

الآليات التقنية والقانونية لحماية التوقيع الإلكتروني

Mécanismes techniques et juridiques pour la protection de la signature électronique

الدكتور : **عقوني محمد**

استاذ محاضر " أ " - كلية الحقوق و العلوم السياسية

جامعة محمد خيضر - بسكرة / الجزائر

mohamedaggoni@gmail.com

الاستاذ : **بلهددي براهيم**

استاذ مساعد " أ " - كلية الحقوق و العلوم السياسية

جامعة محمد خيضر - بسكرة / الجزائر

br.belhd@gmail.com

تاريخ النشر :	تاريخ القبول :	تاريخ الإرسال :
2019/02/04	2019/01/30	2018/09/26

المخلص :

تعالج هذه الدراسة مدى نجاعة الآليات التقنية والقانونية التي أقرها المشرع الجزائري في القانون رقم: 15-04، - المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين -، في حماية التوقيع الإلكتروني. حيث لا يكفي الاعتراف بحجية التوقيع الإلكتروني في الإثبات، دون العمل على إيجاد الآليات الكفيلة ببعث الثقة والاطمئنان لدى المتعاملين به، وتحقيق الحماية الضرورية للتوقيع الإلكتروني من مخاطر التجارة والحفاظ على الدور الوظيفي المنوط به من أي اختراق أو تحايل إلكتروني، ما جعل المشرع يقر عملية التشفير كإجراء تقني لحماية البيانات الإلكترونية، بالإضافة إلى العمل على تنظيم مهام جهة التوثيق الإلكتروني وتحديد مسؤولياتها قصد تحقيق الأمان القانوني للمتعاملين في المجال الإلكتروني.

الكلمات المفتاحية : التوقيع ؛ الإلكتروني ؛ الآليات القانونية.

Résumé :

Cette étude porte sur la mesure de l'efficacité des mécanismes techniques et juridiques approuvés par le législateur algérien dans la loi n °: 15-04 qui détermine les règles générales relatives à la signature et la ratification électroniques dans la protection de la signature électronique.

Où ne suffit pas en raison de la reconnaissance de la signature électronique dans l'affirmation, sans travail pour trouver les mécanismes de confiance et réconfort chez les clients, et réaliser la protection nécessaire à la signature électronique des risques de commerce et de maintenir le rôle électronique qui lui est attribué de toute violation ou fourberie, ce qui rend le législateur reconnaît le processus de chiffrement en tant que mesure technique pour la protection des données électroniques, en plus de travailler à organiser les fonctions de documentation électronique de l'organisation et la détermination de sa responsabilité en raison de réaliser la sécurité juridique pour les clients dans le domaine électronique.

Mots-clés : Signature ; Electronique ; Mécanismes juridiques.

مقدمة :

يسعى الأشخاص في علاقاتهم دائما إلى الاستقرار والبعد عن المخاطر التي من الممكن أن تؤثر على نشاطهم. كذلك الحال بالنسبة للتعاملات الإلكترونية، فالمتعاملون يسعون إلى البعد عن المخاطر التي تؤثر على سلامة عملياتهم المبرمة عبر الوسائط الإلكترونية التي من الممكن أن تسبب عدم الأمان لهم و القلق المستمر عند استخدام شبكة الانترنت، ما قد يجعلهم يدعون إلى الانسحاب من الأسواق الإلكترونية والعودة إلى التعامل بالنظام التقليدي.

فرغم ما تقدمه الثورة الرقمية و التقدم التكنولوجي في هذا المجال من رقي وازدهار، إلا أن دخول إلى العالم الافتراضي لا يهمل من تحديات جديدة تخلق عدة إشكالات، تتعلق بالاختراقات الأمنية التي قد تؤدي إلى عدم الثقة في استخدام البيانات الإلكترونية نتيجة عدم توفير الأمن القانوني والاستقرار للتصرفات المبرمة من خلالها، ما يؤدي إلى إرهاب المتعاملين.

ورغم أن الجزائر بدأت خطوات دخول العالم الافتراضي متأخرة، إلا أن هناك مؤشرات تعكس إرادة جادة رغم النقصان العديدة التي تمس هذا المجال، في الذهاب إلى رقمنة التعاملات و النشاطات المختلفة في جميع القطاعات، وهو ما يؤكد صدور القانون رقم : 05-18، المتعلق بالتجارة الإلكترونية¹، وقبله القانون رقم : 04-15، المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين²، الذي جاء بعدة نصوص تعمل على توفير الحماية اللازمة للتوقيع الإلكتروني، حيث لا يخفى على أحد أهمية ودور هذا الأخير الذي أصبح بديلا عن التوقيع التقليدي في إثبات التصرفات و العقود القائمة على الدعامة الإلكترونية و المساهمة في إعطاء الثقة لهذا النوع من التعاملات.

انتشار العقود و التعاملات الإلكترونية يبقى رهين مدى توفير الحماية التقنية و القانونية الكافية لنظام التعامل الإلكتروني ككل و التوقيع الإلكتروني خاصة، لإعطاء ضمانات تجمع المتعاملين على الولوع إلى العالم الافتراضي وهم مطمئنين على معلوماتهم و تعاملاتهم و توقيعاتهم من أي احتيال أو تسريب أو اختراق.

وبناء على ما سبق، نحاول الإجابة في بحثنا عن تساؤل مهم يمثل إشكالية الدراسة، وهو إلى أي مدى يمكن اعتبار الوسائل والأليات التقنية والقانونية التي أقرها المشرع الجزائري في القانون رقم : 04-15، المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين، كفيلة بتحقيق الحماية المطلوبة للتوقيع الإلكتروني ؟

وانطلاقا من هذا التساؤل سندرس الموضوع بالاستعانة بالمنهج التحليلي و الوصفي في مطلبين:

نتناول نظام التشفير في المطلب الأول، حيث نتطرق إلى المقصود بالتشفير (الفرع الأول)، ثم ضوابط التشفير (الفرع الثاني)، وفي الأخير نتناول طرق التشفير (الفرع الثالث).

أما في المطلب الثاني فسنتكلم على نظام التصديق من خلال تعريف جهة التوثيق (الفرع الأول)، وتحديد دورها في حماية التوقيع الإلكتروني (الفرع الثاني).

المطلب الأول: نظام التشفير

التوقيع الإلكتروني موجود ضمن محرر على وسيط إلكتروني، يمكن للقراصنة اختراق أنظمة المعلومات والتقاط صورة التوقيع، أو فك شفرته، ثم استخدامه بدون علم صاحبه، وكذا ظهور حالات عديدة لتزوير بطاقات الائتمان، زيادة على ذلك ظهور الفيروسات التي تهدد بإتلاف الملفات المحفوظة، مما يؤدي إلى اضطراب التعامل على الوسائط الإلكترونية³؛ وعلى هذا الأساس وضعت آلية لحماية التوقيع الإلكتروني من أجل تأمين المعاملات الإلكترونية والتجارة الإلكترونية وتجاوز هذه الصعوبات، فتم اعتماد آلية التشفير لكبح مرتكبي جرائم الاختراق و التجاوزات و الاحتيال الإلكتروني.

الفرع الأول: المقصود بالتشفير

لم يتطرق المشرع الجزائري في قانون التجارة الإلكترونية إلى تعريف التشفير، واكتفى بتعريف مفتاح التشفير الخاص ومفتاح التشفير العمومي⁴ في القانون رقم: 04-15، المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكتروني، على خلاف المشرع المصري الذي عرفه في مشروع قانون التجارة الإلكترونية بأنه تغيير في شكل البيانات عن طريق تحويلها إلى رموز أو إشارات لحماية هذه البيانات من إطلاع الغير عليها أو تعديلها أو تغييرها⁵، كما عرفه المشرع التونسي بأنه "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 الوصول إلى المعلومات بدونها".⁶

وقد ورد العديد من التعاريف لأدوات التشفير من قبل الفقه، فذهب البعض إلى تعريفها على أنها "عملية تحويل النص إلى رموز وإشارات غير مفهومة تبدو ذات غير معنى لمنع الغير من الاطلاع عليها إلا الأشخاص المرخص لهم بالاطلاع على النص المشفر وفهمه، فتنبص عملية التشفير على القيام بتحويل النصوص العامة إلى نصوص مشفرة مع إمكانية إعادة النص المشفر إلى نص عادي بعد فك التشفير بمفتاح التشفير الذي تم إنشاؤه للتشفير وفكه⁷، وذهب بعض الفقه إلى اعتماد تعريف من الناحية التقنية بالقول "أن التشفير أو الترميز أو الكتابة المشفرة هو تقنية قوامها خوارزمية رياضية ذكية، تسمح لمن يمتلك مفتاحا سريا بأن يحول رسالة مقروءة إلى رسالة غير مقروءة وبالعكس، أي أن يستخدم المفتاح السري بفك الشفرة وإعادة الرسالة المشفرة إلى وضعيتها الأصلية".⁸

ويتضح من خلال التعريف الأخير أن التشفير يعتمد على عمليات رياضية يتم بها تحويل النص المراد إرساله إلى رموز وإشارات لا يتاح فهم محتواها إلا بواسطة فك الشفرة وتحويل هذه الرموز والإشارات إلى نصوص مقروءة ومفهومة عن طريق استعمال مفاتيح التشفير العامة والخاصة، وبالتالي لا يمكن أن تتم هذه العملية إلا إذا كان مستقبل الرسالة يملك مفتاح التشفير الذي يعيد الإشارات والرموز إلى نصه الأصلي.⁹

وبناء على ما سبق فإن عملية التشفير تتكون من ثلاثة عناصر مترابطة وهي:

- 1- المعلومات التي سيتم تشفيرها.
- 2- خوارزمية التشفير التي ستطبق على المعلومات، و خوارزمية فك التشفير التي تعيدها إلى حالتها الأصلية.
- 3- المفاتيح وهي سلسلة أو أكثر من الرموز تستند إلى صيغ رياضية معقدة في شكل خوارزميات.¹⁰

و لا يقتصر دور التشفير على وظائف الحماية و الأمن و السرية في المعلومات و العقود المتبادلة عن بعد في شبكة الانترنت فحسب، و إنما يقوم فضلا عن ذلك بوظائف أخرى متعلقة بالتحقق من هوية الشخص صاحب التوقيع و المصادقة على مضمون المحرر الموقع عليه إلكترونيا والتأكد من سلامته، ويقصد بذلك التثبت من عدم تغييره في أثناء عبور داخل شبكة الاتصال.¹¹

الفرع الثاني: ضوابط التشفير

أقر المشرع الجزائري بضرورة تشفير البيانات و المعلومات، كما نص على العمل من أجل الحفاظ على سرية البيانات و المعلومات المشفرة. بالإضافة إلى اعتباره أن النص المشفر محررا إلكترونيا و سوف نتناول كل هذه الضوابط بأكثر تفصيل فيما يلي:

أولاً: مشروعية تشفير البيانات و المعلومات: التي يتم تبادلها عن طريق الوسائط الإلكترونية، على غرار ما ذهب إليه أغلب التشريعات المقارنة في تناول نصوص قانونية تتعامل مع تشفير البيانات و المعلومات، أقر المشرع الجزائري من خلال القانون رقم : 15-04، نصوصا تتناول نظام التشفير، و عرف التشفير الخاص العام، و أجاز استخدامه في المراسلات الإلكترونية و التعاملات الإلكترونية التجارية.

و أكد حماية البيانات المشفرة والعناصر المستخدمة في عملية التشفير وفكها من أي اعتداء عليها، سواء تم ذلك باستخدام عناصر التشفير الشخصية الخاصة بالتوقيع من غير طرفي العلاقة، أو بسبب استخدام التشفير في ارتكاب جرائم احتيالية، أو سرقة مفاتيح التشفير التي تفك النص المشفر و تعيده إلى النص الأصلي باستعمال مفتاح التشفير الخاص.¹²

و من المهم الإشارة إلى أن جل التشريعات العربية تناولت في النصوص الخاصة بالتجارة الإلكترونية عملية التشفير بطريقة غير مباشرة من خلال التوقيع الإلكتروني باستثناء المشرع التونسي و المصري الذين تناولوا عملية التشفير بشكل مباشر من خلال نصوص خاصة تجنباً لاختلاف التفسير و الاجتهادات الفقهية بشأنها.¹³

ثانياً: الحق في الحفاظ على سرية البيانات و المعلومات المشفرة: اعتبر المشرع الجزائري من خلال القانون رقم : 15-04، على أن الاعتداء على البيانات المرسله بين طرفي العقد عبر الوسائط الإلكترونية هو اعتداء على خصوصية و سرية البيانات و المعلومات المرسله بين طرفي العلاقة، وبالتالي وجب ضمان سرية البيانات المستخدمة لإنشاء التوقيع الإلكتروني بكل الوسائل التقنية المتوفرة وقت الاعتماد، كما يجب على مؤدي خدمات التصديق الإلكتروني الحفاظ على سرية البيانات و المعلومات المتعلقة بشهادات التصديق الإلكتروني الممنوحة.¹⁴

لأن هذه البيانات و المعلومات تتميز بالخصوصية و السرية و تعبر عن إرادة الطرفين بالقيام بتصرف قانوني، و إطلاع الغير على هذه البيانات و المراسلات يمكن أن يؤدي إلى إلحاق الضرر بطرفي العقد و التعدي على خصوصيتهم بعد فك التشفير.

و أقر المشرع الجزائري نصوصا تعاقب كل من يقوم بانتهاك سرية البيانات المشفرة و إفشائها، سواء كان ذلك من طرف الغير¹⁵ ، أو من طرف مؤدي خدمات التصديق الإلكتروني.¹⁶ أو من طرف الشخص المكلف بالتدقيق.¹⁷

و يبقى أن نشير و في ما تعلق بتقنية التشفير، ضرورة مواكبة التطور السريع للتكنولوجيا، فما يبدا اليوم مستحيلا من إمكانية اختراق التشفير قد يكون مباحا بعد بضع سنوات، زيادة على ذلك نظام التشفير قد يشمل على ثغرات في تصميمه يمكن أن تستغل في كشف الرسالة المشفرة.

ثالثا: اعتبار النص المشفر محررا إلكترونيا: نتيجة إقرار المشرع للنص المشفر وحجته في اثبات كل التصرفات القانونية التي تتم عبر الوسائط الإلكترونية، فإنه يعتبر من المحررات الإلكترونية بالرغم أنها غير مفهومة للعامة، وبالتالي فإنه يتم تحويل الإشارات والرموز إلى نصوص مقروءة ومفهومة تكون حجة على من يخالف ما التزم به طرفي الاتفاق.¹⁸

الفرع الثالث: طرق التشفير

يمكن تصنيف تقنيات التشفير في مجال المعلوماتية إلى فئتين رئيسيتين بالنظر إلى نوعية المفتاح المستخدم في التشفير.

أولاً: المفتاح الخصوصي (تقنية التشفير المتماثل): هو نظام الكتابة المشفرة بالمفتاح الخصوصي، يعمل بواسطة مفتاح واحد يعرف بالخصوصي يمتلكه كل من مرسل الرسالة و متلقيها، وبالتالي يستخدم هذا الصنف من تقنية التشفير المفتاح أو الرمز السري ذاته في تشفير الرسائل و في فك تشفيرها. حيث يتم الاتفاق بين طرفي العلاقة في البداية على كلمة المرور ليتم استخدامها في التشفير وفك التشفير التي تم اعدادها، و في حالة ادخال كلمة المرور يتم تحويل عبارة المرور إلى عدد ثنائي يتم فهمه من قبل أجهزة الحاسب، و عند ارسال الرسالة إلى الطرف الآخر ولكي يتمكن من قراءتها لا بد من إزالة الغموض و بيان الرسالة على شكلها الأصلي عن طريق استخدام كلمة المرور التي تمت بها عملية التشفير.¹⁹

يعاب على هذه التقنية استعمال المفتاح ذاته من قبل شخصين مختلفين (رسل و المرسل إليه)، وهذا قد يضعف من حجية المستندات الرقمية و التوقيع الإلكتروني و قوتها الثبوتية، على أساس الخطر الدائم في أن يكون المفتاح الخصوصي قد سرب أو انتقل بشكل غير شرعي، و ذلك بالنظر إلى صعوبة تحديد مصدر التسرب أو حصول الانتقال، و بالإضافة إلى هذا فإن استعمال هذه

التقنية تجعل، تلقى الرسائل المشفرة القادمة من مصادر مختلفة، عليه أن يقتني عددا من المفاتيح الخصوصية يوازي عدد الرسائل الواردة من هذه المصادر وهو ما يعتبر أمرا مرهقا.²⁰

ثانيا: **المفتاح العمومي (التشفير غير المتماثل):** خلافا للتشفير بالمفتاح الخصوصي لا يستعمل المفتاح ذاته من أجل تشفير الرسائل، بحيث أنه، يستعمل مفتاحين سريين مختلفين من أجل فك تشفيرها، الأول خصوصي يملكه، مستخدم معين لمستعمل الوسائط الإلكترونية و يبقيه سرا و خاصا به، أما الثاني عمومي يوزعه إلى المتعاملين الآخرين الذي يود تلقي رسائل مشفرة منهم.²¹

و بالتالي يتم الاستعانة بمفتاحين مرتبطين بشكل حسابي لإنشاء التوقيع الإلكتروني لتحويل البيانات و المعلومات، ثم تثبيتها مرة أخرى بنظام التشفير غير المتماثل، و لا يمكن للغير لو عرفوا مفتاح الشفرة العام اكتشاف المفتاح الخاص بالم، وقع و استعماله في التعرف على محتوى الرسالة، و المفتاح الخاص يكون معروفا لدى جهة واحدة فقط و هو الم، رسل و يستعمل لتشفير الرسالة أو فك تشفيرها، أما المفتاح العام فعادة ما يكون معروفا لدى أكثر من جهة أو شخص.²²

حققت هذه التقنية إيجابيات عملية وقانونية مهمة، حيث أعطت لكل مستخدم في المعاملات الإلكترونية أن يستعمل مفتاح أو رمز سري واحد في تشفير الرسائل التي يرغب إرسالها، أو في فك تشفير الرسالة التي تلقاها. ورغم أن هناك صعوبات تواجه هذا النوع من التشفير، تتمثل أساسا في مسألة ضمان المفتاح العمومي، أي أنه عائد فعلا إلى المستخدم الحائز على المفتاح الخصوصي إلا أنه تم معالجة هذه العقبة بتدخل جهة ثالثة محايدة ومستقلة تتمثل في جهة التصديق الإلكتروني.²³

المطلب الثاني: نظام مصادقة جهة التوثيق

تتطلب تقنية التشفير بالمفتاح العمومي تدخل طرف ثالث محايد ومستقل بين الحائز على المفتاح الخصوصي وبين الحائز على المفتاح العمومي، يطلق على هذا الشخص بالثالث المصادق مؤدي خدمات التصديق.

الفرع الأول: تعريف مؤدي خدمات التصديق

التصديق أو التوثيق الإلكتروني هي وسيلة فنية أمانة للتحقق من صحة التوقيع أو المحرر، حيث يتم نسبته إلى شخص معين أو جهة معينة أو طرف محايد يطلق عليه، مقدم خدمات التصديق، أو مورد خدمات التصديق أو جهة التوثيق (prestataires de services de certification).

و جهة التوثيق هي هيئة أو جهة عامة أو خاصة تعمل تحت إشراف السلطة التنفيذية تتكون غالبا من مستويات مختلفة من السلطات، تأتي في قممها السلطة الحكومية وهي تختص بالتصديق على تكنولوجيا و ممارسات جميع الأطراف الم، رخص لهم بإصدار أزواج مفاتيح التشفير أو شهادات

تتعلق باستخدام تلك المفاتيح، ثم تأتي سلطة التصديق وهي جهة خاصة بعملية التصديق على أن المفتاح العام لأحد المستخدمين يناظر بالفعل المفتاح الخاص لذلك المستخدم، أما في آخر مستوى فنجد سلطة تسجيل محلية ومهمتها هي الطلبات من الأشخاص الراغبين في الحصول على أزواج مفاتيح التشفير العام والخاص والتثبت من هوية وشخصية هؤلاء المستخدمين ومنح شهادات تصديق تفيد صحة توقيع المتعاملين.²⁴

كما يعرف، «مقدم خدمات التوثيق بأنه "جهة أو منظمة عامة أو خاصة مستقلة محايدة تقوم بدور الوسيط بين المتعاملين لتوثيق تعاملاتهم الإلكترونية بإصدار شهادات إلكترونية».²⁵

وجاء في قانون اليونيسترال النموذجي بشأن التوقيعات الإلكترونية تعريف «مقدم خدمات التصديق في المادة الثانية منه، بأنه "شخص يصدر شهادات ويجوز أن يقدم خدمات أخرى ذات صلة بالتوقيعات الإلكترونية»²⁶، أما التوجيه الأوروبي فعرفه في نص المادة 11/2، بأنه "كل شخص قانوني طبيعي أو معنوي يصدر شهادات توثيق التوقيع الإلكتروني، ويتولى خدمات أخرى مرتبطة بالتوقيع الإلكتروني».²⁷

و يظهر جليا عند النظر في القانون رقم: 04-15، أن المشرع الجزائري استمد تعريف «مقدم خدمات التوثيق من نصوص قانون اليونيسترال النموذجي بشأن التوقيعات الإلكترونية وأحكام التوجيه الأوروبي، عند قوله أنه شخص طبيعي أو معنوي يقوم بمنح شهادات تصديق إلكتروني موصوفة، و يقدم خدمات أخرى في مجال التصديق الإلكتروني».²⁸

الفرع الثاني: دور جهات التوثيق الإلكتروني في إضفاء الحماية اللازمة على التوقيع الإلكتروني

استحدثت جهة التوثيق الإلكتروني لم يكن بغرض تسهيل ومراقبة التعاملات الإلكترونية فحسب، بل يعتبر من أولوياتها ضمان الأمن القانوني وحماية التعاملات الإلكترونية وخاصة التوقيع الإلكتروني من الأخطار التي قد تواجهه بسبب طبيعة هذه المعاملات التي تتم عبر وسائط إلكترونية وبين اشخاص و متعاملين يجمعهما مجلس عقد افتراضي، و يعتبر من أهم الضمانات القانونية لحماية والمحافظة على سلامة التوقيع الإلكتروني هي اصدار شهادة التصديق الإلكتروني التي تثبت ذلك، و العمل على التحقق من هوية الشخص الموقع، بالإضافة إلى اثبات مضمون البيانات الإلكترونية وإصدار مفاتيح التشفير.

أولاً: اصدار شهادة التصديق الإلكتروني

ميز المشرع الجزائري بين الشهادة الإلكترونية البسيطة و الشهادة الإلكترونية الموصوفة في نص المادة 3 مكرر من المرسوم التنفيذي رقم : 162/07²⁹ ، وعرف الأولى بأنها : " وثيقة في شكل إلكتروني تثبت الصلة بين معطيات فحص التوقيع الإلكتروني و الموقع " . أما الثانية فهي " شهادة

إلكترونية تستجيب للمتطلبات المحددة"؛ ثم عاد المشرع الجزائري في القانون رقم : 15-04، لبيان بأكثر تفصيل الفرق بين الشهادتين، فأبقى على نفس التعريف تقريبا لشهادة التصديق في نص المادة 7/2، في حين اسهب في تعريف شهادة التصديق الإلكترونية الموصوفة بقوله أن "شهادة التصديق الإلكترونية الموصوفة هي شهادة تصديق إلكتروني تتوفر فيها المتطلبات الآتية:

1- أن تمنح من قبل طرف ثالث موثوق أو من قبل مؤدي خدمات تصديق إلكتروني طبقا لسياسة التصديق الإلكتروني الموافق عليها.

2- أن تمنح للموقع دون سواء.

3- يجب أن تتضمن على الخصوص:

أ- إشارة تدل على أنه تم منح هذه الشهادة على أساس أنها شهادة تصديق إلكتروني موصوفة.

ب- تحديد هوية الطرف الثالث الموثوق أو مؤدي خدمات التصديق الإلكتروني المرخص له الم صدر لشهادة التصديق الإلكتروني، وكذا البلد الذي يقيم فيه.

ج- اسم الموقع أو الاسم المستعار الذي يسمح بتحديد هويته.

د- إمكانية إدراج صفة خاصة للموقع عند الاقتضاء، وذلك حسب الغرض من استعمال شهادة التصديق الإلكتروني.

هـ- بيانات تتعلق بالتحقق من التوقيع الإلكتروني، وتكون موافقة لبيانات انشاء التوقيع الإلكتروني.

و- الإشارة إلى بداية ونهاية مدة صلاحية شهادة التصديق الإلكتروني.

ز- رمز تعريف شهادة التصديق الإلكتروني.

ح- التوقيع الإلكتروني الموصوف لم ، يؤدي خدمات التصديق الإلكتروني أو للطرف الثالث الموثوق الذي يمنح شهادة التصديق الإلكتروني.

ط- حدود استعمال شهادة التصديق الإلكتروني عند الاقتضاء.

ي- حدود قيمة المعاملات التي قد تستعمل من أجلها شهادة التصديق الإلكتروني عند الاقتضاء.

ك- الإشارة إلى الوثيقة التي تثبت تمثيل شخص طبيعي أو معنوي آخر عند الاقتضاء.³⁰

عند استقصاء النصوص المذكورة أعلاه يتبين لنا أن الشهادة الإلكترونية البسيطة تتطلب إجراءات ترتبط بمعطيات و معلومات تتعلق بالتحقق من توقيع شخص معين، و تؤكد هوية هذا

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

يتضح من خلال ما سبق أن كلا الشهادتين تفي بوجود ارتباط التوقيع الإلكتروني بشهادة إلكترونية والتي تصدر حصريا من جهة تصديق إلكتروني معتمدة ؛ و من ثم فلا بد من توافر شهادة التصديق الإلكتروني لكي يكون التوقيع الإلكتروني موصوفا.

و يتم التحقق من المعلومات الواردة بالشهادة عن طريق استخدام المفتاح العام لمن صدرت عنه شهادة التصديق، حيث تتضمن هذه الشهادة المفتاح العام بالإضافة إلى باقي التفاصيل التي تين أن الم وقع المحدد بالشهادة حائزا للمفتاح الخاص المناظر للمفتاح العام الوارد في الشهادة، الأمر الذي يجعل متلقى الشهادة يستخدم المفتاح العام المذكور فيها للتأكد من أن التوقيع الإلكتروني لمستحدث من المفتاح الخاص المقابل له، وأن الرسالة لم يصيها أي تغيير منذ التوقيع عليها.³¹

ثانياً: التحقق من هوية شخص الم وقع

ينص المشرع الجزائري في القانون رقم: 04-15، على أنه يجب على مؤدي خدمات التصديق الإلكتروني وقبل منح شهادة التصديق الإلكتروني أن يتحقق من تكامل بيانات الإنشاء مع بيانات التحقق من التوقيع، و يمنح مؤدي خدمات التصديق الإلكتروني شهادة أو أكثر لكل شخص يقدم طلبا وذلك بعد التحقق من هويته وعند الاقتضاء التحقق من صفاته الخاصة، أما في حالة الأشخاص المعنوية فإن مؤدي خدمات التصديق الإلكتروني يحتفظ بسجل يدون فيه هوية و صفة الممثل القانوني للشخص المعنوي الم «ستعمل للتوقيع المتعلق بشهادة التصديق الإلكتروني الموصوفة، بحيث يمكن تحديد هوية الشخص الطبيعي عند كل استعمال لهذا التوقيع الإلكتروني.³²

تعمل جهة التصديق أو مقدم أو مزود خدمات التصديق عبر إصدارها شهادة التصديق الإلكتروني من تحقيق الثقة لدى الغير بصحة البيانات التي تحتويها، وخاصة ما تعلق بهوية الم وقع و نسبة التوقيع الإلكتروني إليه، مما يدفع الم «طلع عليها إلى التعاقد بثقة و اطمئنان.³³

كما تختص جهة التوثيق بأن توفر لمن يعول على هذه الشهادة الإلكترونية الوسائل التي تثبت أن الشخص المحددة هويته في الشهادة كان يسيطر على أداة التوقيع و أنها كانت سارية المفعول وقت اجراء التوقيع.³⁴

ثالثاً: اثبات مضمون التبادل الإلكتروني

نص المشرع الجزائري على أنه يلغي مؤدي خدمات التصديق الإلكتروني شهادة التصديق الإلكتروني الموصوفة عندما يتبين أنه قد تم منحها بناء على معلومات خاطئة أو مزورة أو إذا أصبحت

المعلومات الواردة في شهادة التصديق الإلكتروني غير مطابقة للواقع، أو إذا تم انتهاك سرية بيانات إنشاء التوقيع.³⁵

يعتبر من مهام جهة التوثيق التحقق من مضمون التبادل الإلكتروني بين الأطراف وسلامته وبعده عن أي غش أو احتيال، فضلا عن إثبات وجوده ومضمونه، حيث تعمل جهة التوثيق على تعقب المواقع التجارية والتأكد من وجودها الفعلي ومصداقيتها³⁶، فإذا اتضح أن هذه المواقع غير جادة أو حقيقية تعمل على تحذير المتعاملين.

و بالتالي فإن هدف جهة التصديق هو ضمان سلامة و تأمين التعامل عبر الوسائط الإلكترونية، من حيث أطرافه ومضمونه ومحلّه وتاريخه.³⁷

رابعاً: إصدار المفاتيح الإلكترونية

من بين مهام جهة التوثيق الإلكتروني إصدار المفتاح الخاص الذي يستعمل في تشفير المعاملة الإلكترونية و المفتاح العام الذي يتم من خلاله فك هذا التشفير.³⁸

و يتولى مهمة المصادقة على هوية الحائز على المفتاح العمومي و يصدر شهادات إلكترونية من شأنها أن تضمن بأن المفتاح العمومي عائد إلى الجهة الحائزة على المفتاح الخصوصي، ومن ثم استخدام المفتاح العام لفك تشفير الرسالة الأصلية والتأكد من عدم حصول أي تعديل عليها.³⁹

ومن المهم أن نشير بعد التطرق إلى دور جهة التوثيق وفي ما يخص الجانب العملي أن وزارة البريد وتكنولوجيا الاعلام والاتصال أكدت على أنه سوف يتم إنشاء سلطات التصديق الإلكتروني قبل نهاية السنة الماضية، غير أنه يبقى الغموض يكتنف إنشاء هذا الجهاز الفعال الذي يلعب دورا مهما في بعث الثقة في التعاملات الإلكترونية.

الخاتمة:

عملت من خلال هذا البحث تسليط الضوء على الوسائل التقنية و القانونية التي أقرها المشرع في القانون رقم : 04-15، المدعمة لحماية التوقيع الإلكتروني من القرصنة الإلكترونية و الاختراقات ومنع الغير من الدخول و التقاط رسائل البيانات التي يتم تبادلها من خلال شبكة الإنترنت أو تعديلها أو تحريفها و التحايل و التزوير الإلكتروني باستعمال توقيع الغير دون علمه، وهذا من أجل الحفاظ على سريتها وخصوصيتها للأطراف باستعمال وسائل إلكترونية رقمية أو رموز معينة.

فاستمرار التجارة الإلكترونية ودوام التعامل من خلالها يفرض تنظيم تدابير وقائية للحفاظ على التوقيع الإلكتروني الذي يتطلب بنية أساسية و عالمية للمعلومات تتسم بالأمن لمنح المستخدمين الثقة والأمان من أجل تحقيق مواجهة معظم المخاطر التي تعترض مستخدمي الوسائط الإلكترونية.

و قد توصلنا إلى عدة نتائج عند عرض هذه الدراسة، من أهمها أن المشرع الجزائري وبعد صدور القانون رقم : 04-15، حاول مواكبة التطور الحاصل في حماية المعاملات الإلكترونية وازدواج الأمان القانوني على مستعملي التوقيع الإلكتروني من خلال النص على عملية التشفير الإلكتروني كوسيلة تقنية تعتمد على مفاتيح التشفير، تقي البيانات الإلكترونية من أي قرصنة خارجية تهدد سلامة المعاملات فاستخدام التشفير يحقق أكبر درجة من الأمان والحماية لمستخدمي شبكة الإنترنت نتيجة استعمال أفضل طرق التشفير التي يصعب فكها، ورغم أن المشرع لم يبين بالتفصيل آلية التشفير إلا أنه أقر العمل بهذا النظام الذي يعتبر الضامن التقني المعمول به عالميا.

كما نص المشرع إلى جانب استخدام تكنولوجيا التشفير على نظام الشهادات الموقعة الذي ينفذه طرف ثالث لتأكيد أن العميل الحقيقي هو الذي يتعامل مع الموقع من خلال إصدار شهادات إلكترونية تبين فيها نسبة التوقيع الإلكتروني لصاحبه والتأكد من هوية الموقع ومن اتصال التوقيع بالمحرر الإلكتروني وسلامته، بالإضافة إلى التثبت من سلامة البيانات الإلكترونية وإصدار المفاتيح الإلكترونية المستعملة في عملية التشفير، وبذلك يتم من خلال الجمع بين هاتين الوسيلتين - التشفير والتصديق - ضمان سرية المعاملات التجارية وحماية التوقيع الإلكتروني من أجل عقد صفقات آمنة.

وفي الأخير نذكر أهم التوصيات التي خرجنا بها فيما يلي:

- 1- حث لو ينص المشرع على نظام التشفير وأنواعه وطرق العمل به من أجل إضفاء الصبغة القانونية على هذه التقنية المهمة في ضمان المعاملات الإلكترونية.
- 2- ضرورة إنشاء سلطات التصديق الإلكتروني في أقرب وقت، لما لها من دور مهم في حماية التعاملات الإلكترونية بوجه عام والتوقيع الإلكتروني بوجه خاص.
- 3- توعية المتعاملين بأهمية أخذ الحيطة والحذر في تعاملاتهم الإلكترونية وضرورة الاستعانة بالتوقيع الإلكتروني الموصوف الذي يتميز بحماية أكبر من التوقيع الإلكتروني البسيط.
- 4- لا تكفي النصوص المنظمة للتوقيع والتصديق الإلكتروني وحدها في إضفاء الحماية اللازمة على التوقيع الإلكتروني، بل يجب على المشرع الجزائري تعديل واستحداث جميع القوانين والنصوص المرتبطة بالتعاملات الإلكترونية ؛ مثل المنظمة للممارسات التجارية والبنوك والتنظيم العقاري، وغيرها من القوانين.
- 5- ضرورة تكوين القضاة في مجال المنازعات الإلكترونية، وتنظيم ندوات وأيام تكوينية خاصة في ما تعلق بحماية البيانات الإلكترونية والتوقيع الإلكتروني.

الهوامش :

- 1- القانون رقم : 18-05، المؤرخ في 10 ماي 2018، يتعلق بالتجارة الإلكترونية، ج ر ج ج، العدد 28، المؤرخة في 16 ماي 2018.
- 2 - القانون رقم : 15-04، المؤرخ في أول فيفري 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، ج ر ج ج، العدد 06، المؤرخة في 10 فيفري 2015.
- 3 - هناك العديد من طرق الاحتيال و التعدي على البيانات الإلكترونية، أنظر نضال إسماعيل برهم، 2005، "أحكام عقود التجارة الإلكترونية"، دار الثقافة للنشر والتوزيع، الطبعة الأولى، عمان، ص 127-129.
- 4 - تنص المادة 8/2 من القانون رقم : 15-04، على ما يلي : " مفتاح التشفير الخاص، هو عبارة عن سلسلة من الأعداد يحوزها حصريا الموقع فقط، و تستخدم لإنشاء التوقيع الإلكتروني، و يرتبط هذا المفتاح بمفتاح تشفير عمومي". وتنص الفقرة التاسعة من نفس المادة ومن نفس القانون على ما يلي: "مفتاح التشفير العمومي، هو عبارة عن سلسلة من الأعداد تكون موضوعة في متناول الجمهور بهدف تمكينهم من التحقق من الإمضاء الإلكتروني و تدرج في شهادة التصديق الإلكتروني".
- 5 - الفصل الأول من مشروع قانون التجارة الإلكترونية المصري، التعريفات.
- 6 - المادة الثانية من قانون المبادلات و التجارة الإلكترونية التونسي.
- 7 - محمد فواز المطالقة، 2008، "الوجيز في عقود التجارة الإلكترونية"، دار الثقافة للنشر و التوزيع، الطبعة الأولى، الإصدار الثاني، عمان، ص 159.
- 8 - سلطان عبد الله محمود الجواري، 2010، "عقود التجارة الإلكترونية و القانون الواجب التطبيق، دراسة مقارنة"، منشورات الحلبي الحقوقية، الطبعة الأولى، بيروت، ص 202.
- 9- محمد فواز المطالقة، مرجع سابق، ص 159.
- 10- بلقاسم حامدي، 2015، " ابرام العقد الإلكتروني"، أطروحة مقدمة لنيل درجة دكتوراه العلوم في العلوم القانونية، تخصص قانون أعمال، كلية الحقوق والعلوم السياسية، جامعة باتنة، ص 239.
- 11 - سلطان عبد الله محمود الجواري، مرجع سابق، ص 201.
- 12 - أسامة بن غانم العبيدي، (دون ذكر سنة النشر) "حجية التوقيع الإلكتروني في الإثبات"، المجلة العربية للدراسات الأمنية والتدريب، المجلد 28، العدد 56، المملكة السعودية، ص 158 و 159.
- 13 - محمد فواز المطالقة، مرجع سابق، ص 161.
- 14 - أنظر كلا من المادة 1/11/أ، و المادة 42 من القانون رقم: 15-04، مرجع سابق.
- 15 - أنظر المادة 68 من القانون رقم : 15-04، نفس المرجع.
- 16 - أنظر كلا من المادة 70 و 71 من القانون رقم : 15-04، نفس المرجع.
- 17 - أنظر المادة 73 من القانون رقم: 15-04، نفس المرجع.
- 18 - أسامة بن غانم العبيدي، مرجع سابق، ص 160.
- 19 - محمد فواز المطالقة، مرجع سابق، ص 163 و 164.
- 20 - سلطان عبد الله محمود الجواري، مرجع سابق، ص 203 و 204.
- 21 - محمد فواز المطالقة، مرجع سابق، ص 165.
- 22 - أسامة بن غانم العبيدي، مرجع سابق، ص 160 و 161.

- 23 - فادي محمد عماد الدين توكّل، 2010، "عقد التجارة الإلكترونية"، منشورات الحلبي الحقوقية، الطبعة الأولى، بيروت، ص 155.
- 24 - فادي محمد عماد الدين توكّل، نفس المرجع، ص 154 و 155.
- 25 - لزهر بن سعيد، 2012، "النظام القانوني لعقود التجارة الإلكترونية"، دار هومة للطباعة والنشر والتوزيع، الجزائر، ص 172.
- 26 - <https://www.uncitral.org/pdf/Arabic>
تاريخ الاطلاع على الموقع: 2018/05/11.
- 27 - لزهر بن سعيد، مرجع سابق، ص 173.
- 28 - المادة 12/2 من القانون رقم: 04-15، مرجع سابق.
- 29 - المرسوم التنفيذي رقم: 07-162، المؤرخ في 30 ماي 2007، يعدل و يتم المرسوم التنفيذي رقم: 01-123، المؤرخ في 09 ماي 2001، والمتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية و اللاسلكية، ج ر ج، العدد 37، المؤرخة في 07 جوان 2007.
- 30 - المادة 15 من القانون رقم: 04-15، مرجع سابق.
- 31 - آلاء أحمد محمد حاج علي، 2013، "التنظيم القانوني لجهات التصديق على التوقيع الإلكتروني"، أطروحة لاستكمال متطلبات الحصول على درجة الماجستير في القانون الخاص، كلية الدراسات العليا، جامعة النجاح الوطنية نابلس، فلسطين، ص 57.
- 32 - المادة 44 من القانون رقم: 04-15، مرجع سابق.
- 33 - هلا الحسن، 2010، "تصديق التوقيع الإلكتروني"، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 26، العدد الأول، ص 531.
- 34 - زهيرة كيسي، جوان 2012، "النظام القانوني لجهات التوثيق (التصديق) الإلكتروني"، دفتر السياسة والقانون، العدد السابع، ص 216.
- 35 - المادة 45 من القانون رقم: 04-15، مرجع سابق.
- 36 - خلوي (عنان) نصيرة، 2013، "الحماية القانونية للمستهلك عبر الأنترنت - دراسة مقارنة"، مذكرة لنيل شهادة الماجستير في القانون، جامعة مولود معمري تيزي وزو، كلية الحقوق و العلوم السياسية، ص 164.
- 37 - سمير سعد رشاد سلطان، (عدم ذكر العدد و سنة الشر)، "التصديق الإلكتروني دراسة مقارنة"، مجلة كلية الحقوق، جامعة المنصورة، ص 6.
- 38 - لزهر بن سعيد، مرجع سابق، ص 177.
- 39 - محمود عبد الرحيم الشريفات، 2011، "التراضي في تكوين العقد عبر الأنترنت"، دار الثقافة للنشر والتوزيع، الطبعة الثانية، عمان، ص 204.