقد عبر الإنترنت، دار المطبوعات الجامعية، 2004.
- محمد أمين الشوابكة، جرائم الحاسوب والإنترنت، دار الثقافة، 2004.

- محمد صبري السعدي، النظرية العامة للالتزامات، دار الهدى، 2019.
- محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع للإنترنت، دار النهضة، د.ت.
- محمد قاسم، أصول الإثبات في المواد المدنية والتجارية، منشورات الحلي الحقوقية، 2003.
- مقلاتي مونة، الأسس الجديدة للمسؤولية المدنية، مطبوعة بيداغوجية، 2019.
- منير الجنبيهي، جرائم الإنترنت والحاسب الآلي، دار الفكر الجامعي، 2005.
- نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة، ط2.
- هدى قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة، 1992.
- هشام محمد فريد رستم، الجوانب الإجرائية للجرائم الإلكترونية، مكتبة الآلات الحديثة، 1994.
- هشام محمد فريد رستم، العقوبات ومخاطر جرائم المعلوماتية، دار النهضة، 2000.
- هلالي عبد الإله أحمد، حجية المخرجات الكمبيوترية في المواد الجزائية، دار النهضة، 2008.
- يمينة جوجو، عقد البيع الإلكتروني في القانون الجزائري، دار بلقيس، 2016.

ب-الكتب المتخصصة

- إبراهيم بن سطم بن خلف العنزي، التوقيع الإلكتروني وحمايته الجنائية، رسالة دكتوراه، جامعة نايف، 2009.
- إبراهيم سيد أحمد، قانون التجارة الإلكترونية والتوقيع الإلكتروني...، الدار الجامعية، 2005.
- أمير فرج يوسف، التوقيع الإلكتروني، مكتبة الوفاء القانونية، 2011.
- ثروت عبد الحميد، التوقيع الإلكتروني: ماهيته، مخاطره، وكيفية مواجهته، مدى حجيته في الإثبات، دار الجامعة الجديدة، 2007.
- سعيد السيد قنديل، التوقيع الإلكتروني، دار الجامعة الجديدة، 2006.

- عاطف عبد الحميد حسن، التوقيع الإلكتروني: مفهومه، صوره، حجيته في الإثبات، دار النهضة العربية، 2008.
- فيصل سعد الغريب ، التوقيع الالكتروني وحجيته في الاثبات ، المنظمة العربية للتنمية الإدارية ، بحوث ودراسات، لبنان، 2005
- محمد الشهاوي، شرح قانون التوقيع الإلكتروني رقم 15 لسنة 2004، دار النهضة العربية، 2010.
- محمد محروك، خصوصيات التوقيع الإلكتروني وحجيته في الإثبات، مجلة جامعة القاضي عياض، بدون سنة.
- محمد مرسي زهرة، مدى حجية التوقيع الإلكتروني في الإثبات، رسالة دكتوراه، جامعة عين شمس، 1994.
- نايف بن ناشي الغنامي، التوقيع الإلكتروني وحجيته في الإثبات بالتطبيق على النظام السعودي، جامعة الطائف، 2019.
- وسيم شفيق الحجار، الإثبات الإلكتروني، دار المنشورات الحقوقية، بيروت، 2002.

ثانيا: الرسائل والمذكرات الجامعية:

ا-رسائل الدكتوراه

- براهمي حنان، جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية ، أطروحة دكتوراه، جامعة محمد خيضر، بسكرة ، الجزائر، 2014-2015،
- بلقاسم حامدي ، إبرام العقد الالكتروني ، أطروحة دكتوراه في العالم القانونية تخصص قانون أعمال ، كلية الحقوق والعلوم السياسية ، جامعة الحاج لخضر ، باتنة ، 2014
- بلقنيشي حبيب، إثبات التعاقد عبر الأنترنيت (البريد المرئي-دراسة مقارنة-)، رسالة مقدمة لنيل شهادة الدكتوراه في القانون الخاص، كلية الحقوق، جامعة وهران السانيا ،2010/2011

- جمال ديلمي ، أثار التصديق الالكتروني، أطروحة لنيل شهادة الدكتوراه في العلوم ، تخصص قانون أعمال ، كلية الحقوق والعلوم السياسية ، جامعة مولود معمري تيزي وزو ، 2022 –2023
- زروق يوسف، حجية وسائل الإثبات الحديثة، رسالة مقدمة لنيل شهادة دكتوراه في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد تلمسان، 2012/2013،
- عروة فتيحة ، وسائل التبادل المصرفي في القانون الجزائري أطروحة دكتوراه في العلوم ، تخصص قانون أعمال ، كلية الحقوق ، جامعة الجزائر 01 ، 2016
- كوسام أمينة، الشكلية في عقود التجارة الإلكترونية، أطروحة مقدمة لنيل درجة دكتوراه العلوم في العلوم القانونية، كلية الحقوق والعلوم السياسية، جامعة باتنة 2015/2016
- نور خالد عبد المحسن عبد الرزاق، حجية المحررات والتوقيع الالكتروني في الاثبات عبر شبكة الانترنت ، رسالة دكتوراه في الحقوق، جامعة عين شمس ، مصر، 2009

ب–الماجستير:

- أزرو محمد رضا ، التوقيع الالكتروني كوسيلة من وسائل الإثبات ، رسالة تخرج مقدمة لنيل شهادة الماجستير ، تخصص قانون خاص ، كلية الحقوق ، جامعة أبو بكر بلقايد تلمسان 2007
- اياد محمد ، عارف عطا سده، مدى حجية المحررات الالكترونية في الاثبات، دراسة مقارنة، رسالة ماجستير في القانون الخاص، جامعة النجاح الوطنية ، نابلس ، فلسطين ، 2009
- ايهاب سمير محمد صالح، الإثبات بالمحررات الإلكترونية (دراسة مقارنة)، رسالة لاستكمال متطلبات الحصول على درجة الماجستير في القانون الخاص، كلية الحقوق، جامعة الأزهر، غزة 2015
- الربيع سعدي، حجية التوقيع الإلكتروني في التشريع الجزائري ، أطروحة ماجستير في القانون الخاص، جامعة باتنة، 2017
- عائشة بن قارة مصطفى ، حجبة الدليل الإليكتروني في مجال الإثبات الجنائي دراسة مقارنة رسالة ماجستير، كلية الحقوق جامعة الإسكندرية، سنة 2009

- لوصيف عمار الستراتيجيات نظام المدفوعات للقرن الحادي والعشرين، مع الإشارة إلى التجربة الجزائرية، مذكرة مقدمة كجزء من متطلبات نيل شهادة الماجستير في العلوم الاقتصادية، كلية العلوم الاقتصادية وعلوم التسيير قسم العلوم الاقتصادية، جامعة منتوري، قسنطينة 2008/2009

ج-الماستر:

- ا سمير بن حليمة، القصد الجرمي في تزوير التوقيع الإلكتروني، مذكرة مقدمة لنيل شهادة الماستر الاكاديمي، تخصص قانون جنائي، فرع الحقوق كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف المسيلة 2017/2018

- اجحيط حبيبة جهودي مريم النظام القانوني للعقد الإلكتروني (دراسة مقارنة)، مذكرة تخرج لنيل شهادة الماستر في القانون الخاص تخصص القانون الخاص الشامل كلية الحقوق والعلوم السياسية، جامعة عبد الرحمن ميرة بجاية 18/06/2013

- آمنة بومجو، الإثبات في عقود التجارة الإلكترونية، مذكرة تكميلية لنيل شهادة الماستر، تخصص قانون أعمال، كلية الحقوق و العلوم والسياسية،جامعة العربي بن مهيدي. ام البواقي.2016/2015

- أمين، التوقيع الإلكتروني وحجيته في الإثبات، رسالة مقدمة لاستكمال متطلبات الحصول على شهادة ماستر أكاديمي في تخصص قانون الأعمال، كلية الحقوق والعلوم السياسية، جامعة الشادلي بن جديد، الطارف 2018/2019

- بسعر سمية، بوخشة وردة، التوقيع الإلكتروني ودوره في الإثبات في التشريع الجزائري، مذكرة مكملة لنيل شهادة الماستر في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة محمد الصديق بن يحي، جيجل 2015/2016

- بن سعدي فريدة، وسائل الإثبات الحديثة في القانون المقارن، مذكرة مقدمة لنيل شهادة الماستر في الحقوق، تخصص القانون الخاص الشامل، كلية الحقوق و العلوم السياسية، جامعة عبد الرحمن بجاية

- عبد الكريم شيباني الحماية الإجرائية والموضوعية للجريمة المعلوماتية، مذكرة لنيل شهادة ماستر، كلية الحقوق والعلوم السياسية، جامعة الطاهر مولاي، سعيدة ، 2016-2015

- عمار حشمان,الجريمة المعلوماتية في التشريع الجزائري.مذكرة لاستكمال متطلبات شهادة الماستر المهني الطور الثاني .كلية العلوم الاقتصادية و العلوم التجارية و علوم التسيير ،ادارة التحقيقات الاقتصادية و المالية ،جامعة قاصدي مرباح،ورقلة،2019

- عنوش حنان العلاوي عز الدين النظام القانوني للعقد الإلكتروني في التشريع الجزائري، مذكرة تخرج لنيل شهادة الماستر في الحقوق، تخصص القانون العام للأعمال كلية الحقوق والعلوم السياسية، جامعة عبد الرحمن ميرة، بجاية،

- غربي خديجة، التوقيع الإلكتروني»، مذكرة ماستر، جامعة قاصدي مرباح–ورقلة، الجزائر ،2015

- كريمة زايدي، النظام القانوني لجهات التصديق الإلكتروني، مذكرة تكميلية لنيل شهادة الماستر، تخصص قانون أعمال كلية الحقوق والعلوم السياسية، جامعة العربي بن مهيدي، أم البواقي، 2015/2016

- هني بوطيبة جمال ، حجية التوقيع الالكتروني في الإثبات في التشريع الجزائري ، مذكرة ماستر ، كلية الحقوق والعلوم السياسية ، جامعة عبد الحميد بن باديس ، مستغانم 2021

- ياسمينة كواشي الحماية الجنائية للتوقيع والتصديق الإلكترونيين في ظل القانون مذكرة مكملة لنيل شهادة ماستر في تخصص قانون جنائي للأعمال كلية الحقوق والعلوم السياسية جامعة العربي بن مهيدي أم البواقي، 2016/2017

ثالثا: المقالات والمجلات العلمية :

- أبو عرابي غازي القضاة فياض، حجية التوقيع الإلكتروني (دراسة في التشريع الأردني)، مجلة جامعة دمشق للعلوم الإقتصادية والقانونية، المجلد 20 ، العدد الأول

- أبو غرابي غازي، فياض القضاة، حجية التوقيع الإلكتروني ، دراسة في التشريع الاردني، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 20، العدد 1، سوريا، 2004

- بلقاسم حامدي، إبرام العقد الإلكتروني، أطروحة مقدمة لنيل درجة دكتوراء العلوم في العلوم القانونية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة 2014/2015

- بوعلام بوزيدي التوقيع الإلكتروني، مجلة البدر، بشار، بدون سنة
- جبايلي صبرينة ، النظام القانوني للسلطة الوطنية للتصديق الكتروني ، مجلة العلوم الإنسانية ، جامعة الإخوة منتوري قسنطينة ، المجلد أ ، العدد 48 ، ديسمبر 2017 .
- حنان مليكة النظام القانوني للتوقيع الإلكتروني في ضوء قانون التوقيع الإلكتروني السوري، رقم 4، الصادر بتاريخ 25 فيفري 2009، مجلة جامعة دمشق للعلوم الاقتصادية والفكرية، المجلد 26، العدد 2010
- درار نسيمة ، التوثيق الرقمي ومسؤولية سلطات المصادقة الالكترونية في القانون الجزائري 04/15 ، مجلة الأستاذ الباحث للدراسات القانونية والسياسية ، المجلد 02 ، العدد 9 ، 2018
- رحال بومدين،سعداني نورة ،الحماية الجنائية للتوقيع الالكتروني وفق القانون الجزائري 15_04،قسم الحقوق ،كلية الحقوق و العلوم السياسية ،جامعة طاهري محمد،بشار ، د ت
- رحمان يوسف، سلطات التصديق الإلكتروني في التشريع الجزائري طبقا للقانون 15-04 دراسة مقارنة، مجلة الدراسات القانونية والسياسية، جامعة تلمسان، الجزائر
- رشيدة بوكر التوقيع الإلكتروني في التشريع الجزائري (دراسة مقارنة)، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة عبد الحميد بن باديس، مستغانم العدد الرابع ديسمبر 2016- - زهيرة كيسي النظام القانوني لجهات التوثيق (التصديق) الإلكتروني، مجلة دفاتر السياسة والقانون، المركز الجامعي بتمنراست، الجزائر، العدد السابع، جوان 2012
- غانى جابر السعدي وآخرون، النظام القانوني لشهادة التوثيق الالكتروني، مجلة المحقق المحلي للعلوم القانونية والسياسية، العدد 02 ، 2017
- لينده بلحارث ، النظام القانوني لمزودي خدمات التصديق الالكتروني في القانون الجزائري محلة العلوم القانونية والسياسية، جامعة محند أولحاج البويرة ، المجلد 09 ، العدد 03 ، 2018
- محمد المهدي بكراوي ، جامعي مليكة ، يوم دراسي حول الاتجاهات الحديثة في نظرية المسؤولية المدنية ، كلية الحقوق والعلوم السياسية ، قسم الحقوق ، جامعة ادرار ، الجزائر ، 2013

- مصطفى هنشور وسيمة النظام القانوني للتوقيع الإلكتروني في التشريع الجزائري، مجلة الحقوق والعلوم السياسية، العدد 24، المجلد الثاني، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس مستغانم، دون سنة
- مليسا حمود، الحجية القانونية للعقد الإلكتروني في التشريع الجزائري، مجلة العلوم الإنسانية، مجلّد 32 ، جامعة الاخوة منتوري ، قسنطينة ، الجزائر ، 2021
- من خلال – بلحاج بلخير، مداخلة بعنوان حجية التوقيع الإلكتروني في الإثبات الملتقى الوطني حول الإطار القانوني للتوقيع والتصديق الإلكتروني في الجزائر 2016
- هاني سليمان الطعيمات حجية الكتابة والتوقيع الإلكترونين في إثبات المعاملات المالية، دراسة فقهية قانونية مقارنة. المجلة الأردنية في الدراسات الإسلامية، المجلد 14، العدد 2، 2018

2- المراجع الأجنبية :

- D. Gobert et E. Montero, L'ouverture de la preuve littérale aux écrits sous forme électronique, op.cit., p. 124
- Didier GOBERT, «Cadre juridique pour les signatures électroniques et les services de certification loi du 9 juillet 2001», Disponible la : analyse de sur: www.consultandtraining.com
- Eric. A. CAPRIOLI sécurité et confiance dans le commerce électronique, sécurité numérique et autorité de certification, J.C.P Ed G 1998, P58
- Lisant de belle fonds et A . Holland , pratique du droit de l'informatique ,4 éme éd ,Delmas ,paris ,1998
- M.AMEGE, La signature électronique fragilise-t-elle le contrat», 2001. www.lexana.com

- Taylor ,R, computer crime, criminal investigation edited, « by Charles Swanson ,N, chamelin and L. Teritto hill,inc.5 edition,1992,p450.

الفهرس

بسملة .....أ

شكر وعرفان ..... ج

إهداء ..... هـ

قائمة المختصرات .....د

مقدمة 2

الفصل الازل: الاطار المفاهيمي والقانوني للتوقيع الالكتروني

المبحث الأول: ماهية التوقيع الإلكتروني ومزاياه 9

المـطلب الأول: مفهوم التوقيع الالكتروني..... 9

الفرع الاول : التعريف الفقهي 9

الفرع الثاني : تعريف التوقيع حسب المشرع الجزائري.....11

المـطلب الثاني: انواع التوقيع الالكتروني و صوره 16

الفرع الاول: انواع التوقيع الالكتروني 16

الفرع الثاني : صور التوقيع الالكتروني 19

الفرع الثاني: صور التوقيع البسيط.....32

المبحث الثاني: النظام القانوني للتوقيع الالكتروني.....33

المطلب الأول: أهمية التوقيع الإلكتروني ووظائفه 34

الفرع الأول: الأهمية القانونية للتوقيع الإلكتروني 34

الفرع الثاني: وظائف التوقيع الإلكتروني 36

المطلب الثاني : شروط صحة التوقيع الالكتروني 38

الفرع الاول : الشروط الشكلية 39

الفرع الثاني : الشروط الموضوعية.....45

خلاصة الفصل الاول 56

الفصل الثاني: الحماية الجزائية للتوقيع الالكتروني في التشريع الجزائري

المبحث الأول: الحماية المدنية للتوقيع الالكتروني في التشريع الجزائري 59

المطلب الأول : المسؤولية المدنية وأثارها على التوقيع الالكتروني 59

الفرع الأول : المسؤولية المدنية لجهة التصديق الالكتروني 59

الفرع الثاني : التزامات مقدمي خدمات التصديق والمسؤولية الناشئة عن ذلك 69

المطلب الثاني : حجية شهادة التصديق الالكتروني في الإثبات 72

الفرع الأول : حجية التوقيع الالكتروني البسيط.....72

الفرع الثاني: حجية التوقيع الالكتروني الموصوف 76

المبحث الثاني: الحماية الجزائية للتوقيع الالكتروني.....79

المطلب الاول: الاطار العام للجريمة المعلوماتية 79

الفرع الأول : ماهية الجريمة المعلوماتية 80

الفرع الثاني: خصائص وأنواع الجريمة الالكترونية 81

المطلب الثاني: مكافحة الجرائم المتعلقة بالتوقيع الالكتروني في التشريع الجزائري.....87

الفرع الثاني: المتابعة الجزائية لجرائم التوقيع الالكتروني 90

خلاصة الفصل الثاني 106

الخاتمة 108

قائمة المراجع والمصادر 112

ملخص 126

ملخص

تسعى هذه الدراسة إلى بيان الإطار القانوني الناظم للتوقيع الإلكتروني، ومدى اعتباره وسيلة إثبات قانونية تحقّق ذات الوظيفة التي يؤديها التوقيع التقليدي، خصوصًا في ظل بيئة المعاملات الرقمية. وقد تم اعتماد المنهجين التحليلي والوصفي لبيان الجوانب النظرية والتطبيقية للتوقيع الإلكتروني، من خلال تحليل النصوص القانونية الوطنية والمقارنة. وتوصلت الدراسة إلى أن التوقيع الإلكتروني، متى استوفى الشروط القانونية، يتمتع بحجية كاملة في الإثبات، ويُعدّ أداة فعّالة لتعزيز الثقة في التجارة الإلكترونية، رغم ما يشوب الإطار التشريعي الجزائري من بعض النواقص. وتؤكد الدراسة على أهمية تطوير التشريع الوطني بما يواكب المعايير الدولية ويضمن أمن المعاملات الإلكترونية.

الكلمات المفتاحية: التوقيع الإلكتروني، الإثبات، البيئة الرقمية، القانون الجزائري، الحماية القانونية، المعاملات الإلكترونية، التشريع المقارن.

Abstract ;

This study aims to explore the legal framework governing electronic signatures and assess their evidentiary value compared to traditional signatures, particularly within the context of digital transactions. The research adopts both analytical and descriptive methods to examine the legal and technical dimensions of electronic signatures through national and comparative legal texts. The findings confirm that, when legally compliant, electronic signatures enjoy full probative force and serve as a reliable tool to foster trust in e-commerce. However, the study also highlights certain gaps in Algerian legislation, stressing the need for legal reform aligned with international standards to ensure secure digital transactions.

Keywords: Electronic signature, evidence, digital environment, Algerian law, legal protection, electronic transactions,

.