جامعة الشهيد حمه لخضر - الوادي
كلية الحقوق والعلوم السياسية
قسم الحقوق

الآليات القانونية لحماية التوقيع الالكتروني في التشريع الجزائري

مذكرة تخرج تدخل ضمن متطلبات نيل شهادة الماستر في الحقوق تخصص: قانون أعمال

إعداد الطالبة: شيبه صوريا

لجنة المناقشة:

الاسم واللقب	الجامعة	الصفة
د.شريفي عماد	جامعة الشهيد حمه لخضر - الوادي	رئيسا
أ. سارة شيبات	جامعة الشهيد حمه لخضر - الوادي	مشرفا ومقررا
أ.بلجاني وردة	جامعة الشهيد حمه لخضر - الوادي	مناقشا

السنة الجامعية: 2022/2021


بسم الله الرحمن الرحيم

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

** وَمَا تَوْفِيقِي إِلَّا بِاللَّهِ عَلَيْهِ تَوَكَّلْتُ وَإِلَيْهِ أُنِيبُ **

(سورة هود - الآية 88)

الاهداء

الحمد لله رب العالمين والصلاة والسلام على أشرف المرسلين سيدنا محمد وعلى آله وصحبه ومن اتبعه إلى يوم الدين.

أهدي ثمرة جهدي وعملي إلى:

إلى والدي الكريمين رمز المحبة والعطاء أطال الله عمرهما.

إلى شريك حياتي الذي شجعني كثيرا على مواصلة البحث.

إلى كل أفراد عائلتي الكريمة.

إلى أساتذتي وزملائي.

إلى أسرة كلية الحقوق والعلوم السياسية.

شكر وعرفان

قال الله تعالى" لئن شكرتم لأزيدنكم"

الحمد لله حمدا يوافي نعمه ويكافئ مزيده، وشكره على توفيقه لنا في إتمام العمل والاقتداء برسوله الذي حثنا على الشكر كما قال" الشكر قيد النعمة وسبب دوامها ومفتاح المزيد منها"

أقدم جزيل الشكر والتقدير إلى الأستاذة المشرفة "أ.شيبات سارة" حفظها الله ورعاها، عرفانا وتقديرا على توجيهاتها وملاحظاتها القيمة التي أنارت لي طريق البحث والتقصي.

كما اتقدم بجزيل الشكر لكافة أعضاء لجنة المناقشة على قبولهم مناقشة هذا العمل المتواضع.

ولا يفوتني كذلك بان أتوجه بالشكر إلى أساتذتي الكرام في كلية الحقوق والعلوم السياسية من بداية مشواري الدراسي إلى وصولي إلى هذه المرحلة.

والشكر موصول لكل أعضاء مكتبة كلية الحقوق والعلوم السياسية، ولكل من ساعدني في إعداد هذا البحث.

وما بحوزتنا أن نقول "اللهم ارزقنا شفاعة سيدنا محمد صل الله عليه وسلم و اوردنا حوضه واسقنا من يده الشريفتين شربة ماء لا نظمأ بعدها أبدا يارب العالمين "

مقدمة

بعد ظهور شبكة الانترنت أصبح العالم بموجبها قرية صغيرة، مما أدى إلى وجود ثورة تكنولوجية هائلة، أثرت على المجتمع بصفة عامة وعلى المشرعين في القانون الداخلي و الدولي بصفة خاصة، بالإضافة إلى ثورة الاتصالات والمعلومات والتطور التقني الكبير في استخدام الحاسب الآلي وشبكة الانترنت إلى تطور كبير في التعاملات الالكترونية، وبالتالي تطوير النشاط التجاري، و ظهور ما يسمى بالتجارة الالكترونية وكذلك المعاملات التجارية، من بينها إبرام العقود الكترونية ومنها جاءت فكرة التوقيع الالكتروني.

والذي يقصد به: انه ما يوضع على محرر الكتروني ويتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها، ويكون له طابع متفرد، يسمح بتحديد شخص صاحب التوقيع، ويميزه عن غيره. ويتميز التوقيع الالكتروني بمجموعة من الخصائص والتي نذكر أهمها: انه بحمي خصوصية البيانات من الاستخدامات الغير مشروعة، ويحدد هوية المستخدم، انه يمنع إنكار الشخص استلامه للرسالة المرسلة إليه، كذلك يمكن من تحديد تاريخ توقيع الرسالة، بالإضافة إلى انه يوفر الوقت والسرعة والدقة في انجاز المعاملات.

إلا أن هذا التطور لا سيما في مجال التجارة الالكترونية وما يحققه من مزايا، له سلبيات عديدة ونذكر أهمها عدم توفر الأمان فيها، الأمر الذي مهد لمخترقي النظم المعلوماتية بالتجسس على البيانات الشخصية للأفراد وخاصة التوقيعات الالكترونية، واستخدام هذه البيانات أو المعلومات بطرق غير مشروعة وهذا يؤدي إلى انعدام الأمن والخصوصية على شبكة الانترنت، وبالتالي انعدام الثقة.

لذلك فان توفر عنصر الأمان والثقة ضروري لتطوير التجارة الالكترونية عامة والمعاملات الالكترونية خاصة، والتي أصبحت عبارة عن رسائل بين المتعاملين يتم تشفيرها من اجل ضمان عم الاطلاع عليها أو تحريفها أو تزويرها، وفك تشفيرها بعملية عكسية وذلك من اجل معرفة محتواها ومضمونها.

وقصد بعث الثقة والأمان في مجال المعاملات الالكترونية التي تتم بين هذه الأطراف، سارع المشرع الجزائري إلى إيجاد طرف محايد موثوق به يتكفل بطرقه القانونية والتقنية، بضمان صحة المعلومات والبيانات المقدمة، باعتبارها آلية رقابية وضبطية تهدف إلى حماية الأطراف المتعاقدة، وذلك من خلال العمل على ترقية وتطوير استعمال التوقيع والتصديق الالكترونيين وضمان موثوقية استعمالها، حيث يتمثل هذا الطرف المحايد في شركات أو هيئات مستقلة تقوم بور الوسيط بين المتعاقدين وذلك بهدف توثيق المعاملات الالكترونية، والذي يسمى بجهات التصديق الالكتروني.

ونظرا للمشكلات القانونية التي يثيرها التوقيع الالكتروني يستلزم وضع آليات وضمانات تحمي التوقيع الإلكتروني للمتعاملين في البيئة الالكترونية.

أهمية الموضوع:

تكمن أهمية الدراسة في محاولة استقراء النصوص القانونية بالإضافة إلى الوقوف على أهم الأحكام المتعلقة بنظام التشفير والتصديق الالكتروني كونها من المواضيع الحديثة التي تتطلب تدخل المشرع لتنظيمها، لتحقيق الحماية القانونية اللازمة.

أسباب اختيار الموضوع:

تعود الأسباب الذاتية اختيار الموضوع الرغبة في الإلمام بموضوع التوقيع الالكتروني وتحديد الآليات التقنية والقانونية لحمايته، وذلك مواكبة للتطور الرقمي في مجال التجارة الالكترونية الذي يهم الفرد والمجتمع، والتعرف على الأجهزة والبرمجيات الحديثة المستعملة في مجال الرقمنة.

أما الأسباب الموضوعية وهي إزالة اللبس حول كيفيات توثيق وتصديق التوقيع الالكتروني، وحمايتها، البحث المستمر للتطلع على مستجدات التقدم العلمي والتكنولوجي في مجال التجارة الالكترونية.

أهداف الدراسة:

تهدف هذه الدراسة إلى تبيان دور القانون والتشريع في حماية المعاملات التجارية الالكترونية عامة والتوقيع الالكتروني على وجه الخصوص.

- تحديد أهمية و دور التشفير في حماية التوقيع الالكتروني
- إبراز دور جهات التصديق الالكتروني في ضمان حماية التوقيع الالكتروني

صعوبات الموضوع:

ومن الصعوبات التي واجهت هذه الدراسة ندرة المراجع والدراسات المتخصصة وخاصة الجزائرية منها، وذلك لكون طبيعة هذا الموضوع تقنية أكثر من كونها قانونية، وبالتالي صعوبة احتوائه من الناحية القانونية أو التشريعية، بالإضافة إلى تشعب الموضوع و الذي يتطلب بذل جهد اكبر، وذلك للإحاطة بالموضوع من كل جوانبه.

منهج الدراسة:

وللإلمام بموضوع البحث من كافة جوانبه اعتمدنا على المنهج الوصفي التحليلي من خلال تحليل النصوص القانونية وفهم مضمونها، والمنهج الوصفي في تبيان خصائص الموضوع وصفاته، وكذلك المنهج المقارن، وذلك بإبراز أوجه الشبه أو الاختلاف بين كل من القانون الجزائري والقوانين الأجنبية الأخرى.

الإشكالية:

ومن هنا نطرح الإشكالية الأساسية لموضوع دراستنا:

ما مدى فعالية الآليات القانونية التي وضعها المشرع في تحقيق الحماية القانونية للتوقيع الالكتروني؟

والتي تتفرع عنها مجموعة من التساؤلات الفرعية وهي:

- فيما تتمثل الآليات القانونية التي اقرها المشرع لحماية التوقيع الالكتروني؟

- ما المقصود بالتشفير الالكتروني ؟
- ما هو موقف التشريع الجزائري من التشفير؟
- فيما تتمثل جهات التصديق الالكتروني؟

وفي سبيل اعداد البحث والدراسة والوصول إلى حل الإشكالية المطروحة، ارتأينا إلى تقسيم البحث إلى فصلين حيث نتعرض في الفصل الأول إلى التشفير كآلية لحماية التوقيع الالكتروني، والذي قسمناه إلى مبحثين وخصصنا المبحث الأول إلى مفهوم التشفير الالكتروني، أما المبحث الثاني إلى أساليب التشفير الالكتروني.

أما الفصل الثاني فيتناول التصديق الالكتروني كآلية لحماية التوقيع الالكتروني والذي قسمناه إلى مبحثين في المبحث الأول تعرضنا إلى هيئات التصديق الالكتروني وفي المبحث الثاني إلى شهادة التصديق الالكتروني.

الفصل الأول

التشفير كآلية لحماية التوقيع الإلكتروني

الفصل الأول: التشفير كآلية لحماية التوقيع الإلكتروني

إن الحديث عن أنظمة وشبكات الانترنت والمعلومات يؤدي بنا إلى التطرق لمختلف التقنيات التي تهدف إلى حماية نظم معلومات المؤسسة ضد أي اختراق غير قانوني، وذلك من خلال جملة من الوسائل التي تسعى إلى الاعتماد عليها لتوفير الحماية اللازمة لمختلف الأنظمة والتي نجد في مقدمتها التشفير الالكتروني والذي حظي باهتمام كبير في مجال امن المعلومات باعتباره الوسيلة الأكثر أهمية لتحقيق سرية قواعد البيانات والمعلومات. حيث سنتعرف إلى مفهوم التشفير (المبحث الأول)، والى الاحكام القانونية للتشفير المتخذة في حماية التوقيع الالكتروني (المبحث الثاني).

المبحث الأول: مفهوم التشفير الالكتروني

إن تحقيق الحماية الضرورية للتوقيع الالكتروني من أي اختراق أو تزوير، يتطلب وجود آليات تضمن ذلك والذي يبعث الثقة والأمان لدى المتعاملين به، مما جعل مختلف التشريعات على إقرار تقنية التشفير والتي تعد أفضل تقنية لحماية البيانات والمعلومات المرسلة عبر الشبكة الانترنت من أي تعديل أو تغيير غير مرغوب، ولذلك، سنتطرق إلى تعريف التشفير (المطلب الأول)، والى أحكام نظام التشفير (المطلب الثاني).

المطلب الأول: تعريف التشفير الالكتروني

التشفير هو منظومة تقنية رياضية متعلقة بعدد من المظاهر الأمنية والمعلومات، والذي يستخدم مفاتيح خاصة لتحويل البيانات والمعلومات المقروءة الكترونيا. بحيث لا يستطيع أي شخص الوصول إلى تلك المعلومات إلا عن طريق مفتاح تلك الشفرة. لذا ستطرق إلى تعريف التشفير فنيا (الفرع الأول) وتعريف التشفير من الناحية الفقهية (الفرع الثاني) بالإضافة إلى التعريف القانوني للتشفير (الفرع الثالث).

الفرع الأول: التعريف التقني للتشفير

إن الفكرة الأساسية لتكنولوجيا التشفير وهي تحويل رسالة البيانات المكتوبة على جهاز الكمبيوتر، باستخدام برنامج تشفيري معين إلى معلومات أو إشارات غير مفهومة بالنسبة للغير، ثم يتم نقل هذه الرسالة إلى حاسوب الشخص المستقبل، الذي يستخدم تكنولوجيا معينة أيضا– تسمى تكنولوجيا التشفير– لتحويل الرسالة غير المفهومة إلى وضعها الأصلي كرسالة مقروءة ومفهومة.[1]

عرف التشفير من الناحية الفنية بأنه: "تقنية قوامها خوارزمية رياضية ذكية، وبالعكس تسمح لمن يمتلك مفتاح سريا بان يحول رسالة مقروءة إلى رسالة غير مقروءة، أي يستخدم المفتاح السري بفك الشفرة و إعادة الرسالة المشفرة إلى وضعيتها الأصلية. "[2]

أي أن التشفير من الناحية الفنية يقصد به إعادة كتابة رسالة البيانات قبل إرسالها، باستخدام مفتاح معين يفترض الربط بين البيانات والأرقام، بشرط تمكن المرسل إليه على استعادة الرسالة في صورتها الأصلية قبل تشفيرها، وذلك عن طريق استخدام المفتاح ذاته الذي استخدمه المرسل، أو باستعمال مفتاح آخر، وذلك حسب نوع التشفير المستعمل.[3]

[1] عبيدات يوسف محمد،دراركة لافي محمد، وسائل حماية التوقيع الرقمي التي جعلته عنصرا مهما في زيادة العمل عبر الانترنت"دراسة تحليلية في قانون المعاملات الالكترونية الأردني، مؤتة للبحوث والدراسات "سلسلة العلوم الإنسانية"، جامعة مؤتة، الأردن، مجلد24، عدد01، ،سنة2009، ص47.

[2] سلطان عبد الله محمود الجواري، عقود التجارة الالكترونية والقانون الواجب التطبيق"دراسة مقارنة"، طبعة01، منشورات الحلبي الحقوقية، بيروت،لبنان، سنة2010، ،ص202.

[3] ليندا بو محراث، تسوية منازعات التجارة الالكترونية"دراسة مقارنة بين الفقه الإسلامي والقانون الوضعي، دار الجامعة الجديدة، الإسكندرية، مصر، سنة 2019، ص289.

الفرع الثاني: التعريف الفقهي للتشفير

تباين الفقه في تعريف التشفير الالكتروني لذلك سنحاول التطرق لبعض المفاهيم المطروحة لتشفير.

عرف جانب من الفقه التشفير على انه: "تغيير في شكل البيانات عن طريق تحويلها إلى رموز أو إشارات لحماية هذه البيانات من اطلاع الغير عليها أو من تعديلها أو تغييرها."[1]

من خلال هذا التعريف يتبين أن التشفير يعتمد على عمليات رياضية يتم بها تحويل النص المراد إرساله إلى رموز وإشارات لا يمكن فهم محتواها إلا بواسطة فك الشفرة وتحويل الرموز والإشارات إلى نصوص مقروءة ومفهومة باستخدام مفاتيح التشفير العامة والخاصة، فهذه العملية لا تتم إلا إذا كان مستقبل الرسالة يملك مفتاح التشفير الذي يحول الإشارات والرموز إلى النص الأصلي.[2]

وذهب جانب آخر إلى تعريفه بأنه: "عبارة عن عملية تقنية قوامها خوارزمية رياضية ذكية تسمح لمن يمتلك مفتاحا سريا بان يحول رسالة مقروءة إلى رسالة غير مقروءة، و أن يستخدم المفتاح السري لفك الشفرة وإعادة الرسالة المشفرة إلى وضعيتها الأصلية."[3]

وعرفه البعض بأنه: "عملية الحفاظ على سرية المعلومات، باستخدام برامج لها القدرة على تحويل وترجمة تلك المعلومات إلى رموز، بحيث إذا تم الوصول إليها من أشخاص غير مخول لهم بذلك، لا يستطيعون فهم أي شيء لان ما يظهر لهم هو خليط من الرموز والأرقام والحروف غير المفهومة، وهي طريقة عملية لحماية المعلومات التي تنقل من خلال شبكات

[1] عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الالكترونية، طبعة01، دار الفكر الجامعي، الإسكندرية، سنة 2002س، ص203.

[2] أسامة بن غانم العبيدي، حجية التوقيع الالكتروني في الإثبات، المجلة العربية للدراسات الأمنية والتدريب، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية مجلد28، العدد56، سنة 2012، ص158.

[3] عيسى غسان ريضي، القواعد الخاصة بالتوقيع الالكتروني، طبعة01، دار الثقافة للنشر والتوزيع، الأردن، 2009ص73، 74.

الاتصال، ويمكن استخدامها لغرض صلاحية وسلامة الرسائل والحماية من مرسل الرسالة الذي ينكر الإرسال لاحقا.[1]

كما عرفه البعض الآخر هو: "عملية تحويل المعلومات إلى رموز، بحيث تصبح محمية من عمليات الوصول غير المرخص بها، باستخدام برنامج مفتاح تشفير قبل إرسال الرسالة، وتكون لدى المستقبل قدرة استعادة الرسالة الأصلية بعملية عكسية لفك التشفير"décryptions"، والهدف هو جعل المعطيات المخزنة والمعطيات التي يجري نقلها على الانترنت أمنة، ثم إن عملية التشفير تحقق تكاملية الرسالة وتحقق عدم النكران والتوثق والسرية."[2]

وعرفه آخرون بأنه:"تحويل البيانات إلى شفرة سرية لا يمكن قراءتها إلا باستعمال كلمة مرور أو مفتاح سري، يمكن استعمال مفتاح متماثل، مما يعني أن مفتاحا واحدا يستعمل لتشفير النص وفك التشفير."[3]

من خلال التعاريف السابقة للفقهاء نلاحظ انه ركزت وفقط على دور التشفير وهدفه والوسائل التي تستخدم لعمله، ولم يعرف التشفير كالتقنية، كون وسيلة التشفير تقنية أكثر من كونها قانونية، وبالتالي يصعب على رجال القانون تقديم تعريف واضح وشامل للتشفير الالكتروني.

الفرع الثالث: التعريف القانوني للتشفير

تناولت التشريعات التشفير بطريقة مباشرة وغير مباشرة وفي هذا الصدد سنتناول تعريف التشفير في القانون. فقد عرفه المشرع التونسي التشفير في قانون المبادلات والتجارة الالكترونية بأنه: "استعمال رموز أو إشارات غير متداولة تصبح بمقتضاها المعلومات المرغوب تحريرها أو

[1] ندى بدر جراح، تقنيات التشفير في التبادل التجاري الالكتروني، مجلة ميسان للدراسات الأكاديمية، جامعة ميسان، العراق المجلد07، العدد14، ،سنة2009، ص194.195.

[2] امحمد بن الدين، محمد شهيدي، وهيبة حليمي، امن الشبكات من مخاطر التهديدات ودوره في تعزيز التجارة الالكترونية، يوم دراسي حول:التجارة الالكترونية في الجزائر –الواقع والأفاق–، كلية الآداب والعلوم الإنسانية، قسم علوم التسيير، الجامعة الإفريقية العميد احمد دراية، ادرار، الجزائر، ص10.

[3] اندي اوبل، كشف أسرار قواعد البيانات، طبعة1، الدار العربية للعلوم، لبنان، 2014، ص263.

إرسالها غير قابلة للفهم من قبل الغير، أو استعمال رموز أو إشارات لا يمكن وصول المعلومة بدونها."[1]

أما المشرع المصري فقد عرفه في مشروع قانون التجارة الالكترونية بأنه: " تغيير في شكل البيانات عن طريق تحويلها إلى رموز أو إشارات لحماية هذه البيانات من اطلاع الغير عليها أو من تعديلها أو تغييرها."[2]

فيما عرفه المشرع المغربي في القانون 53/05 المتعلق بالتبادل الالكتروني للمعطيات القانونية بأنه:"هو كل عتاد أو برمجة لو هما معا، ينشا ويعدل من اجل تحويل معطياته سواء كانت عن معلومات أو شعارات أو رموز استنادا إلى اتفاقيات سرية أو من اجل انجاز عملية عكسية لذلك بموجب اتفاقية سرية أو بدونها."[3]

نلاحظ أن المشرع المغربي لم يعرف التشفير بشكل واضح، بعكس كل من المشرع التونسي والمشرع المصري الذين بينا المقصود من التشفير ودوره وكيفية العمل به.

على خلاف ذلك لم يتطرق المشرع السعودي للمقصود بالتشفير في نظلم التعاملات الالكترونية السعودي، وتجدر الإشارة إلى إن باقي التشريعات العربية التي تعاملت مع التجارة الالكترونية، تطرقت إلى تقنية التشفير بشكل غير مباشر، وذلك من تطرقها التوقيع الالكتروني الذي يعتمد بشكل أساسي على عملية التشفير.[4]

أما المشرع الجزائري لم يعرف التشفير في القانون 04/15 المتعلق بالقواعد العامة للتوقيع التصديق الالكترونيين، وإنما تطرق إلى تعريف مفتاحي التشفير العام والخاص، حيث عرف مفتاح التشفير الخاص في المادة 02 فقرة08على انه: "عبارة عن سلسلة من الأعداد يحوزها حصريا الموقع فقط، وتستخدم لإنشاء التوقيع الالكتروني، ويرتبط هذا المفتاح بمفتاح تشفير

[1] المادة05/02، قانون المبادلات والتجارة الالكترونية التونسي، رقم83، الصادر في 2000/08/09، المنشور في الجريدة الرسمية للجمهورية التونسية في 2000/08/11.

[2] قانون تنظيم التوقيع الالكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات، رقم 15، سنة 2004، الجريدة الرسمية، مصر، عدد18، في2004/04/22.

[3] القانون رقم 53/03، المؤرخ في2007/11/30، المتعلق بالتبادل الالكتروني للمعطيات القانونية، الجريدة الرسمية المغربية، عدد5584، في2007/12/06.

[4] أسامة بن غانم العبيدي، مرجع سابق ص157.

عمومي". ومن جهة أخرى يعرف مفتاح التشفير العمومي في الفقرة الموالية (09)بأنه: "عبارة عن سلسلة من الأعداد تكون موضوعة في متناول الجمهور بهدف تمكينهم من التحقق من الإمضاء الالكتروني وتدرج في شهادة التصديق الالكتروني".[1]

المطلب الثاني: أحكام نظام التشفير الالكتروني

مما لا شك فيه أن التشفير يعد من التطبيقات والبرامج التي تضمن الحماية والسرية، للتوقيع الالكتروني وللمعلومات والبيانات، المرسلة بين أطرافه، وذلك بامتلاكهم، لكلمة السر الخاصة، والتي تعد ضمان بان معلوماتهم المتبادلة، لم يطلع عليها الغير، ولم يتم تغيير محتواها، أو تحريفها. بالإضافة إلى ضمان عدم إنكار التصرفات، عبر شبكة الانترنت، وبالتالي سنتطرق في هذا المطلب إلى ضوابط التشفير(الفرع الأول) والى أهداف التشفير (الفرع الثاني).

الفرع الأول: ضوابط التشفير

استلزم التشفير قواعد تشريعية في ميدان المعايير المقبولة حتى لا تحد فائدته من الايجابيات، وتنعكس إلى سلبيات في مجال انسياب المعلومات ونشرها، ومساسها في كثير من الحالات بالخصوصية، خصوصا عند إجراء عملية التوثق وتفتيش النظم، التي تتطلب اطلاعا على معلومات مخزنة في النظام خارجة عن العلاقة العقدية المعنية.[2]حيث أن هناك ضوابط ترد على التشفير والتي سنجيزها فيما يلي:

أولا: إباحة تشفير البيانات والمعلومات

ويقصد به أن القانون أباح استخدام تقنية التشفير، وذلك لترميز السندات والمحررات والتواقيع الالكترونية.

---

[1] انظر قانون رقم 04/15، المؤرخ في 2015/02/01، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، الجريدة الرسمية العدد 06، الصادر في 2015/02/11.

[2]محمد فواز المطالقة، الوجيز في عقود التجارة الالكترونية "دراسة مقارنة"، طبعة01.دار الثقافة للنشر والتوزيع، عمان، الأردن، سنة2006، ص155-156.

إن غالبية التشريعات المقارنة وضعت قواعد ونصوص قانونية تتعامل مع تشفير البيانات والمعلومات والتواقيع الالكترونية، وأصدرت تلك الدول قوانين خاصة بالتجارة الالكترونية للتعامل مع التشفير، فنجد على سبيل المثال لا الحصر أن القانون التونسي الخاص بالمبادلات والتجارة الالكترونية تعامل معه بشكل مباشر من خلال نصوص خاصة، وأجاز استخدامه في المراسلات الالكترونية وفي التعاملات الالكترونية التجارية عبر شبكة الانترنت.

كما انه أكد على أهمية حماية البيانات المشفرة والتواقيع الالكتروني والعناصر المستخدمة في عملية التشفير وفكها، من أي اعتداء عليها سواء تم ذلك باستخدام عناصر التشفير الشخصية الخاصة بتوقيع من غير طرفي العلاقة لاستخدام التشفير في ارتكاب جرائم احتيالية آو سرقة مفاتيح التشفير التي تقوم بفك النص المشفر وإرجاعه إلى النص الأصلي، وذلك باستخدام مفاتيح التشفير الخاصة.[1]

ثانيا: الحق في الحفاظ على سرية البيانات والمعلومات المشفرة

إن البيانات والمعلومات التي يتم تبادلها الكترونيا تمتاز بالخصوصية، فهي تعبر عن إرادة طرفي العقد في إبرام التصرفات القانونية كيفما كان نوعها، والاطلاع على هذه البيانات والمعلومات قد يؤدي إلى إلحاق الضرر بأصحابها والاعتداء على خصوصياتهم، وبالتالي يتطلب الاعتراف بحق أصحابها في الحفاظ على سرية تلك المعلومات وتجريم الاعتداء عليها.

اعتبر المشرع الجزائري من خلال القانون رقم04/15 أن الاعتداء على البيانات المرسلة بين طرفي العقد عبر الوسائط الالكترونية هو اعتداء على خصوصية وسرية البيانات والمعلومات المرسلة بين طرفي العلاقة، وبالتالي وجب ضمان سرية البيانات المستخدمة لإنشاء التوقيع الالكتروني بكل الوسائل التقنية المتوفرة وقت الاعتماد كما يجب على مؤدي خدمات التصديق الالكتروني الحفاظ على سرية البيانات والمعلومات المتعلقة بشهادات التصديق الالكتروني الممنوحة.[2]

[1] مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الالكترونية، دون طبعة.دار النهضة العربية، القاهرة، سنة2001، ص31.

[2] عقوني محمد، الآليات التقنية والقانونية لحماية التوقيع الالكتروني، مجلة الفكر، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، الجزائر،عدد18، في فيفري2019، ص304-305.

والمشرع الجزائري اوجد نصوصا قانونية تعاقب كل من يقوم بالكشف عن سرية البيانات المشفرة ونشرها، سواء من طرف مؤدي خدمات التصديق الالكتروني أو من طرف الغير، أو من طرف الشخص المكلف بالتدقيق.

لان تلك البيانات والمعلومات تتميز بالخصوصية والسرية وتعبر عن إرادة الطرفين بالقيام بتصرف قانوني، واطلاع الغير على هذه البيانات والمعلومات يمكن أن يؤدي إلى إلحاق الضرر بطرفي العلاقة، والاعتداء على خصوصيتهم بمعرفة البيانات التي تم كشفها بعد فك التشفير.[1]

ثالثا: اعتبار استخدام التشفير مرتبط بالتصريح المسبق

كأثر لإقرار المشرع للنص المشفر وحجيته في إثبات التصرفات، فانه يعتبر من المحررات الالكترونية، حيث يمكن تحويل الإشارات والرموز إلى نصوص مقروءة ومفهومة، تكون حجة على من قام بمخالفة الاتفاق المبرم بين الطرفين.[2]

حيث أن التشفير يمكن أن ينصب على العقد أو المحرر الالكتروني أو على التوقيع الالكتروني، في حالة ما إذا كان العقد الكترونيا والموقع عليه الكترونيا يمكن أن تشفر بيانات العقد، وفي حالات أخرى تكون البيانات غير مشفرة على الرغم من أن التوقيع على العقد مشفر، أي أن بيانات العقد الالكتروني يمكن الاطلاع عليها وفهم محتوى العقد وبنوده، ومن ناحية أخرى لا يمكن لمن اطلع عليه أن يكشف هوية الموقع على العقد ذلك أن التوقيع مشفر.[3]

ويبقى أن نشير وذلك في فيما يتعلق بتقنية التشفير، على ضرورة مواكبة التطور السريع للتكنولوجيا، فما يبدو اليوم مستحيلا من إمكانية اختراق التشفير قد يكون من سهل اختراقه بعد

[1] عبد الفتاح بيومي حجازي، مرجع سابق، ص204.

[2] عبيدات يوسف محمد، درادكة لافي محمد، مرجع سابق، ص138.

[3] إسماعيل عبد النبي شاهين، امن المعلومات في الانترنت بين الشريعة والقانون، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون، جامعة الإمارات، مجلد02، الجزء03، ،سنة 2000، ص10.

سنوات قليلة، وزيادة على ذلك فنظام التشفير قد يشمل على ثغرات في تصميمه يمكن أن تستغل في كشف الرسالة المشفرة.[1]

الفرع الثاني: أهداف التشفير

تبرز أهداف التشفير في منع الغير من مستخدمي شبكات الانترنت من الدخول إلى البيانات والمعلومات والحفاظ على سريتها وخصوصيتها للأطراف باستخدام وسائل الكترونية رقمية أو رموز معينة بدل الكتابة التقليدية التي لا يعرفها إلا أطراف التعامل التجاري بما لا يسمح باستخدامها من قبل الغير.[2]، ولذالك نجد أن مختلف التشريعات ومن بينها التشريع الجزائري اقروا بضرورة استخدام تقنية التشفير في التوقيع الالكتروني وذلك من اجل تحقيق الأمن ألمعلوماتي في المعاملات التجارية الالكترونية.

كذلك يعتبر التشفير من الدعائم الأساسية التي تقوم عليها التجارة الالكترونية، وذلك لاكتساب ثقة المستهلك وإدخال الطمأنينة عليه وحتى لا تكون بياناته أو توقيعه الالكتروني عرضة للاختراق أو التزوير.[3]حيث انه توجد أربعة أهداف رئيسة لاستخدام التشفير الالكتروني والتي نذكرها فيما يلي:

- الخصوصية أو السرية:هي التأكد من أن المعلومات لا تكشف ولا يطلع عليها من قبل أشخاص غير مسموح لهم بذلك.
- تكاملية البيانات: التأكد من أن المعلومات لم تتغير ولم يتم تعديلها أو تحريفها، و خاصة انه لن يتم تدمير التوقيع الالكتروني أو محتوى البيانات في مرحلة من مراحل المعالجة أو التبادل، سواء كان في مرحلة التعامل الداخلي مع المعلومات أو عن طريق تدخل غير مشروع.

[1]عقوني محمد، مرجع سابق، ص305.

[2]أسامة بن غانم العبيدي، مرجع سابق ص160.

[3]نادية ياس البياتي، التوقيع الالكتروني عبر الانترنت و مدى حجيته في الإثبات، طبعة01، دار البداية، عمان، الاردن، سنة2014، ص250.

- عدم إنكار التصرف المرتبط بالمعلومات ممن قام به: أي ضمان عدم إنكار الشخص الذي قام بتصرف ما "متصل بالمعلومات أو مواقعها" إنكار انه هو الذي قام بهذا التصرف. [1]

- التحقق من هوية صاحب التوقيع: أي يجب أن تكون المعلومات المستلمة مطابقة شخصيا للمعلومات الأصلية التي أرسلت وكذلك تاريخ إرسال المعلومات ومحتواها ووقت الإرسال. [2]

كذلك نذكر أهداف أخرى للتشفير والمتمثلة في:

- حماية التوقيع الالكتروني: وهو طريقة لربط المعلومات بصاحبها.
- الصلاحية: وهي نقل الصلاحية إلى شخص أخر أو قرار معتمد لفعل شيء ما.
- مدة الصلاحية: أي توفير وسائل لتحديد سقف زمني للصلاحيات المخولة لاستخدام أو معالجة المعلومات أو مصدرها.[3]
- استمرارية توفير المعلومات أو الخدمات: وذلك بالتحقق من استمرار عمل النظام ألمعلوماتي.
- تحويل المعلومات إلى شفرات غير مفهومة تبدو غير ذات معنى، لمنع الأشخاص الغير مرخص لهم من الاطلاع عليها أو فهمها.
- أثبات الوقت: وذلك بتسجيل وقت إنشاء المعلومات والبيانات الموجودة.
- الاستلام والتأكيد: أي الاعتراف بان المعلومات والبيانات قد سلمت وقد تم إرسالها.
- الملكية: وهي وسيلة لتوفير الحق القانوني لجهة التصديق في نقل المصدر إلى الآخرين.
- الإلغاء: سحب التأييد أو الصلاحية.[4]
- النزاهة: يجب أن يكون من الممكن التحقق من أن الرسالة لم يتم تعديلها أثناء إرسالها.

---

[1] عرعار الياقوت، التشفير وسيلة لتامين التجارة الالكترونية من المخاطر التقنية، مجلة البحوث القانونية والاقتصادية، كلية الحقوق والعلوم السياسية، جامعة البويرة، الجزائر، مجلد05، عدد01، ،ديسمبر 2021، ص543.

[2] علي محمددهب، التشفير وامن المعلومات، كلية دراسات الحاسوب والإحصاء، جامعة كردفان، السودان، ص10.

[3] علي محمددهب، المرجع نفسه، ص09.

[4] علي محم ذهب، المرجع السابق، ص09.

- التحكم في الدخول: وهي الطرق والآليات التي تستخدم لمنع وصول الغير المخول لهم الدخول إلى الأنظمة التي تقوم بالتشفير. [1]

بالإضافة إلى ذلك يستخدم التشفير من اجل تجنب المخاطر التي تواجه سرية البيانات والتي نذكر منها:

- الاطلاع على المعلومات المحظورة.
- إعادة توجيه المعلومات والبيانات إلى جهة أخرى.
- تجنب محاولة أي تعديل للبيانات المنقولة على شبكة الانترنت.
- تغيير محتوى الرسائل المتبادلة.
- تغيير كلمات السر الخاصة بالمستخدمين
- تعديل بيانات المخزنة على أجهزة الكمبيوتر. [2]

إن توفر ووجود هذه التقنية (التشفير)في عالم التكنولوجيا يساعد على تنظيم المعاملات الالكترونية، وحماية التواقيع الالكترونية، وعدم الاطلاع والتعديل بمحتوى البيانات والمعلومات، وبالتالي تمكن أصحابها من استخدامها، والذي يؤدي إلى الثقة والأمان في هذه المعاملات، والذي يعتبر من أهم مقوماتها، والذي يؤدي بدوره إلى إقبال المتعاملين على استخدامها والاعتماد عليها وحماية حجيتها في الإثبات.

[1] موقع https://attaa.sa/library/view/1363 ،تاريخ الاطلاع،2022/03/28، على الساعة 14:22.

[2] غازي بن فهد بن غازي المزيني، الحماية القانونية للمستهلك في عقود التجارة الالكترونية "دراسة تأصيلية تطبيقية مقارنة"، طبعة01، دار الكتاب الجامعي للنشر والتوزيع، الرياض، السعودية، سنة2018، ص 276-277.

المبحث الثاني: الأحكام القانونية للتشفير الالكتروني

يتضمن التشفير تحويل النص العادي المقروء بالنسبة للإنسان إلى نص غير مفهوم، وهو ما يعرف بالنص المشفر يعني هذا بشكل عام اخذ بيانات قابلة للقراءة وتغييرها بحيث تظهر بشكل عشوائي ويتضمن التشفير استخدام تقنيات تشفير، وهو مجموعة من القيم الرياضية يتفق عليها كل من المرسل والمتلقي، وبالتالي سنتطرق إلى أنظمة التشفير (المطلب الأول) والى خوارزميات التشفير والى موقف المشرع الجزائري من التشفير الالكتروني (المطلب الثاني)

المطلب الأول: أنظمة التشفير الإلكتروني

تتواجد تقنيتي التشفير بمفتاح متناظر و التشفير بمفتاح غير متناظر جنبا إلى جنب حيث إنهما يكمل كل منهما الآخر، حيث يكمن الفرق بينهما، وهو كيفية المحافظة على سرية وامن التوقيع الرقمي والمعلومات، وبالتالي سنتعرف على تقنية التشفير المتناظر(الفرع الأول)والى تقنية التشفير غير المتناظر (الفرع الثاني).

الفرع الأول: التشفير المتناظر

1. أولا: المقصود بالتشفير المتناظر

والذي يطلق عليه "التشفير السيمتري" وفي هذا النوع من التشفير يوجد لدى كل من المرسل والمرسل إليه نفس مفتاح لتشفير وفك تشفير للبيانات، حيث أن للشخص الذي يملك المفتاح بإمكانه فك التشفير وقراءة محتوى الرسائل والملفات.[1]

حيث تقسم الخوارزميات التناظرية إلى صنفين، خوارزميات تعمل على النص الواضح كثنائية واحدة وفي نفس الوقت، ويطلق عليها خوارزميات التدفق. وخوارزميات أخرى تعمل على النص الواضح بشكل مجموع من الثنائيات والتي تسمى كتل، ويطلق على هذه الطرق

[1] احمد غريبي، حورية قاسمي، دور سياسة التشفير الالكتروني في حماية نظم معلومات الإدارة الالكترونية بمؤسسة بريد الجزائر فرع المدية، مجلة الاقتصاد الجديد، كلية الاقتصاد، جامعة المدية مجلد12، عدد01، جانفي 2021، ص313.

خوارزميات الكتلة أو شفرات الكتل، حيث نجد أن معظم تقنيات التشفير المتناظرة هي شفرات كتل. [1]

2. ثانيا: آلية عمل تقنية التشفير المتناظر

1-يختار المرسل (أو المستلم) خوارزمية تشفير، وينشئ مفتاحا، ويبلغ المرسل إليه (أو المرسل، حسب الحالة) بالخوارزمية المحددة، ويرسل المفتاح عبر قناة اتصال أمنة.

2-يقوم المرسل بتشفير الرسالة باستخدام المفتاح، ويرسل الرسالة المشفرة إلى المرسل إليه

3-يتلقى المرسل إليه الرسالة المشفرة ويفك تشفيرها بنفس المفتاح.[2]

يوفر التشفير بالمفتاح المتناظر فائدتين وهما:

1-الفعالية: حيث أن المستخدمين لا يعانون من تأخير طويل نتيجة عمليتا التشفير وفك التشفير.

2-إثبات الهوية: يمنح التشفير بالمفتاح العام رجة مقبولة من إثبات هوية طرفي الاتصال، حيث انه لا يمكن فك تشفير المعلومات والبيانات باستخدام مفتاح أخر غير الذي استخدم في التشفير، ويستطيع الطرفان التحقق من هوية الطرف الأخر طوال فترة بقاء المفتاح التناظري غير معروف لطرف ثالث. [3]

إلا انه التشفير وفق هذه قد يؤدي إلى ضياع المفتاح السري خلال تبادل البيانات والمعلومات بين مرسل الرسالة والمرسل إليه، من طرف أشخاص غير مرخص لهم بذلك، أي أن هذه الطريقة من التشفير لا تقم الحماية الكافية للبيانات والمعلومات، والذي ق يؤثر سلبا على سلامة البيانات المحررات الرقمية والتوقيع الالكتروني في وأيضا فقدانها للشرط الأساسي لاكتسابها حجية الإثبات.[4]

---

[1] علي محمد دهب، مرجع سابق، ص46.

[2] موقع مدونة https://mustafasadiq0.com، تاريخ الاطلاع 2022/04/08 على الساعة 11:33.

[3] عبد الرحمان غسان زعرور، خوارزمية التشفير DES، المعهد المتوسط لتقنيات الحاسوب، حماه، سوريا، ص01.

[4] زروقي خديجة، الحماية الرقمية كآلية لتفعيل مبدأ المساواة بين الأدلة الكتابية والالكترونية، مجلة الاجتهاد للدراسات القانونية والاقتصادية، معهد الحقوق والعلوم السياسية، المركز الجامعي أمين العقال الحاج موسى اق اخموك تامنغست، مجلد10، عدد03، في اكتروبر 2021، ص302.

وبالرجوع إلى القانون 04/15 السالف الذكر نجد أن المشرع الجزائري لم ينص على هذا الأسلوب من التشفير، وذلك لمعرفة المشرع بهشاشة هذا الأسلوب من التشفير والذي لا يقدم الحماية والأمن الكافيين لسلامة البيانات والمعاملات.

الشكل رقم 01: يوضح عملية التشفير المتماثل

المصدر: مدونة مصطفى صادق العلمية[1]

[1]موقع مدونة https://mustafasadiq0.com، تاريخ الاطلاع 2022/04/08 على الساعة 11:33.

الفرع الثاني: التشفير غير المتناظر

أولا: المقصود بالتشفير غير المتناظر

ويقصد بهذا التشفير استخدام مفتاح أو رمز مختلف في تشفير نفس السندات الالكترونية، أي يتم استخدام مفتاحين أو رمزين مختلفين لفك تشفير السن الالكتروني، حيث يكون الأول سريا خاص بمستخدم معين المستعمل للأجهزة الالكترونية، أما المفتاح أو الرمز الثاني فهو عمومي يوزعه ويبلغه إلى المستخدمين الآخرين الذين يتعامل معهم من خلال الرسائل الالكترونية الموقعة بالمفتاح الخاص.[1]

أي انه يتم الاستعانة بمفتاحين مختلفين مرتبطين بشكل حسابي لإنشاء التوقيع الالكتروني وذلك لتحويل البيانات والمعلومات، ثم يتم تثبيتها مرة أخرى بنظام تشفير غير المتماثل، حيث انه لا يمكن للغير اكتشاف المفتاح الخاص بالموقع واستعماله في التعرف على محتوى الرسالة، حتى لو تمكنوا من معرفة مفتاح التشفير العام، والمفتاح الخاص يكون معروفا لدى جهة واحة فقط وهو المرسل ويستعمل لتشفير الرسالة أو فك تشفيرها، بخلاف المفتاح العام والذي يكون عادة معروفا لدى أكثر من جهة أو شخص.[2]

ومن خلال القانون 15/ 04السالف الذكر وتحديدا المادة 02 في الفقرتين 9/8 نجد أن المشرع الجزائري قد عرف كل من المفتاح العام والمفتاح الخاص.

- مفتاح التشفير الخاص: "وهو عبارة عن سلسلة من الأعداد يحوزها حصريا الموقع فقط، وتستخدم لإنشاء التوقيع الالكتروني، ويرتبط هذا المفتاح بمفتاح تشفير عمومي "[3].
- مفتاح التشفير العمومي: "هو عبارة عن سلسلة من الأعداد تكون موضوعة في متناول الجمهور بهدف تمكينهم من التحقق من الإمضاء الالكتروني، وتدرج في شهادة التصديق الالكتروني".[4]

---

[1] إكرام رقيعي، خصوصية التوقيع الالكتروني في العقد التجاري الالكتروني على ضوء القانون رقم 05/18، مجلة العلوم القانونية والسياسية، مخبر الرقمنة والقانون، جامعة البليدة2مجلد 10، عدد02، في سبتمبر 2019، ص1682.

[2] عقوني محمد، بلمهدي إبراهيم، مرجع سابق، ص306.

[3] المادة8/02، من القانون 04/15 سابق الذكر.

[4] المادة9/02، من القانون04/15سابق الذكر.

وتعتبر طريقة التشفير غير متناظر أكثر موثوقية وأمنية من طريقة التشفير المتناظر، وذلك لأنه من اكتشف المفتاح العام فانه يحتاج لمعرفة المفتاح الخاص والذي يصعب إيجاده، وبالتالي عدم إمكانية فك شفرة الرسالة.

حسب هذا النظام غير المتماثل يتم تبادل الرسائل المشفرة عبر شبكة الإنترنت من خلال برامج NETSCAPE و digicash، إضافة لنظام pgp الذي أدى إلى الكشف عن نظام احدث يسمى "clipper ship" "التشفير الائتماني النموذجي"، الذي وضعته وكالة الأمن القومية الأمريكية لاستخدامه في مجال المعدات الالكترونية. [1]

حققت هذه التقنية ايجابيات عملية وقانونية كبيرة، أين أتاحت لكل مستخدم في المعاملات الالكترونية أن يستعمل مفتاح أو رمز سري واحد في تشفير الرسالة التي يريد إرسالها أو التوقيع الالكتروني الخاص به ، أو فك الرسالة التي تلقاها، ورغم أن هناك صعوبات تواجه هذا النوع من التشفير، والمتمثلة أساسا في مسالة ضمان المفتاح العمومي.أي انه يعود إلى المستخدم الذي يملك المفتاح الخصوصي، إلا انه تم التصدي لهذه المشكلة وذلك بتدخل جهة ثالثة مستقلة ومحايدة والمتمثلة في جهة التصديق الالكتروني.[2]

[1] عرعار الياقوت، مرجع سابق، ص540-541.

[2] فادي محمد عماد الدين توكل، عقود التجارة الالكترونية، منشورات الحلبي الحقوقية، طبعة 01، بيروت، سنة 2010، ص155.

ثانيا: آلية عمل تقنية التشفير غير المتناظر:

فتشفر الرسالة بمفتاحين عبر عدة مراحل:

1- كتابة النص الأصلي أو التوقيع وتشفيره بالمفتاح العام للمرسل إليه، حتى لا يتمكن لأي شخص أخر فك تشفيرها ما عاداه هو.

2- تشفر نفس الرسالة أو التوقيع مرة أخرى باستخدام المفتاح الخاص لمرسل الرسالة، وهذا للتأكد من مرسلها وقابلية فكها باستخدام المفتاح العام للمرسل.

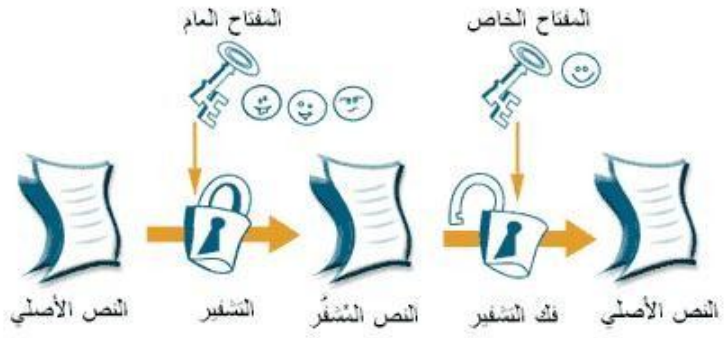
3- إرسال الرسالة إلى المرسل إليه عبر الوسائط الالكترونية.

4- وصول الرسالة إلى المرسل إليه المشفرة بالمفتاح المتناظر والمفتاح المتناظر المشفر بالمفتاح العام للمرسل إليه.

5- يقوم المرسل إليه بفك تشفير باستخدام المفتاح العام للمرسل فيتحصل على رسالة مشفرة بمفتاحه العام، فيقوم بفكها باستخدام المفتاح السري الخاص به الذي يكون معلوما لديه.[1]

يمكن أن يتم استخدام تقنية التشفير المزدوج وهو المزج بين التشفير المتناظر والتشفير غير المتناظر: وهذا بتشفير الرسالة المرسلة بمفتاح متماثل (المفتاح السري) ثم يقوم بتشفير المفتاح المتناظر بالمفتاح العام للشخص المرسل إليه الرسالة ويرسل المفتاح المشفر والرسالة المشفرة إلى متلقي الرسالة الذي يقوم بفك شفرة المفتاح بمفتاحه الخاص ليتحصل على المفتاح السري الذي شفرت به الرسالة الأصلية.

الشكل 02: يمثل عملية التشفير غير المتماثل



المصدر: مدونة مصطفى صادق العلمية[2]

[1] حليتيم سراح، خصوصية التوقيع الرقمي في توثيق العقود الالكترونية، مجلة الباحث للدراسات الأكاديمية، كلية الحقوق والعلوم السياسية، جامعة باتنة01، الحاج لخضر، الجزائر، عدد13، في جويلية 2018، ص743.

[2] موقع مدونة https://mustafasadiq0.com، تاريخ الاطلاع 2022/04/08 على الساعة 11:33

المطلب الثاني: موقف المشرع الجزائري من التشفير الالكتروني

يتوقف ازدهار التجارة الالكترونية على قدر ما تتمتع به من ثقة وأمان لدى مستخدمي وسائل وتقنيات الاتصال الحديثة، ولما كانت العقود الالكترونية تتم عن بعد بين أطراف قد لا يعرف بعضهم البعض، وهو الأمر الذي يتطلب توفير ضمانات، ووسائل تكفل تحديد هوية المتعاقدين، وبطريقة يمكن معها نسبة التصرف إلى صاحبه، وهذه المشكلة تتطلب إيجاد حلول تقنية، لا سيما في ظل انتشار القرصنة الالكترونية.

بالرجوع إلى القانون 04/15 [1]السلف الذكر المتعلق بالقواعد العامة بالتوقيع والتصديق الالكترونيين، نجد أن المشرع الجزائري نص في المادة 02 فقرة 03على بيانات إنشاء التوقيع الالكتروني:"بيانات فردية، مثل الرموز أو مفاتيح التشفير الخاصة، التي يستعملها الموقع لإنشاء التوقيع الالكتروني."

نلاحظ أن المشرع الجزائري لم يقدم تعريف لتقنية التشفير، وانما ذكر أن عملية إنشاء التوقيع الالكتروني تستخدم احد أنظمة(مفاتيح) التشفير، سواء المفتاح الخاص أو المفتاح العام.

وبالرجوع إلى الفقرة 08 من المادة 02 نجد أن المشرع الجزائري عرف لنا مفتاح التشفير الخاص:"هو عبارة عن سلسلة من الأعداد يحوزها حصريا الموقع فقط، وتستخدم لإنشاء التوقيع الالكتروني، ويرتبط هذا المفتاح بمفتاح تشفير عمومي."[2]

كذلك الفقرة 09 من نفس المادة عرف لنا مفتاح التشفير العمومي:"هو عبارة عن سلسلة من الأعداد تكون موضوعة في متناول الجمهور بهدف تمكينهم من التحقق من الإمضاء الالكتروني، وتدرج في شهادة التصديق الالكتروني."[3]

من خلال الفقرتين السابقتين (09/08) نلاحظ أن المشرع الجزائري لم يقم تعريف شامل وواضح لنظام التشفير الالكتروني، وإنما تطرق إلى المقصود بمفتاحي التشفير العام والخاص، بالإضافة إلى انه لم يبين الغرض من التشفير.

---

[1]القانون رقم 04/15، المؤرخ في 2015/02/01، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، الجريدة الرسمية العدد 06، الصادر في 2015/02/11.

[2]الماة08/02 من القانون 04/15، المتعلق بالتصديق والتوقيع الالكترونيين.

[3]المادة09/02، من القانون04/15 سابق الذكر.

إلا انه بالرجوع للفقرات من03 إلى 06 نجد المشرع الجزائري حدد لنا برمجيات التشفير:" وهي الآليات المعدة لإعداد التوقيع الالكتروني، تكون عبارة جهاز أو برامج الكترونية معلوماتية، تستعمل خصيصا إما لتطبيق بيانات إنشاء التوقيع الالكتروني أو تطبيق بيانات التحقق من الصلة بين والتوقيع الالكتروني الموقع، ويلزم أن تكون برامج التشفير سريعة، نظرا للتزامن بين الجلستين، وقد عرفت شركة IBM، باختصاصها في تطوير نظام التشفير الالكتروني، والذي شهدا انتشارا واسعا في السوق، لما بتميز به لضمان حماية مفاتيح التشفير الذي يصل طوله إلى حوالي 128بت وهذا ما يحقق قوة التشفير الالكتروني."[1]

ومن خلال ما سبق يتبين انه رغم أن المشرع الجزائري لم يقم تعريفا وواضحا وشاملا لتقنية التشفير إلا انه اقر بضرورة استخدام تقنية التشفير في التوقيع الالكتروني والمحررات الالكترونية وذلك لتحقيق سرية وامن المعلومات والبيانات المرسلة بين طرفي العلاقة.

بالإضافة إلى إقراره نصوص قانونية تعاقب كل شخص يقوم بالاعتداء على سرية البيانات والمعلومات المشفرة وإفشائها للغير.سواء كان ذلك من طرف مؤدي خدمات التصديق الالكتروني أو من الشخص المكلف بالتدقيق ، أو كان من طرف الغير.[2]

[1] حليتيم سراح، مرجع سابق، ص746-747.

[2] عقوني محمد،مرجع سابق،ص305.

ملخص الفصل الأول:

التشفير هو العلم الذي يستخدم الرياضيات لتشفير وفك تشفير البيانات والمعلومات، حيث لا يمكن قراءتها من قبل أي شخص ما عاد الأشخاص المصرح لهم بذلك والمرسل له، حيث عرف التشفير من الناحية القانونية بانه:" استعمال رموز أو إشارات غير متداولة تصبح بمقتضاها المعلومات المرغوب تحريرها أو إرسالها غير قابلة للفهم من قبل الغير، أو استعمال رموز أو إشارات لا يمكن وصول المعلومة بدونها."

وللتشفير ضوابط تحكمه وذلك بهدف الحفاظ على خصوصية البيانات والمعلومات وهي: إباحة تشفير البيانات والمعلومات، الحق في الحفاظ على سرية البيانات والمعلومات المشفرة، اعتبار استخدام التشفير مرتبط بالتصريح المسبق.

يوج نوعين من أنظمة التشفير وهما التشفير بالمفتاح المتناظر والذي يعتم على مفتاح او رمز سري ذاته لعملية التشفير وفك التشفير للبيانات، أما النوع الثاني من أنظمة التشفير وهو التشفير غير المتناظر وهذا النوع من التشفير يعتمد على استخدام مفتاح أو رمز مختلف في تشفير السندات الالكترونية نفسها بحيث يتم استخدام مفتاحين أو رمزين مختلفين لعملية فك التشفير.

ومن خلال مما سبق تبين أن المشرع الجزائري نص على التشفير من خلال نصوص القانون 04/15 المحدد للقواعد العامة للتوقيع والتصديق الالكترونيين، إلا انه لم يقم تعريفا واضحا وشامل له، بالإضافة إلى عدم توضيح آلية عمل هذه التقنية، والتي تعد من أهم الآليات التي تستخدم للحفاظ على سرية وامن البيانات والمعلومات.

الفصل الثاني

التصديق لإلكتروني كآلية لحماية التوقيع الإلكتروني

الفصل الثاني: التصديق الإلكتروني كآلية لحماية التوقيع الإلكتروني

إن الثقة والأمان لدى المتعاملين عبر شبكات الانترنت من أهم الضمانات التي يجب توفرها لتطر وازدهار التعاملات الالكترونية، وعليه استحدث نظام محايد وموثوق فيه يعمل على حماية هذه المعلومات وتأكيد صحتها عن طريق التصديق الالكتروني والذي يعرف بأنه:"التحقق من أن التوقيع الالكتروني قد تم تنفيذه من شخص معين ، باستخدام وسائل التحليل للتعرف على الرموز والكلمات والأرقام وفك التشفير والاستعارة العكسية وأية وسيلة أو إجراءات أخرى تحقق الغرض المطلوب " [1]، حيث تم إسناد حماية هذه البيانات إلى جهات متخصصة ومعتمدة التي أطلق عليها بمؤدي خدمات التصديق الالكتروني وهي:"كل شخص طبيعي أو معنوي يقوم بمنح شهادات التصديق الالكتروني موصوفة ، وقد يقدم خدمات أخرى في مجال التصديق الالكتروني"[2] والتي تعمل على توفير بيئة الكترونية أمنة عبر الانترنت، وعليه سنتطرق إلى هيئات التصديق الالكتروني (المبحث الأول) والى شهادة التصديق الالكتروني (المبحث الثاني)

المبحث الأول: هيئات التصديق الالكتروني

جهات التصديق الالكتروني هي الجهات التي تصدر شهادة تربط بين الموقع وبيانات إنشاء الموقع، وهي جهة محايدة وموثوقة مرخص لها بتقديم خدمات تتعلق بالتوقيع الالكتروني، وعليه سنتطرق إلى سلطات التصديق الالكتروني (المطلب الأول) والتزامات مؤدي خدمات التصديق الالكتروني (المطلب الثاني).

المطلب الأول: سلطات التصديق الالكتروني

استحدث المشرع الجزائري سلطة إدارية مستقلة، وأطلق عليها اسم السلطة الوطنية للتصديق الالكتروني تكلف أساسا بترقية استعمال التوقيع الالكتروني والتصديق عليه وتطويرهما وضمان موثوقية استعمالها، ويتفرع عن هذه السلطة سلطتين الأولى السلطة الاقتصادية للتصديق الالكتروني المكلفة بمراقبة مقدمي خدمات التصديق الالكتروني، أما الثانية السلطة

[1] نضال اسماعيل برهم،أحكام عقود التجارة الالكترونية ، دون طبعة، دار الثقافة للنشر والتوزيع،الأردن،2005،ص170.
[2] المادة 12/02،من القانون04/15،السابق الذكر.

الحكومية والمكلفة بمتابعة ومراقبة نشاط التصديق الالكتروني.حيث سنتطرق إلى كل سلطة على حدة، السلطة الوطنية (الفرع الأول) السلطة الحكومية (الفرع الثاني) السلطة الاقتصادية (الفرع الثالث).

الفرع الأول: السلطة الوطنية للتصديق الالكتروني

أولا: تعريف السلطة الوطنية للتصديق الالكتروني

عرفها المشرع الجزائري حسب نص المادة 16 فقرة 1: " تنشا لدى الوزير الأول سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي، تسمى السلطة الوطنية للتصديق الالكتروني وتدعى في صلب النص "السلطة"[1]، ويتم تحديد مقرها لاحقا بموجب التنظيم حسب نص المادة 17 من نفس القانون.[2]

حيث تكلف بتحديد السياسية الوطنية للتصديق والتوقيع الالكترونيين وتضطلع بمهمة ترقية استعمالها وتطويرهما، وكذا ضمان أمان وموثوقية استعمالها، وتتفرع عنها سلطتين: السلطة الحكومية للتصديق الالكتروني التابعة لوزارة البريد وتكنولوجيا الإعلام والاتصال، والسلطة الاقتصادية للتصديق الالكتروني التابعة لسلطة ضبط البريد والمواصلات.[3]

ثانيا: تشكيل السلطة الوطنية للتصديق الالكتروني

نصت المادة 19 من القانون رقم 04/15 على تنظيم السلطة الوطنية، فهي تتكون من مجلس السلطة والذي يتكون من خمسة أعضاء من بينهم الرئيس يتم تعيينهم من طرف رئيس الجمهورية لمدة 4 سنوات قابلة للتجديد مرة واحدة فقط، يشترط فيهم الكفاءة خاصة في مجال القانون وتكنولوجيا الإعلام والاتصال كما يمكن لهم الاستعانة بأي كفاءة من شانها أن تساعده

[1] المادة 1/16 من القانون 04/15 المتعلق بالتصديق والتوقيع الالكترونيين.

[2] تنص المادة 17 من نفس القانون على: "يحدد مقر السلطة عن طريق التنظيم."

[3] أمينة قهواجي، ليلي مطالي، الإطار المفاهيمي والقانوني للتوقيع والتصديق الالكترونيين في الجزائر، مجلة المشكاة في الاقتصاد التنمية والقانون، المركز الجامعي بلحاج شعيب عين تموشنت، الجزائر، المجلد 04، العدد08، في ماي 2019، ص29.

في أشغاله[1]، ويجب ألا يمارس أعضاء المجلس أي وظيفة سواء كان في القطاع العام أو القطاع الخاص وإلا فإنهم يعتبرون في حالة تنافي، بالإضافة إلى رئيس يقوم بتسيير المصالح التقنية والإدارية المتعلقة بالتصديق والتوقيع الالكترونيين.

ثالثا: اختصاصات السلطة الوطنية للتصديق الإلكتروني

تقوم السلطة الوطنية بمجموعة من الصلاحيات والاختصاصات التي تتميز في عمومها بأنها ذات طبيعة رقابية، وقائية وقمعية كما يلي:

1. الاختصاص التنظيمي

إن السلطة الوطنية للتصديق الالكتروني باعتبارها سلطة ضبط عليا بالرغم من أنها لا تتمتع بالسلطة التنظيمية في المسائل المتعلقة بالتوقيع والتصديق الالكترونيين واضطلاع الوزير الأول بهذا الاختصاص، إلا أنها تتمتع بسلطة إصدار قرارات فردية نافذة تتضمن رخص واعتمادات وتأهيلات تسمح للمتعاملين الدخول في مجالي التجارة الالكترونية والبنوك الالكترونية لتأدية خدمة التصديق الالكتروني، كما تختص بإبرام اتفاقيات الاعتراف المتبادل مع الدول الأجنبية في مجال التصديق الالكتروني.[2]

2. اختصاص استشاري

تعتبر السلطة الوطنية للتصديق الالكتروني الخبيرة المختصة في مجال التوقيع والتصديق الالكترونيين حيث تقوم بعدة تدابير استشارية في هذا المجال، وذلك حسب نص المادة 18 من القانون 04/15 السالف الذكر:

- الموافقة على سياسات التصديق الالكتروني الصادرة عن السلطتين الحكومية والاقتصادية للتصديق الالكتروني.
- اقتراح مشاريع تمهيدية لنصوص تشريعية أو تنظيمية تتعلق بالتوقيع الالكتروني أو التصديق الالكتروني على الوزير الأول.

---

[1] ازرو محمد رضا، سلطات التصديق الالكتروني في التشريع الجزائري، مجلة العلوم القانونية والاجتماعية، جامعة زيان عاشور، الجلفة، العدد07، ص 134.

[2] جبايلي صبرينة، النظام القانوني للسلطة الوطنية للتصديق الالكتروني، مجلة العلوم الإنسانية، جامعة الإخوة منتوري قسنطينة، الجزائر، المجلد أ، العدد48، سنة2017، ص492.

- القيام بعمليات التدقيق على مستوى السلطتين الحكومية والاقتصادية للتصديق الالكتروني، عن طريق الهيئة الحكومية المكلفة بالتدقيق.
- تتم استشارة السلطة عند إعداد أي مشروع نص تشريعي أو تنظيمي ذي صلة بالتوقيع أو التصديق الالكترونيين.

3. اختصاص قمعي

بما أن السلطة الوطنية للتصديق الالكتروني سلطة تنسيقية للسلطتين الحكومية والاقتصادية فان كل الاختصاصات التنظيمية والقمعية من فرض العقوبات المالية والإدارية التي تقوم بها السلطة الاقتصادية، فإنها ترجع دائما إلى موافقة "السلطة الوطنية للتصديق الالكتروني" فهي بذلك كباقي السلطات الإدارية المستقلة تملك سلطة توقيع العقوبات بطريقة غير مباشرة وذلك في حالة عدم احترام مؤدي خدمات التصديق الالكتروني لأحكام دفتر الأعباء أو سياسة التصديق الالكتروني الخاصة به والموفقة عليها من طرف السلطة الاقتصادية، أو في حالة انتهاكه للمقتضيات التي يتطلبها الدفاع الوطني والأمن العمومي.[1]

الفرع الثاني: السلطة الحكومية للتصديق الالكتروني

أولا: تعريف السلطة الحكومية للتصديق الالكتروني

عرفتها المادة 26 من القانون 04/15:"تنشا لدى الوزير المكلف بالبريد وتكنولوجيات الإعلام والاتصال سلطة حكومية للتصديق الالكتروني تتمتع بالاستقلال المالي والشخصية المعنوية. "[2] "وتحدد طبيعة هذه السلطة الحكومية للتصديق الالكتروني وتشكيلها وتنظيمها وسيرها عن طريق التنظيم."[3]

[1] امينة قهواجي، ليلى مطالي، مرجع سابق ص30.

[2] المادة 26 من القانون 04/15، المتعلق بالتصديق والتوقيع الالكترونيين.

[3] المادة 27 من نفس القانون.

ثانيا: اختصاصات السلطة الحكومية للتصديق الالكتروني

بينت المادة 28 من القانون 04/15 مهام السلطة الحكومية، والمتمثلة في متابعة ومراقبة نشاط التصديق الالكتروني للأطراف الثلاثة الموثوقة وتوفير خدمات التصديق الالكتروني لفائدة المتدخلين في الفرع الحكومي، كما لها مهام أخرى تتفرع عن المهمة الأساسية وهي:

- إعداد سياستها للتصديق الالكتروني وعرضها على السلطة للموافقة عليها والسهر على تطبيقها.
- الموافقة على سياسات التصديق الالكتروني الصادرة عن الأطراف الثلاثة الموثوقة والسهر على تطبيقها.
- الاحتفاظ بشهادات التصديق الالكترونية المنتهية صلاحيتها، والبيانات المرتبطة بمنحها من قبل الطرف الثالث الموثوق، بغرض تسليمها إلى السلطات القضائية المختصة، عند الاقتضاء، طبقا للأحكام التشريعية والتنظيمية المعمول بها.
- إرسال كل المعلومات المتعلقة بنشاط التصديق الالكتروني إلى السلطة دوريا أو بناء على طلب منها.
- القيام بعمليات التدقيق على مستوى الطرف الثالث الموثوق، عن طريق الهيئة الحكومية المكلفة بالتدقيق، طبقا لسياسة التصديق.

الفرع الثالث: السلطة الاقتصادية للتصديق الالكتروني

أولا: تعريف السلطة الاقتصادية للتصديق الالكتروني

لم يعرف المشرع الجزائري هذه السلطة، وإنما تطرق للجهة المكلفة بتعيينها في المادة 29 من القانون 04/15، وهي السلطة المكلفة بضبط البريد والمواصلات السلكية واللاسلكية، والى المهمة الرئيسية لهذه السلطة من خلال المادة 30 من نفس القانون والمتعلقة أساسا بمتابعة ومراقبة مؤدي خدمات التصديق الالكتروني الذين يقدمون خدمات التوقيع والتصديق الالكترونيين لصالح الجمهور.[1]

[1] دريس كمال فتحي، آلية التصديق الالكتروني كضمانة للتعاملات التجارية بالوسائل الحديثة في التشريع الجزائري، مجلة البحوث والدراسات، كلية الحقوق والعلوم السياسية، جامعة الوادي، العدد24، صيف 2017، ص169.

ثانيا: اختصاصات السلطة الاقتصادية للتصديق الالكتروني

وتكلف السلطة الاقتصادية بعدة مهام، وذلك حسب المادة 30 من القانون 04/15 السالف الذكر والتي سنذكرها في النقاط التالية:

- متابعة ومراقبة مؤدي خدمات التصديق الالكتروني.
- منح مؤدي خدمات التصديق التراخيص، وذلك بعد موافقة السلطة الوطنية للتصديق الالكتروني.
- حفظ الشهادات المنتهية الصلاحية الممنوحة من طرف مؤدي خدمات التصديق، حتى تسلم للجهات القضائية عند الاقتضاء.
- نشر شهادات التصديق للمفتاح العمومي.
- السهر على المنافسة النزيهة بين مؤدي خدمات التصديق.
- التحكيم في النزاعات القائمة بين جهات التصديق، أو بين جهات التصديق وبين المستخدمين.
- تبليغ النيابة العامة بكل فعل ذو طابع جزائي يكتشف أثناء تأديتهم للمهام.[1]

[1] فضيلة يسعد، القوة الثبوتية للتوقيع الالكتروني في التشريع الجزائري، مجلة العلوم الانسانية، جامعة الإخوة منتوري قسنطينة 1، الجزائر، المجلد 30 العدد 03، ،2019، ص512.

المطلب الثاني: التزامات مقدم خدمات التصديق الالكتروني

نظرا للدور الهام الذي تقدمه جهات التصديق الالكتروني في تامين وحماية التوقيع الالكتروني، من كافة أنواع الاحتيال والتزوير، بالإضافة إلى كونها تنشئ علاقة بينها وبين مستخدميها، والتي تفرض هذه العلاقة التزامات بين كل من جهة التصديق ومتعامليها، والذي يهمنا هنا الالتزامات التي تقع على مؤدي خدمات التصديق الالكتروني، حيث سنتطرق في هذا المطلب إلى الالتزامات الخاصة بمؤدي خدمات التصديق الالكتروني (الفرع الأول) والى الالتزامات المتعلقة بشهادة التصديق الالكتروني(الفرع الثاني).

الفرع الأول: التزامات خاصة بمؤدي خدمات التصديق الالكتروني

وضع المشرع الجزائري على عاتق مؤدي خدمات التصديق مجموعة من الالتزامات وذلك بموجب نصوص المواد من 41 إلى 50 من القانون 04/15 السالف الذكر ، حيث تتلخص أهم التزامات الخاصة بمزود خدمات التصديق الالكتروني في الحصول على ترخيص مسبق من الجهات المختصة والحفاظ على سرية المعلومات بالإضافة إلى مسك سجل الكتروني لشهادات التصديق الالكتروني ، و التي نفصل فيها كما يلي في:

أولا: ضرورة الحصول على ترخيص من الجهة المختصة

بالرجوع إلى المادة 33 من القانون 04/15[1] السابق الذكر فانه على مؤدي خدمات التصديق الحصول على ترخيص مسبق من السلطة الاقتصادية للتصديق الالكتروني، لمزاولة نشاطه أو عمله، على أن يستوفي طالب الترخيص مجموعة من الشروط محددة قانونا، إلا انه يجب الحصول على شهادة تأهيل سابقة للترخيص، لمدة سنة كاملة قابلة للتجديد، حيث يتم منح الترخيص لكل شخص طبيعي أو معنوي، متحصل مسبقا على شهادة التسجيل.

في حالة الموافقة يمنح الترخيص خلال 60 يوما ابتداء من تاريخ استلام طلب الترخيص المثبت بإشعار الاستلام، حيث يرفق الترخيص بدفتر الشروط الذي يحدد شروط و كيفيات

[1] انظر الماة 33 من القانون 04/15، المتعلق بالتوقيع والتصيق الالكترونيين.

تأدية خدمات التصديق الالكتروني، ويكون صالحا لمدة 05 سنوات قابلة للتجديد. حيث لا يجوز التنازل عنه للغير. [1]

أما في حالة رفض منح شهادة الترخيص، فانه يجب أن يكون هذا الرفض مسببا، مع تبليغ المعني بالأمر مقابل أشعار بالاستلام.

ثانيا: الالتزام بالسرية

تنص المادة 42 من القانون 04/15 المذكور سابقا على: "يجب على مؤدي خدمات التصديق الالكتروني الحفاظ على سرية البيانات والمعلومات المتعلقة بشهادة التصديق الالكتروني الممنوحة. " [2]

فيجب على مقدم خدمات التصديق الالكتروني، المحافظة على سرية المعلومات والبيانات الممنوحة له بخصوص شهادة التصديق الالكتروني، حيث يستثنى من ذلك الحالات التي رخصت له فيها صراحة من صاحب الشهادة سواء كانت كتابية أو الكترونية، أو التي أقرها القانون.

ثالثا: مسك سجل الكتروني لشهادات التصديق الالكتروني

بالإضافة إلى الالتزامين السابقين مسك سجل الكتروني يدون فيه الشهادات التي قامت بإصداره وذلك بهدف توثيق المعلومات لضمان سلامتها، ومنع الغير من الاطلاع عليها و التلاعب فيها ، وتوفر له إمكانية استرجاع هذه البيانات عند الحاجة إليها ، وهذا السجل يمكن أن يحتوي على تاريخ تعليق العمل بالشهادات أو إلغائها.[3]

---

[1] رضوان قرواش، هيئات التصديق الالكتروني في ظل قانون 15-04 المتعلق بالقواعد العامة للتوقيع والتصديق الالكترونيين(المفهوم والالتزامات)، مجلة العلوم الاجتماعية، كلية الحقوق والعلوم السياسية، جامعة سطيف2 العدد24، جوان 2017، ص417.

[2] المادة 42 من القانون 04/15 سابق الذكر.

[3] ألاء احمد محمد حاج علي، التنظيم القانوني لجهات التصديق على التوقيع الالكتروني، أطروحة لاستكمال متطلبات الحصول على درجة الماجستير في القانون الخاص، كلية الدراسات العليا، جامعة النجاح الوطنية نابلس، فلسطين،ص18.

وفي الأخير يتبين أن المشرع الجزائري ألزم مؤدي خدمات التصديق الالكتروني بضرورة المحافظة على سرية تلك المعاملات التي عهدت إليهم، وذلك لتشجيع وتحفيز المتعاملين على الإقدام العمل بالمعاملات الالكترونية.

الفرع الثاني: الالتزامات المتعلقة بشهادة التصديق الالكتروني

إن الهدف من الحصول على شهادة التصديق الالكتروني، هو ضمان لعدم إنكار احد الطرفين لتوقيعه الموضوع على الوثيقة المرسلة، وهو من قام بالتوقيع، وبالتالي فان من بين الالتزامات المتعلقة بشهادة التصديق الالكتروني، الالتزام بالتحقق من صحة البيانات المقدمة، الالتزام بإصدار شهادة التصديق الالكتروني وأيضا إيقاف أو إلغاء شهادة التصديق الالكتروني.

أولا: الالتزام بالتحقق من صحة البيانات المقدمة

يلتزم مؤدي خدمات التصديق الالكتروني بالتحقق من صحة البيانات والمعلومات المتحصل عليها من طرف الأشخاص المصدر لهم شهادات التصديق الالكتروني وصفاتهم المميزة والتي تمت المصادقة عليها وتضمينها في شهادة التصديق، ويعتبر هذا الالتزام من بين الالتزامات المهمة والضرورية بالنسبة لمزود خدمات التصديق الالكتروني. [1]

حيث أكد المشرع الجزائري على هذا الالتزام في المادة 44 فقرة 01 من القانون 04/15 المتضمن القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، والتي نصت على: "يجب على مؤدي خدمات التصديق الالكتروني، قبل منح شهادة التصديق الالكتروني، أن يتحقق من تكامل بيانات الإنشاء مع بيانات التحقق من التوقيع."

وتتمثل البيانات المقدمة عادة والمصرح بها من المشترك كالهوية الشخصية وجواز السفر وغير ذلك من الأوراق الثبوتية، والتي يتم الحصول عليها عبر الاتصال المباشر، أو بطريق إرسال هذه السندات بالبريد أو الهاتف أو عبر الانترنت. [2]

[1] زهيرة كيسي، النظام القانوني لجهات التوثيق(التصديق) الالكتروني، مجلة دفاتر السياسة والقانون، جامعة قاصدي مرباح ورقلة، العدد07، جوان2012، ص214.

[2] وسيمة مصطفى هنشور، النظام القانوني لمقدمي خدمات التصديق الالكتروني في التشريع الجزائري، تخصص قانون العلاقات الاقتصادية الدولية، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن بديس، مستغانم، افريل 2017ص160.

وتلتزم جهة التوثيق الالكتروني بالتعويض في حالة وجود بيانات غير صحيحة مادام المتعامل ليس له وسيلة التحقق من صحة البيانات والمعلومات الواردة في شهادة التصديق الالكتروني.[1]

ثانيا: الالتزام بإصدار شهادة التصديق الالكتروني

عرف المشرع الجزائري في المادة 03 من المرسوم التنفيذي رقم 162/07 الشهادة الالكترونية: "أنها وثيقة في شكل الكتروني تثبت الصلة بين معطيات فحص التوقيع الالكتروني والموقع. [2]

إن إصدار شهادة التصديق الالكتروني من بين أهم الخدمات المقدمة من جهات التصديق الالكتروني، إذ تقوم بتزويد أطراف العقد الالكتروني بشهادات الكترونية معتمدة لهدف الاعتماد عليها، سواء من طرف المرسل للرسالة الالكترونية أو من طرف المستقبل للرسالة، حيث أن طبيعة هذا الالتزام هو التزام بتحقيق نتيجة والمتمثلة في إصدار شهادة التصديق الالكتروني، والتي تحتوي على جميع البيانات اللازمة والضرورية.

كما تؤكد الشهادة أن البيانات الموقع عليها بيانات صحيحة صادرة من الموقع ولم يتم التلاعب بها أو تغييرها أو تعديلها سواء بالحذف أو الإضافة.[3]

وبالتالي فان الدور الرئيسي لشهادة التصديق الالكتروني هو ربط المفتاح الخاص بصاحب التوقيع بعملية حسابية معقدة بالمفتاح العام الذي يتاح للعموم بقصد التعرف على هوية صاحب الرسالة الالكترونية الموقعة، بينما يبقى المفتاح الخاص عند الموقع الذي يقوم بالحفاظ على أي حامل الكتروني مؤمن.[4]

---

[1] زهيرة عبوب، المسؤولية المدنية لمقدم خدمات التصديق الالكتروني، مجلة الدراسات القانونية المقارنة، كلية الحقوق والعلوم السياسية، جامعة حسيبة بن بو علي، الشلف، المجلد06، العدد02، ديسمبر2020، ص426.

[2] المرسوم التنفيذي رقم162/07، المؤرخ في 2007/05/30، المعدل والمتمم للمرسوم التنفيذي رقم 123/01، المؤرخ في 2001/05/09.

[3] نذير قورية، دور مؤدي خدمات التصديق الالكتروني في حماية المستهلك على ضوء القانون رقم 04/15، مجلة العلوم القانونية و الاجتماعية، جامعة زيان عاشور، الجلفة، العدد10، جوان2018، ص192.

[4] زهيرة عبوب، مرجع سابق، ص427.

وبعد تأكد مقدم خدمات التصديق الالكتروني من تطابق المفتاح العام مع المفتاح الخاص يصدر شهادة التصديق الالكتروني.

ثالثا: إيقاف أو إلغاء شهادة التصديق الالكتروني

يقع على عاتق هيئة التصديق الالكتروني بعد إصدار شهادة التصديق الالكتروني ضمان متابعة وتحيين المعلومات المتعلقة بصاحب التوقيع وكل ما يطرأ على مركزه القانوني من تغييرات لها علاقة بالبيانات المدونة في الشهادة، وفي خلال عملية التحيين أو التحديث قد

يتبين له بأنها أصبحت غير قابلة للاعتماد عليها أو غير جديرة بالثقة، مما يستوجب الأمر اتخاذ إجراءات إلغائها، وذلك تحت طائلة المسؤولية مع اعتبار هذا الالتزام التزاما بتحقيق نتيجة.[1]

والإخلال بهذا الالتزام قد يرتب أثارا خطيرة كعقد الصفقات أو إجراء تحويلات نقدية أو سحب أموال أو إصدار أوامر أو شراء أو بيع بشهادات الالكترونية غير صحيحة أو مشكوك فيها.

ومن خلال نص المادة 45 من القانون 04/15 السالف الذكر يتبين أن الحالات التي يجب على مؤدي خدمات التصديق الالكتروني إلغاء شهادة التصديق الالكتروني وهي:

أ- إلغاء شهادة التصديق الالكتروني بطلب من صاحب الشهادة

تصدر شهادة التصديق الالكتروني بناء على إرادة العميل الذي قدم طلب إصدارها، ومن ثم يكون له الحق في طلب إلغائها، فهي تحمل الصفة الشخصية لصاحبها وهو المعني بإلغائها، ولا يجب عليه ذكر أي سبب أو مبرر في طلب إلغائها، وما على مقدم خدمات التصديق سوى التحقق من أن طالب الإلغاء هو صاحب الشهادة، وتتعدد الأسباب التي تدفع صاحب الشهادة إلى تقديم طلب إلغائها، فقد يتم العدول عن الغاية التي من اجلها طلب إصدار الشهادة، أو فقد مفتاحه الخاص أو اطلاع الغير على بيانات أو آليات إحداث التوقيع الالكتروني أو غير ذلك من الأسباب. [2]

[1] رضوان قرواش، مرجع سابق، ص419.

[2] أمال بوبكر، النظام القانوني لمؤدي خدمات التصديق الالكتروني في الجزائر، ماجستير دولة ومؤسسات في إطار مدرسة الدكتوراه، جامعة خميس مليانة، ص148.

ولا يمكن للغير طلب إلغاء شهادة التصديق وإنما له فقط أن يطلع جهة التصديق عن الأسباب والوقائع التي تبرر الإلغاء، ولجهة التصديق سلطة إلغاء الشهادة من عدمه. كما له الحق في طلب التعويض من صاحب الشهادة إذا لحقه ضرر من جراء الإلغاء.

ب- إلغاء الشهادة بسبب وفاة الشخص الطبيعي أو انحلال الشخص المعنوي

تعد شهادة التصديق الالكتروني من الوثائق اللصيقة بصاحبها والتي تقوم على الاعتبار الشخصي، أي انه لا يجوز للغير استخدامها، ولذلك وجب إلغاء شهادة التصديق الالكتروني من طرف مقدم خدمات التصديق الالكتروني متى علم بوفاة الشخص الطبيعي أو انحلال الشخص المعنوي، وإذا لحق الغير ضرر جراء هذا الإلغاء فلا يكون أمامه سوى الرجوع إلى الورثة أو الشركاء ومطالبتهم بالتعويض.[1]

وذلك حسب نص المادة 45فقرة2 من القانون 04/15: "يلغي مؤدي خدمات التصديق الالكتروني أيضا شهادة التصديق الالكتروني الموصوفة عندما يتبين انه تم إعلام مؤدي خدمات التصديق الالكتروني بوفاة الشخص الطبيعي أو بحل الشخص المعنوي صاحب شهادة التصديق."

ت- أن تكون الشهادة منحت بناء على معلومات خاطئة أو مزورة

يجب أولا التفرقة بين المعلومات المغلوطة والمعلومات المزيفة، فالمعلومات المغلوطة صحيحة ولكنها تخص شخص أخر كأن يقوم مؤدي خدمات التصديق الالكتروني بتسليم شهادة التصديق إلى شخص له نفس الاسم الثلاثي لصاحب الشهادة الأصلي، وهنا يلتزم مقدم خدمات التصديق الالكتروني بإلغاء الشهادة من تلقاء نفسه بمجرد علمه بالخطأ الحاصل وذلك لخطورة النتائج المترتبة عن ذلك. [2]

أما المعلومات المزيفة فهي معلومات غير صحيحة تصدر شهادة التصديق بناء على تلك المعلومات، كأن يقوم شخص بتزوير بطاقته الشخصية أو العائلية أو شهادة ميلاده أو جواز

[1] الزهرة بره، جميلة حميدة، شهادة التصديق الالكتروني كآلية لتعزيز الثقة في المعاملات التجارية، مجلة العلوم القانونية والسياسية، جامعة لونيسي علي البلية2، الجزائرالمجلد10، العدد01، افريل 2019، ص906.

[2] أمال بوبكر، مرجع سابق، ص 149.

سفره، حيث أن الشهادة الصادرة بناء على معلومات مزيفة شهادة مزورة ويعرض صاحب الشهادة للمسألة المدنية والجزائية. [1]

[1] رضوان قرواش، مرجع سابق، ص 420.

المبحث الثاني: شهادة التصديق الالكتروني

تصدر جهات التصديق الالكتروني شهادة الكترونية وظيفتها الربط بين الموقع ومفتاحه العام، حيث تعد هذه الشهادة ضمانا لعدم إنكار احد الطرفين توقيع الوثيقة المرسلة بوسيلة الكترونية، ودليل واضح وصريح على أن الموقع يمتلك المفتاح الشفري الخاص، وبالتالي هو الذي قام بالتوقيع، وهذه الشهادة تمثل ضمانة هامة وأكيدة للأشخاص الذين يرغبون في التعامل معه بالإضافة إلى ذلك فهي تضمن تحقق السرية والسلامة والثقة، وسنتطرق إلى بيانات شهادة التصديق (الفرع الأول) والآثار القانونية لشهادة التصديق (الفرع الثاني).

المطلب الأول: بيانات شهادة التصديق الالكتروني

إن البيانات المتعلقة بشهادة التصديق الالكتروني لها أهمية كبيرة وذلك لأهمية تلك الشهادة خاصة في مجال الإثبات حيث يعول عليها المتعامل الالكتروني لتحديد هوية المتعامل الأخر فقد خصها المشرع الجزائري بالعناية الخاصة بتحديد بياناتها بدقة، وذلك بنص المادة 15 فقرة3 من القانون 04/15 المتعلق بالتوقيع والتصديق الالكترونيين.

الفرع الأول: بيانات شهادة التصديق في القانون المقارن

بخصوص بيانات شهادة التصديق المنصوص عليها في التشريع المقارن فنجد:

قانون تنظيم التوقيع الالكتروني المصري، الذي أحال إلى اللائحة التنفيذية له أمر تحديد هذه البيانات، والتي حددت البيانات الواجب توفرها في شهادة التصديق التي يصدرها المرخص له بذلك هي:

- ما يفيد صلاحية هذه الشهادة للاستخدام في التوقيع الالكتروني.
- موضوع الترخيص الصادر للمرخص له موضحا فيه نطاقه، ورقمه، وتاريخ إصداره، وفترة سريانه.[1]
- اسم وعنوان الجهة المصدرة للشهادة ومقرها الرئيسي وكيانها القانوني او الدولة التابعة لها إن وجدت.

[1] المادة 20 من اللائحة التنظيمية، قانون التوقيع الالكتروني المصري، الصادر سنة 2004.

- اسم الموقع الأصلي، أو اسمه المستعار، أو اسم شهرته، في حال استخدامه لأحدهما.
- صفة الموقع.
- المفتاح الشفري العام لحائز الشهادة المناظر للمفتاح الشيفري الخاص به.
- تاريخ بدا صلاحية الشهادة وتاريخ انتهائها.
- رقم تسلسل الشهادة
- التوقيع الالكتروني لجهة إصدار الشهادة.
- عنوان الموقع الالكتروني المخصص لقائمة الشهادات الموقوفة أو الملغاة.

ويجوز أن تشمل الشهادة على أي من البيانات الآتية عند الحاجة:

- ما يفيد اختصاص الموقع والغرض الذي تستخدم فيه الشهادة.
- حد قيمة التعاملات المسموح بها.
- مجالات استخدام الشهادة. [1]

كما أن المشرع التونسي وخاصة في القانون الخاص بالمبدلات والتجارة الالكترونية في نص الفصل 17 من الباب الرابع قد حدد البيانات التي يجب أن تتضمنها شهادة المصادقة الالكترونية، مايلي: "....وتتضمن هذه الشهادة بالخصوص:

- هوية صاحب الشهادة.
- هوية الشخص الذي أصدرها وإمضاؤه الالكتروني.
- عناصر التدقيق في إمضاء صاحب الشهادة.
- مجالات استعمال الشهادة. "[2]

أما قانون المعاملات الالكترونية الأردني فلم ترد فيه أي إشارة فيما يخص البيانات الواردة في شهادة التوثيق الالكتروني، إلا ما جاءت به المادة 33 على ضرورة وجود مدة سريان محددة في الشهادة، وكذلك وجود رمز تعريف الغرض منه مطابقته للتوقيع الالكتروني. [3]

[1] التوقيع الالكتروني المصري، المرجع نفسه.

[2] انظر قانون المبادلات والتجارة الالكترونية التونسي.

[3] غني جار السعي، اكرم محمد حسن، النظام القانوني لشهادة التوثيق الالكتروني، " دراسة مقارنة"، مجلة المحقق الحلي للعلوم القانونية والسياسية، العراق العدد02، سنة 2017، ص577.

كما أشترط الملحق 1للتوجيه الأوروبي الخاص بالتوقيعات الالكترونية الصادر في 1999/12/13 على أن تحتوي كل شهادة موصوفة على ما يلي:

- إشارة إلى أن الشهادة قد سلمت باعتبارها شهادة موصوفة.
- تحديد سلطة المصادقة والبلد الذي تتمركز فيه.
- اسم الموقع الحقيقي أو الاسم المستعار لصاحب التوقيع.
- إمكانية إيراد صفة معينة للموقع في ظل الغرض الذي خصصت له الشهادة.
- معلومات تتعلق بالتأكد من التوقيع تقابل المعلومات المستعملة لإنشاء التوقيع
- تحديد تاريخ بدا وانتهاء مدة صلاحية الشهادة.
- التوقيع الالكتروني المتطور لسلطة المصادقة التي سلمت الشهادة.
- الرمز التعريفي للشهادة.
- القيود على قيمة المعاملات التي يمكن استعمال الشهادة فيها.[1]

الفرع الثاني: بيانات شهادة التصديق في التشريع الجزائري

تتمثل البيانات المنصوص عليها في القانون 04/15 في مادته 15 فقرة03 في:

1- هوية صاحب الشهادة: ويقصد بصاحب الشهادة من صدرت الشهادة باسمه وبناء على طلبه، وتشمل الهوية اسم صاحب الشهادة (الموقع) سواء كان اسمه الحقيقي أو كنيته أو اسمه المستعار مادام يدل على هويته ويعرف به.[2]

إلا انه في حال استعمال الاسم المستعار لصاحب التوقيع، بطلب منه، فان لمزود خدمات التصديق ملزم بحفظ الهوية الحقيقية لصاحب التوقيع المرتبطة بالاسم المستعار وذلك بهدف استخدامه في حال وجود رقابة من طرف السلطات المختصة.

2- هوية مقدم خدمات التصديق الالكتروني ومكان إقامته: تكمن أهمية تحديد هوية جهة التصديق إلى زيادة الثقة والائتمان القانوني، فإذا كانت جهة التصديق معتمدة

[1] فاطمة باهة، شهادة التصديق الالكتروني كآلية لضمان حجية المعاملات الالكترونية في ضوء القانون رقم 04/15 المتعلق بالتوقيع والتصديق الالكترونيين الجزائري، مجلة البحوث في الحقوق والعلوم السياسية، جامعة ابن خلدون، تيارت، العدد02، في اكتوبر2015ص394.

[2] الزهرة بره، جميلة حميدة، مرجع سابق، ص896.

ومعترف بها سيضفي هذه الشهادة المزيد من الثقة لمن يتعامل مع المرسل (صاحب الشهادة)، كما أنها تكون مسئولة عن الضرر الذي يلحق المتعامل معها، وهنا يكمن دور تحديد جهات التصديق الالكتروني. [1]

نص المشرع الجزائري في المادة 15 فقرة 3 على:" تحديد هوية الطرف الثالث الموثوق أو مؤدي خدمات التصديق الالكتروني وكذا البلد الذي يقيم فيه ".

3- التوقيع الالكتروني لمزود خدمات التصديق الإلكتروني: تتجلى أهمية التوقيع في إضفاء الثقة والائتمان والتأكيد على أن الشهادة مؤمنة وعير قابلة للتزوير والتحريف وذلك باستخدام جهة التصديق لمفتاح التشفير الخاص بها، كما يعمل هذا الأخير على التطابق بين المفتاح العام و الخاص بها، والذي يقابله المفتاح الخاص (السري) بصاحب الشهادة، وبدوره يؤكد بان هذه الرسالة صادرة عن المرسل نفسه، ولا يعتريها أي تزوير أو تحريف من قبل الغير.[2]

وهذا ما يتبن من خلال نص المادة 15فقرة 3 ج من القانون 04/15 السالف الذكر:"التوقيع الالكتروني الموصوف لمؤدي خدمات التصديق الالكتروني أو للطرف الثالث الموثوق الذي يمنح شهادة التصديق الالكتروني ".

4- تحديد تاريخ سريان وانتهاء شهادة التصديق الالكتروني: وهو يعد من البيانات الجوهرية لأنه يحدد المجال الزمني لمسؤولية جهة التصديق عن صحة بيانات والمعلومات الموجودة على الشهادة، بالإضافة إلى تأكيده بان التوقيع قد تم إنشاؤه خلال فترة سريانها.

نص عليه المشرع الجزائري في المادة 15 فقرة 3 من 04/15: " الإشارة إلى بداية ونهاية مدة صلاحية شهادة التصديق الالكتروني. "

5- رمز تعريف شهادة التصديق نص عليه المشرع الجزائري في المادة 15 فقرة3 ز من القانون04/15: كل شهادة توثيق تصدرها جهات التصديق يتم إعطائها رقما معينا أو

[1] يوسف رحمان، سلطات التصديق الالكتروني في التشريع الجزائري طبقا للقانون 04/15، دراسة قانونية وسياسية، جامعة تلمسان الجزائر، ص192.

[2] لينا إبراهيم يوسف حسان، التوثيق الالكتروني ومسؤولية الجهات المختصة به، دراسة مقارنة، طبعة01، دار الراية للنشر والتوزيع، عمان الأردن، 2009، ص84

ما يطلق عليه الكود الرقمي الخاص بالشهادة، والغرض منه إدراج الشهادة وفق قاعدة بيانات يتم تحديثها بصورة مستمرة من اجل بيان التغييرات التي قد تطرأ عليها.[1]

6- تحديد قيمة ونوع المعاملات التي تستخدم بشأنها الشهادة نصت عليه المادة 15 فقرة 3 ط و ي: وهو من الشروط الجوهرية التي يجب أن تدرج في الشهادة حتى لا تتجاوز الموضوع المخصص لها، وكذا المبلغ المحدد للتعامل به، كأن تتضمن الشهادة بيان ينص على أن هذه الشهادة صالحة لإبرام صفقات تجارية في حدود 300.00 دج أو ما يعادلها بالعملة الصعبة أو الأجنبية، فان تجاوز هذا المبلغ من تصرفات تجارية فلا تعتبر جهات التصديق الالكتروني مسؤولة عنه بل يرجع ذلك إلى تقصير من طرف الشخص الذي تعامل مع هذه الشهادة رغم تحديد المبلغ.[2]

7- إشارة تفيد بان هذه الشهادة صادرة بصفة شهادة موصوفة: وهذا من البيانات البديهية، ولأنه لا يمكن لجهات التصديق الالكتروني ممارسة نشاطها إلا بعد حصولها على ترخيص مسبق من طرف الجهات المختصة في الدولة، لان ذلك يضفي المزيد من الثقة والأمان القانوني.

8- الإشارة إلى الوثيقة التي تثبت تمثيل شخص طبيعي أو معنوي أخر عند الاقتضاء

9- بيانات التحقق من التوقيع الالكتروني الموافقة لبيانات إنشائه: فيجب أن تتضمن شهادة التصديق الوسائل التي يمكن من خلالها التحقق من صحة التوقيع الالكتروني. [3]

10- صفة الموقع: أن هذا البيان يكون ضروريا في حالة ما إذا كان الموقع شخصا معنويا، فيجب في هذه الحالة أن يوضح الشخص الطبيعي الموكل له التوقيع الصفة القانونية التي بموجبها تم منحه هذا الاختصاص. [4]

---

[1] الزهرة بره، جميلة حميدة، مرجع سابق، ص 897.

[2] لينا إبراهيم يوسف حسان، مرجع سابق، ص87.

[3] ألاء احمد محمد حاج علي، مرجع سابق ،ص67.

[4] ازرو محمد رضا، إشكالية إثبات العقود الالكترونية "دراسة مقارنة"، رسالة مقدمة لنيل شهادة الدكتوراه في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، الجزائر، سنة2016، ص300.

حيث نلاحظ أن هذه البيانات بعضها إجباري لا يجوز إهمالها أي يجب ذكرها في جميع الشهادات، وبعضها الأخر اختياري، هذا ما يتبين من صياغة النص القانوني في تحديده لكل بيان من هذه البيانات.

وعليه إذا استوفت شهادة التصديق هذه البيانات تكون قد استوفت كافة الشروط وأصبحت صالحة للتعامل بها، إلا أن المشرع الجزائري لم يحدد الجزاء المترتب عن خلو شهادة التصديق من أحد هذه البيانات، أي هل تكون باطلة أو يتم إلغائها أو يمكن تدارك هذا النقص بالتصحيح.

المطلب الثاني: الآثار القانونية لشهادة التصديق الالكتروني

إذا تم النظر إلى معيار الإقليم الوطني أو الأجنبي في التمييز شهادات التصديق الالكتروني، فنميز بين شهادات تصديق وطنية وأخرى أجنبية، وشهادة التصديق الالكتروني الوطنية هي تلك التي تصدر عن مؤدي خدمات التصديق الالكترونية الوطنيين، أما شهادة التصديق الأجنبية وهي الصادرة في دول أجنبية أو من طرف مزود خدمات أجنبي داخل التراب الوطني، وبالتالي سنتطرق إلى حجية شهادة التصديق الأجنبية (الفرع الأول) والى حجية شهادة التصديق الوطنية (الفرع الثاني).

الفرع الأول: حجية شهادة التصديق الالكتروني الأجنبية

نص المشرع الجزائري على أن سلطة ضبط البريد و المواصلات السلكية واللاسلكية مكلفة بمهمة إبرام اتفاقيات الاعتراف المتبادل لشهادة التصديق الالكتروني الأجنبية وذلك بموجب المادة 3مكرر 1من المرسوم التنفيذي رقم 162/07، وبصدور القانون 04/15 وبموجب نص المادة 18 فقرة 3التي تنص: "كلف السلطة الوطنية للتصديق الالكتروني بإبرام اتفاقية الاعتراف المتبادل".[1]

نصت المادة63 من القانون 04/15 على: "تكون لشهادات التصديق الالكتروني التي يمنحها مؤدي خدمات التصديق الالكتروني المقيم في بلد أجنبي، نفس قيمة الشهادات الممنوحة

[1] المادة 18من القانون 04/15، المحدد للقواعد العامة للتوقيع والتصديق الالكترونيين.

من طرف مؤدي خدمات التصديق الالكتروني المقيم في الجزائر، بشرط أن يكون مؤدي الخدمات الأجنبي قد تصرف في إطار اتفاقية للاعتراف المتبادل أبرمتها السلطة ".[1]

من خلال نص المادة السابقة يتبين أن المشرع الجزائري اعترف بالحجية القانونية للشهادة التصديق الالكتروني الأجنبية وجعلها بنفس قيمة حجية شهادة التصديق الوطنية، وذلك بتحقق شرط وجود اتفاقية مبرمة بين الجزائر وتمثلها السلطة الوطنية للتصديق الالكتروني باعتبارها المخولة قانونا بمراقبة عملية التصديق، وبين الدولة الأجنبية الصادرة منها شهادة التصديق الالكتروني، [2]

بالإضافة إلى مبدأ المعاملة بالمثل، وهو سريان شهادة التصديق الأجنبية في الجزائر، وسريان شهادة التصديق الجزائرية في تلك الدولة الأجنبية، ومن ناحية أخرى هناك شرط تفرضه القواعد العامة للقانون وهو أن لا تكون شهادات التصديق الأجنبية المعترف بها، في الجزائر مخالفة للنظام والآداب العام، وذلك حسب النظام القانوني الجزائري. [3]

الفرع الثاني: حجية شهادة التصديق الالكتروني الوطنية

نص المشرع الجزائري في المادتين 323مكرر والمادة 323 مكرر 1 في القانون المدني على المساواة بين المحررات الكتابية والمحررات الالكترونية من حيث القيمة القانونية في الإثبات، مهما كانت الوسيلة التي تتضمنها، وطرق إرسالها، شريطة أن تضمن إمكانية التأكد من هوية الشخص الذي أصدرها وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها. [4]

بالإضافة إلى نصوص القانون المدني فقد اعترف المشرع الجزائري بحجية التوقيع الالكتروني في نص القانون 04/15 السالف الذكر في المادة 08 على: "يعتبر التوقيع الالكتروني الموصوف وحده مماثلا للتوقيع المكتوب، سواء كان لشخص طبيعي أو معنوي. "

---

[1] المادة 63من القانون 04/15، المحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين.

[2] بن الطيبي مبارك، سرحاني عبد القادر، مرجع سابق، ص614.

[3] إياد محمد عارف عطا سده، مدى حجي المحررات الالكترونية في الإثبات، دراسة مقارنة، أطروحة استكمال متطلبات درجة الماجستير في القانون الخاص، كلية الدراسات العليا، جامعة النجاح الوطنية نابلس، فلسطين، ص130.

[4] بن الطبي مبارك، سرحاني عبد القادر، شهادة التصديق الالكتروني في النظام القانوني الجزائري، مجلة العلوم القانونية والاجتماعية، جامعة زيان عاشور، جلفة، الجزائر، المجلد05، العدد03، سبتمبر، 2020، ص613.

و بالرجوع إلى المادة 07 من نفس القانون والتي تعرف التوقيع الالكتروني الموصوف "...هو التوقيع الالكتروني الذي تتوفر فيه المتطلبات الآتية ":

- أن ينشا على أساس شهادة تصديق الكتروني موصوفة.
- أن يرتبط بالموقع دون سواه.
- أن يمكن من تحديد هوية الموقع.
- أن يكون مصمما بواسطة آلية مؤمنة خاصة بإنشاء التوقيع الالكتروني.
- أن يكون منشأ بواسطة وسائل تكون تحت التحكم ألحصري للموقع.
- أن يكون مرتبطا بالبيانات الخاصة به، بحيث يمكن الكشف عن التغييرات اللاحقة بهذه البيانات. "[1]

أي انه يكون لصاحب التوقيع بيانات وشفرة خاصة به تختلف عن الموقعين الآخرين، وان يتيح لأطراف العلاقة القانونية الآخرين من تحديد هوية صاحب التوقيع أو الموقع، بالإضافة إنشائه عن طريق جهاز أو برنامج معلوماتي معد لتطبيق بيانات إنشاء التوقيع الالكتروني أي يكون التوقيع محمي من أي تزوير أو تحريف، وحتى يكون التوقيع تحت التحكم ألحصري للموقع، يجب أن يحافظ هذا الأخير على مفتاح التشفير الخاص به والمحافظة على سريته، وأيضا ضرورة ارتباط التوقيع الالكتروني بالمحرر الالكتروني وذلك للكشف عن أي تغيير أو تعديل على المحرر الالكتروني بعد إنشائه.

والملاحظ هنا أن المشرع الجزائري لم ينص صراحة بالحجية القانونية لشهادة التصديق الالكتروني، فقد اكتفى بالنص على حجية القانونية للتوقيع الالكتروني والمحررات الالكتروني، وباعتبار شهادة التصديق الالكتروني من المحررات الالكترونية، أي انه تنطبق عليها نفس أحكام التوقيع والمحررات الالكترونية.

[1] انظر قانون 04/15، خاص بالتوقيع والتصديق الالكترونيين.

ملخص الفصل الثاني

حدد القانون 04/15 "المتعلق بالتصديق والتوقيع الالكترونيين"، السلطات المعنية بتنظيم عمل مؤدي خدمات التصديق الالكتروني، والتي يعلوها السلطة الوطنية للتصديق الالكتروني وهي المشرفة على التصديق والتوقيع الالكترونيين في الجزائر، والتي تعمل على مراقبة أعمال كل من السلطة الحكومية والسلطة الاقتصادية.

حيث تقع على جهات التصديق الالكتروني مجموعة من الالتزامات التي حددها القانون وهي:

أولا: التزامات خاصة بهيئات التصديق الالكتروني والمتمثلة في:

- ضرورة الحصول على ترخيص من الجهة المختصة.
- الالتزام بالسرية.

ثانيا: الالتزامات المتعلقة بشهادة التصديق الالكتروني

- الالتزام بالتحقق من صحة البيانات المقدمة.
- الالتزام بإصدار شهادة التصديق الالكتروني.
- إيقاف أو إلغاء شهادة التصديق الالكتروني.
- إيقاف أو إلغاء شهادة التصديق الالكتروني.

حيث اعترف المشرع الجزائري بحجية التوقيع الالكتروني في نص القانون 04/15 السالف الذكر في المادة 08 على:"يعتبر التوقيع الالكتروني الموصوف وحده مماثلا للتوقيع المكتوب، سواء كان لشخص طبيعي أو معنوي، اي هو اعتراف ضمني بحجية شهادة التصديق الالكتروني.

بالإضافة إلى اعتراف المشرع الجزائري بالحجية القانونية للشهادة التصديق الالكتروني الأجنبية وجعلها بنفس قيمة حجية شهادة التصديق الوطنية، وذلك بتحقق شرط وجود اتفاقية مبرمة بين الجزائر وتمثلها السلطة الوطنية للتصديق الالكتروني باعتبارها المخولة قانونا بمراقبة عملية التصديق، وبين الدولة الأجنبية الصادرة منها شهادة التصديق الالكتروني.

خاتمة

من خلال ما سبق دراسته نلاحظ انه يجب مواكبة التطور المتواصل في مجال الاتصالات والتكنولوجية بصفة عامة، وذلك بسن قوانين وتشريعات جديدة تتلاءم مع هذه التطورات، سواء في مجال التجارة الالكترونية بصفة عامة، والتوقيع الالكتروني بصفة خاصة، وغيرها من النظم الالكترونية.

وفي ظل التوسع السريع الذي عرفته التجارة الالكترونية، كان لابد من توفير حماية لمستخدمي ومستعملي هذا المجال، وذلك لاستمرار التجارة الالكترونية ودوام التعامل بها، وذلك بسن تنظيم تدابير وقائية وحماية التوقيع الالكتروني المحافظة عليه، وذلك لمنح المتعاملين والمستخدمين الثقة والأمان في تعاملاتهم الالكترونية.

حيث انه تتطلب عمليات التجارة الالكترونية على شبكة الانترنت أجهزة وبرمجيات متطورة باهظة التكلفة، والآليات القانونية التي من خلالها يمكن حفظ وحماية التوقيع الالكتروني، هي تقنية التشفير الالكتروني، حيث انه يوفر الخصوصية والأمان، للبيانات والمعلومات المنقولة عبر شبكات الانترنت.

فتلعب التدابير التقنية للتواقيع الالكترونية دور هام في حماية معلومات وبيانات المتعاملين ضد القرصنة والانتهاكات، التي تطال التوقيع الالكتروني في المجال الرقمي أو خارجه، إلا أن الحماية المطلقة لا يمكن تحقيقها، لان الحماية بالأنظمة التقنية سرعان ما يتم كسرها، وذلك تبعا لتطور، وسائل القرصنة على الأنظمة التقنية التي تستخدمها الجهات المختصة.

يعتبر نظام التصديق الالكتروني أحد عوامل تطور ونمو المعاملات الالكترونية بصفة عامة والمعاملات الالكترونية التجارية بصفة خاصة، سيما في ظل اتجاه السياسات التشريعية نحو إرساء منظومة قانونية تهدف إلى تنظيم وتشجيع هذا النوع من المعاملات، كالقانون 04/15 المح للقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، وهذه الحماية تتحقق من خلال النص على دور مؤدي خدمات التصديق الالكتروني في هذا الخصوص بصفة أدق في مجال التوقيع الالكتروني.

ومن خلال دراستنا توصلنا إلى عدة نتائج ومن أهمها:

- إن أساس قيام التوقيع الالكتروني تحقيق الحماية والأمان وهذا ما يحققه التشفير الالكتروني.
- أن المشرع الجزائري لم يعطي تعريفا شاملا وواضحا للتشفير.
- يعد التشفير الوسيلة المثالية، التي تقدم الحماية الكاملة للمعلومات والبيانات، المتعلقة بالمعاملات الالكترونية.
- التشفير الالكتروني بمثابة ضمان، لزيادة التعاملات الالكترونية.
- مسايرة عمليات التشفير للتطور التكنولوجي المستمر.
- تتعرض التواقيع الالكترونية للتحريف والتزوير، لذلك يجب حمايتها بالطرق التقنية والقانونية.
- اعتماد المشرع الجزائري على نظام شهادة التصديق الالكتروني، الذي يمكن التأكد من صاحب التوقيع.
- التأكد من سلامة البيانات والمعلومات، واتصال التوقيع الالكتروني بصاحب التوقيع.
- ضرورة الحفاظ على المعلومات والبيانات الشخصية للمتعاملين وحمايتها من التحريف والتزوير.

ومن خلال هذه الدراسة توصلنا إلى مجموعة من التوصيات والتي نذكرها على النحو التالي:

- إدخال بعض التعديلات في أحكام القانون 04/15 وذلك بتحديد دور مؤدي خدمات التصديق الالكتروني.
- تحديد الشروط المتعلقة بممارسة نشاط مؤدي خدمات التصديق الالكتروني.
- ضرورة الاهتمام بالتنظيم القانوني لتحديد الالتزامات الخاصة بجهات التصديق الالكتروني.
- تطوير البرامج والآليات التقنية المستعملة في إنشاء التوقيع الالكتروني.
- شرح وتوضيح آلية التأكد من هوية الشخص الموقع.
- إنشاء مراكز وهيئات وطنية في مجال تقنية المعلومات والاتصالات.
- تحديث وتطوير تقنيات التشفير، وفق ما توصلت إليه المؤسسات العالمية.

- إيجاد نظام قانوني ينص على نظام التشفير وأنواعه وطرق العمل به وذلك من اجل إضفاء الصيغة القانونية على تقنية التشفير، الضرورية لضمان المعاملات الالكترونية بصفة عامة والتوقيع الالكتروني بصفة خاصة.

قائمة المصادر والمراجع

أولا: النصوص القانونية:

1. قانون رقم 04/15، المؤرخ في 2015/02/01، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، الجريدة الرسمية، العدد 06، الصادر في 2015/02/11
2. قانون تنظيم التوقيع الالكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات، رقم 15، سنة 2004، الجريدة الرسمية، مصر، عدد18، في2004/04/22.
3. القانون رقم 53/03، الصادر في2007/11/30، المتعلق بالتبادل الالكتروني للمعطيات القانونية، الجريدة الرسمية المغربية، عدد5584، في2007/12/06
4. المادة 20 من اللائحة التنظيمية، قانون التوقيع الالكتروني المصري، الصادر سنة 2004.
5. المادة05/02، قانون المبادلات والتجارة الالكترونية التونسي، رقم83، سنة2000، المنشور في الجريدة الرسمية للجمهورية التونسية في 2000/08/09.
6. المرسوم التنفيذي رقم162/07، المؤرخ في 2007/05/30، المعدل والمتمم للمرسوم التنفيذي رقم 123/01، المؤرخ في 2007/05/09.

ثانيا: الكتب:

1. اندي اوبل، كشف أسرار قواعد البيانات، طبعة1، الدار العربية للعلوم، لبنان، 2014.
2. سلطان عبد الله محمود الجواري، عقود التجارة الالكترونية والقانون الواجب التطبيق"دراسة مقارنة"، طبعة01، منشورات الحلبي الحقوقية، بيروت، لبنان، سنة2010.
3. عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الالكترونية، طبعة01، دار الفكر الجامعي، الإسكندرية، 2002.
4. عبير ميخائيل الصفدي، النظام القانوني للتوثيق الالكتروني، طبعة01، دار وائل للنشر، عمان، سنة2010.
5. عيسى غسان ريضي، القواعد الخاصة بالتوقيع الالكتروني، طبعة01، دار الثقافة للنشر والتوزيع، الأردن، 2009.

6. غازي بن فهد بن غازي المزبني، الحماية القانونية للمستهلك في عقود التجارة الالكترونية "دراسة تأصيلية تطبيقية مقارنة"، طبعة01، دار الكتاب الجامعي للنشر والتوزيع، الرياض، السعودية، سنة2018.
7. فادي محمد عماد الدين توكل، عقود التجارة الالكترونية، منشورات الحلبي الحقوقية، طبعة 01، بيروت، سنة 2010.
8. لينا إبراهيم يوسف حسان، التوثيق الالكتروني ومسؤولية الجهات المختصة به، دراسة مقارنة، طبعة01، دار الراية للنشر والتوزيع، عمان الأردن، 2009.
9. ليندا بو محراث، تسوية منازعات التجارة الالكترونية "دراسة مقارنة بين الفقه الإسلامي والقانون الوضعي، دون طبعة، دار الجامعة الجديدة، الإسكندرية، مصر، سنة 2019.
10. محمد فواز المطالقة، الوجيز في عقود التجارة الالكترونية "دراسة مقارنة"، طبعة01.دار الثقافة للنشر والتوزيع، عمان، الأردن، سنة2006.
11. مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الالكترونية، دون طبعة، دار النهضة العربية، القاهرة، سنة2001.
12. نادية ياس البياتي، التوقيع الالكتروني عبر الانترنت ومدى حجيته في الإثبات، طبعة01، دار البداية، عمان، الاردن، سنة2014.
13. نضال اسماعيل برهم، أحكام عقود التجارة الالكترونية، دون طبعة، دار الثقافة للنشر والتوزيع، الأردن، 2005.

ثالثا: المقالات:

1. احمد غريبي، حورية قاسمي، دور سياسة التشفير الالكتروني في حماية نظم معلومات الإدارة الالكترونية بمؤسسة بريد الجزائر فرع المدية، مجلة الاقتصاد الجديد، جامعة المدية، مجلد12، عدد01، جانفي 2021.
2. ازرو محمد رضا، إشكالية إثبات العقود الالكترونية "دراسة مقارنة"، رسالة مقدمة لنيل شهادة الدكتوراه في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، الجزائر، سنة2016.
3. ازرو محمد رضا، سلطات التصديق الالكتروني في التشريع الجزائري، مجلة العلوم القانونية والاجتماعية، جامعة زيان عاشور، الجلفة، العدد07.

4. أسامة بن غانم العبيدي، حجية التوقيع الالكتروني في الإثبات، المجلة العربية للدراسات الأمنية والتدريب، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية مجلد28، العدد56، الرياض.
5. إسماعيل عبد النبي شاهين، امن المعلومات في الانترنت بين الشريعة والقانون، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت، جامعة الإمارات، مجلد02، الجزء03، كلية الشريعة والقانون، جامعة الإمارات، سنة 2000.
6. إكرام رقيعي، خصوصية التوقيع الالكتروني في العقد التجاري الالكتروني على ضوء القانون رقم 05/18، مجلة العلوم القانونية والسياسية، مخبر الرقمنة والقانون، جامعة البليدة2، مجلد 10، عدد02، في سبتمبر 2019.
7. امحمد بن الدين، محمد شهيدي، وهيبة حليمي، امن الشبكات من مخاطر التهديدات ودوره في تعزيز التجارة الالكترونية، يوم دراسي حول: التجارة الالكترونية في الجزائر "الواقع والأفاق"، كلية الآداب والعلوم الإنسانية، قسم علوم التسيير، الجامعة الإفريقية العميد احمد دراية، ادرار، الجزائر.
8. امينة قهواجي، ليلي مطالي، الإطار المفاهيمي والقانوني للتوقيع والتصديق الالكترونيين في الجزائر، مجلة المشكاة في الاقتصاد التنمية والقانون، المركز الجامعي بلحاج شعيب عين تموشنت، الجزائر، المجلد 04، العدد08، في ماي 2019.
9. بن الطبي مبارك، سرحاني عبد القادر، شهادة التصديق الالكتروني في النظام القانوني الجزائري، مجلة العلوم القانونية والاجتماعية، جامعة زيان عاشور، جلفة، الجزائر، المجلد05، العدد03، سبتمبر، 2020.
10. جبايلي صبرينة، النظام القانوني للسلطة الوطنية للتصديق الالكتروني، مجلة العلوم الإنسانية، العدد48، المجلد أ، جامعة الإخوة منتوري قسنطينة، الجزائر، سنة2017.
11. حليتيم سراح، خصوصية التوقيع الرقمي في توثيق العقود الالكترونية، مجلة الباحث للدراسات الأكاديمية، جامعة باتنة01، الحاج لخضر، الجزائر، عدد13، في جويلية 2018.

12. دريس كمال فتحي، آلية التصديق الالكتروني كضمانة للتعاملات التجارية بالوسائل الحديثة في التشريع الجزائري، مجلة البحوث والدراسات، جامعة الوادي، العدد24، صيف 2017.

13. رضوان قرواش، هيئات التصديق الالكتروني في ظل قانون 15-04 المتعلق بالقواعد العامة للتوقيع والتصديق الالكترونيين(المفهوم والالتزامات)، مجلة العلوم الاجتماعية، جامعة سطيف2، العدد24، جوان 2017.

14. زروقي خديجة، الحماية الرقمية كآلية لتفعيل مبدأ المساواة بين الأدلة الكتابية والالكترونية، مجلة الاجتهاد للدراسات القانونية والاقتصادية، معهد الحقوق والعلوم السياسية، المركز الجامعي أمين العقال الحاج موسى اق اخموك تامنغست، مجلد10، عدد03، في اكتروبر 2021.

15. الزهرة بره، جميلة حميدة، شهادة التصديق الالكتروني كآلية لتعزيز الثقة في المعاملات التجارية، مجلة العلوم القانونية والسياسية، جامعة لونيسي علي البليدة2، المجلد10، العدد01، افريل 2019.

16. زهيرة عبوب، المسؤولية المدنية لمقدم خدمات التصديق الالكتروني، مجلة الدراسات القانونية المقارنة، جامعة حسيبة بن بو علي، الشلف، المجلد06، العدد02، ديسمبر 2020.

17. زهيرة كيسي، النظام القانوني لجهات التوثيق(التصديق) الالكتروني، مجلة دفاتر السياسة والقانون، جامعة قاصدي مرباح ورقلة، العدد07، جوان2012.

18. عبيدات يوسف محمد، دراركة لافي محمد، وسائل حماية التوقيع الرقمي التي جعلته عنصرا مهما في زيادة العمل عبر الانترنت"دراسة تحليلية في قانون المعاملات الالكترونية الأردني، مؤتة للبحوث والدراسات "سلسلة العلوم الإنسانية"، جامعة مؤتة، الأردن، مجلد24، عدد01، سنة2009.

19. عرعار الياقوت، التشفير وسيلة لتامين التجارة الالكترونية من المخاطر التقنية، مجلة البحوث القانونية والاقتصادية، جامعة البويرة، الجزائر، مجلد05، عدد01 ديسمبر 2021.

20. عقوني محمد، الآليات التقنية والقانونية لحماية التوقيع الالكتروني، مجلة الفكر، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، الجزائرعدد18، في فيفري2019.

21. فاطمة باهة، شهادة التصديق الالكتروني كآلية لضمان حجية المعاملات الالكترونية في ضوء القانون رقم 04/15 المتعلق بالتوقيع والتصديق الالكترونيين الجزائري، مجلة البحوث في الحقوق والعلوم السياسية، جامعة ابن خلدون، تيارت، مجلد01 العدد02، سنة اكتوبر2015.

22. مرتضى مالك أم الحاج، السماني عبد المطلب احمد، تطبيق التوقيع الرقمي بخوارزمية ار اس ايه (RSA) في الشهادات الجامعية بمفاتيح شهادات pkcsv1.5، OpenPGP، وOpenSSL، مجلة الدراسات العليا، جامعة النيلين، مجلد06، العدد23، في سبتمبر2016.

23. ميمونة حميد الحداد، دراسة عامة للمقارنة بين خوارزميتي التشفير DES وTDES، كلية التربية للبنات، قسم الحاسبات، جامعة الكوفة، العراق.

24. ندى بدر جراح، تقنيات التشفير في التبادل التجاري الالكتروني، مجلة ميسان للدراسات الأكاديمية، جامعة ميسان، العراق، المجلد07، العدد14، سنة2009.

25. نذير قورية، دور مؤدي خدمات التصديق الالكتروني في حماية المستهلك على ضوء القانون رقم 04/15، مجلة العلوم القانونية و الاجتماعية، جامعة زيان عاشور، الجلفة، العدد10، جوان2018.

26. وسيمة مصطفى هنشور، النظام القانوني لمقدمي خدمات التصديق الالكتروني في التشريع الجزائري، تخصص قانون العلاقات الاقتصادية الدولية، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن بديس، مستغانم، افريل2017.

رابعا: الرسائل الجامعية:

1. ألاء احمد محمد حاج علي، التنظيم القانوني لجهات التصديق على التوقيع الالكتروني، أطروحة لاستكمال متطلبات الحصول على درجة الماجستير في القانون الخاص، كلية الدراسات العليا، جامعة النجاح الوطنية نابلس، فلسطين.

2. أمال بوبكر، النظام القانوني لمؤدي خدمات التصديق الالكتروني في الجزائر، ماجستير دولة ومؤسسات في إطار مدرسة الدكتوراه، جامعة خميس مليانة.

3. إياد محمد عارف عطا سده، مدى حجي المحررات الالكترونية في الإثبات، دراسة مقارنة، أطروحة استكمال متطلبات درجة الماجستير في القانون الخاص، كلية الدراسات العليا، جامعة النجاح الوطنية نابلس، فلسطين.

خامسا: أبحاث علمية:

1. صلاح الدوه جي، مقدمة في التشفير، الجامعة الافتراضية السورية، الجمهورية العربية السورية، سنة2018.https://www.noor-book.com/
2. عبد الرحمان غسان زعرور، خوارزمية التشفير DES، المعهد المتوسط لتقنيات الحاسوب، حماه، سوريا.https://www.noor-book.com/
3. علي محمددهب، التشفير وامن المعلومات، كلية دراسات الحاسوب والإحصاء، جامعة كردفان، السودان. https://www.noor-book.com/
4. يوسف رحمان، سلطات التصديق الالكتروني في التشريع الجزائري طبقا للقانون 04/15، دراسة قانونية وسياسية. انظر موقع: https://www.noor-book.com/

سادسا: مواقع الالكترونية:

1. موقع مدونة https://mustafasadiq0.com، تاريخ الاطلاع 2022/04/08 على الساعة 11:33
2. https://attaa.sa/library/view/1363 تاريخ الاطلاع، 2022/03/28، على الساعة 14:22

العنوان	الصفحة
إهداء	
شكر و عرفان	
مقدمة	1
الفصل الأول: الإطار القانوني للتشفير الالكتروني	**5**
المبحث الأول: مفهوم التشفير الالكتروني	6
المطلب الأول: تعريف التشفير الالكتروني	6
الفرع الأول: التعريف الفني	7
الفرع الثاني: التعريف الفقهي	8
الفرع الثالث: التعريف القانوني	9
المطلب الثاني: أحكام نظام التشفير الالكتروني	11
الفرع الأول: ضوابط التشفير	11
الفرع الثاني: أهداف التشفير	14
المبحث الثاني: الأحكام القانونية للتشفير الالكتروني	17
المطلب الأول: أنظمة التشفير الإلكتروني	17
الفرع الأول: التشفير المتناظر	17
الفرع الثاني: التشفير غير المتناظر	20
المطلب الثاني: موقف المشرع الجزائري من التشفير الالكتروني	23
ملخص الفصل الأول	25
الفصل الثاني: دور التصديق الالكتروني في حماية التوقيع الالكتروني	**26**
المبحث الأول: هيئات التصديق الالكتروني	27
المطلب الأول: سلطات التصديق الالكتروني	27
الفرع الأول: السلطة الوطنية للتصديق الالكتروني	28

الفرع الثاني: السلطة الحكومية للتصديق الالكتروني	30
الفرع الثالث: السلطة الاقتصادية للتصديق الالكتروني	31
المطلب الثاني: التزامات مقدم خدمات التصديق الالكتروني	33
الفرع الأول: التزامات خاصة بمؤدي خدمات التصديق الالكتروني	33
الفرع الثاني: التزامات المتعلقة بشهادة التصديق الالكتروني	35
المبحث الثاني: شهادة التصديق الالكتروني	40
المطلب الأول: بيانات شهادة التصديق الالكتروني	40
الفرع الأول: بيانات شهادة التصديق الالكتروني في قانون المقارن	40
الفرع الثاني: بيانات شهادة التصديق الالكتروني في القانون الجزائري	42
المطلب الثاني: الآثار القانونية لشهادة التصديق الالكتروني	45
الفرع الأول: حجية شهادة التصديق الإلكتروني الأجنبية	45
الفرع الثاني: حجية شهادة التصديق الإلكتروني الوطنية	46
ملخص الفصل الثاني	48
الخاتمة	49
قائمة المراجع	52
الفهرس	58
ملخص البحث بالعربية والانجليزية	

ملخص البحث

وفي الأخير نستخلص أن المعاملات الالكترونية عموما والتجارة الالكترونية خصوصا أصبحت جزء من التعاملات اليومية للشخص، مما استوجب توفير الحماية له من أي تزوير أو تحريف، حيث انتهجت مختلف التشريعات، أنظمة واليات من اجل توفير ذلك، ومنها التشريع الجزائري، وذلك من خلال التشفير الالكترونية الذي يعد من الطرق الفعالة المستعملة في حماية البيانات، والذي نص عليه المشرع الجزائري في القانون04/15 المتعلق بالقواعد العامة للتوقيع والتصديق الالكترونيين.

بالإضافة إلى تنظيم مهام جهات التصديق الالكتروني وتحديد التزاماتهم قصد تحقيق الأمان للمتعاملين في المجال الالكتروني، حيث يعد التصديق الالكتروني كضمان لصحة المعلومات والبيانات الموقعة من الشخص، أي أنها لا يشوبها التزوير ولا التحريف، بالإضافة إلى عمد إنكار الشخص لتوقيعه، أو لأي تصرف آخر صدر منه.

Summary

Finally ،we conclude that electronic transactions in general and electronic commerce in particular have become part of a person's daily dealings ،which necessitated the provision of protection against any forgery or distortion. Various legislations have adopted regulations and mechanisms to provide this ،including Algerian legislation ،through electronic encryption ،which is one of the effective methods used to protect data ،and which was stipulated by the Algerian legislature in Law 15/04 on general rules for electronic signature and authentication.

In addition ،the functions of the electronic certification authorities are regulated and their obligations are defined in order to ensure the safety of users in the electronic field. Electronic authentication is considered to be a guarantee of the authenticity of information and data signed by the person ،that is ،it is free from forgery or distortion ،in addition to the person's non-denial of his or her signature or any other behavior.