جامعة اكلي محند أولحاج البويرة
كلية الحقوق والعلوم السياسية
قسم القانون الخاص

التوقيع الإلكتروني وحمايته

مذكرة تخرج مقدمة لنيل شهادة ماستر في الحقوق

تخصص قانون اعمال

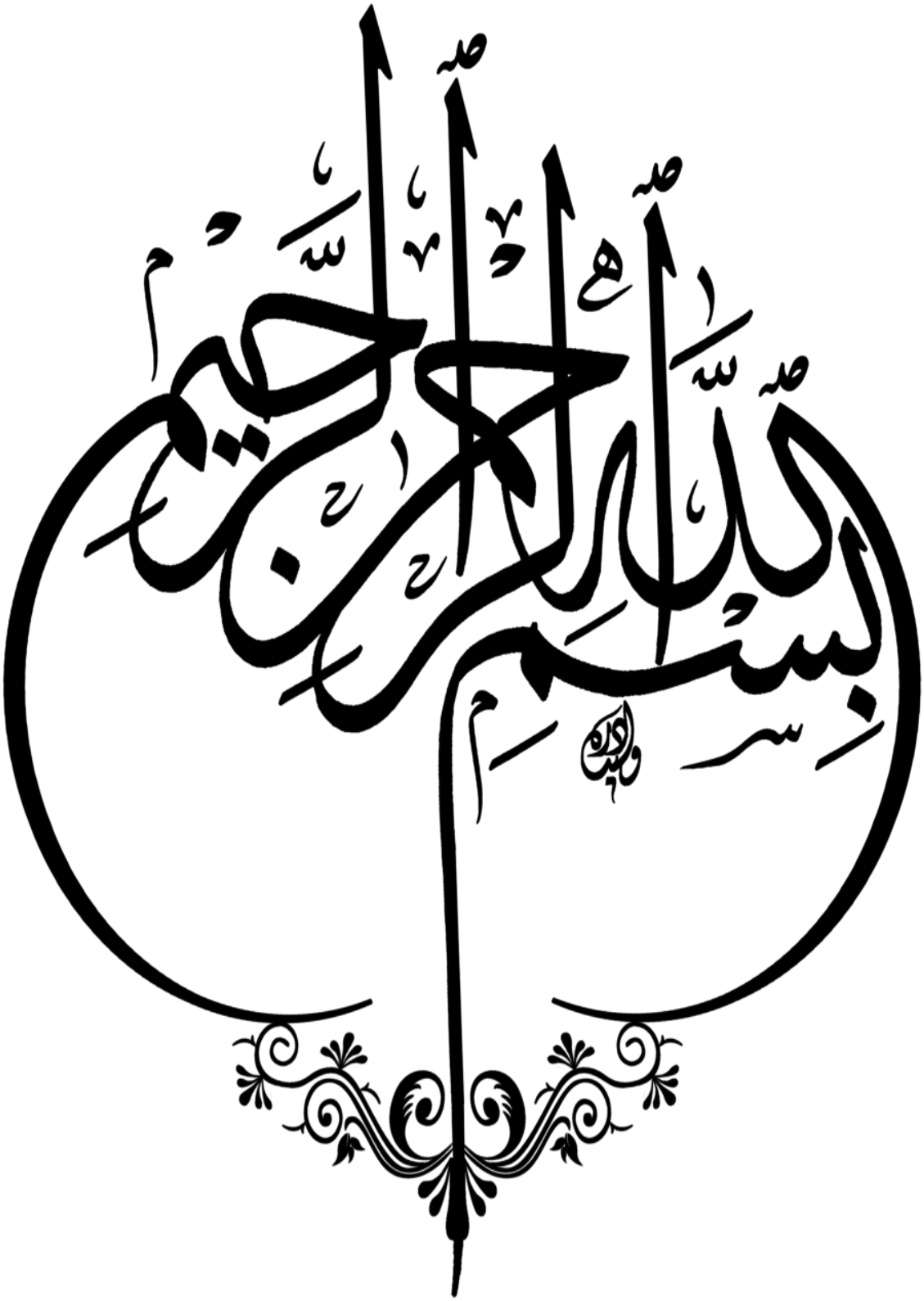
إعداد الطالب:
قاضي رشيد

تحت إشراف الأستاذ:
أ-أركام جودي

أعضاء لجنة المناقشة:

الأستاذ	رئيسا
الأستاذ: أركام جودي	مشرفا ومقررا
الأستاذ:	ممتحنا

السنة الجامعية: 2024-2025


بسم الله الرحمن الرحيم

شكر وعرفان

إن الحمد الله على ما وهبنا إياه من نعم، وهو الأحق بالشكر والثناء، والصلاة والسلام على أفضل الخلق وخاتم الأنبياء والمرسلين وعلى أله وصحبه أجمعين، وبعد إتمام هذه المذكرة ووفاء وتقديرا مني أتقدم بجزيل الشكر إلى الأستاذ"أركام جودي"على رحابة صدره وسعته بتحمل مشقة الإشراف على هذا العمل، فله جزيل الشكر والامتنان.

كما أتقدم بخالص شكري إلى عائلتي التي كانت خير عون طوال المشوار.

كما أتقدم بالشكر إلى الأساتذة الكرام أعضاء اللجنة الذين تشرفت بقبولهم مناقشة هذا العمل، وكل من قدم لنا يد العون طيلة سنوات الدراسة ولو بشق كلمة.

الإهداء

بتوفيق من الله تعالى على إتمام هذا العمل لا يسعني في هذا المقام إلى أهيب تواضعا واحتراما إلى من ربياني صغيرا وفتحا لي أبواب العلم والمعرفة إلى من أحمل اسمه بكل افتخار، الذي أفنى حياته لأجلي وبذل الغالي والنفيس لأكون ما أنا عليه اليوم " والدي العزيز" تقديروفخر إليه.

إلى التي أنارت أيامي وسهلت لي شدائد بدعائها الإنسانة العظيمة التي لا طالما تمنت أن تقرعينها لرؤية هذا اليوم " والدتي الغالية "

إلى ضلعي الثابت وأماني أيامي إلى من شددت عضدي بهم فكانوا لي ينابيع ارتوي منها إلى "أخواني"

إلى من كان عون وسند لي في هذا الطريق إلى الأصدقاء رفقاء السنين.

رشيد

قائمة أهم المختصرات

ص: الصفحة

ع: العدد

ق.ا.ج. : قانون إجراءات جزائية

ج.ر: جريدة رسمية

ط: الطبعة

ص ص: من الصفحة إلى الصفحة

مقدمـــة

مع التطور السريع للتكنولوجيا والاعتماد المتزايد على الوسائل الرقمية في مختلف مجالات الحياة أصبحت الحاجة إلى أدوات تضمن الأمانة والمصداقية في المعاملات الالكترونية أمرا ضروريا في هذا السياق برز التوقيع الالكتروني كوسيلة حديثه وفعاله للتحقق من هوية الأفراد والمؤسسات والتأكد من صحة المستندات والمعاملات دون الحاجة إلى التوقيع اليدوي التقليدي.

يعرف التوقيع الالكتروني بأنه تقنية رقمية تستخدم للمصادقة على المستندات والمعاملات عبر الانترنت حيث يضمن للمستخدمين إمكانية إتمام معاملاتهم بسرعة وأمان دون الحاجة إلى استخدام الورق أو التوقيع اليدوي والاعتماد على تقنيات التشفير لضمان عدم التلاعب بالمحتوى الموقع عليه مما يجعله بديلا فعالا في عالم يشهد توجها نحو الرقمنة.

لقد أصبح التوقيع الالكتروني جزءا أساسيا في العمليات التجارية والإدارية حيث تستخدمه الشركات الكبرى والمؤسسات المالية والهيئات الحكومية لتبسيط الإجراءات وتسريع العمليات وتخفض التكاليف المرتبطة بالمعاملات الورقية التقليدية كما انه يساهم في تعزيز التحول الرقمي حيث يقلل الحاجة إلى السفر والتواجد الفعلي لإنجاز المعاملات الرسمية مما يوفر الوقت والجهد للمستخدمين مع دلك فان التوقيع الالكتروني يثير عددا من القضايا والتحديات التي يجب معالجتها لضمان فعاليته وأمانة فعلى المستوى القانوني تختلف التشريعات المنظمة للتوقيع الالكتروني من دولة إلى أخرى مما يستدعي وضع معاير موحده لضمان الاعتراف به على نطاق عالمي أما من الناحية الأمنية فيجب توفير تقنيات تشفير متقدمة لمكافحه عمليات الاحتيال والتزوير لاسيما في ظل تزايد الهجمات السبيرانية التي تستهدف البيانات الرقمية.

إن انتشار التوقيع الالكتروني لم يقتصر على قطاع الأعمال فحسب بل امتد ليشمل المعاملات الشخصية مثل التوقيع على العقود الالكترونية والطلبات الرسمية والمعاملات المصرفية وحتى العمليات الطبية عن بعد كما انه أصبح عنصرا أساسيا في التجارة الالكترونية حيث يتيح للعملاء والشركات إبرام الصفقات بسهولة وأمان دون الحاجة إلى اللقاءات أو التعامل مع الأوراق التقليدية.

في ظل التحولات الرقمية المتسارعة بات من الضروري أن تدرك الحكومات والمؤسسات أهمية تبني التوقيع الالكتروني وتعزيز الوعي حول استخدامه وضمان توافقه مع الأنظمة القانونية والأمنية القائمة كما أن التطور المستمر في تقنيه التشفير والمصادقة الرقمية سيساهم في تعزيز ثقة المستخدمين بهذه التقنية مما يجعلها أكثر قبولا واعتمادا في المستقبل أين بدأت الدول تهتم به خصوصا مع تزايد استعمل التكنولوجيا و تشجيعا للتجارة الالكترونية وتضافر الجهود على المستوى الدولي و الإقليمي لاستصدار تشريعات و أحكام قانونية تنظيمية ومن أهم هذه التشريعات نجد –قانون الأونسيترال النموذجي بشأن التجارة 1996 و2001 والتوجيه الأوروبي للتجارة الالكترونية لسنة 2000كما تجدر الإشارة إلى أن الجزائر كغيرها من الدول التي سعت لاستصدار قانون ينظم التوقيع والتصديق الالكتروني وهذا بموجب القانون رقم 15-04 المؤرخ 01-02-2015 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكتروني

تهدف دراسة موضوع التوقيع الإلكتروني الى تسليط الضوء على الإطار المفاهيمي للتوقيع الإلكتروني من خلال التعريف بمفهومه، وظائفه، وأهم تطبيقاته. كما تهدف الدراسة إلى تحليل دور القوانين والتشريعات في وضع آليات فعّالة لحماية التوقيع الإلكتروني على الصعيدين التقني والقانوني. بالإضافة إلى ذلك، تهدف الدراسة إلى استعراض أهم المستجدات التي وردت في القانون رقم 15-04 المتعلق بالتوقيع

والتصديق الإلكترونيين،[1] وكيفية تأثيره على تطوير نظم الأمان والتوثيق الإلكتروني في مختلف المجالات.

وتُعنى الدراسة أيضًا بتوضيح كيفية تعامل التشريعات مع تحديات الأمان الرقمي في ظل التطور التكنولوجي المستمر، وضرورة تعزيز الثقة في التوقيعات الإلكترونية من خلال إطار قانوني يضمن حماية حقوق الأفراد والمؤسسات.

لذا يعد التوقيع الإلكتروني من الموضوعات القانونية والتقنية الحديثة التي فرضت نفسها فيظل التطور التكنولوجي السريع، فقد أصبح التوقيع الإلكتروني عنصرًا أساسيًا في مجالات متعددة مثل التجارة الإلكترونية، والخدمات المصرفية، والمعاملات الحكومية الرقمية.

يساهم التوقيع الإلكتروني بشكل ملحوظ في تسهيل الإجراءات، وتقليل التكاليف، وتسريع العمليات، مما يعزز من كفاءة البيئة الرقمية التي تتميز بالموثوقية والأمن.

كما أن المشرع الجزائري قد اعترف بأهمية التوقيع الإلكتروني من خلال إصدار قوانين تنظم استخدامه، بالإضافة إلى سن تشريعات لحماية التوقيع الإلكتروني وصد الجرائم المعلوماتية، فضلاً عن التصدي للاعتداءات على التوقيع والتصديق الإلكتروني.

اقتضت الدراسة المزج بين أكثر من منهج فاعتمدنا على المنهج الوصف بتقديم وصف دقيق للموضوع من خلال تحديد الإطار المفاهيمي للتوقيع الإلكتروني وجمع البيانات المتعلقة به ويساعد هذا المنهج في تقديم فهم شامل لمختلف جوانب الموضوع، مما يسمح بتوضيح المفاهيم المرتبطة بالتوقيع الإلكتروني بشكل منظم ودقيق.

1- قانون رقم 15-04 مؤرخ في 1 فيفري 2015، المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، الصادر في ج ر ع 06، مؤرخة في 10 فيفري2015.

كما استخدمنا المنهج التحليلي الذي بهدف إلى فحص وتحليل النصوص القانونية المتعلقة بالتوقيع الإلكتروني، سواء في التشريعات الوطنية أو الدولية، بالإضافة إلى دراسة ما تضمنته الاتفاقيات الدولية من أحكام ذات صلة وتقييم النصوص القانونية بشكل دقيق وتحليل الأطر القانونية المتاحة لتنظيم التوقيع الإلكتروني وحمايته.

ووظفنا المنهج المقارن للمقارنة بين التشريعات المتعلقة بالمعاملات الإلكترونية وذلك من خلال دراسة القوانين المتعلقة بالتوقيع الإلكتروني في دول مختلفة، إذ يتيح هذا المنهج الاطلاع على التوجهات القانونية المتنوعة وكيفية تعامل كل تشريع مع هذا الموضوع، مما يساعد في تحديد أوجه التشابه والاختلاف بين الأنظمة القانونية المختلفة.

بالنظر إلى الأهمية التي حضي بها التوقيع الالكتروني في المعاملات الالكترونية سوء على المستوى الدولي أو الوطني وباعتباره من المواضيع المستحدثة ارتأينا إلا إلى طرح هذه الإشكالية:**كيف نظم المشرع الجزائري التوقيع الإلكتروني وما هي الآليات المعتمدة لحمايته؟**

وتتطلب الإجابة عن هذه الإشكالية دراسته في شقين إذا نتطرق في الشق الأول من البحث إلى **مفهوم التوقيع الإلكتروني(الفصل الأول)**أما الشق الثاني فسنتناول **آليات حماية التوقيع الإلكتروني (الفصل الثاني).**

الفصل الأول

مفهوم التوقيع الالكتروني

تمهيد

يُعدّ التوقيع في المنظومة القانونية التقليدية، أداة جوهرية للتعبير عن الإرادة المنشئة للالتزام، وعن القبول الواعي لمضمون المحررات القانونية، وقد استقر الفقه والاجتهاد القضائي على اعتبار التوقيع الخطي المنجز بخط اليد على دعامة ورقية، شرطًا أساسًا لصحة كثير من التصرفات، وعنصرًا من عناصر القوة الثبوتية للوثيقة، غير أن الاعتماد الحصري على التوقيع الورقي لم يعد يواكب متطلبات العصر، خاصة في ظل ما تشهده العلاقات القانونية من تحول جذري نحو الرقمنة والمعاملات عن بعد.

وفي هذا السياق، جاء التوقيع الإلكتروني كآلية تقنية وقانونية مستحدثة، تتيح إثبات هوية الموقع والتصديق على صحة المحرر الإلكتروني بطريقة تضمن سلامته من أي تحريف، مع توفير درجة عالية من الأمان والموثوقية. وقد حظي هذا النوع من التوقيع باعتراف صريح في التشريعات الوطنية والدولية، التي أولته عناية خاصة بوضع ضوابط وشروط تضمن حجيته القانونية وفي هذا السياق، جاء التوقيع الإلكتروني كآلية وتعادله مع التوقيع التقليدي من حيث الآثار، سنتناول في هذا الفصل الإطار للمفاهيمي التوقيع الإلكتروني (المبحث الأول)، ثم وظائف وتطبيقات التوقيع الالكتروني(المبحث الثاني).

المبحث الأول

الإطار المفاهيمي للتوقيع الالكتروني

يعد التوقيع الالكتروني الركيزة الاساسية لصحة المعاملات الالكترونية والذي يضمن الامان و الموثوقية و المعتمد من جميع التشريعات سواء الدولية او المحلية وله دور كبير مما جعل هذه التشريعات تعترف به و تعطيه اولية و في هذا المبحث سوف نعرض التعريفات الفقهية و القضائية و كذا تعريف جل التشريعات في المطلب الاول اما في المطلب الثاني سوف نعرض الشروط الواجب توفرها في التوقيع الالكتروني بالإضافة الي اهم صور التوقيع الالكتروني

المطلب الأول

تعريف التوقيع الالكتروني

إن ظهور التوقيع الإلكتروني كآلية جديدة للتعاملات قد أثار تساؤلات عديدة حول طبيعته القانونية وتناول الفقه هذا المفهوم بتفسيرات متعددة وكذا تعامل القضاء معه، حتى جاء المشرّع ليمنحه إطارًا قانونيًا واضحًا وفي هذا المطلب، سنتطرق إلى التعريف الفقهي والقضائي (الفرع الأول)، ثم التعريف التشريعي للتوقيع الإلكتروني في محاولة لفهم الأساس القانوني الذي يستند إليه (الفرع الثاني).

الفرع الأول

التعريف الفقهي والقضائي للتوقيع الالكتروني

أولا: التعريف الفقهي.

حيث عرفه البعض انه "علامة أو رمز متمايز شخص بعينه يعبر الشخص عن إرادته ويؤكد حقيقة البيانات المتضمنة في المستند الذي وقعه"[1].

كما عرفه البعض على انه "مجموعة من الإجراءات التقنية أو الفنية التي يستطيع من خلالها التوصل لشخص الموقع والتعرف بشكل لا يقبل الشك في تحديد هويته والاستيثاق من أن الإجراء صدر عنه وقبل به" [2]

وعرف أيضا انه " مجموعة من الأرقام التي تختلط وتمتزج بعمليات حسابية معقدة ليظهر في النهاية كود سري خاص بشخص معين"[3].

و نجد أيضا من عرفه على انه "إجراء معين يقوم به الشخص المراد توقيعه على المحرر سواء كان الإجراء في شكل رقم أو رمز أو شفرة خاصة من شأنه إن يمنح الشخص و يفيد مما لا شك فيه إن مثل هذا التوقيع هو فعل صادر عن صاحبه أي حامل الشفرة أو الرقم"[4].

بعد التعرض إلى العديد من التعريفات الفقهية للتوقيع الإلكتروني، كل حسب الزاوية التي يُنظر منها إلى هذا المفهوم فبعض التعريفات تركز على الجانب التقني للتوقيع

---

[1]– حملاوي خلود، بركاوي نورة، التوقيع الالكتروني وحجيته في الإثبات، مذكرة نيل شهادة الماستر تخصص أعمال، جامعة 08 ماي 1945، قالمة، 2017، ص13.

[2] – محمد بن محمد أيوب، أثر التطورات التكنولوجية الحديثة في وسائل الإثبات التجاري والتوقيع الرقمي والسندات التجارية دراسة مقارنة، ط1، مركز الدراسات العربية، مصر، 2024، ص 234.

[3] – بولافة سامية، غيلاني طاهر، التوقيع الالكتروني في ظل القانون 04/15 ،مجلد05 ،العدد01 ،2019 ،ص112

[4] – خالد سعد وغلول ، الحماية القانونية للتجارة الالكترونية، مجلة الحقوق، عدد خاص، الكويت،2005

الإلكتروني، حيث يُعتبر التوقيع الإلكتروني مجرد أداة تستخدم تقنيات ووسائل إلكترونية لإثبات صحة الوثائق والمعاملات، بينما هناك تعريفات أخرى تعتمد على الجانب الوظيفي، حيث يتم تحديد التوقيع الإلكتروني بناءً على الوظائف التي يؤديها في سياق المعاملات القانونية والإلكترونية، مثل التوثيق وإثبات الهوية وتأكيد الموافقة على محتوى المستندات[1].

ثانيا: التعريف القضائي التوقيع الالكتروني.

يعد القضاء الفرنسي وبوجه خاص محكمة النقض الفرنسية السابقة في الاعتراف بالتوقيع الالكتروني، حيث انه يحقق نفس الغرض، وهي تحديد هوية الموقع والتعبير عن إرادته وربط المحرر به، كما أن هذه الوسيلة الحديثة للتوقيع الالكتروني تقدم نفس ضمانات التوقيع التقليدي وقد يفوقه من حيث صعوبة التقليد أو التزوير، إذا الرمز السري لا يمكن أن يعرفه إلا الشخص صاحب الرمز، كما توجد أحكام قضائية تعترف بتوقيع الالكتروني على انه كل رمز خطي مميز وخاص يسمح بتحديد صاحب التوقيع من جهة ومن جهة أخرى يعبر عن انصراف إرادته إلى الالتزام بمحتوى المحرر الموقع[2]

الفرع الثاني

التعريف القانوني للتوقيع الالكتروني

يعد التوقيع الالكتروني من الوسائل التقنية الحديثة والذي برز كبديل للتوقيع التقليدي نظرا للأهمية والدور الذي يلعبه بالمعاملات القانونية والإدارية والتجارية، مما جعل جل التشريعات سواء الوطنية منها أو الدولية على القيام بتنظيمه وإعطائه تعاريف قانونية والتي سوف نتطرق إليها:

1 – وسيم حسام الدين الأحمد، الإطار القانوني للإثبات الالكتروني، ط1، دار الراية للنشر والتوزيع، الأردن، 2025، ص18.

2– محمد بن محمد أيوب، المرجع السابق، ص235.

أولا: تعريف التوقيع الالكتروني في التشريعات الدولية النموذجية

تعد هذه التشريعات الدولية النموذجية كمرجع تستند أو تعتمد عليه جل التشريعات الوطنية في وضع قواعد للمعاملات الالكترونية وتوحيد المفاهيم القانونية المتعلقة بالبيئة الرقمية وفي مقدمتها التوقيع الالكتروني فنتطرق إلى تعاريفه:

1- قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية1996:لقد منح قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية لسنة 1996 حجية قانونية لرسائل البيانات الإلكترونية الموقعة توقيعاً إلكترونياً، مساوياً بذلك بين التوقيع الإلكتروني والتوقيع التقليدي من حيث الأثر القانوني في الإثبات.[1]

وبالرجوع إلى أحكام هذا القانون يُلاحظ أنه لم يضع تعريفاً مباشراً للتوقيع الإلكتروني وإنما اكتفى في المادة السابعة منه ببيان الشروط الواجب توافرها للاعتداد بالتوقيع الإلكتروني،[2]ويتضح من النص المادة 07 أن المشرّع النموذجي اعتمد نهجاً وظيفياً في تحديد التوقيع الإلكتروني، مرتكزاً على تحقق أمرين جوهريين: تعيين هوية الموقّع، والتعبير عن إرادته بالموافقة على محتوى الرسالة، مع ضرورة أن تكون الوسيلة المستخدمة في التوقيع محل ثقة وفقاً للغرض والسياق الذي تم فيه استخدام الرسالة.[3]

---

1 – قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية، قرار الجمعية العامة للأمم المتحدة 162/51، منشورات الأمم المتحدة، المؤرخ في 16 ديسمبر 1996.

https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/ar/ml-ecomm-a_ebook_1.pdf

2 – لالوش راضية امن التوقيع الإلكتروني، مذكرة لنيل شهادة الماجيستير، فرع القانون الدولي للأعمال، جامعة تيزي وزو 2012، ص 9.

3- قانون الأونسيترال النموذجي، السالف الذكر، فقد نصت الفقرة الأولى من المادة 07 على أن: "**عندما يُشترط القانون وجود توقيع منسوب إلى شخص ما إذا استُخدمت طريقة لتحديد هوية ذلك الشخص، وللدلالة على موافقته على المعلومات الواردة في رسالة البيانات، وكانت تلك الطريقة موثوقاً بها بما يكفي للغرض الذي أُنشئت أو أُبلغت من أجله رسالة البيانات، وذلك في ضوء الظروف، بما في ذلك أي اتفاقذي صلة بالأمر.**"

2-قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية لسنة 2001:نص قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية لسنة 2001 في مادته الثانية على تعريف التوقيع الإلكتروني بأنه :"**بيانات تتخذ شكلاً إلكترونياً، تُدرج ضمن رسالة البيانات أو تُضاف إليها أو ترتبط بها منطقياً، وتُستخدم لتحديد هوية الموقع، وللدلالة على موافقته على محتوى رسالة البيانات**".[1]

يُفهم من هذا التعريف أن قانون الأونسيترال لم يُحدد شكلًا أو وسيلة تقنية معينة للتوقيع الإلكتروني، سواء كانت موجودة حاليًا أو قد تظهر في المستقبل، وذلك في سياق إنشاء التوقيع الإلكتروني، بل منح القانون الدول حرية اختيار الطريقة التقنية التي تراها مناسبة، بشرط أن تكون هذه الطريقة قادرة على تحقيق الوظائف الجوهرية التي يتطلبها التوقيع الإلكتروني، والتي تتمثل في:

- التحقق من هوية الشخص الموقع.
- التعبير عن إرادة الموقع وموافقته على محتوى رسالة البيانات.

بناءً على ذلك فإن معيار اعتماد التوقيع الإلكتروني لا يعتمد على شكله أو وسيلته التقنية فقط، بل على مدى قدرته على تحقيق هذه الوظائف القانونية الأساسية التي تضمن صحة التوقيع وفاعليته في المعاملات القانونية[2].

1 - قرار رقم 56-80 للجمعية العامة للأمم المتحدة للقانون التجاري الدولي، يتضمن قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية، الجلسة العامة 75، منشورات الأمم المتحدة،12 ديسمبر 2001.

https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/ar/ml-elecsig-a.pdf

2 - ربحي تبوت فاطمة الزهراء، قانون المعاملات الالكترونية وفقا لقانون 18-05، ط2، بيت الافكار، الجزائر2022، ص246.

3-التوقيع الإلكتروني في توجيهات الاتحاد الأوروبي 93-1999: تهدف التوجيهات الأوروبية بشكل أساسي إلى التنسيق بين التشريعات الوطنية للدول الأعضاء، بما يساهم في تحسين التعاون القانوني بينها وإزالة العقبات القانونية[1]، فضلاً عن تحديث التشريعات لمواكبة التقدم التكنولوجي المتسارع وآثاره ويُعتبر التوقيع الإلكتروني أداة قانونية وتقنية أساسية في سياق التحول الرقمي والمعاملات الإلكترونية.

في توجيه الاتحاد الأوروبي رقم 93-1999، تم تعريف التوقيع الإلكتروني في المادة 2، الفقرة 1، على أنه "بيانات في شكل إلكتروني تكون مرفقة أو مرتبطة بشكل منطقي ببيانات إلكترونية أخرى وتُستخدم كوسيلة للمصادقة.[2]

كما قام التوجيه بتمييز أنواع مختلفة من التوقيعات الإلكترونية، والتي تشمل:

أ-التوقيع الإلكتروني العادي:يُعرَّف على أنه معلومة تأخذ شكلاً إلكترونيًا ترتبط بشكل منطقي ببيانات إلكترونية أخرى. وبالتالي، يُعتبر التوقيع الإلكتروني العادي وسيلة إلكترونية لإثبات الموافقة على محتوى معين أو المصادقة عليه.

ب- التوقيع الإلكتروني المتقدم والمؤهل:هو توقيع يرتبط ارتباطًا غير قابل للفصل بالنص الموقع، ويجب أن يحقق مجموعة من الشروط لكي يُعتبر متقدمًا ومؤهلًا، وهي:

- أن يكون التوقيع مرتبطًا ارتباطًا فريدًا ومحددًا بالموقع.

- أن يكون من الممكن تحديد هوية صاحب التوقيع بشكل دقيق.

- أن يُنشأ باستخدام وسائل يتحكم فيها الموقع وحده، أي تحت إشرافه الكامل.

1 - ربحي تبوت فاطمة الزهراء، المرجع السابق، ص 246.

2- Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques.

-https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=celex%3A31999L0093

– أن يرتبط التوقيع بالبيانات التي وُضع عليها، بحيث يُكشف أي تعديل لاحق لتلك البيانات.

بناءً على هذه الشروط يُعتبر التوقيع الإلكتروني المتقدم والمؤهل أكثر موثوقية وقوة قانونية مقارنة بالتوقيع الإلكتروني العادي، ويُعد وسيلة أكثر أمانًا للمصادقة في المعاملات الإلكترونية[1].

ثانيا: تعريف التوقيع الالكتروني في التشريعات الدولية الأجنبية

1- التشريع الفرنسي: أقرّ المشرع الفرنسي، بموجب القانون رقم 2000-230 المتعلق

بتكييف قواعد الإثبات في القانون المدني مع تكنولوجيا المعلومات، تعديلاً مهماً تم بموجبه إدراج أحكام جديدة تتعلق بالتوقيع الإلكتروني، وذلك تنفيذاً لأحكام التوجيه الأوروبي رقم93-1999 لاسيما المادة 5فقرة 2 منه، التي تُلزم الدول الأعضاء باعتماد القواعد والإرشادات المتعلقة بالتوقيع الإلكتروني.

وقد نصّت المادة 1316 من القانون المدني[2]، بعد التعديل، على أن التوقيع الإلكتروني يُعد وسيلة تقنية تتيح التحقق من هوية الموقع وتضمن سلامة الوثيقة الموقعة

1- دحماني سمير، التوقيع الإلكتروني الموصوف، مجلة العلوم الإنسانية، المجلد 01، العدد01، المركز الجامعي تندوف، 20جوان 2017، ص ص 181-183. ص ص 179-191.

2- Art 2-2-d du Décrit 93-1999 CE, de 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques, j.o n 13 du 19 janvier 2000, Art 1-2-c du Décrit n 2001-272du 30,ars 2001, pris pour l'application de l'article 1316-4 code civil et relatif a la signature électronique, j.o n 77 du 31 mars 2001.

– أنظر المادة 1316 من القانون المدني الفرنسي 2000-230، مؤرخة بتاريخ13-03-2000، الجريدة الرسمية، 14-03-2000

ويُضفي عليه نفس الحجية القانونية التي يتمتع بها التوقيع التقليدي، شريطة أن يستند إلى آلية موثوقة[1]تضمن هذه الوظائف.

كما نص المرسوم رقم 272-2001، الذي يطبق أحكام المادة 1316-4 من القانون المدني الفرنسي، على التمييز بين نوعين من التوقيعات الإلكترونية[2]: التوقيع العادي والتوقيع الموصوف، كما أقرّ هذا المرسوم مجموعة من الشروط الأساسية التي يجب توافرها في التوقيع الإلكتروني لضمان مصداقيته وفاعليته القانونية، وتنص المادة 1 من المرسوم في فقرتيها 1 و2 على الشروط التالية:

أ- أن يكون التوقيع خاصًا ومنسوبًا إلى الشخص الموقع: أي أنه يجب أن يكون التوقيع مميزًا بحيث يمكن ربطه بشكل غير قابل للشك بالشخص الذي قام بتوقيعه، مع ضمان عدم إمكانية التلاعب أو التزييف في نسبه إليه.

ب- أن يتم إنشاؤه بواسطة وسائل تضمن احتفاظ الشخص الموقع ويكون تحت سيطرته: يجب أن يتم التوقيع الإلكتروني بواسطة وسيلة تكنولوجية آمنة وموثوقة، مثل رمز سري أو شهادة رقمية، تكون تحت سيطرة الشخص الموقع بشكل حصري ودقيق، مما يمنع أي طرف آخر من التلاعب أو الوصول غير المصرح به إلى التوقيع.

ج- أن يضمن ارتباط البيانات بالتوقيع الإلكتروني بما يمنع أي تعديل أو تزوير مع إمكانية الكشف عنها لاحقًا: يجب أن تكون البيانات المرفقة بالتوقيع الإلكتروني مترابطة بطريقة تضمن عدم إمكانية تعديلها أو تغييرها بعد توقيعها، كما يجب أن يتيح النظام إمكانية التحقق من صحة التوقيع في وقت لاحق، حتى في حالة حدوث أي نزاع أو حاجة لإثبات صحة الوثيقة الموقعة.

---

1 - محمد بن محمد أيوب، المرجع السابق، ص237

2-محمد بن محمد ايوب، المرجع نفسه، ص238

تم إلغاء المرسوم رقم 272-2001 بموجب الأمر رقم 131-2016 المؤرخ في 10 فبراير 2016، حيث تم استبدال المادة 1316-4 من القانون المدني الفرنسي بالمادة 1367 الجديدة[1]، التي تعكس التعديلات القانونية في مجال التوقيع الإلكتروني، هذه التعديلات تأتي في إطار تحديث المنظومة القانونية لضمان التوافق مع التطورات التقنية المتسارعة في مجال تكنولوجيا المعلومات[2].

مع صدور المرسوم رقم 1416-2017 بتاريخ 30 سبتمبر 2017،وتطبيقا لأحكام المادة 04 من الأمر السالف الذكر حيث أحالت المادة 02 منها لأحكام المرسوم السابق الذكر الملغى،[3]إلى الأحكام الواردة في اللائحة الأوروبية الجديدة رقم 910-2014 المتعلقة بالخدمات التوثيقية الإلكترونية(eIDAS) ،[4]هذه اللائحة الأوروبية تهدف إلى تنظيم التوقيع الإلكتروني وتوثيقه، مما يعزز التفاهم بين الدول الأعضاء في الاتحاد الأوروبي ويساهم في تحسين أطر العمل القانونية المتعلقة بالتوقيعات الإلكترونية عبر الحدود وبذلك، أصبحت المعايير القانونية المتعلقة بالتوقيع الإلكتروني أكثر توافقًا مع النظام الأوروبي الموحد، مما

1-Ordonnance n° 2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations, JORF n°0035 du 11 février 2016.

-**Article 1367-02**:Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'Etat.

2- محمد بن محمد أيوب، المرجع السابق، ص237.

3-Ordonnance n° 2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations

4- Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

- https://eur-lex.europa.eu/eli/reg/2014/910/oj/eng

يعزز الثقة في هذه الوسيلة الحديثة ويمكّن الأطراف المتعاملة إلكترونيًا من ضمان حقوقهم في جميع الدول الأعضاء في الاتحاد الأوروبي.[1]

1- المشرع الأمريكي: عرف المشرع الأمريكي في القانون المعاملات الالكترونية الموحد في المادة 02-102 التوقيع الالكتروني بأنه التوقيع الذي يصدر شكل الكتروني ويرتبط بسجل يقوم بتنفيذها واقرارها شخص بقصد التوقيع على السجل.[2]

في هذا التعريف، اكتفى بالاعتراف بالتوقيع الإلكتروني كوسيلة تقنية، دون تحديد شكل أو نوع محدد له، مما يتيح له مرونة في التكيف مع مختلف الأساليب التكنولوجية المتطورة كما أُشترط أن يرتبط التوقيع بسجل إلكتروني لضمان مصداقيته وقيمته القانونية[3].

وفي إطار قانون التجارة الإلكترونية الفيدرالي، تم تعريف التوقيع الإلكتروني على أنه "صوت إلكتروني أو رمز أو عملية معالجة إلكترونية مشتركة أو مرتبطة منطقيًا بعقد أو سجل آخر ويتم إعداده وتنفيذه من قبل شخص بنية التوقيع.

بمعنى آخر، التوقيع الإلكتروني ليس مجرد صورة لتوقيع مكتوب بخط اليد، بل هو أي طريقة رقمية تدل على هوية الشخص وتصميمه على الالتزام بمحتوى السجل الإلكتروني، يمكن أن يكون هذا الصوت، أو الرمز، أو العملية المادية، أو الإجراء الإلكتروني أو أي مزيج منها.[4]

1-محمد بن محمد أيوب المرجع نفسه، ص238.

2 - 114 stat.464, Electronic signatures in global and national commerce act; public law 106-229, 106th congress, 30 June 2000.

3- نقلا عن ترجمان نسيمة، الحماية الجنائية للتوقيع الالكتروني دراسة مقارنة، أطروحة لنيل شهادة الدكتوراه تخصص التجريم في قانون الاعمال، كلية الحقوق، جامعة ابن خلدون تيارت ،2020-2021، ص17.

4-114 stat.464, Electronic signatures in global and national commerce act, cit p.

من خلال هذا التعريف، نلاحظ أن المشرع قد ذكر بعض الصور المحتملة للتوقيع الإلكتروني، دون حصرها أو تقييدها بنوع محدد الهدف من ذلك هو فتح المجال أمام وسائل تكنولوجية مبتكرة أخرى قادرة على الوفاء بمتطلبات التوقيع الإلكتروني، بشرط أن تكون موثوقة وتقابل نفس الأغراض القانونية التي يؤديها التوقيع التقليدي.

بذلك يسمح هذا التوجه القانوني بتوسيع نطاق التوقيع الإلكتروني ليشمل كافة الوسائل التكنولوجية الحديثة التي توفر إمكانية التأكد من هوية الموقع وضمان سلامة الوثيقة الموقعة، بما يواكب التطور السريع في تكنولوجيا المعلومات[1].

ثانيا: تعريف التوقيع الالكتروني في التشريعات العربية

1- المشرع الأردني:وفقا لأحكام المادة 02 فقرة 9 من القانون رقم 85 لسنة 2001 الملغى[2] نلاحظ بان المشرع الأردني انه قد تطرق إلى صور التوقيع وأوردها على سبيل الحصر وهو بدلك لم يترك المجال لأنواع جديدة قد تفرزها التكنولوجيا مستقبلا بالإضافة إلى إدراجه مجموعة من الوظائف وهي تحديد هوية الشخص وما يميزه عن غيره مع الموافقة على ما ورد في مضمونه، كما ورد في المادة 7 فقرة ا من نفس القانون أين منح المشرع وسوى بين التوقيعين التقليدي والالكتروني وسوى بينهما في الحجية.

تدارك المشرع الأردني هذه النقائص وقام بإصدار قانون جديد متعلق بالمعاملات الالكترونية رقم 15 سنة 2015[3] ، وعرفه في المادة 02 فقرة 10 وأين فتح المجال لأي وسيلة مرتبطة به قصد تحديد هوية الموقع وانفراده في استخدامه وتمييزه عن غيره

1- ترجمان نسيمة، المرجع نفسه، ص17.

2- انظر المادة02 فقرة 9 من القانون رقم 85 لسنة 2001، متعلق بالقانون المؤقت للمعاملات الالكترونية الأردني،ج ر ،ع 4524،الصادر في 2001/12/31

3-أنظر المادة 02 فقرة10 قانون رقم 15 لسنة 2015، متعلق بقانون المعاملات الالكترونية الأردني،ج ر،ع 5341،الصادر في 201510/05/17

2- المشرع المصري: عرف المشرع المصري التوقيع الالكتروني في المادة 01 فقرة ج من القانون رقم 15 لسنة 2004 المتضمن القانون الخاص بالتوقيع الالكتروني المصري[1] أين نجد المشرع لم يحدد صور التوقيع على سبيل الحصر بل على سبيل المثال ليتيح لأنواع جديدة قد تفرزها التكنولوجيا مستقبلا بالإضافة إلى تبيان وظائف التوقيع.

كما أصدر المشرع المصري قرارا وزاريا رقم 361 لسنة 2020 المتضمن اللائحة التنفيذية لقانون تنظيم التوقيع الالكتروني وإنشاء هيئة تنمية وصناعة تكنولوجيا المعلومات والدي أتي لتحديث وتطوير منظومة التوقيع الالكتروني ونجده في مادته الأولى قد جاء بنفس التعريف والصيغة المشار إليها سابقا.

4- تعريف التوقيع الإلكتروني في القانون الجزائري: تفاعل المشرع الجزائري مع التحولات التكنولوجية السريعة واستخداماتها المتزايدة في المعاملات الإلكترونية، فحرص على مواكبة التشريعات النموذجية الدولية فيما يتعلق بالاعتراف بالتوقيع الإلكتروني في هذا السياق، جاء تعديل القانون المدني رقم 05-10 المؤرخ في 20 يوليو 2005، الذي نص في مادته 327 فقرة 2 [2]على الاعتراف القانوني بالتوقيع الإلكتروني.

كما اشترط المشرع الجزائري في المادة 323 مكرر 01 توفر مجموعة من الشروط الأساسية لإضفاء الطابع القانوني على التوقيع الإلكتروني، والتي تتمثل أولا في التأكد من هوية الشخص الذي أصدر التوقيع الإلكتروني مما يضمن ضمان صحة التوقيع والمصداقية القانونية له، وثانيا **أن تكون منظومة إنشاء التوقيع الإلكتروني محفوظة في ظروف تضمن سلامته:**وهو ما يعكس شرط الأمان التقني اللازم لضمان عدم التلاعب أو التزوير في التوقيع الإلكتروني.

1- انظر المادة 01 فقرة ج قانون رقم 15-2004 مؤرخ في 21 أفريل 2004، يتضمن تنظيم التوقيع الالكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات، الصادر في ج ر ع 17 تابع (د)، مؤرخة في 22 أفريل 2004

2- أنظر المادة 327 من القانون رقم 05-10، يعدل ويتمم للقانون المدني، ج ر، عدد44، مؤرخ في 20-07-2005.

تعتبر هذه الشروط مشابهة لتلك المتعلقة بالكتابة الإلكترونية حيث يُنظر إلى التوقيع الإلكتروني والكتابة الإلكترونية على أنهما يؤديان نفس الوظيفة القانونية من حيث التأكد من هوية الموقع والربط بينه وبين الوثيقة الموقعة،[1]علاوة على ذلك، أشار المشرع الجزائري في المادة 3، الفقرة 1 والفقرة 2 من المرسوم التنفيذي رقم 07-162 المؤرخ في 30 مايو 2007، الذي تم إلغاؤه لاحقًا، إلى تعريف التوقيع الإلكتروني وأوضح في الفقرة 2 التوقيع الإلكتروني المؤمن، مشددًا على ضرورة استيفاء مجموعة من الشروط المحددة في المواد 323 و323 مكرر 01 من القانون[2].

بصدور القانون رقم 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين، تم تعريف التوقيع الإلكتروني في المادة 2، الفقرة 1 على أنه "بيانات في شكل إلكتروني، مرفقة أو مرتبطة منطقيًا ببيانات إلكترونية أخرى، وتُستخدم كوسيلة توثيق قانوني" هذه التعريفات تعزز من حجية التوقيع الإلكتروني في المعاملات القانونية وتضمن قابليته للإثبات أمام القضاء.

كما أُصدر المرسوم التنفيذي رقم 16-142 المؤرخ في 5 مايو 2016، الذي حدد كيفية حفظ الوثائق الموقعة إلكترونيًا[3]، تنفيذًا لأحكام المادة 4 من القانون رقم 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين[4]، أين يتضمن هذا المرسوم مجموعة من الإجراءات

1 -ربحي تبوت فاطمة الزهراء، المرجع السابق، ص249

2-أنظر المادة 3 من المرسوم التنفيذي رقم 07-162 مؤرخ في 30-05-2007، يعدل ويتمم المرسوم التنفيذي رقم 01-123 مؤرخ في 09-05-2001 المتعلق بنظام الاستغلال الطبق على كل نوع من أنواع الشبكات، ج ر، عدد37، سنة 2007.

3- المرسوم التنفيذي رقم 16-142 مؤرخ في 05-05-2016، المحدد لكيفيان حفض الوثيقة الكترونيا، ج ر، عدد 28، سنة 2016.

4 - أنظر المادة 4 من القانون 15-04 مؤرخ في 01-02-2015، المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، ج ر، عدد06، سنة 2015.

التي تهدف إلى ضمان التمييز بين الوثائق الموقعة إلكترونيًا وغير الموقعة[1]، وتوضيح الشروط والضوابط المتعلقة بالتصديق على التوقيعات الإلكترونية في المعاملات القانونية..

المطلب الثاني

شروط وصور التوقيع الالكتروني

بعد التطرق في المطلب الأول إلى التعريفات للتوقيع الالكتروني واعتراف من العديد من التشريعات الدولية و الوطنية و بروزه كآلية جديدة أثبتت فاعليتها و بديلا قانونيا للتوقيع التقليدي في التعاملات الرقمية ، وكما أثرت بحجية ولكن شرط أن يستوفي شروط محددة تضمن حجية قانونية و تكفل سلامة التعاملات و يكسب قوته الإلزامية في مواجهة الغير، إلا أن التوقيع الالكتروني لا يرد في صورة واحدة بل يأخذ عدة صور تختلف من حيث القوة القانونية ، و مستوى التقني و مدى الحماية التي توفرها و سوف نتطرق إلى أهم هذه الشروط التي تصيف على التوقيع حجية و كذا اهم صور التوقيع الالكتروني

الفرع الأول

شروط التوقيع الالكتروني

التوقيع الالكتروني وسيلة من الوسائل القانونية المعترف بها في الإثبات وقد اشترط الفقه لاكتساب هذه الحجية توافر 3 شروط أساسية لابد من التوقيع الالكتروني أن يحقها وهي: أن يكون التوقيع علامة مميزه للموقع وكذا وجوب ارتباط التوقيع بالمحرر و أن يكون التوقيع مقروءا ومستمرا.

1-محمد بن محمد أيوب، المرجع السابق، ص 242.

أولا: أن يكون التوقيع علامة مميزه للموقع

يعد التوقيع الإلكتروني من أبرز الأدوات المميزة التي تحدد هوية الشخص الموقع وتفرده عن غيره، يعد من العلامات المميزة للشخص الموقع عن غيره حيث لا يمكن أن تتشابه التواقيع الإلكترونية أو أن يتم إصدار توقيع مماثل لشخص آخر وهذا يعزز من مستوى الأمان في المعاملات الإلكترونية، خصوصًا في العقود التي تُعقد عبر الإنترنت باستخدام التوقيع الإلكتروني.[1]

نجد التوقيع بالقلم الإلكتروني، الذي يُعد وسيلة فعالة لتمييز الشخص الموقع عن غيره، يتم تخزين هذا التوقيع في نظام إلكتروني يسمح بمقارنته مع التوقيع المعتمد مسبقًا، مما يتيح التحقق من صحته ومصداقيته عند الحاجة.

أما التوقيع الرقمي فيعتمد على تقنيات التشفير الحديثة التي تستخدم مفتاحين الأول مفتاح عام يستخدمه المستقبل للتحقق من التوقيع، والثاني مفتاح خاص يحتفظ به الشخص الموقع ولا يمكن لأي طرف آخر الاطلاع عليه، هذه الآلية تضمن الأمان الكامل في التوثيق الإلكتروني، حيث يتيح للمستلم التحقق من صحة التوقيع الرقمي عبر الجهات المعتمدة، مما يجعل عملية التحقق من التوقيع أكثر موثوقية.[2]

كما يعتمد التوقيع البيومتري على الخصائص الذاتية والفريدة التي تميز كل شخص، مثل بصمة الإصبع أو قزحية العين أو حتى الصوت، نظرًا لأن هذه الخصائص لا يمكن أن تتطابق بين شخصين، فإن التوقيع البيومتري يوفر مستوى عالٍ من الأمان، بالإضافة إلى

1- نضال سليم برهم، أحكام عقود التجارة الالكترونية، دار الثقافة، الاردن، 2010، ص299.

2 - فتيحة حزام، قانون المعاملات الالكترونية دراسة على ضوء القانون 18-05، لفا للوثائق، قسنطينة الجزائر2022، ص121.

ذلك، يُعتبر الرقم السري المصاحب للتوقيع البيومتري سرًا شخصيًا لا يمكن معرفته إلا من قبل الموقع، مما يضمن عدم إمكانية تكرار التوقيع أو التلاعب به في النظام.[1]

ثانيا: ارتباط التوقيع بالمحرر

يعتمد هذا الشرط بشكل أساسي على قدرة الآليات والتقنيات المستخدمة في توفير أقصى درجات الأمان والحماية والسرية، بحيث يضمن ارتباط التوقيع بالمحرر بشكل لا يقبل الفصل أو التلاعب به كما يضمن ألا يتمكن أي شخص آخر غير صاحب المحرر من الاطلاع عليه أو تعديل محتواه، وذلك من خلال استخدام نظم تشفير متطورة وتقنيات حماية متقدمة هذا الشرط يعزز من مصداقية الوثيقة الإلكترونية، ويضمن سلامتها القانونية في أي اعتداء، سواء كان في المعاملات التجارية أو العقود القانونية، مما يضفي عليها طابعًا من الثقة والموثوقية.[2]

ثالثا: ان يكون التوقيع مقروءا ومستمرا

يعتبر التوقيع الإلكتروني من أشكال الكتابة القانونية، وبالتالي فإنه يخضع للأحكام والشروط المقررة لصحة الكتابة التقليدية. يجب أن يكون التوقيع مقروءًا وواضحًا بما يتيح الرجوع إليه والاطلاع عليه في وقت لاحق أما بالنسبة للاستمرارية، فيتمثل ذلك في توفير الوسائل الإلكترونية التي تضمن الحفاظ على المعلومات المخزنة لفترة زمنية محددة وقد حدد المشرع الجزائري مدة صلاحية هذه الوسائل الإلكترونية بما يتناسب مع مدة الحفظ التي يجب أن تظل خلالها البيانات الموقعة محفوظة وسليمة، وفقًا للمعايير القانونية المحددة في التشريعات ذات الصلة.[3]

1- يمينة حوحو، عقد البيع في القانون الجزائري، دار بلقيس، الدار البيضاء الجزائر، 2016، ص182.

2- نضال سليم برهم، المرجع السابق، ص 136.

3- محمد بن محمد أيوب، المرجع السابق، ص 265.

الفرع الثاني

صور التوقيع الالكتروني

إن اختلاف التقنيات المستخدمة التوقيع الالكتروني أدت إلى ظهور العديد من الأشكال والصور لهذا التوقيع ولعل أهمها وأكثرها انتشارا توقيع باستخدام القلم الالكتروني(أولا)، ثم التوقيع الرقمي (ثانيا) وفي الأخير التوقيع البيومتري أو التوقيع بالخواص الذاتية (ثالثا).

أولا: توقيع باستخدام القلم الالكتروني

يتم إنشاء التوقيع الإلكتروني من خلال استخدام قلم إلكتروني خاص، يُمكِّن المستخدم من إدخال بيانات التوقيع عبر برامج إلكترونية مخصصة لهذا الغرض. وتقوم هذه البرامج بتسجيل كافة الحركات والتفاعلات التي تتم أثناء عملية التوقيع على الشاشة، بما في ذلك الشكل، الحجم، النقاط، الخطوط، ودرجة الضغط على القلم، حيث يتم تحويل هذه البيانات إلى توقيع رقمي ذي خصائص تقنية مميزة وفريدة.

وتُخزّن هذه البيانات في النظام الإلكتروني، بحيث يمكن الرجوع إليها عند الحاجة للتحقق من صحة التوقيع المعروض، وذلك من خلال مقارنته بالتوقيع الأصلي المخزن داخل البرنامج المعتمد، وتُوفر هذه التقنية مستوى عالٍ من الحماية والأمان مما يُحد من إمكانية التلاعب أو التزوير كما يُحقق هذا النوع من التوقيع وظيفتين أساسيتين[1]:

- التقاط التوقيع الإلكتروني بدقة واحترافية، بما يضمن تمثيل الإرادة الحقيقية للموقّع.

1- نضال سليم برهم، المرجع السابق، ص ص 240 – 241.

- التحقق من صحة التوقيع الرقمي، وهو ما يُضفي على الوثيقة الإلكترونية حجية قانونية ويضمن موثوقيتها وسلامتها من الناحية الفنية والقانونية.

ويُعد هذا النوع من التوقيع وسيلة فعالة تحقق الغاية القانونية المرجوة منه والمتمثلة في ضمان صحة ومشروعية المعاملات الإلكترونية.

ثانيا: التوقيع الرقمي

يعرف التوقيع الرقمي على أنه بيان أو معلومة مرتبطة بمنظومة بيانات أخرى أو صيغة مشفرة تُستخدم للتحقق من مصدر البيانات، وهو الأوسع والأكثر استعمالا لاعتماده على خاصية التشفير القائم على خوارزميات المفتاح الخاص والمفتاح العام مما يتيح للمرسل إليه التأكد من سلامة مضمون الرسالة وضمان أمانها ضد أي تعديل أو تحريف قد يطرأ عليها، وبذلك يُعتبر التوقيع الرقمي وسيلة فعالة لضمان التحقق من صحة المعاملات الإلكترونية وحمايتها من التزوير أو التعديل غير المصرح به.[1]

ثالثا: التوقيع البيومتري أو التوقيع بالخواص الذاتية

يرتكز هذا النوع من التوقيع أساسًا على الخصائص الشخصية والفردية لكل إنسان، أي السمات الفيزيائية، الطبيعية، والسلوكية التي تميز كل فرد عن غيره، يتم ذلك من خلال استخدام تقنيات متقدمة لالتقاط صورة لأحد أجزاء جسم الإنسان التي تختلف من شخص إلى آخر، وتخزين هذه الصورة بطريقة مشفرة بعد ذلك، يتم التحقق من صحة التوقيع من خلال مقارنة السمات الشخصية المسجلة سابقًا مع تلك التي يتم جمعها في الوقت الفعلي [2] وتشمل هذه الأنواع من التوقيعات ما يلي:

1- ربحي تبوت فاطمة الزهراء، المرجع السابق، ص252.

2 - اياد احمد سعيد الساري، النظام القانوني لإبرام العقد الإلكتروني على ضوء قانون التوقيع الالكتروني والمعاملات الالكترونية، ط1، منشورات الحلبي الحقوقية، لبنان 2016، ص 129.

1- التوقيع بمسح العين البشرية: يشمل نوعين رئيسيين هما مسح شبكية العين ومسح قزحية العين، حيث يتم التقاط صورة للعين وتخزينها، ثم يتم التحقق من صحتها من خلال مقارنة الصورة المسجلة مع تلك المسجلة مسبقًا.

2- التوقيع ببصمة الوجه: يتم التقاط صورة للوجه باستخدام برنامج تصوير متخصص، ثم تخزين هذه الصورة عند التحقق من التوقيع، تتم المقارنة بين الصورة المسجلة والمخزنة في النظام وفي حال وجود أي اختلاف أو عدم تطابق، يتم رفض الدخول.

3-التوقيع بنبرة الصوت: يعتمد هذا النوع من التوقيع على رصد الصوت، حيث يتم تحويل الموجات الصوتية إلى صورة رقمية وتخزينها للتحقق من صحة التوقيع، تتم مقارنة الصوت الحالي مع الصوت المسجل مسبقًا لضمان تطابقهما وفي حال كان هناك أي اختلاف في النبرة أو الصوت، يتم رفض التوقيع.

المبحث الثاني

وظائف وتطبيقات التوقيع الالكتروني

بعد التطور التكنولوجي الذي شهده العالم اليوم، برز التوقيع الالكتروني كوسيلة قانونية وتقنية لضبط واثبات المعاملات الالكترونية، ولقد أصبح بديلا للتوقيع التقليدي، كما أصبح يؤدي وظائف متعددة تمكنه من إضفاء المشروعية على كل التعاملات الالكترونية وتعزيز الثقة والأمان بين الأطراف، كما امتد تطبيق التوقيع الالكتروني إلى عدة مجالات تمس مختلف القطاعات نظرا لما ما يقدمه من فعالية وسرعة وتوفير للجهد والتكلفة وسوف نتطرق في هدا المبحث إلى أهم وظائف التوقيع الالكتروني في المطلب الأول وكذا مجالات تطبيق التوقيع الالكتروني في المطلب الثاني.

المطلب الأول

وظائف التوقيع الالكتروني

إن للتوقيع الالكتروني وظائف أساسية يعبر فيها طرف المتعاقد عن إرادته وحضوره والتي تهدف أساسا لتحقيق الأمان في توثيق المستندات الالكترونية وهي نفسها الشروط التي يجب ان يوفرها فيه حتى يحوز على الحجية في الإثبات[1]ولعل أبرز هذه الوظائف نجد تحديد هوية الموقع والتعريف بشخصه (الفرع الأول) ثم التعريف بإرادة الموقع وقبوله لموضوع المحرر ومضمونه (الفرع الثاني)، مع إثبات سلامة المحرر (الفرع الثالث).

1-فيصل سعيد الغريب، التوقيع الإلكتروني و حجيته في الاثبات، منشورات العربية للتنمية الادارية، مصر، ص233

الفرع الأول

تحديد هوية الموقع والتعريف بشخصه

يعتبر التوقيع علامة شخصية تنسب إلى شخص معين بذاته. فالتوقيع التقليدي على الورق لا يثير أي إشكال قانوني، إذ تُعتبر الورقة الموقعة منسوبة إلى الشخص الموقع عليها، سواء كان التوقيع مقروءًا أم غير مقروء، وبالاسم الحقيقي أو المستعار، أو حتى باستخدام بصمة الإصبع ويظل التوقيع صحيحًا ما لم ينكر الموقع ما صدر منه، مع إمكانية الاستعانة بالخبراء للمضاهاة بين الخطوط والوثائق المتعلقة بتحديد الهوية في حالة نشوء نزاع.

وقد نصت المادة 327 من القانون المدني في شقها الأول على أن العقد العرفي يُعتبر صادرًا من الشخص الذي كتبه أو وقعه أو وضع عليه بصمة إصبعه، ما لم ينكر ذلك صراحة، وهو ما يعكس قدرة التوقيع التقليدي على إثبات هوية الموقع وموثوقية توقيعه[1].

أما فيما يتعلق بالتوقيع الإلكتروني الذي يتم في بيئة افتراضية غير مادية تتضمن تبادلًا للمعلومات والخدمات بين أطراف قد لا يعرفون بعضهم البعض ولا يرتبطون بأي علاقة مسبقة، فإن الأمر يستدعي ضرورة تحديد هوية الموقع بدقة وذلك يتم من خلال استخدام وسائل وتقنيات موثوقة، مثل التوقيع بالقلم الإلكتروني، التوقيع الرقمي، واستخدام أنظمة التشفير، لضمان موثوقية التوقيع الإلكتروني.[2]

1- راجع المادة 327 من الأمر رقم 75-58، السالف الذكر.

2- محمد بن محمد أيوب، المرجع السابق، ص ص 256 257.

أشار المشرع في المادة 327 من نفس القانون المدني في شقها الثاني إلى أنه يُعتد بالتوقيع الإلكتروني وفقًا للشروط المنصوص عليها في المادة 323 مكرر 1، والتي تشترط أن يتيح التوقيع الإلكتروني التحقق من هوية الموقع وشخصه[1].

كما نصت المادة 06 من **قانون** 15-04المتعلق بالتوقيع والتصديق الإلكترونيين على أن التوقيع الإلكتروني يُستخدم لتوثيق هوية الموقع وإثبات قبوله مضمون الكتابة في الشكل الإلكتروني[2].

علاوة على ذلك، أشار قانون الأونسيترال النموذجي لسنة2001**في** المادة 02 فقرة (أ) إلى أن التوقيع الإلكتروني يعني البيانات التي يمكن استخدامها لتحديد هوية الموقع بالنسبة للرسالة، وإظهار موافقته على المعلومات الواردة فيها.[3]

في حالة عدم قدرة التوقيع الإلكتروني على كشف هوية صاحبه بشكل دقيق وموثوق، فإنه لا يُعتد به قانونيًا، ولا يترتب عليه أي أثر قانوني[4].

الفرع الثاني

التعريف بإرادة الموقع وقبوله لموضوع المحرر ومضمونه

يقصد بالتعبير عن الإرادة قيام الشخص بإظهار مقصده بنية إحداث أثر قانوني، وذلك عبر إرادته الحرة والمستقلة في التوقيع التقليدي، يُعتبر وضع التوقيع على المحرر بمثابة دليل على اطلاع الموقع على ما ورد في الوثيقة وموافقته على محتواها ويعتبر التوقيع في هذه الحالة تعبيرًا عن الإرادة يقترن بالإقرار بالمحتوى وما يتضمنه المحرر.

1- راجع المادة 323 مكرر01 من الأمر رقم 75-58، السالف الذكر.

2- أنظر المادة 06 من القانون 15-04، السالف الذكر.

3- راجع المادة 02 ف أ من قانون الأونسيترال النموذجي لسنة2001، السالف الذكر

4- ربحي تبوت فاطمة الزهراء، المرجع السابق، 256

نصت المادة 60من القانون المدني على أن تعبير الإرادة يمكن أن يتم باللفظ أو الكتابة أو بالإشارة المتداولة عرفًا، كما يُعتبر اتخاذ موقف دال على المقصود من صاحبه تعبيرًا عن إرادته، حتى وإن لم يكن باللفظ أو الكتابة.[1]

أما في التوقيع الإلكتروني، فإنه بمجرد القيام بالفعل المادي الخاص بتوقيع المستند بشكل إلكتروني (سواء كان ذلك باستخدام رموز، أو أصوات، أو أي من الأساليب المعتمدة) يُعتبر ذلك إظهارًا للموافقة على مضمون المستند أو المعاملة الإلكترونية ويُعد التوقيع الإلكتروني تعبيرًا عن التزام الشخص بما ورد في الوثيقة، أو بمثابة إقرار قانوني بالالتزام بالمحتوى الإلكتروني[2].

أكدت المادة 327من القانون المدني على أن التوقيع الإلكتروني يُعد تعبيرًا عن الإرادة بما ورد في المحرر أو المستند الإلكتروني،[3] وكما ورد في المادة 06 منقانون15-04المتعلق بالتوقيع والتصديق الإلكترونيين، والتي نصت على أن التوقيع الإلكتروني يُستخدم لإثبات إرادة الموقع والقبول بالمضمون الوارد في الوثيقة الإلكترونية.[4]

أشار قانون الأونسيترال النموذجي لعام 2001فيالمادة 02 إلى أن التوقيع الإلكتروني يُعتبر بيانات تُستخدم لتحديد هوية الموقع، وكذلك لإظهار موافقته على المعلومات الواردة في الرسالة الإلكترونية، مما يعكس قوة حجية التوقيع الإلكتروني في التعبير عن الإرادة[5].

1- راجع المادة 60 من الأمر رقم 75-58، السالف الذكر.

2 - وسيم حسام الأحمد، المرجع السابق، ص27.

3- أنظر المادة 327 من الأمر رقم 75-58، السالف الذكر.

4- أنظر المادة 6 من القانون 15-04، السالف الذكر

5- أنظر المادة 2 من قانون اليونيسترال النموذجي 2001، السالف الذكر.

الفرع الثالث

إثبات سلامة المحرر

يقصد بسلامة المحرر أن مضمون الوثيقة أو العقد الالكتروني لم يتعرض لأي تعديل أو تحريف وتعد هذه الوظيفة أكثر حداثة وظهرت بظهور التوقيع الالكتروني، حيث أصبحت جميع التعاملات الالكترونية التي تتم عبر شبكة الانترنت عرضة لمخاطر أمنية وللحد من هذه المخاطر يجب استخدام آليات تحمي الوثيقة من التعديل وتمنع فصل الدعامة عن المضمون المحرر.[1]

يستند في هذا على إلي تقنية التشفير القائمة على نصام المفتاحين وذلك لضمان صحة وسلامة الوثيقة من أي تلاعب وتقوم هذه التقنية بتحويل المحتوى إلي رموز ثم يتم مقارنة النتائج بعد فك التشفير فادا كان التوقيع غير صحيح فان هدا يشير إلى أن البيانات قد تم تعديلها أو تحريفها وبالتالي لا يمكن فك الرموز مما يثبت عدم تطابق التوقيع مع الوثيقة الأصلية.[2]

المطلب الثاني

تطبيقات التوقيع الالكتروني

يعد التوقيع الإلكتروني ضرورة ملحة في المعاملات الإلكترونية الحديثة، خاصة في ظل غياب شرط الحضور الفعلي أثناء التعاقد، الذي يعد أساسًا في التعاملات التقليدية. بينما لا يُعد هذا الشرط ضروريًا في المعاملات الإلكترونية، فإن التوقيع الإلكتروني يوفر نوعًا من الأمان والثقة في هذه العمليات إذ يعمل كوسيلة للتحقق من هوية الموقع، مما يعزز

1- محمد بن محمد أيوب، المرجع السابق، ص261.

2- محمد بن محمد ايوب المرجع نفسه، ص262

مصداقية التعاملات ويُساهم في ضمان سلامة وسلاسة العمليات المالية وحمايتها من المخاطر المحتملة.

ويُعتبر التوقيع الإلكتروني أداة فعالة في تقديم ضمان قانوني وحماية للأطراف المتعاقدة، مما يساهم في تسهيل العملية التجارية والمالية، ويعزز من فعالية المعاملات الإلكترونية وفي هذا الفرع، سنتطرق إلى أهم تطبيقات التوقيع الإلكتروني في وسائل الدفع الإلكترونية.

الفرع الأول

بطاقات الدفع الالكترونية

بعدما كان السحب للنقود في الماضي وجوب حضور وتوقيع العميل أي وجود دليل كتابي على عمليه السحب أو الدفع لكن مع تطور التكنولوجيا وزيادة التعاملات البنكية ما اجبر البنوك أو المؤسسات المؤهلة لتسهيل هذه العمليات لذلك قامت باستصدار بطاقات الصرف الآلي أو ما يسمى بالبطاقات البنكية[1] والتي انتشرت وتعددت بشكل كبير في مجال المعاملات البنكية والتجارية والتي سوف نتعرض إليها بالتفصيل.

أولا: بطاقة الوفاء وتسمى أيضا بطاقة الدفع

تمنح بطاقة الدفع الإلكترونية لصاحبها القدرة على دفع مستحقاته من سلع وخدمات باستخدام الأموال المودعة في البطاقة بعد فتح حساب، دون الحاجة إلى تحويل الأموال مباشرة إلى حساب المتعاقد الآخر. يتم ذلك من خلال إدخال البطاقة في جهاز آلي للتحقق من صحة المعلومات وإدخال الرقم السري، حيث يُشترط وجود رصيد في البطاقة لضمان

1- فيصل سعيد الغريب، المرجع نفسه، ص 236

نجاح عملية الدفع[1] وتُعتبر بطاقة الدفع الإلكترونية بديلاً فعالًا للطرق التقليدية في المعاملات المالية.

تطرق المشرع الفرنسي في المادة 1132 من قانون النقد والقرض إلى البطاقة الإلكترونية، مُعرفًا إياها كأداة صادرة من المؤسسات الائتمانية التي تُمارس النشاط المصرفي، كما نصت المادة 511 من نفس القانون على السماح لحامل البطاقة بسحب أو تحويل الأموال[2].

أما المشرع الأردني فقد أشار إلى البطاقة الإلكترونية في المادة 21 من قانون المعاملات الإلكترونية رقم 15 لسنة2015، حيث أقر باستخدام الوسائل الإلكترونية لتحويل الأموال، مُعتبرًا إياها وسيلة مقبولة لإجراء الدفع الإلكتروني كما رفع البنك المركزي الأردني من مكانة هذه البطاقات باعتبارها أداة تتيح لحاملها إجراء العمليات المصرفية بشكل آمن ومريح عبر قنوات الدفع المعتمدة[3]، و سلك المشرع الجزائري نفس النهج في المادة 543 مكرر 23فقرة1 من القانون رقم05-02 المتضمن القانون التجاري[4]، حيث اعتبرت البطاقة الإلكترونية أداة صادرة من البنوك والهيئات المالية المؤهلة التي تسمح لحاملها بسحب أو تحويل الأموال.

1 – غراب نجاة، النظام القانوني للتوقيع الالكتروني في التشريع الجزائري، مذكرة لنيل شهادة الماستر، جامعة محمد خيضر بسكرة،2022ص 23

2- voir l'art 1132 et 511, de loi n° 99-1071 du 16 décembre 1999, Comprend le code monétaire et financier français, Modifié le 2025-05-29 par le Décret n°2025-470 du 28 mai 2025.

3 – أنظر المادة 21 من قانون المعاملات الالكترونية الأردني رقم15 لسنة 2015،الصادرة في ج ر ع 5341، مؤرخة في 17-05-2015.

4 –أنظر المادة 543 مكرر23 فقرة 1 من القانون رقم 05-02مؤرخ في 06-02-2005، يعدل ويتمم الامر رقم 75-58 مؤرخ في 26 سبتمبر 1975 يتضمن القانون التجاري، الصادرة في ج ر ع 11، مؤرخة في 09-05-2005.

وتدارك المشرع في القانون 18-05 المتعلق بالقواعد العامة للتجارة الإلكترونية[1]، وأوضح أنه لم يعد إصدار البطاقة مقتصرًا على البنوك والهيئات المالية فحسب، بل يمكن لأي وسيلة دفع مرخصة بموجب التشريع المعمول به أن تتيح لحاملها إجراء عمليات الدفع أو التحويل عبر المنظومة الإلكترونية[2].

ثانيا: بطاقة السحب الآلي

بطاقة تمنح للعميل بعد فتح حسابات لديها وإيداع مبلغ مالي معين بحيث تمنح لحامل تلك البطاقة السحب والتحويل من حساب إلى أخر والكشف عن الرصيد إلى غيرها من الخيارات من خلال أجهزة الصراف الآلي وذلك بإدخال البطاقة في الصراف الآلي وتأكيد إدخال الرقم السري الذي يعد توقيعا الكترونيا للعميل ويعد إتماما للعملية بسحبه لبطاقته بطريقه آلية[3].

أشار المشرع الجزائري إلى تعريفها بموجب المادة 543 مكرر 23 فقره اثنان بأنها بطاقة سحب صادرة عن البنوك أو الهيئات المالية المؤهلة قانونا حيث تسمح لصاحبها سحب الأموال.[4]

ثالثا: البطاقات الائتمانية

تعرف على إنها بطاقات تصدرها البنوك والمؤسسات المالية وحتى الشركات التجارية بحيث تتعهد بناء على عقد مع حامل البطاقة بدفع وتسديد جميع مشترياته مقابل التزام

1- القانون رقم 18-05 المتعلق بالتجارة الالكترونية، مؤرخ في 10-05-2018، الصادرة في ج ر ع 28، مؤرخة في 18-05-2018.

2- حملاوي خلود بركاوي نورة، المرجع السابق، ص52

3غراب نجاة، النظام القانوني للتوقيع الالكتروني في التشريع الجزائري، مذكرة ماستر، تخصص قانون اعمال، كلية الحقوق والعلوم السياسية جامعة محمد خيضر بسكرة، 2022، ص23.

4- انظر المادة 543 مكرر23 من القانون نفسه

صاحب البطاقة بتعبئتها في الآجال المحددة وإلا تعرض لدفع فوائد عالية كما أنها تحدد سقفا معينا لا يمكن تجاوزه مع اشتراط تقديمه لضمانات عينية أو شخصية ويتم تطبيق التوقيع الالكتروني في هذه البطاقة بواسطة التوقيع الرقمي.

هو نظام يعتمد على التشفير وذلك من خلال نقل البيانات الموجودة بالبطاقة إلى مركز بطاقة الائتمان للتأكد من صحة وصلاحية البيانات وتحويل المال المستحق بطريقة الكترونية أمنة ويكون إثبات الدفع بالبطاقة الائتمانية عند استعمالها بواسطة سندات ورقية كما يمكن أن يتم ذلك بواسطة وسائل الكترونية بحيث يتم تسجيل وتخزين العمليات المنجزة بواسطة أجهزة الكترونية التي تمر من خلالها البطاقة، بالإضافة إلى أن طريقة صنعها و التكنولوجيا التي تتمتع بها هذه البطاقات والتي تسمح بتسجيل كل العمليات التي استخدمت فيها.[1]

كما ألزم المشرع الجزائري بموجب المادة 111 من قانون المالية لسنة 2018حيث يتعين على كل متعامل اقتصادي القائم على تقديم السلع والخدمات أن يوفر للمستهلكين وسائل الدفع الكترونية تسمح لهم بدفع ثمن المشتريات وحدد أجال لبداية العمل بهذه البطاقة في اجل أقصى سنة من تاريخ نشره في الجريدة الرسمية[2]، وقانون المالية 2019 أكد الالتزام بالعمل بالمادة 111 المعدلة والمتممة إضافة إلى تحديد الجهات المعتمدة والمصدرة للبطاقة ألا وهي البنوك وبريد الجزائر كما حدد كحد أقصى للامتثال لهذه الأحكام إلى 31 ديسمبر 2020.[3]

1- محمد بن محمد أيوب، المرجع السابق، ص272

2 - أنظر المادة 111 من القانون 17-11 يتضمن قانون المالية لسنة 2018، مؤرخ في 27-12-2017، الصادرة في ج ر ع 76، مؤرخة في 28-12-217

3 - أنظر المادة 111 من القانون19-04 يتضمن قانون المالية لسنة2019، مؤرخ في 11-12-2019، الصادرة في ج ر ع 81، مؤرخة في 30-12-2019

الفرع الثاني

الشيكات والعملات الالكترونية

ان التطور السريع للتكنولوجيا ساهم بشكل كبير في بروز وسائل دفع وتحويلات للأموال ومن أبرز هذه الوسائل نجد العملات الافتراضية والشيكات الإلكترونية، التي تعتبر بديلاً مبتكرًا لوسائل الدفع التقليدية. هذه الوسائل ساهمت في تسريع العمليات المالية وتقليل التكاليف، بالإضافة إلى تحسين الكفاءة، مما يعكس التوجه العالمي نحو مستقبل مالي رقمي أكثر مرونة ومواكبة للتطورات الحديثة.

وفي هذا السياق، يلعب التوقيع الإلكتروني دورًا محوريًا في ضمان مصداقية هذه المعاملات المالية الرقمية، سواء في الاقتصاديات العالمية أو المحلية، حيث يوفر مستوى من الأمان والثقة يساهم في تأكيد صحة العمليات ويعزز من قبولها في الأنظمة القانونية.

وفي هذا الفرع، سنتناول بالتفصيل الشيكات الإلكترونية أولا ثم العملات الافتراضية ثانيا

أولا: الشيك الالكتروني

يُعد الشيك الإلكتروني شكلاً حديثًا من وسائل الدفع، يتشابه من حيث البيانات والمحتوى مع الشيك الورقي التقليدي، غير أنه يُحرر في شكل إلكتروني ويُتداول عبر وسائط إلكترونية مؤمّنة، وهو عبارة عن رسالة إلكترونية موثقة وآمنة يُرسلها مصدر الشيك إلى المستفيد، الذي يقوم بدوره بتقديمه إلى البنك عبر الوسائل الرقمية، حيث يُراجع البنك الشيك ويتحقق من صحة الأرصدة والتوقيعات الإلكترونية، ثم يُعيده إلى المستلم باعتباره دليلًا على تنفيذ عملية الدفع[1].

1- محمد بن محمد أيوب، المرجع السابق، ص291.

وما نص عليه القانون 23-09 بأن كل الأدوات التي يستعملها الشخص والتي تمكنه من تحويل أموال باستعمال أي سند أو أسلوب تقني أو عملة الكترونية تعتبر في نظر هذا القانون من وسائل الدفع.[1]

برغم أن المشرّع الجزائري لم يضع تعريفًا صريحًا للشيك الإلكترونيبل ذكر بصفة ضمنية وبالنظر إلى المادة 69 من القانون 03-11 المتعلق بالنقد والقرض التي تعتبر وسائل الدفع هي جميع الوسائل التي تمكن الأفراد من تحويل الأموال بغض النضر الي الوسيلة.[2]

كما نظم البيانات الأساسية التي يجب أن يتضمنها الشيك، وذلك في المادة 472 من القانون التجاري، وهي:ذكر كلمة "شيك" في متن السند، وأمر غير معلق على شرط بدفع مبلغ معين من النقود، مع اسم الشخص المُكلَّف بالدفع، وتاريخ ومكان إنشاء الشيك، ثم توقيع مصدر الشيك، وقد أشارت المادة 502 من القانون التجاري إلى إمكانية تقديم الشيك للوفاء عبر وسائل الاتصال الإلكترونية ما يُعَدّ اعترافًا ضمنيًا بالتعامل بالشيك الإلكتروني.[3]

كما نصّت المادة 46 الفقرة 4 من القانون رقم 18-04 المتعلق بالبريد والاتصالات الإلكترونية على أن تحويل الأموال يتم عبر كافة وسائل الدفع، سواء كانت كتابية أو إلكترونية،[4]بالإضافة أي المادة 06 من القانون 18-05 المتعلق بالتجارة الالكترونية أن أي

1- راجع المادة 74 من القانون رقم 23-09 مؤرخ في 21 جوان 2023، يتضمن القانون النقدي والمصرفي، الصادرة في ج ر ع 43، مؤرخة في 27 جوان 2023.

2- الأمر رقم 11-03 مؤرخ في 26 أوت 2003، يتعلق بالنقد والقرض، الصادرة في ج ر ع 52، مؤرخة في 27 أوت 2003.

3- راجع المواد 472 و502 من الأمر رقم 75-59 مؤرخ في 26 سبتمبر 1975، يتضمن القانون التجاري، مؤرخة في ح ر ع 101، مؤرخة 19 ديسمبر 1975، معدل ومتمم بموجب القانون رقم 22-09 مؤرخ في 05 ماي2022، الصادرة في ج ر ع 32، مؤرخة في 14 ماي 2022.

4-أنظر المادة 46 من القانون رقم 18-04 المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الالكترونية، مؤرخة في 10-05-2018، الصادرة في ج ر ع 27، مؤرخة في 13-05-2018.

وسيلة للدفع مرخص لها وفقا للتشريع المعمول تمكن صاحبها من القيام بالدفع سواء عن قرب أو عن بعد أو عبر منظومة الكترونية هي من وسائل الدفع.[1]

ويُضاف إلى ذلك ما نصّت عليه المادة 502 مكرر 1 من القانون التجاري التي تسمح باستعمال التوقيع الإلكتروني في المستندات التجارية، بما في ذلك الشيكات، مما يعزز من الإطار القانوني المنظّم لهذا النوع من المعاملات.[2].

ويتبين من المشرع بالاعتراف بإمكانية استعمال للشيكات الالكترونية في مختلف التعاملات بين الأفراد سواء التعاملات التجارية أو العادية وهذا يعتبر مؤشر ايجابي وقفزة نوعية نحو تنظيم استعمال هذه التقنيات الحديثة عبر مختلف قنوات الاتصال المفتوحة.

ثانيا: العملات الافتراضية

إن النقود الافتراضية موجودة حصرا في الفضاء الرقمي ويتم تداولها بواسطة الحواسيب أو الهواتف الذكية ولقد اعترفت بها التشريعات الدولية والوطنية وقد تم تعريفها كل على حده وهي كالاتي:

1- التوجيه الأوروبي رقم 46 - 2000 الخاص بالنقود الالكترونية الصادر 8 سبتمبر 2000: وقد عرفت على أنها بديل الكتروني للوحدات والأوراق النقدية المخزنة على دعامة الكترونية والمخصصة عموما للوفاء الالكتروني.[3]

2- التوجيه الأوروبي رقم 110-2019 الصادر في 16 سبتمبر 2009: عرفتها المادة02 فقره 2على أن العملة الالكترونية هي القيمة النقدية المخزنة بطريقة الكترونية على

1- أنظر المادة 06 من القانون رقم 18-05، السالف الذكر.

2- راجع المادة 502 مكرر 01 من الأمر رقم 75-59، السالف الذكر.

3-التوجيه الأوروبي رقم 46 - 2000 الخاص بالنقود الالكترونية مؤرخة 8 سبتمبر 2000.

وسيلة الكترونية أو مغناطيسية وتمثل دينا على عاتق الجهة المصدرة له مقابل إيداع مبلغ مالي من الشخص المعني.[1]

3- التشريع المصري: في القانون رقم 194 لسنة2020 البنك المركزي والجهاز المصرفي في المادة 01 على أنها قيمة النقدية مقومه بالجنيه المصري أو بإحدى العملات المصدرة من هيئات مرخصة[2]، وتُعد العملات الافتراضية هنا تلك التي تُخزن إلكترونيًا ويتم التعامل بها كوسيلة دفع، وتكون مستحقة للمرخص لهم بالعمل بها، كما يتم تداولها خارج نطاق التعامل النقدي التقليدي القطع النقدية والأوراق المالية.

وفقاً للمادة 206 من نفس القانون، يُحظر التعامل بالعملات الافتراضية أو إنشاء منصات للتداول بها في السوق المصري، إلا بعد الحصول على الترخيص أو الموافقة اللازمة من البنك المركزي. تُعد العملات الافتراضية هنا تلك التي تُخزن إلكترونيًا ويتم التعامل بها كوسيلة دفع، وتكون مستحقة للمرخص لهم بالعمل بها، كما يتم تداولها خارج نطاق التعامل النقدي التقليدي القطع النقدية والأوراق المالية.

- **التشريع الفرنسي:** لقد أخذ المشرع الفرنسي حذو الاتجاه الأوروبي في هذا الصدد حيث أعاد صياغة هذا المبدأ في المادة 135 فقرة 2 من قانون النقد والقرض الفرنسي.[3]

5- التشريع الجزائري: أدرج المشرع الجزائري العملة الافتراضية في المادة 117 فقرة 2 من قانون المالية لعام 2018 حيث بيّن فيها خصوصية التعامل بها عبر شبكة الإنترنت،

1- التوجيه الأوروبي رقم 110-2019 مؤرخة في 16 سبتمبر 2009.

2- انظر المادة 01 من القانون 194 لسنة 2020 قانون البنك المركزي و الجهاز المصرفي،ج ر،ع37 ،الصادر في 2020/09/15

3- Voir art 135 de la loi n° 99-1071, cit pre.

وتتميز هذه العملات بعدم وجود دعم مادي لها مثل القطع النقدية أو الأوراق النقدية، مما يجعلها غير قابلة للتداول كمادة مادية ملموسة[1].

كما نصت المادة 117 فقرة 1 من قانون المالية الجزائري على معاقبة كل من يتعامل بالعملة الافتراضية في مخالفة صريحة لهذا التنظيم، وفقًا للمادة 117 فقرة 3، والتي تبرر ذلك بعدم وجود الدعم المادي لهذه العملات مما يُهدد استقرار النظام المالي والاقتصادي[2]، أما العملة الرقمية فلم يعرفها القانون النقدي والمصرفي بل نص على أن العملة النقدية الوطنية يمكن أن تأخذ شكلا رقميا وتسمى العملة الرقمية للبنك المركزي بمعنى الدينار الرقمي الجزائري.[3]

1- قانون رقم 17-17 مؤرخ في 27 ديسمبر 2017، يتضمن قانون المالية لسنة 2018، مؤرخة في ج رع 76، مؤرخة في 28ديسمبر 2017.

2- أنظر المادة 117 من القانون رقم 17-17، السالف الذكر.

3- المادة 02 ف 02 من القانون رقم 23-09، السالف الذكر.

خلاصة الفصل الأول:

الفصل الثاني

أمن وحماية التوقيع الإلكتروني

تمهيد

في إطار التحول الرقمي الذي يشهده العالم في الوقت الراهن، يُعتبر التوقيع الإلكتروني أداة أساسية تُمنح لها شرعية قانونية وتعمل على تأكيد مصداقية التفاعلات الرقمية، بدءًا من العقود التجارية مرورًا بالمراسلات الرسمية. ومع تزايد هذه الأهمية، أصبح من الضروري توفير نظام حماية وأمن شامل يكفل سلامة التواقيع الإلكترونية من محاولات التزوير أو الإنكار أو أي سوء استخدام.

يتطلب هذا النظام التكامل بين عنصرين رئيسيين الأول الحماية التقنية المتقدمة التي تعتمد على تقنيات التشفير المتطورة لضمان سرية وسلامة البيانات المرتبطة بالتوقيع الإلكتروني بالإضافة إلى الشهادات الرقمية التي تضمن التحقق من هوية الشخص الموقّع وربطها بتوقيعه بشكل موثوق، بينما تلعب البنية التحتية للمفاتيح العامة دورًا أساسيًا في إدارة دورة حياة هذه الشهادات والمفاتيح. كما أن الختم الزمني يُعد أداة هامة توثق تاريخ التوقيع والبيانات ذات الصلة، في حين أن آليات المصادقة المتقدمة تضمن تحقق هوية الموقع بشكل دقيق.

أما من الناحية القانونية، فإنه يتعين إصدار تشريعات صريحة تعترف بالحجية القانونية للتوقيع الإلكتروني، وتحدد أنواع التوقيعات المختلفة ومستويات الأمان المتطلبة لكل نوع. كما يجب أن تتضمن هذه التشريعات تنظيم عمل جهات التصديق الإلكتروني، وتحديد مسؤوليات الأطراف المعنية باستخدام التوقيع الإلكتروني، بالإضافة إلى تجريم الأفعال غير المشروعة المرتبطة به، مع توفير آليات فعالة لحل المنازعات التي قد تنشأ نتيجة لذلك.

يعد التضافر بين هذه الجوانب التقنية والقانونية الضمانة الحقيقية لإرساء بيئة رقمية آمنة وموثوقة، تساهم في تعزيز الثقة في المعاملات الإلكترونية، وتفتح المجال نحو اقتصاد

رقمي مستدام ومزدهر، فبغياب هذه الحماية المتكاملة، تصبح التواقيع الإلكترونية عرضة للمخاطر مما يُقوض من قيمتها القانونية وفاعليتها في العالم الرقمي.

وفي هذا الفصل سوف نتطرق إلي الآليات التقنية لحماية التوقيع الالكتروني في المبحث الأول و الآليات القانونية لحماية التوقيع الالكتروني في المبحث الثاني

المبحث الأول

الحماية التقنية لتوقيع الالكتروني

يشهد العالم في العقود الأخيرة تطورًا متسارعًا في مجال تكنولوجيا المعلومات والاتصال، مما أدى إلى انتقال عدد كبير من المعاملات والعقود إلى البيئة الرقمية، واستبدال الوثائق الورقية بالتعاملات الإلكترونية. هذا التحول، على الرغم من إيجابيات من حيث السرعة والفعالية، فرض تحديات قانونية وتقنية متعلقة بسلامة المعاملات الإلكترونية، وفي مقدمتها إثبات صحة التوقيعات وهوية المتعاملين وضمان عدم التلاعب بالمحتوى.

ومن هنا ظهرت أهمية التوقيع الإلكتروني كوسيلة قانونية لإثبات التصرفات والإرادات الرقمية، غير أن فعالية هذا التوقيع لا يمكن أن تتحقق إلا من خلال توفير حماية تقنية عالية له، تضمن عدم تزويره أو انتحاله أو التلاعب بمضمونه وتُعد تقنية التشفير ووجود جهات التصديق الإلكتروني من أبرز آليات هذه الحماية، حيث تُستخدم لضمان سرية المعلومات وسلامة البيانات المتبادلة، فضلاً عن التأكد من هوية الموقعين.

لذلك، يأتي هذا المبحث لدراسة الأسس التقنية التي يقوم عليها التوقيع الإلكتروني، والوسائل التي تضمن حمايته من الناحية الأمنية والتشغيلية، وعلى رأسها أنظمة التشفير (المطلب الأول)، وجهات التصديق الإلكتروني (المطلب الثاني)، مع ابراز ما أقرّه المشرع الجزائري في هذا المجال.

المطلب الأول

التشفير الالكتروني

يعد التشفير من أبرز الوسائل التقنية المستخدمة لحماية التوقيع الإلكتروني، حيث تبنّت معظم التشريعات هذا النظام الذي يقوم على تحويل المعلومات من شكلها الأصلي إلى

رموز وإشارات غير قابلة للفهم أو القراءة، إلا بعد إعادة تحويل هذه الشفرات إلى نصوص مقروءة باستخدام مفاتيح التشفير[1].

ويُعتبر التشفير تقنية تهدف أساسًا إلى ضمان سرية وسلامة البيانات والمعلومات، ونظرًا لأهميته، حرصت مختلف التشريعات الدولية والوطنية على تنظيمه وإدراجه ضمن الأطر القانونية المتعلقة بالمعاملات الإلكترونية[2].

فنجد أن **قانون الأونسيترال النموذجي** لم يقدّم تعريفًا صريحًا ومباشرًا للتشفير، بل تناوله بشكل ضمني كوسيلة لضمان سرية وسلامة البيانات والمعلومات الإلكترونية بعد تحويلها إلى صيغة غير قابلة للقراءة.

وبالمثل، لم يعرّف **المشرّع الجزائري** التشفير تعريفًا مباشرًا في القانون 04-15 المتعلق بالتوقيع والتصديق الإلكتروني، وإنما اكتفى بالإشارة إليه بشكل غير مباشر في المادة 02 الفقرتين 8 و9، حيث تم التمييز بين نوعين من التشفير :التشفير العام **و**التشفير الخاص[3].

غير **أن** كلاً من المشرّع المصري والتونسي تميّزا عن باقي التشريعات العربية من خلال تقديم تعريفات دقيقة للتشفير[4].

حيث عرّف المشرّع التونسي التشفير بأنه عملية استخدام رموز وإشارات غير متداولة لتحرير أو إرسال معلومات بحيث تكون غير قابلة للفهم من قبل الغير، ولا يمكن الوصول إلى المعلومة إلا باستخدام هذه الرموز والإشارات.

1- محمد فواز محمد المطالقة، الوجيز في عقود التجارة الالكترونية، دار الثقافة للنشر والتوزيع، الاردن، 2008، ص159.

2- يمينة حوحو، عقد البيع الالكتروني في القانون الجزائري، دار بلقيس للنشر، الجزائر،2016 ،ص 185.

3- انظر المادة 02 الفقرة 8 و9 من القانون رقم 15-04، السالف الذكر.

4 - براهيمي فريدة-بوخاري نسيمة، النظام القانوني للتوقيع الالكتروني في القانون الجزائري، مذكرة لنيل شهادة ماستر قانون الأعمال، جامعة مولود معمري تيزي وزو،2017، ص84.

أما المشرع المصري فقد عرفه بأنه عملية تحويل البيانات إلى رموز أو إشارات بهدف حمايتها من الوصول غير المصرّح به، ومنع تعديلها أو تغييرها من قبل أطراف غير مخولة.

الفرع الأول

أساليب التشفير

ومن خلال هذه التعاريف سوف نتطرق الي اهم اساليب التشفير و المتمثل في التشفير المتماثل و التشفير الغير المتماثل.

أولا: التشفير المتماثل

يعتمد هذا النظام أساسًا على استخدام مفتاح واحد مشترك يحمل رقما سريا ومعلوما بين المُرسل والمُرسل إليه، حيث يُستخدم المفتاح نفسه في عمليتي التشفير وفك التشفير، سواء عند الإرسال أو الاستقبال ويُعرف هذا النوع من التشفير باسم التشفير المتناظر[1].

ويستند هذا النوع من التشفير إلى خوارزمية شهيرة تُعرف ب .DES، والتي تُعد من أقدم وأشهر خوارزميات التشفير، وتعتمد خوارزمية DES على مفتاح طوله 56بت فعليًا[2]، بالرغم من أن الطول الكلي للمفتاح هو 64 بت، حيث تُستخدم 8بتات فقط لأغراض الفحص والتدقيق.

ورغم شهرتها، تُعتبر خوارزمية DES غير آمنة في الوقت الحالي، بسبب قدرتها 6المحدودة على مقاومة محاولات الاختراق والقرصنة، وذلك نتيجة لقصر طول المفتاح وسرعة فك تشفيره باستخدام تقنيات الحوسبة الحديثة.

1 – يمينة حوحو، المرجع نفسه، ص188.

2– محمد فواز محمد المطالقة، المرجع نفسه، ص164.

نتيجة لذلك، تم التراجع عن استخدامها تدريجيًا، على الرغم من محاولة تطويرها من خلالDES3أوTriple DES، وهي نسخة محسّنة تستخدم التشفير ثلاث مرات متتالية لزيادة الأمان، لكنها ما زالت تُعد أبطأ وأقل فعالية مقارنة بالخوارزميات الحديثة مثل .AES

ثانيا: التشفير لا متماثل

جاء التشفير **غير المتماثل** كحلّ لمجموعة من التحديات والمشكلات التي يعاني منها **التشفير المتماثل**، وعلى رأسها ضرورة تقاسم المفتاح السري بين الأطراف، مما يهدد أمن البيانات في حال اعتراضه.

ويعتمد التشفير غير المتماثل على استخدام زوج من المفاتيح[1]:

1- **مفتاح عام(Public Key)** ، يمكن لأي شخص الحصول عليه واستخدامه لتشفير البيانات.

2- **مفتاح خاص(Privat Key)** ، يحتفظ به صاحبه بسرية تامة، ويُستخدم لفك تشفير البيانات المشفّرة باستخدام المفتاح العام المقابل.

يعرف هذا النظام أيضًا باسم **RSA**، Rivest–Shamir Adleman نسبة إلى مخترعيه ويعتمد هذا النظام على خاصية رياضية تجعل من المستحيل تقريبًا فك التشفير بالمفتاح العام دون امتلاك المفتاح الخاص، إذ إن كل مفتاح في الزوج يُعد عكسيًا للآخر وقد حقق هذا النظام نجاحًا واسعًا، واعتُبر أكثر أمانًا من خوارزمية **DES**، خاصةً في التطبيقات التي تتطلب التحقق من هوية الطرف الآخر أو حماية البيانات أثناء نقله ورغم أمانه ، إلا أن نظام RSA ليس بمنأى عن المخاطر، إذ إنه معرّض للاختراق باستخدام تقنيات الحوسبة المتقدمة وقد أدى هذا إلى تطوير أنظمة أكثر تعقيدًا وأمانًا، مثل نظام

1- محمد ابراهيم ابو الهيجاء، عقود التجارة الالكترونية ط2، دار الثقافة والنشر، الاردن،2011، ص135.

(PrettyGood Privacy) **PGP**، الذي يستخدم مفتاحًا بطول 128 بت ويعتمد كذلك على تقنيات متقدمة مثل البصمة الإلكترونية(Digital Fingerprint) لضمان التحقق والتوثيق الآمن[1].

الفرع الثاني

ضوابط التشفير

يُعد التشفير ضرورة حتمية للمحافظة على أمن المعاملات الإلكترونية، ومنحها عناصر المصداقية والثقة والأمان، كما يُعتبر وسيلة فعالة لضمان حماية البيانات والمعلومات التي يتم تبادلها عبر الوسائط الإلكترونية ولتحقيق هذه الأهداف، يجب احترام مجموعة من الضوابط القانونية الأساسية وهي:

أولاً: مشروعية تشفير البيانات والمعلومات

تُعد البيانات والمعلومات المتبادلة عبر الوسائط الإلكترونية من العناصر التي تستوجب الحماية، خاصة عندما تكون مشفّرة، إذ يوفر التشفير مستوى متقدمًا من الحماية ضد أي اعتداء، سواء من خلال الحصول غير المشروع على مفاتيح التشفير، أو باستخدام التشفير كأداة لارتكاب الجرائم الإلكترونية[2].

أكدت غالبية التشريعات الوطنية والمقارنة على مشروعية التشفير، من خلال إدراج نصوص قانونية تنظم هذه التقنية وتحمي استخدامها وفي هذا السياق، جاء القانون الجزائري في القانون رقم 15-04 ليعالج موضوع التشفير من خلال تقديم تعريف لكل من التشفير العام والتشفير الخاص، وإن لم يقدّم تعريفًا عامًا وشاملاً لمفهوم التشفير بحد ذاته.

---

1 – اياد احمد سعيد الساري، النظام القانوني لإبرام العقد الالكتروني على ضوء قانون التوقيع الالكتروني والمعاملات الالكترونية، ط1، منشورة الحلبي الحقوقية، لبنان، 2016، ص128.

2- عقوني محمد- بلمهدي براهيم، اليات تقنية ولقانونية لحماية التوقيع الالكتروني، مجلة الفكر، مجلد 14،ع 1 ، 2019/02/04 ، ص 18

وبالمقابل، نجد أن المشرع المصري، في اللائحة التنفيذية لقانون التوقيع الإلكتروني رقم15لسنة 2004في المادة 1الفقرة 8، والمشرع التونسي في قانون المبادلات والتجارة الإلكترونية لسنة 2000المادة 2 الفقرة 5 قد قدما تعريفات واضحة ومباشرة للتشفير، مما ساهم في تقليص هامش التفسير والتأويل القانوني، وضمان التطبيق السليم للنصوص ذات الصلة[1].

ثانيًا: وجوب الحفاظ على سرية البيانات والمعلومات المشفّرة

تُعد السرية من المبادئ الجوهرية في نظام التشفير، ويُعدّ أي مساس بها انتهاكًا خطيرًا واعتداء لخصوصية الأفراد وحقوقهم الرقمية، خاصةً عندما يتعلق الأمر بالمراسلات والبيانات الشخصية[2].

أقر المشرع الجزائري بهذه الأهمية من خلال القانون رقم 15-04، حيث نصت المادتان 42 و43 منه على التزامات صارمة تقع على عاتق مقدمي خدمات التصديق الإلكتروني، تلزمهم بعدم استعمال البيانات الشخصية الواردة ضمن الشهادات إلا في إطار الغرض المخصص لها ووجوب الحفاظ على سريتها[3].

كما عزز هذا الاتجاه المرسوم التنفيذي رقم 98-257 المتعلق باستغلال خدمات الإنترنت، حيث نص في المادة 14 على ضرورة احترام مقدمي خدمات الإنترنت لسرية معلومات المشتركين، وعدم الكشف عنها إلا في الحالات المنصوص عليها قانونًا[4].

1- محمد فواز المطالقة، مرجع سابق، ص161

2- عبان عميروش، التنظيم القانوني للتشفير كآلية التصديق الالكتروني في التشريع الجزائري والمقارن، مجلة الاستاذ الباحث للدراسات القانونية والسياسية،مجلد7،ع 2 ، 2022،ص1243

3- انظر المادة 42 و43 من القانون 15-04، السالف الذكر.

4- أنظر المادة14 من المرسوم التنفيذي 98-257 المتعلق باستغلال خدمات الانترنت

ولتأكيد هذه الحماية، فرض المشرّع الجزائري عقوبات صارمة على كل من يخرق مبدأ السرية، سواء أكان ذلك من الغير أو من قبل مؤدي خدمات التصديق أو الأشخاص المكلفين بمهام التدقيق، حمايةً لثقة المتعاملين في البيئة الرقمية وصونًا لخصوصيتهم[1].

ثالثًا: ضرورة الحصول على ترخيص مسبق لاستخدام التشفير

تبنّت العديد من الدول مثل فرنسا، تنظيمات مشددة بخصوص استخدام تقنيات التشفير، بسبب ارتباطها الوثيق بالأمن القومي فقد كان استخدام التشفير في فرنسا في بداياته محصورًا في المجال العسكري، وممنوعًا على الأفراد المدنيين ومع تطور التكنولوجيا، انتقل المشرّع الفرنسي إلى مرحلة تحرير التشفير، حيث سُمِح باستخدامه لأغراض مدنية، مع الإبقاء على الرقابة الحكومية لضمان عدم إساءة الاستعمال[2].

في هذا الإطار، نصّت المادة 31 من قانون الثقة في الاقتصاد الرقمي الفرنسي على ضرورة التصريح باستخدام التشفير، وذلك من خلال تقديم إشعار إلى رئيس الوزراء، على أن تُحدَّد شروط استخدامه بموجب مرسوم يصدر عن مجلس الدولة.

كما جاء المرسوم رقم 2007-633 ليعفي عمليات التوريد والنقل والاستيراد والتصدير الخاصة بخدمات وتقنيات التشفير داخل دول الاتحاد الأوروبي من أي إجراءات مسبقة، بينما اشترط الحصول على ترخيص مسبق عند تصديرها إلى خارج الاتحاد.

أما المشرع الجزائري، فلم يخصّص إطارًا قانونيًا دقيقًا ينظم استخدام التشفير، واكتفى بالإشارة إليه ضمن نصوص متفرقة دون وضع تنظيم شامل ومفصل يحدد شروط الترخيص والرقابة والمسؤولية القانونية، كما هو معمول به في التشريع الفرنسي.

1- عقوني محمد، المرجع السابق، ص306.

2 - عبان عميروش، المرجع السابق، ص1242

رابعا: اعتبار النص المشفر محررا الكترونيا

يعتبر النص المشفر محررا الكترونيا يحوز حجيته القانونية في الإثبات، طالما تم إنشاؤه أو تحويله باستخدام خوارزميات تشفير معترف بها تضمن سرية البيانات وسلامتها ويستند هدا الاعتراف إلى قيام نظام التشفير بتحويل النص الأصلي إلى رموز أو إشارات رقمية ثم إمكانية فكها لاحقا لإعادته إلى صورته القابلة للقراءة والفهم[1] ويعد هذا النص ملزم قانونيا للطرفين بمجرد التوقيع عليه، شانه شان الوثائق الورقية التقليدية، متى توافرت فيه الشروط الفنية والقانونية المقررة.

المطلب الثاني

التصديق الالكتروني

شهد العالم في العقود الأخيرة تسارعًا غير مسبوق في وتيرة التحول الرقمي والتطور التكنولوجي، مما أدى إلى انتقال العديد من المعاملات والخدمات إلى الفضاء الإلكتروني، فلم تعد التعاقدات محصورة في اللقاءات المباشرة أو الأوراق الموقعة يدويًا، بل أصبحت تتم بشكل افتراضي بين أطراف قد لا يجمعهم مكان أو زمان واحد، وهو ما وفّر الكثير من الجهد والوقت، لكنه في الوقت ذاته أثار تساؤلات جوهرية حول مدى الثقة والمصداقية في هذه التعاملات

الإلكترونية، ومع تزايد حجم المعاملات الرقمية، ظهرت تحديات تتعلق بإثبات هوية المتعاملين وصحة التوقيعات، وسلامة البيانات المتبادلة، مما أدى إلى نوع من عدم الثقة بين الأطراف ومن هنا برزت الحاجة إلى إيجاد آلية تقنية وقانونية تضمن الأمان، وتُحقق الثقة في البيئة الرقمية، فكان التصديق الإلكتروني هو الحل الفعال، حيث يُوفر وسيلة

1- محمد فواز محمد المطالقة، المرجع السابق، ص161.

للتحقق من الهوية وتأكيد صحة البيانات والتوقيعات في المعاملات الإلكترونية، وهو ما تم الاعتراف به قانونًا في العديد من الأنظمة التشريعية حول العالم.

لذا سنتناول في هذا المطلب تعريف التصديق الإلكتروني(الفرع الأول)، ثم جهات التصديق الإلكتروني (الفرع الثاني)وفي الأخير شهادات المصادقة الإلكترونية(الفرع الثالث).

الفرع الأول

تعريف التصديق الالكتروني

أصبح التصديق الإلكتروني ضرورة حتمية لا يمكن الاستغناء عنها في ظل التحول الرقمي المتسارع، ويُعد أداة أساسية لبناء بيئة رقمية آمنة ومستقرة تُحفّز على مزيد من التعاملات الإلكترونية بثقة واطمئنان.

ولا يمكن تحقيق ذلك إلا باستحداث طرف ثالث محايد، تكون وظيفته توطيد العلاقات وتوثيقها بين الأشخاص وقد اختلفت التسميات لهذا الطرف[1]، ولتحديد الطبيعة القانونية لهذه الجهة المستحدثة، قامت التشريعات الدولية والوطنية بتعريفه.

فقد عرّفه **قانون الأونسيترال النموذجي للتوقيعات الإلكترونية** في المادة 02 فقرة 11 بأنه شخص يُصدر شهادات وقد يُقدّم خدمات أخرى ذات الصلة بالتوقيعات الإلكترونية.

كما عرّفه **التوجيه الأوروبي رقم 1999-93** الملغى في مادته 02 الفقرة 11[2]بأنه كل كيان أو شخص طبيعي أو معنوي يُقدّم شهادات توثيق إلكترونية أو يُقدّم خدمات أخرى متصلة بالتوقيع الإلكتروني.

1- يمينة حوحو، المرجع السابق، ص189

2- انظر المادة 2 الفقرة 11 من التوجيه الاوروبي 93-1999 الملغى

أما **اللائحة الأوروبية 910-2014**، فقد ورد فيها في المادة 03 الفقرة 19 والفقرة 20، تمييز بين نوعين من مؤدي خدمات التوثيق[1]:

الفقرة 19: مؤدي خدمات التوثيق هو شخص طبيعي أو معنوي يُقدّم خدمة أو عدة خدمات ثقة، سواء كان مؤهلًا أو غير مؤهل.

الفقرة 20: مؤدي خدمات التوثيق المؤهل هو من يُقدّم خدمة أو مجموعة خدمات ثقة مؤهلة، ويحصل على صفة المؤهل من هيئة الرقابة.

كما عرّف **القانون المصري للتوقيع الإلكتروني** هذه الجهة في المادة 01 من اللائحة التنفيذية رقم 01 لسنة 2020بأنها:الجهة المرخص لها بإصدار شهادات التصديق الإلكتروني وتقديم خدمات تتعلق بالتوقيع الإلكتروني.[2]

وقد أشار إليها **المشرّع الأردني** في المادة 02 الخاصة بالتعريفات من قانون المعاملات الإلكترونية، المادة 15 فقرة، على أنها: الجهة المرخصة أو المعتمدة من هيئة تنظيم قطاع الاتصالات أو المخولة قانونًا بإصدار شهادات التوثيق وتقديم خدمات متعلقة بهذه الشهادات، وفقًا لأحكام هذا القانون والأنظمة والتعليمات الصادرة بموجبه.[3]

أما **المشرع الجزائري**، فقد عرّفها في المادة 02، الفقرة (د) من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها[4]، مستخدمًا مصطلح "مقدمو خدمات التصديق"، على النحو التالي:

1- انظر المادة 03 الفقرة 19 و20 من اللائحة الاوروبية 910-2014.

2- انظر المادة 1 من اللائحة التنفيذية رقم 1 من سنة 2020 للتوقيع الالكتروني المصري

3 انظر المادة 2 من القانون الاردني رقم 15 من سنة 2015 المتعلق بالمعاملات الالكترونية، ج ر ع 5341، الصادر في 17-05-2015

4- المادة 2 الفقرة د من القانون 04/09 المؤرخ في 05 اوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها، ج ر ،ع 47 ،الصادرة في 16 اوت 2009

– أي كيان عام أو خاص يُتيح لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية أو نظام للاتصالات.

–أي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها.

كما أشار إليها أيضًا في المادة 02، الفقرتين 11 و12 من القانون رقم 15–04 المتعلق بالتوقيع والتصديق الإلكتروني[1]:

الفقرة 11: الطرف الثالث الموثوق هو شخص معنوي يقوم بمنح شهادات تصديق إلكترونية موصوفة، وقد يُقدّم خدمات أخرى متعلقة بالتصديق الإلكتروني لفائدة المتدخلين في الفرع الحكومي.

الفقرة 12: مؤدي خدمات التصديق هو شخص طبيعي أو معنوي يقوم بمنح شهادات تصديق إلكترونية موصوفة، ويُقدّم خدمات أخرى في مجال التصديق الإلكتروني.

إن جهات التصديق الإلكتروني يمكن أن تكون شخصًا طبيعيًا أو معنويًا يتولى إصدار شهادات التصديق التي تُثبت هوية صاحب التوقيع الإلكتروني ومدى ارتباطه بمضمون المحرر الإلكتروني كما تُقدّم هذه الجهات خدمات أخرى مرتبطة بالتوقيع الإلكتروني[2].

1– انظر المادة 2 الفقرة 11و12 من القانون 15–04، السالف الذكر.

2– محمد بن محمد أيوب، المرجع نفسه، ص 307

الفرع الثاني

جهات التصديق الالكتروني

تلعب جهات التصديق الإلكتروني كطرف ثالث محايد دورًا مهمًا في ضمان سلامة التوقيع الإلكتروني، ومنع أي تلاعب أو تغيير أو إنكار لاحق للتوقيع[1] ويشترط في هذه الجهات أن تتوفر على مجموعة من الإمكانيات التقنية والقانونية التي تؤهلها للقيام بمهامها، نظرًا لكونها الجهة الحاسمة في تحديد مدى صلاحية التوقيعات الإلكترونية.

لتحقيق هذه الأهداف، قام المشرّع الجزائري بتنظيم سلطات التصديق الإلكتروني بموجب القانون 15-04 المتعلق بالتوقيع والتصديق الإلكتروني، حيث أسند مهمة إصدار شهادات التصديق إلى "مؤدي خدمات التصديق"، الذي يجب أن يكون طرفًا محايدًا، ويحمل ترخيصًا رسميًا صادرًا عن سلطة مختصة.

اعتمد المشرّع في تنظيمه لهياكل التصديق على ثلاث سلطات أساسية مكملة، تم تحديدها وتنظيم سيرها ومهامها بموجب المرسوم التنفيذي رقم 16-134.[2]

أولا: السلطة الوطنية للتصديق الإلكتروني

استحدث المشرّع الجزائري هذه السلطة بموجب المادة 16 من القانون 15-04، حيث تنص على إنشاء سلطة إدارية مستقلة لدى الوزير الأول، تتمتع بالشخصية المعنوية والاستقلال المالي، وتُسمى السلطة الوطنية للتصديق الإلكتروني. وتُدرج الاعتمادات المالية اللازمة لسير وعمل هذه الهيئة ضمن ميزانية الدولة.

1- ربحي تبوت، فاطمة الزهراء، المرجع السابق، ص267

2- المرسوم التنفيذي رقم 16-134، مؤرخ في 25 أفريل 2016 يحدد تنظيم المصالح التقنية والادارية للسلطة الحكومية للتصديق الالكتروني وتشكيلها وتنظيمها وسيرها، الصادرة في ج ر ع 26، مؤرخة في 28 أفريل 2016.

يتبيّن من هذه المادة أن المشرّع أسس هيئة قانونية جديدة ضمن المنظومة التشريعية الجزائرية، لا تندرج ضمن الهيئات الإدارية التقليدية، بل تتمتع بطابع قانوني خاص واستقلالية تامة في الجوانب الإدارية والمالية، مما يضمن حياد قراراتها وعدم خضوعها لأي وصاية تنفيذية[1].

يتم تنظيم هذه الهيئة وفق أحكام المرسوم التنفيذي رقم 16-134، الذي يحدد تشكيلها وتنظيم مصالحها وسيرها، مع مقر رئيسي يقع في الجزائر العاصمة، ويمكن نقله إلى أي موقع آخر داخل التراب الوطني[2].

تتكون من مجلس يضم خمسة (5) أعضاء، من ضمنهم رئيس يُعيّنه رئيس الجمهورية بناءً على كفاءته التقنية والقانونية والاقتصادية في مجال تكنولوجيات الإعلام والاتصال[3] ويتم تسيير الهيئة تقنيًا وإداريًا من قبل مدير عام يُعيّن من طرف رئيس الجمهورية باقتراح من الوزير الأول[4].

تم تحديد مهامها في المادة 18من القانون رقم 15-04، وتندرج ضمن صلاحيات تنظيمية ورقابية وتشريعية خاصة بقطاع التصديق الإلكتروني[5].

ثانيًا: السلطة الحكومية للتصديق الإلكتروني

نصّت المادة 26 من القانون 15-04 على إنشاء سلطة حكومية للتصديق الإلكتروني لدى الوزير المكلف بالبريد وتكنولوجيات الإعلام والاتصال، تتمتع بالشخصية المعنوية

1- بلقايد ايمان، النظام القانوني للتصديق الالكتروني، مذكرة لنيل شهادة الماستر في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، 2016، ص34.

2- انظر المادة 2 من المرسوم التنفيذي رقم 16-134، السالف الذكر.

3- انظر المادة 19 من القانون 15-04 والمادة 3 من المرسوم التنفيذي رقم 16-134

4- انظر المادة 20 من القانون 15-04.

5 -انظر المادة 18 من القانون 15-04.

والاستقلال المالي، وأوضحت المادة 27 أن تشكيل هذه السلطة وطبيعتها وتنظيمها وسيرها يتم عن طريق المرسوم التنفيذي رقم 16-135 [1] .

يتضح من هذه النصوص أن المشرّع منح السلطة الحكومية للتصديق نفس التكييف القانوني الذي منحه للسلطة الوطنية، باعتبارها هيئةإدارية مستقلة تتمتع بالشخصية المعنوية ومستقلة ماليًا[2]، وكدا نفس المقر ويقع مقرها في الجزائر العاصمة، مع إمكانية نقله داخل التراب الوطني بحسب مقتضيات العمل[3].

وتُدار من قبل مدير عام يُعيّن بموجب مرسوم رئاسي بناء على اقتراح الوزير المكلف بتكنولوجيات الإعلام والاتصال[4]وتدعم هذه الهيئة بهياكل تنظيمية تشمل مجلسًا للتوجيه وهيئات تقنية وإدارية[5].

مجلس التوجيه يتكوّن من المدير العام رئيسًا، وممثل عن رئاسة الجمهورية، وممثلين عن وزارات: الدفاع الوطني، الداخلية، العدل، المالية، وتكنولوجيات الإعلام والاتصال،ويُعيّن أعضاء المجلس بقرار من الوزير المختص ويُشترط أن يكونوا على رتبة مدير عام على الأقل، وأن يتمتعوا بالكفاءة والخبرة التقنية والأمنية ذات الصلة بالتصديق الإلكتروني ولا يجوز تفويض أو تعويض العضو المتغيب[6].

أما الهياكل التقنية والإدارية فتشمل مديرية الإدارة العامة مديرية الأنظمة المعلوماتية، مديرية امن البنية التحتية، مديرية الدراسات والبحث والتطوير، مديرية البنية التحتية لتسيير

1 - المرسوم رقم 16-135، مؤرخ في 25 أفريل 2016، يحدد طبيعة السلطة الحكومية للتصديق الالكتروني وتشكيلها وتنظيمها وسيرها، الصادرة في ج ر ع 26، مؤرخة في 28 أفريل 2016.

2- انظر المادة 2 من المرسوم التنفيذي 16-135، السالف الذكر.

3- انظر المادة 3 من المرسوم التنفيذي 16-135، السالف الذكر.

4- المادة 20 من القانون 15-04، السلف الذكر، والمادة 13 من المرسوم التنفيذي رقم 16-135، السالف الذكر.

5- المادة 4 من المرسوم التنفيذي 16-135، السالف الذكر.

6- المادة 05 من المرسوم التنفيذي 16-135، السالف الذكر.

المفاتيح[1]، تُعنى السلطة الحكومية بالتنسيق والتوجيه لنشاط التصديق الإلكتروني، وضمان امتثاله للمعايير القانونية والتقنية.[2]

ثالثًا: السلطة الاقتصادية للتصديق الإلكتروني

تُعد هذه الهيئة امتدادًا لـ سلطة ضبط البريد والمواصلات السلكية واللاسلكية، حيث أُسندت إليها مهام إضافية في مجال التوقيع والتصديق الإلكترونيين، بموجب المادة 29 من القانون15-04 والمادة11 من القانون 18-04[3]، التي نصت على إنشاء "سلطة ضبط البريد والاتصالات الإلكترونية"، متمتعة بالشخصية المعنوية والاستقلال المالي، ويقع مقرها بالجزائر العاصمة.

لمعرفة أكثر حول هذه السلطة ينبغي الرجوع إلى أحكام القانون 2000-03 المحدد للقواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية ،[4] والتي منحها المشرّع استقلالية إدارية كاملة، مع إعفائها من أي رقابة وصائية أو رئاسية[5]، ويتم التصديق على نظامها الأساسي ونظام تسيير المستخدمين من طرف مجلسها دون تدخل أي جهة خارجية ما تتمتع بالاستقلال المالي ويوجد مقرها بالجزائر العاصمة[6].

1- المادة 18 من المرسوم التنفيذي 16-135، السالف الذكر.

2- المادة 28 من القانون رقم 15-04، السالف الذكر.

3 - قانون رقم18-04، مؤرخ في 10 ماي 2018، المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الالكترونية، الصادر في ج ر ع 27، صادرة في 13 ماي 2018.

4- قانون رقم 2000-03 ، مؤرخ في 05 أوت 2000، يحدد القواعد العامة المتعلقة بالبريد و بالمواصلات السلكية واللاسلكية، ج ر ع 48 الصادر بتاريخ 06 اوت 2000، المعدل والمتمم بموجب القانون رقم 06-24 مؤرخ في 26 ديسمبر 2006، المتضمن قانون المالية لسنة 2007، الصادرة في ج ر ع 85، مؤرخة في 27 ديسمبر 2006.

5- سعيود محمد طاهر، المرجع السابق، ص47

6- انظر المادة 10 من القانون رقم 2000-03، السالف الذكر.

ومن الناحية العضوية نجد أنها تتكوّن من مدير عام ومجلس للسلطة[1] يضم سبعة أعضاء من بينهم الرئيس يُعيّن الأعضاء بقرار من رئيس الجمهورية باقتراح من الوزير الأول، ويُشترط فيهم الكفاءة التقنية والعلمية وعهدة الأعضاء تستمر ثلاث سنوات قابلة للتجديد مرة واحدة، وفي حال شغور المنصب يُستخلف العضو بنفس إجراءات التعيين[2].

تم تحديدها مهامها بموجب المادة 30 من القانون 15-04 وتشمل الإشراف التقني والاقتصادي على خدمات التصديق الإلكتروني، وضمان توافقها مع التشريعات المعمول بها، ومراقبة أداء مؤدي خدمات التصديق، وضمان حماية المستخدمين[3].

رابعا: مؤدي خدمات التصديق

يُعتبر مؤدي خدمات التصديق الإلكتروني طرفًا ثالثًا محايدًا (أي من غير أطراف العلاقة التعاقدية)، يتولى دور الوسيط التقني والقانوني لضمان سلامة وسرية البيانات التي يتم تبادلها بين المتعاقدين، إضافةً إلى التحقق من هوية الأطراف وحفظ وإدارة الشهادات الإلكترونية المرتبطة بالمعاملات.

وقد نصّ المشرّع الجزائري على تعريف مؤدي خدمات التصديق في المادة 2 من القانون 15-04 المتعلق بالتوقيع والتصديق الإلكتروني، باعتباره:كل شخص طبيعي أو معنوي يقوم بمنح شهادات تصديق إلكترونية موصوفة، وقد يقدم خدمات أخرى في مجال التصديق الإلكتروني.[4]

1- انظر المادة 14 من القانون رقم 2000-03، السالف الذكر.

ـــــ والمادة 19 من القانون رقم 18-04، السالف الذكر.

2- المادة 20 من القانون رقم 18-04، السالف الذكر.

3- انظر المادة 30 من القانون رقم 15-04، السالف الذكر.

4- المادة 02 من القانون رقم 15-04، السالف الذكر.

يستفاد من هذا التعريف أن مؤدي خدمات التصديق يمكن أن يكون شخصًا طبيعيًا أو معنويًا، ويضطلع بعدة وظائف رئيسية في نظام التصديق الإلكتروني، أهمها إصدار الشهادات الإلكترونية، وحفظها، وضمان أمنها[1].

أولا: الشروط القانونية لممارسة نشاط مؤدي خدمات التصديق

حتى يتمكن الشخص من مزاولة هذا النشاط، اشترط المشرّع الجزائري توفر مجموعة من الشروط الأساسية التي تنقسم إلى نوعين:

1- **الشروط الشخصية لمؤدي الخدمة:** نصّت المادة34 من القانون 15-04 على جملة من المتطلبات التي يجب أن تتوفر في الشخص الراغب في ممارسة نشاط مؤدي خدمات التصديق[2]، وتتمثل فيما يلي:

أ- **الجنسية** :يُشترط أن يكون المتقدم جزائريًا، أو حائزًا على شروط تعاقدية معتمدة داخل الدولة وفقًا للتنظيمات المعمول بها.

ب- **القدرة المالية** :يجب أن يثبت توفر الموارد المالية الكافية لضمان تأمين الخدمات المقدمة واستمراريتها.

ت-**المستوى العلمي والكفاءة التقنية** :يُشترط توفر مؤهلات علمية وتقنية مناسبة لطبيعة العمل، بما يضمن الإلمام الكامل بتكنولوجيا التوقيع الإلكتروني وأمن المعلومات.

1- بلقايد ايمان، المرجع السابق، ص 43

2- انظر المادة 34 من القانون رقم 15-04، السالف الذكر

ثانيا: شروط الحصول على التأهيل والترخيص

لا يكفي توفر الشروط الشخصية لممارسة النشاط بل يشترط القانون الحصول على شهادة تأهيل، تليها رخصة رسمية تصدر عن السلطة الاقتصادية للتصديق الإلكتروني كما يلي:

1- شهادة التأهيل: تُمنح لمدة سنة واحدة قابلة للتجديد، وتُعد بمثابة المرحلة التحضيرية لتهيئة الوسائل والتجهيزات اللازمة لتقديم خدمة التصديق ويجب تبليغ صاحب الطلب بالنتيجة خلال 60 يومًا من تاريخ استلام الملف[1] وفي حال الرفض، يجب أن يكون القرار مسببًا ويتم تبليغه للمترشح مع إشعار بالاستلام[2].

2- رخصة التأدية: بعد التأهيل يُشترط الحصول على الترخيص النهائي، والذي يُرفق بـ دفتر شروط يحدد كيفية تقديم الخدمة وشروطها التقنية والتنظيمية يتعين على مؤدي الخدمة توقيع شهادة التصديق الخاصة به شخصيًا[3]، والتي لا يمكن التنازل عنها للغير[4].

تسري مدة صلاحية الرخصة لخمس (5) سنوات، قابلة للتجديد وفق الشروط المبينة في دفتر الأعباء[5] ويُدفع مقابل مالي مقابل منح الترخيص، ويُحدَّد هذا المبلغ بموجب نص تنظيمي.

الفرع الثالث

شهادات التصديق الالكتروني

تلعب شهادات التصديق الإلكتروني دورًا هامًا وفعّالًا في مجال المعاملات الإلكترونية حيث تُعدّ من أبرز الوثائق التي تصدرها جهات التصديق الإلكتروني[6]وتعتبر هذه الشهادة

1- انظر المادة 35 من القانون رقم 15-04، السالف الذكر.
2- انظر المادة 37 من القانون رقم 15-04، السالف الذكر.
3- انظر المادة 38 القانون رقم 15-04، السالف الذكر.
4- انظر المادة 39 القانون رقم 15-04، السالف الذكر.
5- انظر المادة 40 القانون رقم 15-04، السالف الذكر.
6- ربحي تبوت – فاطمة الزهراء، المرجع نفسه ص 271

بمثابة دليل على أن التوقيع الإلكتروني ينسب لصاحبه وأنه صحيح ولم يتعرض لأي تعديل سواء بالإضافة أو الحذف أو التغيير، ولإصدار هذه الشهادة يشترط وجود تكامل بين بيانات إنشاء التوقيع وبيانات التحقق منه[1].

أولا: تعريف شهادات التصديق: تم تنظيم هذه المسألة من قبل عدد من التشريعات منها

1-قانون الأونسيترال(UNCITRAL): عرفتها المادة (2) على أن الشهادة عبارة عن رسالة بيانات يؤكد فيها طرف ثالث الارتباط بين الموقّع وبيانات إنشاء التوقيع[2].

2- اللائحة الأوروبية عرّفت شهادة التصديق المؤهلة في المادة (3) بأنها شهادة تصديق إلكترونية صادرة عن مزود خدمة مؤهل تستجيب لمتطلبات الملحق الخامس.[3]

3- المشرع المصري في قانون التوقيع الإلكتروني رقم 15 لسنة 2004، نص في المادة الأولى على أن الشهادة "هي الشهادة التي تصدرها جهة مرخص لها بالتصديق وتثبت الارتباط بين الموقّع والشهادة.[4]

4- المشرع الجزائري في المادة (2) من القانون رقم 15-04، اعتبر الشهادة وثيقة في شكل إلكتروني تثبت الصلة بين بيانات التحقق من التوقيع والموقع، كما أضاف في المادة15أن شهادة التصديق الموصوفة تتضمن مجموعة من المتطلبات التقنية والقانونية.[5]

من خلال هذه التعاريف، يتضح أن شهادة التصديق الإلكتروني تصدر من جهات موثوقة، وتحتوي على بيانات معينة تمنحها الحجية القانونية وتضفي عليها الثقة كما تختلف هذه الشهادات في درجة الموثوقية والمصداقية التي توفرها حسب نوعها ودرجة التأهيل.

1- انظر المادة 44 القانون رقم 15-04، السالف الذكر.

2- راجع المادة 02 من قانون الأونسيترال، السالف الذكر.

3- أنظر المادة 03 من اللائحة الأوربية السالفة الذكر.

4- المادة 01 من قانون التوقيع الإلكتروني المصري رقم 15 لسنة 2004، السالف الذكر.

5- راجع المادة 02 من القانون رقم 15-04، السالف الذكر.

ثانيا: أنواع شهادات التصديق الإلكتروني

تتعدد أنواع شهادات التصديق الإلكتروني، ومن أبرزها:

1- شهادة التصديق الإلكتروني الموصوفة: وهي الشهادات التي تصدر عن مزوّد خدمات التصديق وتستجيب لمجموعة من المتطلبات القانونية والفنية. وقد أشار إليها المشرع الجزائري في المادة (15) من القانون رقم 15-04 مبينًا المتطلبات الواجب توفرها فيها، مثل التحقق من هوية الموقع، والتأكد من سلامة بيانات التوقيع، معا لالتزام بمعايير أمنية محددة[1].

3- شهادة التصديق الإلكتروني البسيطة:وهي شهادات أقل في درجة التوثيق والموثوقية، حيث لا تتطلب نفس المستوى من التحقق والتدقيق، اذا تصدر من أي جهة تكون مختصة وتُستخدم غالبًا في المعاملات التي لا تستلزم حماية عالية[2].

3- شهادة الإذن: وهي شهادة يتم فيها إضافة معلومات إضافية عن صاحب التوقيع الإلكتروني مثل المؤهلات العلمية، محل الإقامة، المهنة أو الوظيفة والتراخيص التي يملكه وتُستخدم هذه الشهادة لتوسيع نطاق المعلومات المتعلقة بالموقّع وتمنحها الجهات المختصة وفق ضوابط محددة[3].

4- شهادات ختم الوقت: هي شهادات تُستخدم لإثبات تاريخ ووقت إصدار التوقيع الإلكتروني على المحرر الإلكتروني، بما يضمن أن التوقيع قد تم في وقت معين، ويمنع لاحقًا أي نزاع يتعلق بتوقيت الإنشاء أو التعديل.[4]

1- أنظر المادة 15 من القانون رقم 15-04، السالف الذكر.

2- يمينة حوحو، المرجع السابق، ص202.

3- محمد بن محمد أيوب، المرجع السابق، ص323.

4 - محمد بن محمد أيوب، المرجع نفسه، ص323.

ثالثا: أداة التصديق الأجنبية

تتمثل في الشهادات التي تصدرها **جهات تصديق إلكترونية أجنبية** خارج إقليم الدولة، وقد اعترفت العديد من التشريعات بهذه الشهادات، شريطة أن تصدر من مزود خدمة موثوق فيه ومقيم في دولة أجنبية.

في الجزائر، لا يتم الاعتراف بشهادة التصديق الأجنبية إلا وفقًا لأحكام المادة63 من القانون 15-04، والتي تشترط:أن يكون مقدم الخدمة من دولة أبرمت الجزائر معها اتفاقية اعتراف متبادل في مجال التصديق الإلكتروني[1].

رابعا: البيانات الواجب توفرها في شهادة التصديق الإلكتروني

وفقًا للمادة 15 من القانون الجزائري رقم 15-04حدد المشرع الجزائري الشروط والبيانات الواجب توافرها في شهادة التصديق الإلكتروني الموصوفة[2]وتشمل ما يلي:

1- شروط إصدار الشهادة: يجب أن تُمنح من طرف جهة موثوقة وتصدر عن مقدّم خدمات تصديق إلكتروني مرخص له، كم يجب أن تكون مطابقة لسياسة التصديق الإلكتروني المعتمدة وأن تمنح للموقع دون سواه.

3-**البيانات الإلزامية في الشهادة:** ينبغي أن تتضمن الشهادة الإلكترونية على وجه الخصوص المعلومات التالية:اسم صاحب الشهادة الموقّع، بيانات التحقق من التوقيع الإلكتروني، فترة صلاحية الشهادة، هوية الجهة المصدرة للشهادة، رقم تسلسلي خاص بالشهادة، خوارزميات التوقيع والتشفير المستخدمة، بيانات الترخيص أو الاعتماد للجهة المصدرة.

1- راجع المادة 63 من القانون رقم 15-04، السالف الذكر.

2- انظر المادة 15 من القانون 15-204

المبحث الثاني

الحماية القانونية للتوقيع الالكتروني

لقد واكب التوقيع الإلكتروني التطور المتسارع في مجال التكنولوجيا والمعلومات، وأصبح يحتل مكانة متميزة في المنظومة القانونية، حيث بات عاملاً أساسياً في إتمام المعاملات الإلكترونية التي تتم عبر شبكة الإنترنت ويُعزز التوقيع الإلكتروني من موثوقية هذه المعاملات من خلال دعمه لمفاهيم السرية والأمان، مستنداً إلى تقنيات متقدمة مثل التشفير والمصادقة وعلى الرغم من هذه المزايا، فإن التوقيع الإلكتروني لم يكن بمنأى عن المخاطر؛ فقد أصبح هدفاً لهجمات إلكترونية متعددة من قبل مجرمين في البيئة الرقمية وتشمل هذه التهديدات الاعتداء على محل التوقيع، أو الوسائل التقنية المستخدمة في إنشائه، أو حتى التشكيك في حجيته القانونية.

ونظراً لتزايد هذه المخاطر، برزت الحاجة الملحة إلى سن تشريعات متكاملة، سواء على المستوى الدولي أو الوطني، لضمان الحماية الجنائية الكافية للتوقيع الإلكتروني وسوف نتناول في ما يلي أبرز هذه المخاطر والجهود التشريعية المبذولة لمواجهتها.

المطلب الاول

الجرائم الماسة والمرتبطة بالتوقيع الالكتروني

تعدّ الحماية القانونية للتوقيع الإلكتروني من الأمور الأساسية في ضمان أمان وسرية المعاملات التجارية عبر الفضاء الإلكتروني، فالتوقيع الإلكتروني يُعتبر أداة حيوية لإضفاء المصداقية على المعاملات الرقمية ويُسهم في تعزيز الثقة بين الأطراف المتعاملة، ومع ذلك فإن استخدام هذه التقنية الحديثة في المعاملات التجارية قد أفرز العديد من التحديات القانونية أبرزها الجرائم الإلكترونية، التي تُشكل تهديدًا حقيقيًا على نزاهة المعاملات

وسلامتها، وبالتالي تؤثر على ثقة الأطراف المتعاملة في بيئة الإنترنت وإن غياب آلية قانونية فعّالة لحماية التوقيع الإلكتروني قد يؤدي إلى تهديد هذه الثقة، ويجعل المعاملات عرضة للاستغلال والتلاعب ومن هنا تنبع الحاجة الملحة للمشرع إلى توفير الحماية القانونية للتوقيع الإلكتروني، وذلك من خلال تجريم الأفعال التي قد تؤدي إلى الاعتداء عليه وهي جميعها تهديدات تتطلب تدخلاً قانونياً صارماً لحماية الحقوق.

الفرع الأول

الجرائم التقليدية الماسة بالتوقيع الالكتروني

تعد الجرائم التقليدية من الأفعال التي استقر المجتمع على أنها جرائم تمس بمصالح الأفراد وممتلكاته وما تشكله من اعتداء مباشر وتتسم هذه الجرائم في الغالب على عنصر العنف أو التهديد كمات انها تخضع لإجراءات التقليدية في التحقيق والمحاكمة، سوف نسلط الضوء على هذه الجرائم ومدى توافقها مع الجريمة الالكترونية و المتداولة في العالم الافتراضي وهي:

أولا :جريمة السرقة الإلكترونية

تُعدّ جريمة السرقة الإلكترونية من الجرائم المستحدثة في ظل التطور التكنولوجي المتسارع، وهي تختلف عن السرقة التقليدية من حيث الوسيلة والمحل، ففي الوقت الذي تتعلق فيه السرقة التقليدية بالاستيلاء على أشياء مادية ملموسة، فإن السرقة الإلكترونية تنصب أساساً على المعلومات والبيانات والبرمجيات المخزنة داخل أنظمة الحواسيب، أو عبر الشبكات الإلكترونية[1]، وذلك دون علم أو إذن من صاحب الحق الشرعي فيها.

1- سمير دانون،العقود الالكترونية في اطار تنظيم التجارة الالكترونية، المؤسسة الحديثة للكتاب، لبنان،2012، ص91

ويمكن تعريف السرقة الإلكترونية بأنها: الاستيلاء غير المشروع على بيانات أو معلومات أو برمجيات مخزنة في نظم إلكترونية، ودلك عن طريق اختراق الأنظمة أو استخدام هذه الأنظمة بشكل غير قانوني يتيح للفاعل الانتفاع بها أو حجبها عن صاحبها الشرعي، وذلك دون علم أو إذن من صاحب الحق الشرعي فيها[1].

1- الأركان القانونية لجريمة السرقة الإلكترونية

الركن المادي: يتمثل في فعل الاستيلاء غير المشروع على المعلومات أو البيانات.

الركن المعنوي: يتجسد في القصد الجنائي، أي أن يكون الجاني على علم بأن فعله غير مشروع، وأن لديه نية الاستيلاء أو الإضرار بصاحب الحق و هو ذات القصد المتوفر في السرقة التقليدية[2].

2- العقوبات المقررة

لم يرد في قانون العقوبات الجزائري نص صريح يعالج جريمة السرقة الإلكترونية كجريمة قائمة بذاتها، لكن يمكن الاستناد إلى بعض المواد لتكييفها قانونياً. ومن أبرز هذه النصوص:

المادة 350 من قانون العقوبات الجزائري، والتي تنص على أن: كل من اختلس شيئاً غير مملوك له يعد سارقاً والتي وسّعت من مفهوم السرقة لتشمل الوسائل الإلكترونية في تنفيذ الجريمة.

1- ترجمان نسيمة، الحماية الجنائية للتوقيع الالكتروني دراسة مقارنة، اطروحة لنيل شهادة الدكتوراء طور ثالث، تخصص تجريم في قانون الاعمال، جامعة ابن خلدون تيارت،2021، ص 70.

2- محمد عبد المحسن بن طريف- فيصل سعيد العبادي- هبة عبد المطلب الفضلي، جريمة السرقة المعلوماتية، مجلة الدراسات و البحوث القانونية، مجلد 7 العدد 2 سنة 22 ،ص23

المادة 350 مكرر 1 والتي تعاقب على الدخول غير المشروع إلى نظم المعلومات، وتحديداً إذا تعلق الأمر بسرقة أو تعديل أو حذف بيانات.

وحسب المادة 394 مكرر 1 فإن العقوبة المقررة لمرتكب جريمة السرقة الإلكترونية تتراوح بين سنة إلى عشر سنوات حبسا، وغرامة مالية من 200,000 دج إلى 1,000,000 دج، وذلك إذا ثبت أن الجاني قام بسرقة أو إتلاف بيانات أو برمجيات أو أدخل تغييرات ضارة في نظام معلوماتي محمي.

ثانيا : جريمة التزوير الإلكتروني

تُعد جريمة التزوير الالكترونية من الجرائم الخطيرة و الأكثر انتشارا في مجال الاعتداء على المعلومات المخزنة والمتبادلة عبر شبكات الإنترنت التي تمس الثقة في المحررات والمعاملات القانونية وهو تحريف متعمد للحقيقة في وقائع أو بيانات، سواء بالحذف أو الإضافة، باستخدام الوسائل الإلكترونية، على نحو يُحدث أثراً يُمكن إدراكه بالحواس ويمس مراكز قانونية ثابتة[1].

ويتحقق التزوير الإلكتروني عندما يتم التغيير أأو التعديل في المعطيات الإلكترونية التي تتضمنها الوثائق أو المحررات الرقمية، وهو ما يجعل هذه الجريمة تأخذ أبعاداً فنية وقانونية معقّدة تتطلب تدخلاً تشريعياً دقيقاً.

1- أركان جريمة التزوير الإلكتروني

الركن المادي يتحقق الركن المادي في جريمة التزوير الإلكتروني من خلال وجود فعل التحريف المتعمد للحقيقة، ويكفي في ذلك أن يكون التغيير الذي أُدخل على الحقيقة نسبياً، أي أنه يخالف إرادة صاحب الشأن أو يهدف إلى الإضرار بالغير أو المساس بمركزه

1- فتيحة عمارة ، جريمة التزوير الالكتروني، مجلة القانون و المجتمع المجلد 7، ع01، 2019

القانوني[1]، كما أن العلاقة السببية تتحقق عندما يكون استخدام منظومة التوقيع الإلكتروني أو البيانات المزورة هو السبب المباشر في وقوع الضرر أو التغيير القانوني[2].

الركن المعنوي يشترط لقيام الركن المعنوي في جريمة التزوير الإلكتروني توفر القصد الجنائي بشقيه:

القصد العام: ويقصد به علم الجاني بجميع عناصر الجريمة، وإرادته في ارتكاب الفعل وهو يعلم أنه مخالف للقانون.

القصد الخاص: ويظهر في نية الجاني باستعمال المحرر المزور لتحقيق هدف غير مشروع، مثل الإضرار بالغير أو الحصول على منافع غير قانونية. و أن يكون الجاني قد ارتكب فعل التزوير عن علم وإرادة، أي أنه تعمّد تغيير الحقيقة وكان يعلم بالأثر القانوني الناتج عن فعله.

مقارنة بجريمة التزوير التقليدية لا تختلف جريمة التزوير الإلكتروني في عناصرها الأساسية عن التزوير التقليدي من حيث الأركان الثلاثة المادي، المعنوي، والضرر، إلا أن الاختلاف الجوهري يكمن في وسيلة ارتكاب الجريمة، حيث يتم في الحالة الإلكترونية عبر نظم الحاسوب والشبكات أو تقنيات التوقيع الرقمي، ما يستوجب وسائل فنية خاصة للكشف عنها وإثباتها.

1- نهلا عبد القادر المومني، الجرائم المعلوماتية ،دار الثقافة ، لبنان 2010،ص143

2- علجي اميرة –سعد الدين خونة ،الحماية الجنائية للتوقيع الالكتروني في التشريع الجزائري مدكرة لنيل شهادة الماستر برج بوعريريج ،ص 51

2- العقوبات المقررة

و يمكن القول ايضا انه يمكننا تطبيقها على جريمة التزوير الالكتروني و كون المشرع في المواد 25 و 214 الى غاية 229 قد استعمل مصطلح المحرر دون التمييز بينه و بين المحرر الالكتروني[1]

ثالثا: جريمة إتلاف التوقيع الإلكتروني

تُعدّ من الجرائم المعلوماتية التي تهدف إلى المساس بسلامة البيانات والبرامج، ويُعرَّف "الإتلاف" في هذا السياق بأنه التعديل الكلي أو الجزئي للمعلومات أو البرامج الإلكترونية، أو تدميرها أو تشويهها، بما يجعلها غير صالحة للاستخدام.

يمتد مفهوم الإتلاف ليشمل كل ما يمس البيانات والمعلومات المخزنة داخل النظام الإلكتروني، وليس فقط العناصر المادية. ويشمل ذلك البيانات المخزنة، والبرمجيات، والمعلومات الحساسة التي يتم التلاعب بها بوسائل مختلفة، من بينها الفيروسات والبرامج الضارة[2].

ونجد جل التشريعات تُشرّع هذه الأفعال ضمن القوانين الخاصة بالجرائم الإلكترونية، حيث يُفرّق بين نوعين الإتلاف المادي المرتبط بالأجهزة والنظم، أي التعطيل أو الإفساد الذي يصيب البنية التحتية للنظام والإتلاف المعنوي المرتبط بالبيانات والمعلومات، مثل تزوير أو محو أو تعديل التوقيع الإلكتروني أو البيانات المخزنة[3].

1- علجي اميرة-سعد الدين خونة، نفس المرجع، ص 64

2- نهلة عبد القادر المومني ، ص125

3- ترجمان فتيحة ، نفس المرجع ، ص 88

1- أركان الجريمة

الركن المادي لقيام هذه الجريمة يتطلب توافر فعل مادي يتمثل في قيام الجاني بإدخال أو محو أو تعديل غير مشروع للمعطيات. ويشترط أن يتم هذا الفعل بطريقة احتيالية تمس محتوى المعلومات المخزنة في نظام المعالجة الآلية، بحيث يؤدي ذلك إلى تغيير البيانات الأصلية أو إفسادها.

الركن المعنوي، فيتطلب توافر القصد الجنائي بشقَّيه:

العلم: أن يكون الجاني مدركًا أنه يقوم بإدخال أو تعديل أو محو لمعطيات إلكترونية من شأنها أن تؤدي إلى تغيير في المحتوى الأصلي.

الإرادة: أن تتجه إرادة الجاني إلى ارتكاب هذا الفعل وتحقيق النتيجة المترتبة عليه، أي التأثير غير المشروع في البيانات أو المحررات الإلكترونية.

2- **العقوبات المقررة**

وقد نص المشرع الجزائري على هذه الجريمة في المادة 394 مكرر 1 من قانون العقوبات[1]، والتي يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات، وبغرامة من مليون 1.000.000 دج إلى 2.000.000 دج، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية، أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها.

1- انظر المادة 394 مكرر 1 من قانون العقوبات

الفرع الثاني

الجرائم المستحدثة الاعتداء على للتوقيع الإلكتروني

بعد التطرق في الفرع الأول إلى أهم الجرائم التقليدية مثل التزوير، السرقة، والإتلاف، سيتم في هذا الفرع تناول أبرز الجرائم المستحدثة وهي جريمة الاعتداء على النظام المعلوماتي و كدا جريمة إتلاف أو تعطيل النظام المعلوماتي للتوقيع الالكتروني والتي نص عليها القانون الجزائري،

أولا : جريمة الاعتداء على النظام المعلوماتي للتوقيع الالكتروني

تتحقق جريمة الاعتداء على النظام المعلوماتي للتوقيع الإلكتروني بمجرد اختراق للنظام المعلوماتي للتوقيع أي قيام شخص غير مخول بالدخول أو البقاء داخل نظام معلوماتي مخصص للتوقيع الإلكتروني[1]، سواء كان ذلك الدخول جزئيًا أو كليًا، وسواء أدى إلى تلف أو عطل في النظام أم لا. وتُعد هذه الجريمة من الجرائم الشكلية، أي لا يشترط لقيامها حدوث ضرر فعلي، بل يكفي مجرد ارتكاب السلوك المجرم الدخول أو البقاء غير المشروع.

1- اركان الجريمة

الركن المادي يتمثل الركن المادي للجريمة في الدخول أو البقاء غير المشروع داخل نظام معلوماتي للتوقيع الإلكتروني ويكفي تحقق الفعل الإجرامي بمجرد الدخول سواء تم هذا الفعل بصورة إيجابية اختراق أو سلبية البقاء دون إذن كما يُعتبر الدخول بهدف الحصول على بيانات أو محررات الإلكترونية المخزنة[2].

1- نهلة عبد القادر المومني، نفس المرجع، ص156

2- ماني صلاح الدين-رمضان انور ، الحماية الجنائية للتوقيع الالكتروني في التشريع الجزائري، مدكرة لنيل شهادة الماستر تخصص جنائي و علوم جنائية جامعة البويرة، سنة2021، ص86

الركن المعنوي تُصنف هذه الجريمة ضمن الجرائم العمدية، أي التي تتطلب توافر العلم والإرادة لدى الجاني ويجب أن يكون الجاني على علم بأنه غير مخول بالدخول أو البقاء في النظام المعلوماتي، ومع ذلك يُقدم على هذا الفعل بإرادته.

2- العقوبات المقررة

نصت المادة 394 مكرر من قانون العقوبات الجزائري على ما يلي:

يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة مالية من 50,000 إلى 200,000 دج، كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة معالجة المعطيات، أو يحاول ذلك.

كما تطرقت المادة إلى إمكانية تشديد العقوبة في حالات معينة ذكرت في الفقرة 27

ثانيا : جريمة إتلاف أو تعطيل النظام المعلوماتي

تتحقق هذه الجريمة عند توقف النظام المعلوماتي عن أداء وظائفه المعتادة بشكل كلي أو جزئي، ما يؤدي إلى نتائج غير مألوفة أو غير صحيحة[1]، ويشمل ذلك الإضرار بالوظائف الحيوية للنظام وتتنوع الأساليب المستخدمة للاعتداء على المعلومات الإجرامية و بحسب الهدف[2] مثل الفيروسات الإلكترونية الدودة الإلكترونية القنابل المنطقية أو الزمنية او عن طريق الاعتداء المادي مثل تدمير أو حرق أجهزة الخوادم أو أدوات التخزين.

1- ترجمان نسيمة، نفس المرجع، ص115

2-رامي حليم، جرائم الاعتداء على أنظمة المعالجة الآلية للمعلومات، دراسات وأبحاث، المجلد 01، العدد 01، جامعة زيان عاشور الجلفة، 15 سبتمبر 2009، ص148

1- أركان الجريمة

- **الركن المادي** يتمثل في النشاط الإجرامي الذي يؤدي إلى تعطيل أو إتلاف النظام المعلوماتي، سواء كان ذلك من خلال وسيلة تقنية مثل البرمجيات الخبيثة أو وسيلة مادية مباشرة مثل كسر أو إحراق مكونات النظام. ويكفي لتحقق الركن المادي القيام بالفعل المؤدي إلى العطب أو الخلل، بغض النظر عن تحقق النتيجة الضررية بشكل مباشر.

- **الركن المعنوي:** تُعد هده الجريمة من الجرائم العمدية التي يشترط فيها توافر القصد الجنائي العام، والمتمثل في العلم بأن الفعل سيؤدي إلى إتلاف أو تعطيل النظام والإرادة الحرة في إتيان هذا الفعل دون رضا صاحب الحق أو دون أي مبرر قانوني.

2- العقوبات المقررة:

لم يفرد المشرع الجزائري نصًا صريحًا ومستقلًا لهذه الجريمة بذاتها، بل أوردها ضمن الظروف المشددة لجريمة الدخول أو البقاء غير المشروع في نظام معلوماتي. فحين يقترن الدخول أو البقاء بإتلاف أو تعطيل، فإن العقوبة تكون مشددة، وتصل إلى:

الحبس من 6 أشهر إلى 3 سنوات وغرامة تصل إلى 300,000 دج أو أكثر بحسب ما ورد في المادة 394 مكرر وما يليها.

ثالثا : جرائم الاعتداء على التوقيع الإلكتروني في القانون الجزائري

أقرّ المشرّع الجزائري في إطار القانون رقم15-04 المؤرخ في 1 فبراير 2015، نظامًا قانونيًا خاصًا بتنظيم التوقيع الإلكتروني وخدمات التصديق الإلكتروني، وذلك لضمان مصداقية المعاملات الرقمية وحمايتها من الاعتداءات الإلكترونية الواقعة عليه.

1-الاعتداء من طرف مقدّم خدمات التصديق الإلكتروني

أ-الإخلال بواجب الإعلام عند التوقف عن النشاط

نصّت المادتان 58 و59 من القانون 04/15 [1]على وجوب إخطار السلطة الاقتصادية المختصة في الآجال المحددة قانونا عند الرغبة في وقف النشاط أو تعليق خدمة التصديق

ويعاقب في المادة 67 من القانون 04/15[2] كل من يُخلّ بهذا الالتزام بالحبس من شهرين إلى سنة وغرامة مالية من 200,000 إلى 1,000,000 دج أو بإحدى العقوبتين.

ب- خرق سرية بيانات شهادة التصديق

نصت المادة 42 من القانون 04/15 [3]على وجوب الحفاظ على سرية البيانات المتعلقة بشهادة التصديق.

ووفقًا لـ المادة 70 من القانون 04/15[4] فيعاقب فاعلها بالحبس ثلاثة أشهر إلى سنتين وغرامة من 200,000 إلى 2,000,000 دج أو إحدى العقوبتين.

ج- جنحة حيازة أو إفشاء أو استعمال بيانات توقيع موصوفة

تشمل هده الجنحة هده الأفعال وهي حيازة بيانات توقيع موصوفة دون وجه حق إفشاء هذه البيانات واستعمالها دون إذن والتي وردت في المادة 43 من القانون رقم 15-04 [5]و التي يعاقب عليها في المادة 68 من القانون 04/15 [6]بالحبس من ثلاثة أشهر إلى ثلاثة سنوات وغرامة من1,000,000 إلى 5,000,000 دج.

1- انظر المادة 58و59 من القانون 04/15

2- انظر المادة 67 من القانون نفسه

3- انظر المادة 42 من القانون نفسه

4- انظر المادة 70 من القانون نفسه

5- انظر المادة 43 من القانون نقسه

5- انظر المادة 68 من القانون 04/15

د-جمع أو استعمال البيانات الشخصية خارج نطاق خدمات التصديق

بحسب المادة من 43 من القانون 04/15 [1]، يُمنع على مقدّمي خدمات التصديق جمع بيانات الموقع دون موافقته الصريحة، أو استعمالها لأغراض خارجة عن إصدار شهادة التصديق.

ويعاقب عليها وفقًا لـ المادة 71 من القانون 04/15 [2] بالحبس من 6 أشهر إلى ثلاثة سنوات وغرامة مالية من200000دج الى 1000000دج أو إحدى العقوبتين.

هـ-مزاولة نشاط التصديق الإلكتروني دون ترخيص

تشمل هذه الجريمة قيام شخص أو جهة بإصدار شهادات تصديق دون الحصول على ترخيص مسبق أو بعد سحب الترخيص سواء برغبة المقدم أو بقرار إداري

ويعاقب عليها في المادة 72 من القانون 04/15[3] بالحبس من سنة إلى ثلاث سنوات وغرامة من 200,000 إلى 2,000,000 دج أو بإحدى العقوبتين.

2- تقديم إقرارات كاذبة للحصول على شهادة تصديق

تتمثل هذه الجريمة في قيام الغير بتقديم بيانات أو مستندات مزورة إلى مقدم خدمات التصديق الإلكتروني بغرض الحصول على شهادة توقيع موصوفة.

ويعاقب عليها في المادة 66 من القانون 04/15 [4]بالحبس من ثلاثة أشهر إلى ثلاثة سنوات سنوات

1- انظر المادة 43 من القانون نفسه

2- انظر المادة 71 من القانون نفسه

3- انظر المادة 72 من القانون نفسه

4- انظر المادة 66 من القانون نفسه

غرامة مالية من 20,000 إلى 200,000 دج أو بإحدى العقوبتين.

3-الاعتداء من طرف صاحب التوقيع الإلكتروني

يتجلى هذا النوع من الاعتداء في استخدام صاحب شهادة التصديق الإلكتروني لها في غير الغرض الذي مُنحت من أجله.

ويعاقب عليها في المادة 74من القانون 15-04 [1]بغرامة مالية من 2,000 إلى 200,000 دج.

المطلب الثاني

اجراءات الاثبات الجنائي في جرائم التوقيع الالكتروني

لقد أحدثت هذه التكنولوجيا تحديات جديدة في المجال الجنائي، حيث أصبحت تُستعمل في ارتكاب أفعال غير قانونية، يرتكبها أفراد غير مرئيين ومجهولين. كما أن هذه الجرائم تتعقّد بفعل غياب الحدود الجغرافية الواضحة، مما يستدعي أخذ مسألة الاختصاص بعين الاعتبار، لما تطرحه من إشكالات، سواء كان الاختصاص دوليًا أو محليًا أو عدليًا. ويُعد هذا من التحديات الصعبة، خاصة أن مواجهتها تتطلب أدوات وتقنيات متقدمة في مجال التحقيقات الجنائية.

وسنتناول في هذا المطلب دراسة أهم أدوات الإثبات الجنائي للوصول إلى الجريمة، بالإضافة إلى الاختصاص.

1- انظر المادة 74 من القانون 04/15

الفرع الأول

الإثبات الجنائي في جرائم التوقيع الالكتروني

يعد الدليل الالكتروني من ابرز ما تطور كي يتناسب مع تطور الجريمة الالكترونية أصبح الدليل يشكل تحديا للقائمين على مكافحة هذه الجرائم، اد يتسم الدليل الالكتروني كونه غير ملموس وغير مرئي يتخذ عده أشكال بيانات رقمية محفوظ وتم تخزينها عبر الشبكات الرقمية كالصور الرقمية والتسجيلات الرقمية والنصوص المكتوبة وكذا صعوبة في محوه وتحطيمه لمكانية إعادته من خلال ذاكرة الآلة التي تحتوي على الدليل والحديثة وهذا ما سنتناوله.

أولا : الوسائل التقليدية للإثبات الجنائي في جرائم التوقيع الالكتروني

تُعد إجراءات الإثبات في الجرائم التقليدية ذات أهمية كبيرة حتى في ظل الاعتماد على الدليل الرقمي، حيث تهدف هذه الإجراءات إلى الوصول إلى الدليل المعلوماتي الذي يُعد عنصرًا محوريًا في الكشف عن الجرائم الإلكترونية. وسنتطرق فيما يلي إلى أهم هذه الإجراءات:

1. المعاينة

يقصد بالمعاينة الانتقال إلى مكان ارتكاب الجريمة، أي إلى مسرح الجريمة، من أجل ضبط كل ما يتعلق بها، سواء كان من العناصر المادية مثل الحواسيب والهواتف الذكية أو غير المادية مثل فحص أنظمة الاتصال، ومسارات الإنترنت وإثبات حالة الموجودات والأشخاص المرتبطين بالجريمة، وتحديد الوسيلة والمكان الذي ارتكبت فيه الجريمة .

وقد أُسندت مهمة المعاينة إلى الشرطة القضائية والتي تقوم بإخطار وكيل الجمهورية بوجود الجريمة[1]، ثم الانتقال إلى مكانها من أجل الحفاظ على الأدلة من الاندثار، وحماية كل ما قد يساهم في الوصول إلى الحقيقة، وذلك عبر التحفظ على مكان الجريمة وكل مكوناته[2].

2.التبليغات

بعد تلقي التبليغات أو الشكاوى بوقوع جريمة إلكترونية، سواء عن طريق البريد، الهاتف، الإنترنت[3]، يتوجب على الشرطة القضائية اتخاذ الإجراءات القانونية اللازمة وقد تم إنشاء مركز للوقاية من جرائم الإعلام والجرائم الإلكترونية، وفقًا للمرسوم التنفيذي رقم 261/15 بهدف تعزيز التنسيق والوقاية من هذا النوع من الجرائم.

3.التفتيش

يُقصد بالتفتيش الانتقال إلى مكان الجريمة وضبط الأدلة المتعلقة بها قصد العثور على ما يساهم في إثبات الجريمة أو تحديد هوية الجاني ويشمل التفتيش المكونات المادية والتقنية التي يُشتبه في استخدامها في ارتكاب الجريمة، مثل الأجهزة التي تعالج البيانات إلكترونيًا، مع استخراج البيانات المخفية أو المحذوفة المرتبطة بالفعل الإجرامي.

وقد أُسندت مهمة التفتيش إلى ضباط الشرطة القضائية، بأمر من وكيل الجمهورية أو النيابة العامة، باعتبارها الجهة المخولة قانونًا بالإشراف على التحقيقات وتوجيهها.

ويُشترط في عملية التفتيش أن:

1- انظر المادة 18 من قانون الإجراءات الجزائية

2- فلاك مراد- الية الحصول على الدليل الرقمي كوسائل اثبات في الجرائم الالكترونية، مجلة الفكر القانوني و السياسي عدد 5، نشر 2019/06/12 ص210

3- انظر المادة 17 من القانون نفسه

– تتم في نطاق الجريمة وألا تمتد إلى خصوصيات الأفراد.

– تُنفذ من قبل جهات مؤهلة علميًا وتقنيًا.

– تُحترم فيها الضمانات القانونية، من بينها التوقيت، إلا في حالات استثناها المشرع الجزائري، خاصة في الجرائم المتعلقة بأنظمة معالجة المعطيات، نظرًا لإمكانية محو أو تدمير الأدلة سريعًا [1].

كما يجب أن يتم التفتيش بحضور المتهم أو من ينوب عنه، أو شاهدين اثنين، وفق ما ينص عليه القانون[2].

وفي ختام عملية التفتيش، يتم جمع الأدلة وتوثيقها بطريقة قانونية ومنظمة لضمان حجيتها أمام القضاء، مع حفظها في ظروف مناسبة تمنع التعرض أو التلف ويُحرر محضر التفتيش وفقًا لقواعد قانونية دقيقة، يُرفع إلى قاضي التحقيق أو النيابة العامة[3]، يوقع من قبل الطرفين قاضي التحقيق وكاتب الضبط[4].

ووفقًا للمادة 5 من القانون 04-09 [5]، يمكن للجهات المكلفة بالتفتيش تسخير خبير مختص و متمكن في موضوع الجريمة، أو مقدّم خدمات التصديق الإلكتروني، إضافة إلى الاستعانة بـ الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، في سبيل تحقيق أكبر قدر من الكفاءة والدقة في الإجراءات.

1- انظر المادة 47 من قانون اجرائات الجزائية

2- انظر المادة 45 من القانون نفسه

3- ترجمان نسيمة، نفس المرجع،162

4- انظر المادة 79 من القانون نفسه

5- انظر المادة 05 من القانون 04/09

ثانيا : الإجراءات المستحدثة في مواجهة الجرائم الإلكترونية

نظرًا لصعوبة تحديد الجريمة أو مرتكبها في الجرائم الإلكترونية بالطرق التقليدية، وجد المشرع الجزائري نفسه مضطرًا إلى استحداث آليات جديدة تتماشى مع طبيعة هذا النوع المعقّد من الجرائم وقد تجلّت هذه الجهود في القانون رقم04/09 ، الذي تضمّن إجراءات استثنائية تهدف إلى دعم عملية الإثبات وضبط الأدلة الرقمية ومن أبرز هذه الإجراءات:

1.التسرب الإلكتروني اوالاختراق

يُعد التسرب الإلكتروني أو الاختراق من الجرائم التي تمس خصوصية الأفراد، ويُصنف كاعتداء مباشر على الحياة الخاصة[1] ونظرًا لطبيعة هذا النوع من الجرائم، فقد رأى المشرع الجزائري أنه لا يمكن الاعتماد على وسائل الإثبات التقليدية وحدها من اجل جمع الادلة و خصوصًا في ظل تكرار هذه الأفعال في الفضاء السيبراني ولذلك، تم التنصيص في المادة 65 مكرر 12 [2]من قانون الإجراءات الجزائية على ضرورة اتخاذ جميع التدابير الكفيلة بحماية الأدلة الرقمية وضبطها كما تم الاعتراف بالمواقع التي يتم اختراقها، وكأن الكلمة الصادرة عنها صادرة من الفاعل الحقيقي، خاصة عند انتحال صفات وهمية ويُشترط أن تتم هذه المهمة بإذن من النيابة العامة وتحت إشراف السلطة القضائية.

ويُشترط في عملية التسرب (الاختراق) ما يلي:

السرية: حيث يقوم ضابط الشرطة القضائية بإخفاء هويته، والعمل تحت اسم مستعار، حفاظًا على سلامته وسلامة عائلته. ولا يعد هذا الإجراء باطلًا قانونًا[3].

1- وداعي عز الدين، التسرب كاسلوب البحث والتحري الخاصة على ضوء قانون الاجراءات الجزائرية و المقارنة، مجلة الأكاديمية للبحث القانوني، مجلد 16 ،ع 02 ،2017، ص202

2- انظر المادة 65 مكرر12

3- أنظر المادة 65 مكرر1/16من القانون 22/06من ق ا ج

الحيلة و الخديعة: وهي تتجلى في قيام الضابط بكل ما يساهم في كشف الجريمة، باستخدام الذكاء والمكر في التفاعل مع الجاني[1].

التداخل: ويقصد به التأثير على الطرف الآخر (الجاني) وخلق علاقة معه للوصول إلى الحقيقة.

2- اعتراض المراسلات

يعني اعتراض المراسلات قيام جهة أو طرف ثالث بالحصول على رسائل أو محادثات بين شخصين دون إذنهما، بهدف استخدامها كأدلة في الإثبات أمام القضاء.

وقد استحدث المشرع هذه الوسيلة في إطار القانون رقم 06-22 المعدل لقانون الإجراءات الجزائية، في المواد من 65 مكرر 5 إلى 65 مكرر 10.

كما نصت المادة 65 مكرر 9 ومكرر10 [2] على ضرورة تحرير محضر من طرف ضابط الشرطة القضائية عن كل إجراء متعلق بالاعتراض وذكر تاريخ كل عملية اعتراض، ونسخ المحتوى المعترض عليه، وترجمته إذا استُعين بمترجم.

وألا تكون لهذه الإجراءات قوة ثبوتية أمام القضاء إلا إذا تم استيفاء كافة الشروط القانونية المنصوص عليها في المادة 214 من قانون الإجراءات الجزائية.

ويخضع ادن الاعتراض لعدة شروط قانونية[3]، من أهمها:

1. أن يتم بأمر مكتوب من وكيل الجمهورية وقاضي التحقيق[4].

1- وداعي عز الدين، المرجع نفسه، ص205

2- انظر المادة 65 مكرر09 و مكرر10

3- انظر المادة 65 مكرر7

4- انظر المادة 65 مكرر 5

2. أن يكون صالحًا لمدة لا تتجاوز أربعة (4) أشهر، قابلة للتجديد وفق مقتضيات التحقيق.

3. أن يكون صادرا عن جهة مختصة نوعيًا ودلك حسب نوع الجريمة ومكانيًا اين تم ارتكاب الجريمة او محل اقامته او اين تم القبض علي المتهم[1].

4. أن يتضمن الأمر جميع العناصر التي تسمح بتحديد الاتصالات المراد اعتراضها، مع تبرير اللجوء إلى هذا الإجراء.

الفرع الثاني

الاختصاص في جرائم التوقيع الالكتروني

يُعد الاختصاص في جرائم التوقيع الإلكتروني من الإشكالات القانونية المعقدة التي يسعى المشرّع إلى معالجتها، نظرًا لكون هذه الجرائم تُرتكب في فضاء افتراضي، ما يجعلها من الجرائم المستحدثة التي فرضت نفسها بقوة على الصعيدين الإقليمي والدولي وتتميّز هذه الجرائم بأنها لا تدخل ضمن الإطار التقليدي للمكان، إذ قد يقع السلوك الإجرامي في دولة، بينما تتحقق النتيجة الإجرامية في دولة أخرى، وهو ما يُثير إشكالية حول تنازع الاختصاص في المتابعة وتطبيق العقوبة.

أدى هذا الوضع إلى بروز الحاجة الملحّة إلى جهود دولية منسقة، خاصة على مستوى توحيد القواعد القانونية وتعزيز آليات التعاون القضائي بين الدول، من أجل وضع أسس واضحة لمكافحة هذا النوع من الجرائم، وسدّ الثغرات القانونية التي تُستغل للتهرب من العقاب، بل وتُستخدم لنشر الجريمة على نطاق عابر للحدود[2].

1- صالح شنين، اعتراض المراسلات و تسجيل الاصوات و التقاط الصور في قانون الاجراءات الجزائية الجزائري ،جامعة عبد الرحمان ميرة بجاية ص68

2- لموسخ محمد، تنازع الاختصاص في الجرائم الالكترونية، دفاتر السياسة والقانون، مجلد02، عدد2، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح ورقلة، 01-06-2009، صص151 – 153. 51 – 67.

ومن بين أبرز الإشكالات المطروحة في هذا السياق، مسألة القانون الواجب التطبيق في حالة ارتكاب جريمة تمس بالتوقيع الإلكتروني، خاصة عند تعدد الدول المتداخلة في وقائع الجريمة. ويندرج هذا البحث في إطار محاولة الإجابة عن هذا الإشكال، من خلال دراسة:

أولا: الاختصاص التشريعي في جرائم التوقيع الالكتروني

تُعد مسألة تحديد القانون الواجب التطبيق في جرائم التوقيع الإلكتروني من المسائل الجوهرية التي ترتبط بالاختصاص التشريعي، والذي يُستمد أساسًا من النصوص والقوانين الداخلية لكل دولة ورغم أن هذا التوجه يستند تقليديًا إلى مبدأ إقليمية النص الجنائي، إلا أن تطور الجرائم الإلكترونية وسمتها العابرة للحدود جعل من الضروري إعادة النظر في كفاية هذا المبدأ، واعتماد معايير إضافية أكثر ملاءمة لطبيعة الجرائم الرقمية[1].

1- مبدأ الإقليمية: يقوم هذا المبدأ على أن الدولة تُطبّق قانونها الجنائي على كل الجرائم التي تُرتكب داخل إقليمها، سواء تم ارتكابها كليًا أو جزئيًا داخل حدودها، وبصرف النظر عن جنسية الفاعل[2].

وهذا ما أكدته المادة 3 من قانون العقوبات الجزائري، التي تقضي بخضوع كل جريمة تُرتكب في الإقليم الجزائري لأحكام القانون الجزائري،[3] كما تدعمه أيضًا المادتان 585 و586 من قانون الإجراءات الجزائية، واللتان توسعتا في إقرار الاختصاص عندما يكون الجرم قد بدأ أو ظهرت آثاره داخل الدولة[4].

1- عراب مريم، الاختصاص القضائي في الجرائم المعلوماتية، حوليات كلية الحقوق والعلوم السياسية، المجلد 07، العدد03، كلية الحقوق والعلوم السياسية، جامعة محمد بن أحمد وهران 02، 22 ديسمبر 2015، ص ص 283-284. ص ص 268 – 294.

2- عراب مريم،المرجع السابق، ص 277.

3- راجع المادة 3 من الأمر رقم 66-156، السالف الذكر.

4- أنظر المواد 585 – 586 من الأمر رقم 66-155، السالف الذكر.

لكن في الجرائم الإلكترونية، ومنها جرائم التوقيع الإلكتروني، يصعب دائمًا تحديد مكان وقوع الجريمة بدقة نظرًا للطبيعة الافتراضية لهذه الأفعال، مما يحد من فعالية هذا المبدأ وحده، خصوصًا إذا كانت الجريمة موزعة بين عدة دول.[1]

2- مبدأ الشخصية: يسمح هذا المبدأ بتطبيق القانون الوطني على أساس جنسية الفاعل أو المجني عليه وهذا يعني سريان القانون الوطني على جميع رعايا الدولة الذين يرتكبون جرائم خارج حدودها بغض النظر على جنسية المجني عليه[2].

فتمكّن من تطبيق القانون على أي شخص، أجنبي كان أو وطني، إذا كانت الضحية من رعايا الدولة، حتى وإن وقعت الجريمة في الخارج.

وهذا المبدأ يُطبّق كذلك في الجزائر، خصوصًا في الجرائم الماسة بالأمن السبيريانى أو التوقيعات الإلكترونية التي يكون أحد أطرافها جزائريًا.

3- مبدأ العينية: ينصرف هذا المبدأ إلى تطبيق القانون الوطني على الجرائم التي تمس مصالح الدولة الأساسية، بغض النظر عن مكان ارتكاب الجريمة أو جنسية مرتكبها. وقد أشار إليه المشرّع الجزائري في المادة 588 من قانون الإجراءات الجزائية والمادة 15 من القانون 09-04،خاصة عندما تتعلق الجريمة باعتداءات تمس أمن الدولة أو أنظمتها المعلوماتية[3].

1- لسود موسى، معايير الاختصاص القضائي في جرائم قانون التجارة الالكترونية الجزائري 18-05، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 04، العدد02، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف المسيلة، 08 جانفي 2020، ص – ص 373-374. ص ص 366 – 382.

2- ترجمان نسيمة، المرجع السابق، ص187.

3- أنظر المادة 588 من الأمر 66-155، السالف الذكر.

ـــــ راجع المادة 15من القانون 04-09 مؤرخ في 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الصادر في ج ر ع 47، مؤرخة في 16 أوت 2009.

امتد نطاق التطبيق كذلك بموجب القانون 15-04 إلى الشركاء في الجريمة الإلكترونية، وليس فقط الفاعلين الأصليين، مما يعكس وعي المشرع بخطورة الاشتراك الرقمي أو الدعم الفني في الجرائم الإلكترونية العابرة للحدود[1].

ثانيا: الاختصاص القضائي في جرائم التوقيع الإلكتروني

بعد التعرض لمبادئ الاختصاص التشريعي، كالإقليمية، الشخصية والعينية، تبرز أهمية دراسة الاختصاص القضائي في الجرائم المستحدثة، وعلى رأسها جرائم التوقيع الإلكتروني، لما تتسم به من خصوصية وصعوبة في تحديد مكان وقوعها. ولقد حاول المشرّع الجزائري التكيّف مع هذا النوع من الجرائم من خلال إقرار قواعد مرنة في تحديد الجهة القضائية المختصة، مستندًا إلى قانون الإجراءات الجزائية وبعض النصوص الخاصة.

1- اختصاصات وكيل الجمهورية: حدد المشرّع اختصاص وكيل الجمهورية في المادة من37 من قانون الإجراءات الجزائية حيث يمارس صلاحياته في النطاق المحلي بناءً على مكان ارتكاب الجريمة، مكان إقامة المتهم، مكان القبض عليه أو حتى القاء القبض عليه خارج تلك الجريمة[2]، وتُطبّق هذه القاعدة كذلك على الجرائم الإلكترونية بما فيها جرائم التوقيع الإلكتروني بالرغم من التحديات التي تفرضها الطبيعة الافتراضية لهذه الجرائم.

كما نصت المادة 37 فقرة 2 وأقر به المرسوم التنفيذي رقم 06-348 إمكانية تمديد اختصاص وكيل الجمهورية ليشمل كامل الاقليم الوطني في أنواع معيّنة من الجرائم التي تقتضي ظروفها ذلك، ومنها الجرائم المعلوماتية، وهو ما يسمح لوكيل الجمهورية بمباشرة إجراءات المتابعة خارج نطاقه الجغرافي في حالات محددة[3].

---

1 - قانون رقم 15-04 مؤرخ في 01 فيفري 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، الصادر في ج ر ع 06، مؤرخة في 10فيفري 2015.

2- راجع المادة 37 من الأمر 66-155، السالف الذكر.

3- أنظر المادة 37 ف 2 من الأمر 66-155، السالف الذكر.

2-اختصاصات قاضي التحقيق: بموجب المادة 40 من قانون الإجراءات الجزائية يباشر قاضي التحقيق مهامه ضمن نطاق اختصاص المحكمة التي يتبعها، بناءً على نفس المعايير مكان الجريمة، إقامة المتهم، أو القبض عليه غير أن التطور في طبيعة الجرائم دفع بالمشرع إلى توسيع هذا الاختصاص، لا سيما بالنسبة للجرائم الإلكترونية التي قد تتطلب إجراء تفتيش أو تحرٍ يمتد إلى أكثر من ولاية[1].

أجاز القانون في المادة 40 الفقرة 2 من قانون الإجراءات الجزائية، وكذلك المرسوم التنفيذي رقم 06-348، في حالات الضرورة امتداد إجراءات التفتيش والتحقيق إلى كامل التراب الوطني، وذلك في إطار الجرائم التي تستدعي مرونة في الاختصاص[2].

كما نصت المادة 47 الفقرة 4 من نفس القانون على ما يُتيح لقاضي التحقيق ملاحقة الجناة، والقيام بعمليات التفتيش والمعاينة في أي وقت ومكان، متى تعلق الأمر بجرائم ذات طابع خاص، على غرار جرائم المخدرات، والجرائم المنظمة العابرة للحدود، والجرائم التي تمس بأنظمة المعالجة الآلية للمعطيات[3].

3- اختصاصات الضبطية القضائية: تقوم الضبطية القضائية، تحت إشراف وكيل الجمهورية أو قاضي التحقيق، بمباشرة إجراءات البحث والتحري في إطار الاختصاص المحلي إلا أن طبيعة الجريمة الإلكترونية تتطلب أحيانًا امتداد صلاحيات الضبطية القضائية إلى خارج نطاقها الترابي، خصوصًا في الجرائم التي تشمل شبكات أو أجهزة تقع في ولايات مختلفة، وأجاز المشرّع في المادة 16 مكرر من قانون الإجراءات الجزائية إمكانية مراقبة

1- أنظر المادة 40 من الأمر 66-155، السالف الذكر.

2- مرسوم تنفيذي رقم 06-348 مؤرخ في 05 أكتوبر 2006، يتضمن تحديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، الصادر في ج ر ع 63، مؤرخة في 08 أكتوبر 2006.

3- أنظر المادة 47 فقرة4 من الأمر 66-155، السالف الذكر.

الأشخاص عبر كامل التراب الوطني، خاصة في الحالات المتعلقة بالجرائم التقنية والمعلوماتية.

4-اختصاص المحاكم: يتحدد نطاق عمل المحاكم وفقا لأحكام المادة 324 من ق ا ج في الظروف العادية [1]وبموجب المرسوم التنفيذي رقم 06-348، الذي نص على إمكانية تمديد الاختصاص لمعالجة هذا النوع من القضايا كما سمح هذا المرسوم بتمديد اختصاص هذه الجهات إلى قضايا تقع خارج دائرتها الترابية متى تعلق الأمر بجرائم معقّدة تستلزم تنسيقًا وطنيًا، وهو ما يُمثل تطورًا هامًا في إطار تخصص القضاء في الجرائم الإلكترونية، ومنها التوقيع الإلكتروني[2].

1- راجع المادة 324 من الأمر رقم 66-155، السالف الذكر

2- مرسوم تنفيذي رقم 06-348، السالف الذكر.

خلاصة الفصل

خاتمـــــة

مع التسارع الكبير الذي يشهده العالم في مجال التكنولوجيا الرقمية، خاصة في ميدان المعاملات التجارية الإلكترونية، برز التوقيع الإلكتروني كأداة فعالة لتوفير الأمان والسرية في التبادلات عبر الفضاء الافتراضي.

وقد دفع هذا الواقع الجديد معظم التشريعات الدولية إلى التدخل لوضع إطار قانوني يعرّف التوقيع الإلكتروني بدقة ويزيل الغموض الذي كان يكتنفه.

من بين أبرز هذه المبادرات نذكر قانون الأونسيترالال نموذجي والتوجيه الأوروبي المتعلق بالتوقيعات الإلكترونية، واللذَان أسهما في توجيه الدول نحو تبني تشريعات وطنية تُنظّم هذا المجال وتضبطه قانونيًا.

وفي هذا الإطار سارت الجزائر على خطى هذه التشريعات الدولية، حيث أقرّ المشرع الجزائري الاعتراف الرسمي بالتوقيع الإلكتروني كبديل عصري للتوقيع التقليدي، وذلك تماشياً مع متطلبات التطور التكنولوجي وتحديث المعاملات الإدارية والتجارية لكن لا يُمكن الاعتراف بالتوقيع الإلكتروني كوسيلة قانونية ملزمة مالم تتوفر فيه مجموعة من الشروط والضوابط التي تضمن صحته وسلامته وقوته الإلزامية أمام الغير.

ويُذكر أن التوقيع الإلكتروني يتعدد في صوره القانونية، ويختلف من حيث درجته في الحماية والمصداقية، لاسيما في القطاعات الحساسة مثل المعاملات البنكية، والتجارة الإلكترونية، والتعامل بالنقود الافتراضية.

ومع أنه ذه التكنولوجيات وفر العديد من المزايا، إلا أن المخاوف لاتزال قائمة، خاصة في ظل تطور الجريمة السيبريانية وانتشارها على الصعيدين الوطني والدولي.

وقد أدرك المشرع الجزائري هذه التحديات، فعمد إلى إنشاء ثلاث سلطات وطنية مختصة تعنى بمراقبة الطرف الثالث الموثوق الذي يُمنح له دور أساسي في تقديم خدمات التوثيق

والتصديق الإلكتروني وتتمثل مهام هذه السلطات في الإشراف على إصدار شهادات المصادقة الرقمية، مراقبة مصدرها، وضمان أمنها، وتطبيق رقابة صارمة على كل من يصدرها أو يحتفظ بها، أو يتعامل بها.

ورغم هذه الجهود يبقى التوقيع الالكتروني مهددا لذا وجب العمل على تطوير القوانين بما يتماشى مع التغيرات التكنولوجية وسد الثغرات والعمل على توحيد التشريعات لأجل صياغة قانون موحد لضبط التوقيع الالكتروني والحد من جرائم المعلوماتية وكذا التنسيق بين الدول فيما يخص جمع الأدلة والإثباتات والتحقيق في هذه الجرائم.

قائمة المصادر والمراجع

قائمة المراجع

أولا : المراجع باللغة العربية

I. الكتب

1) إياد احمد سعيد الساري، النظام القانوني لإبرام العقد الالكتروني على ضوء قانون التوقيع الالكتروني والمعاملات الالكترونية، ط1، منشورة الحلبي الحقوقية، لبنان، 2016.

2) ربحي تبوت فاطمة الزهراء، قانون المعاملات الالكترونية وفقا لقانون 18-05، ط2، بيت الأفكار، الجزائر2022.

3) سمير دانون، العقود الالكترونية في إطار تنظيم التجارة الالكترونية، المؤسسة الحديثة للكتاب، لبنان، 2012.

4) فيصل سعيد الغريب، التوقيع الإلكتروني وحجيته في الإثبات، ط 01، المنظمة العربية للتنمية الإدارية، مصر، 2005.

5) محمد إبراهيم أبو الهيجاء، عقود التجارة الالكترونية ط2، دار الثقافة والنشر، الأردن،2011.

6) محمد بن محمد أيوب، أثر التطورات التكنولوجية الحديثة في وسائل الإثبات التجاري والتوقيع الرقمي والسندات التجارية دراسة مقارنة، ط1، مركز الدراسات العربية، مصر، 2024.

7) محمد فواز محمد المطالقة، الوجيز في عقود التجارة الالكترونية، دار الثقافة للنشر والتوزيع، الأردن، 2008.

8) نضال سليم برهم، أحكام عقود التجارة الالكترونية، دار الثقافة، الأردن، 2010.

9) نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة، لبنان 2010.

10) وسيم حسام الدين الأحمد، الإطار القانوني للإثبات الالكتروني، ط1، دار الراية للنشر والتوزيع، الأردن، 2025.

11) يمينة حوحو، عقد البيع الالكتروني في القانون الجزائري، دار بلقيس، الدار البيضاء الجزائر، 2016.

II. الرسائل الجامعية:

- **أ – أطروحة الدكتوراه**

1) ترجمان نسيمة، الحماية الجنائية للتوقيع الالكتروني دراسة مقارنة، أطروحة لنيل شهادة الدكتوراه تخصص التجريم في قانون الاعمال، كلية الحقوق، جامعة ابن خلدون تيارت ،2020-2021.

- **ب- مذكرات الماجستير**

1) لالوش راضية امن التوقيع الإلكتروني، مذكرة لنيل شهادة الماجستير، فرع القانون الدولي للأعمال، جامعة تيزي وزو، 2012.

- **ج- مذكرات الماستر**

2) براهيمي فريدة – بوخاري نسيمة، النظام القانوني للتوقيع الالكتروني في القانون الجزائري، مذكرة لنيل شهادة ماستر قانون الأعمال، جامعة مولود معمري تيزي وزو،2017.

3) بلقايد ايمان، النظام القانوني للتصديق الالكتروني، مذكرة لنيل شهادة الماستر في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، 2016.

4) حملاوي خلود، بركاوي نورة، التوقيع الالكتروني وحجيته في الإثبات، مذكرة نيل شهادة الماستر تخصص أعمال، جامعة 08 ماي 1945، قالمة، 2017.

5) غراب نجاة، النظام القانوني للتوقيع الالكتروني في التشريع الجزائري، مذكرة ماستر، تخصص قانون أعمال، كلية الحقوق والعلوم السياسية جامعة محمد خيضر بسكرة، 2022.

6) ماني صلاح الدين – رمضان انور، الحماية الجنائية للتوقيع الالكتروني في التشريع الجزائري، مذكرة لنيل شهادة الماستر تخصص جنائي وعلوم جنائية، جامعة البويرة، 2021.

III. المقالات:

1) دحماني سمير، التوقيع الإلكتروني الموصوف، مجلة العلوم الإنسانية، المجلد 01، العدد01، المركز الجامعي تندوف، 20 جوان 2017.

2) رامي حليم، جرائم الاعتداء على أنظمة المعالجة الآلية للمعلومات، دراسات وأبحاث، المجلد 01، العدد 01، جامعة زيان عاشور الجلفة، 15 سبتمبر 2009.

3) سعيود محمد طاهر، استقلالية ضبط البريد والاتصالات الالكترونية في ظل أحكام القانون 04/18، مجلة الدراسات حول فعالية القاعدة القانونية، مجلد 04، ع01، جيجل، 2020/01/08.

4) عبان عميروش، التنظيم القانوني للتشفير كآلية التصديق الالكتروني في التشريع الجزائري والمقارن، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 07، العدد02، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف المسيلة، 10 جوان 2022.

5) عبان عميروش، النظام القانوني للتشفير كآلية التصديق الالكتروني في التشريع الجزائري والتشريعات المقارنة، مجلة الأستاذ الباحث والسياسية، مجلد 07، ع02، مستغانم، 2020/06/10.

6) عراب مريم، الاختصاص القضائي في الجرائم المعلوماتية، حوليات كلية الحقوق والعلوم السياسية، المجلد 07، العدد03، كلية الحقوق والعلوم السياسية، جامعة محمد بن أحمد وهران 02، 22 ديسمبر 2015.

7) عقوني محمد- بلمهدي براهيم، الآليات التقنية والقانونية لحماية التوقيع الالكتروني، مجلة المفكر، المجلد 14، العدد 01، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، 04 فيفري 2019.

8) علجي اميرة – سعد الدين خونة، الحماية الجزائية للتوقيع الالكتروني في التشريع الجزائري، مذكرة لنيل شهادة الماستر، تخصص قانون إعلام آلي وانترنيت، كلية الحقوق والعلوم السياسية، جامعة البشير الإبراهيمي برج بوعريريج، 2022-2023.

9) غراب نجاة، النظام القانوني للتوقيع الالكتروني في التشريع الجزائري، مذكرة لنيل شهادة الماستر، جامعة محمد خيضر بسكرة، 2022.

10) فتيحة حزام، قانون المعاملات الالكترونية دراسة على ضوء القانون 18-05، لفا للوثائق، قسنطينة الجزائر2022.

11) فتيحة عمارة، جريمة التزوير الالكتروني، مجلة القانون والمجتمع، المجلد 7، العدد 01، جامعة أحمد دراية أدرار، 01 جوان 2019.

12) فلاك مراد- آليات الحصول على الدليل الرقمي كوسائل إثبات في الجرائم الالكترونية، مجلة الفكر القانوني والسياسي، المجلد 03، العدد 01، كلية الحقوق والعلوم السياسية، جامعة عمار تليجي الأغواط،23 سبتمبر 2019.

13) لسود موسى، معايير الاختصاص القضائي في جرائم قانون التجارة الالكترونية الجزائري 18-05، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 04، العدد02، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف المسيلة، 08 جانفي 2020.

14) لموسخ محمد، تنازع الاختصاص في الجرائم الالكترونية، دفاتر السياسة والقانون، مجلد02، عدد2، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح ورقلة، 01-06-2009.

15) محمد عبد المحسن بن طريف- فيصل سعيد العبادي- هبة عبد المطلب الفضلي، جريمة السرقة المعلوماتية، مجلة الدراسات والبحوث القانونية، مجلد 7 العدد 2 جامعة محمد بوضياف المسيلة.

IV. النصوص القانونية

- **النصوص القانونية الوطنية**

- **القوانين**

1) القانون رقم 05-10، يعدل ويتمم للقانون المدني، ج ر، عدد44، مؤرخ في 20-07-2005.

2) القانون رقم 23-09 مؤرخ في 21 جوان 2023، يتضمن القانون النقدي والمصرفي، الصادرة في ج ر ع 43، مؤرخة في 27 جوان 2023.

3) القانون رقم 18-04 المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الالكترونية، مؤرخة في 10-05-2018، الصادرة في ج ر ع 27، مؤرخة في 13-05-2018.

4) القانون رقم 15-04 مؤرخ في 01 فيفري 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، الصادر في ج ر ع 06، مؤرخة في 10فيفري 2015.

5) القانون 04-09 مؤرخ في 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الصادر في ج ر ع 47، مؤرخة في 16 أوت 2009.

6) القانون19-04 يتضمن قانون المالية لسنة2019، مؤرخ في 11-12-2019، الصادرة في ج ر ع 81، مؤرخة في 30-12-2019

7) القانون رقم 17-17 مؤرخ في 27 ديسمبر 2017، يتضمن قانون المالية لسنة 2018، مؤرخة في ج رع 76، مؤرخة في 28ديسمبر 2017.

8) القانون رقم 06-22 مؤرخ في 20 ديسمبر 2006 يعدل ويتمم الأمر رقم 66-155 مؤرخ في 08 جوان 1966 والمتضمن قانون الإجراءات الجزائية، الصادر في ج ر ع 84، مؤرخة في 24 ديسمبر 2006.

9) القانون رقم 05-02 مؤرخ في 06-02-2005، يعدل ويتمم الامر رقم 75-58 مؤرخ في 26 سبتمبر 1975 يتضمن القانون التجاري، الصادرة في ج ر ع 11، مؤرخة في 09-05-2005.

10) القانون رقم 2000-03، مؤرخ في 05 أوت 2000، يحدد القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية، ج ر ع 48 الصادر بتاريخ 06 اوت 2000، المعدل والمتمم بموجب القانون رقم 06-24 مؤرخ في 26 ديسمبر 2006، المتضمن قانون المالية لسنة 2007، الصادرة في ج ر ع 85، مؤرخة في 27 ديسمبر 2006.

11) القانون رقم 18-05 المتعلق بالتجارة الالكترونية، مؤرخ في 10-05-2018، الصادرة في ج ر ع 28، مؤرخة في 18-05-2018.

- **الأوامر:**

1) الأمر رقم 75-59 مؤرخ في 26 سبتمبر 1975، يتضمن القانون التجاري، مؤرخة في ح ر ع 101، مؤرخة 19 ديسمبر 1975، معدل ومتمم بموجب القانون رقم 22-09 مؤرخ في 05 ماي2022، الصادرة في ج ر ع 32، مؤرخة في 14 ماي 2022.

2) الأمر رقم 66-165 مؤرخ في 08 جوان 1966 والمتضمن قانون العقوبات الصادر في ج ر ع 49، مؤرخة في 11 جوان 1966، معدل ومتمم بموجب القانون 24-06 مؤرخ في 28 أفريل 2024، الصادر في ج ر ع 30، مؤرخة في 30 أفريل 2024.

3) الأمر رقم 66-155 مؤرخ في 08 جوان 1966، يتضمن قانون الإجراءات الجزائية، الصادر في ج ر ع 48، مؤرخة في 10 جانفي 1966، المعدل والمتمم بالأمر 21-11 مؤرخ في 25 أوت 2021، الصادر في ج ر ع 65، مؤرخة في 26 أوت2021.

4) الأمر رقم 11-03 مؤرخ في 26 أوت 2003، يتعلق بالنقد والقرض، الصادرة في ج ر ع 52، مؤرخة في 27 أوت 2003.

- **المراسيم:**

1) المرسوم التنفيذي 98-257 مؤرخ في 25 أوت 1998 الذي يضبط شروط وكيفيات إقامة خدمات الانترنت واستغلالها، الصادر في ج ر ع 63، مؤرخة في 26 أوت 1998، المعدل والمتمم بموجب المرسوم التنفيذي 2000-307، المؤرخ في 14 أكتوبر 2000، الصادر في ج ر ع 60، مؤرخة في 15 أكتوبر 2000.

2) المرسوم التنفيذي رقم 16-134، مؤرخ في 25 أفريل 2016 يحدد تنظيم المصالح التقنية والإدارية للسلطة الحكومية للتصديق الالكتروني وتشكيلها وتنظيمها وسيرها، الصادرة في ج ر ع 26، مؤرخة في 28 أفريل 2016.

3) المرسوم التنفيذي رقم 16-142 مؤرخ في 05-05-2016، المحدد لكيفيان حفض الوثيقة الكترونيا، ج ر، عدد 28، سنة 2016.

4) المرسوم تنفيذي رقم 06-348 مؤرخ في 05 أكنوير 2006، يتضمن تحديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، الصادر في ج ر ع 63، مؤرخة في 08 أكتوبر 2006.

5) المرسوم رقم 16-135، مؤرخ في 25 أفريل 2016، يحدد طبيعة السلطة الحكومية للتصديق الالكتروني وتشكيلها وتنظيمها وسيرها، الصادرة في ج ر ع 26، مؤرخة في 28 أفريل 2016.

6) المرسوم رئاسي رقم 15-261 مؤرخ في 08 أكتوبر 2015يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من جرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الصادر في ج ر ع 53، مؤرخة في 08 أكتوبر 2015.

7) المرسوم التنفيذي رقم 07-162 مؤرخ في 30-05-2007، يعدل ويتمم المرسوم التنفيذي رقم 01-123 مؤرخ في 09-05-2001 المتعلق بنظام الاستغلال الطبق على كل نوع من أنواع الشبكات، ج ر، عدد37، سنة 2007.

ب - النصوص القانونية الأجنبية

1) قرار رقم 56-80 للجمعية العامة للأمم المتحدة للقانون التجاري الدولي، يتضمن قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية، الجلسة العامة 75، منشورات الأمم المتحدة، 12 ديسمبر 2001.

2) القانون رقم 194 لسنة 2020، يتعلق بإصدار قانون البنك المركزي والجهاز المصرفي، الصادرة في ج ر ع 37، مؤرخة في 15 سبتمبر 2020.

3) قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية، قرار الجمعية العامة للأمم المتحدة 162/51، منشورات الأمم المتحدة، المؤرخ في 16 ديسمبر 1996.

4) القانون الأردني رقم 15 من سنة 2015 المتعلق بالمعاملات الالكترونية، ج ر ع 5341، الصادر في 17-05-2015

5) التوجيه الأوروبي رقم 46 - 2000 الخاص بالنقود الالكترونية مؤرخة 8 سبتمبر 2000.

6) التوجيه الأوروبي رقم 110-2009 مؤرخة في 16 سبتمبر 2009.

V. المواقع الإلكترونية

1) https://eur-lex.europa.eu/eli/reg/2014/910/oj/eng

2) https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/ar/ml-ecomm-a_ebook_1.pdf

3) https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/ar/ml-elecsig-a.pdf.

4) https://eurlex.europa.eu/legalcontent/FR/ALL/?uri=celex%3A31999L0093

➢ **المراجع باللغة الأجنبية**

I. Texts legislatives/

1) Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques.

2) 114 stat.464, Electronic signatures in global and national commerce act; public law 106-229, 106th congress, 30 June 2000.

3) Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

4) Décrit 93-1999 CE, de 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques, j.o n 13 du 19 janvier 2000, ,modifier par le Décrit n 2001-272du 30,ars 2001, pris pour l'application de l'article 1316-4 code civil et relatif a la signature électronique, j.o n 77 du 31 mars 2001.

5) loi n° 99-1071 du 16 décembre 1999, Comprend le code monétaire et financier français,Modifié le 2025-05-29 par le Décret n°2025-470 du 28 mai 2025.

6) Ordonnance n° 2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations

7) Ordonnance n° 2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations, JORF n°0035 du 11 février 2016.

فهرس المحتويات

فهرس المحتويات

الموضوع	الصفحة
بسملة	
شكر وعرفان	
إهداء	
مقدمة	**أ-ب**
الفصل الأول : ماهية التوقيع الالكتروني	
تمهيد	**07**
المبحث الأول مفهوم التوقيع الالكتروني	**08**
المطلب الأول: تعريف التوقيع الالكتروني	**08**
الفرع الاول :التعريف الفقهي والقضائي للتوقيع الالكتروني	**09**
الفرع الثاني: التعريف القانوني للتوقيع الالكتروني	**10**
المطلب الثاني: شروط وصور التوقيع الالكتروني	**21**
الفرع الاول: شروط التوقيع الالكتروني	**21**
الفرع الثاني: صور التوقيع الالكتروني	**24**
المبحث الثاني: وظائف و تطبيقات التوقيع الالكتروني	**27**
المطلب الاول: وظائف التوقيع الالكتروني	**27**
الفرع الاول: تحديد هوية الموقع والتعريف بشخصه	**28**
الفرع الثاني: التعريف بإرادة الموقع وقبوله لموضوع المحرر ومضمونه	**29**
الفرع الثالث : إثبات سلامة المحرر	**31**
المطلب الثاني: تطبيقات التوقيع الالكتروني	**31**
الفرع الاول: بطاقات الدفع الالكترونية	**31**
الفرع الثاني: الشيكات والعملات الافتراضية	**36**
خلاصة الفصل الأول	**41**

الفصل الثاني: أمن وحماية التوقيع الالكتروني	
تمهيد	**44-43**
المبحث الاول : الحماية التقنية للتوقيع الالكتروني	**45**
المطلب الأول: التشفير الالكتروني	**45**
الفرع الأول: اساليب التشفير.	**47**
الفرع الثاني :ضوابط التشفير.	**49**
المطلب الثاني: التصديق الالكتروني.	**52**
الفرع الأول : تعريف التصديق الالكتروني	**53**
الفرع الثاني: جهات التصديق الالكتروني.	**56**
الفرع الثالث: شهادات التصديق الالكتروني	**62**
المبحث الثاني:الحماية القانونية للتوقيع الالكتروني	**66**
المطلب الاول:الجرائم الماسة و المرتبطة بالتوقيع الالكتروني	**66**
الفرع الأول: الجرائم التقليدية الماسة بالتوقيع الالكتروني	**67**
الفرع الثاني : الجرائم المستحدثة الاعتداء على للتوقيع الإلكتروني	**73**
المطلب الثاني: اجراءات الاثبات الجنائي في جرائم التوقيع الالكتروني	**78**
الفرع الأول : الإثبات الجنائي في جرائم التوقيع الالكتروني	**79**
الفرع الثاني : الاختصاص في جرائم التوقيع الالكتروني	**84**
خلاصة الفصل	**90**
خاتمة	**92**
قائمة المصادر والمراجع	**95**
فهرس المحتويات	