مجلة الباحث في العلوم القانونية و السياسية
ISSN: 2676-1955
الإيداع القانوني: جوان 2019 Al-Bahith journal in legal and political sciences
E-ISSN: 2716-7925 / العدد: الخامس الشهر: جوان / السنة: 2021

الآليات القانونية لحماية الخصوصية المعلوماتية في البيئة الافتراضية

Legal mechanisms to protect information privacy in the virtual environment

تاريخ الإرسال: 2021/04/03 تاريخ القبول: 2021/05/20

د. عقوني محمد، أستاذ محاضر أ، جامعة بسكرة.
m.aggoni@univ-biskra.dz
د. ماجري يوسف، أستاذ محاضر أ، جامعة سوق أهراس.
mdjryoucef@yahoo.com

ملخص:

تعالج هذه الدراسة آليات الحماية التي أقرها المشرع الجزائري في القانون رقم:15-04، المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين-، لحماية البيانات والمعطيات الشخصية للمتعاملين.

حيث تعتبر مسألة حماية المعطيات ذات الطابع الشخصي في البيئة الافتراضية من المواضيع المهمة، بسبب التقدم التكنولوجي الذي أدى الانتشار الواسع لهذه المعاملات، وأيضاً بسبب طبيعة البيئة الافتراضية التي تكثر فيها مخاطر الاعتداء على حرمة الحياة الخاصة، عند مباشرة عمليات جمع وتخزين البيانات الاسمية وتشغيلها ومعالجتها؛ ما جعل المشرع الجزائري يعمل على إيجاد الآليات الكفيلة ببعث الثقة والاطمئنان لدى المتعاملين عبر الوسائط الإلكترونية، لتحقيق الحماية الضرورية للمعطيات ذات الطابع الشخصي من أي اختراق أو تلاعب أو تحايل إلكتروني، بإقراره لعملية التشفير كإجراء تقني لحماية البيانات الإلكترونية والمعلومات ذات الطابع الشخصي، بالإضافة إلى العمل على تنظيم مهام جهة التوثيق الإلكتروني وتحديد مسؤولياتها.

الكلمات المفتاحية: البيانات – الإلكترونية – طابع شخصي.

Abstract:

This study deals with the protection mechanisms approved by the Algerian legislator in Law No. 15-04, which specifies general rules related to electronic signature and ratification, to protect data and data of a personal nature for customers.

Whereas, the issue of protection of data of a personal nature in the virtual environment is considered an important topic, due to the technological progress that led to the widespread spread of these transactions, and also because of the nature of the virtual environment in which the risks of attacking the privacy of private life abound, when undertaking the collection, storage, operation and processing of nominal data; What made the Algerian legislator work to find mechanisms to send confidence and confidence among customers via the

electronic media, to achieve the necessary protection for data of a personal nature from any electronic penetration, tampering or fraud, by approving the encryption process as a technical measure to protect electronic data and information of a personal nature, in addition to Work to organize the tasks of the electronic documentation authority and define its responsibilities to achieve the same purpose.

KeyWords: data, electronic, character, personal.

مقدمة:

رغم ما تقدمه الثورة الرقمية و التطور التكنولوجي في هذا المجال من رقي وازدهار، إلا أن الدخول إلى العالم الافتراضي لا يَسْلَم من تحديات جديدة تخلق عدة إشكالات، من أهمها الاختراقات الأمنية و القرصنة الإلكترونية التي قد تودي إلى عدم الثقة في استخدام البيانات الإلكترونية، وخاصة المعطيات ذات الطابع الشخصي للمتعاملين، نتيجة عدم توفر الأمن القانوني في المعاملات الإلكترونية وكذا الاستغلال غير قانوني للمعطيات ذات الطابع الشخصي أثناء المعالجة الالكترونية.

حيث تشكل المعطيات ذات الطابع الشخصي جزءاً مهماً من الحق في الحياة الخاصة التي كفل المشرع الجزائري حمايتها دستورياً طبقاً لنص الفقرة الرابعة من المادة 46 من دستور 2016، حيث نصت على ما يلي" حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي حق أساسي يضمنه القانون ويعاقب على انتهاكه."[1]

تعتبر المعطيات ذات الطابع الشخصي كل معلومة كيف ما كان نوعها بغض النظر عن دعامتها، حيث عرفها المشرع في القانون رقم: 18- 07[2]، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي في

نص المادة الثالثة، بما يلي: " بأنها كل معلومة بغض النظر عن دعامتها, متعلقة بشخص معرف أو قابل للتعرف عليه و المشار إليه أدناه،"الشخص المعني"، بصفة مباشرة أو غير مباشرة لا سيما بالرجوع إلى رقم التعريف أو عنصر أو عدة عناصر خاصة بهويته البدنية أو الفيزيولوجية أو الجينية أو البيومترية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية".

تعتبر مسألة حماية المعطيات الشخصية في البيئة الافتراضية أكثر أهمية، بسبب التقدم التكنولوجي والانتشار الواسع لهذه المعاملات، وأيضاً بسبب طبيعة البيئة الافتراضية التي تكثر فيها مخاطر الاعتداء على المعطيات و البيانات الشخصية، حيث يسهل التلاعب بالبيانات الإلكترونية التي تستغل بطريقة غير قانونية وغير أخلاقية لأغراض متعددة، سواء من طرف الجهات المعالجة لهذه البيانات والمعطيات أو من طرف الغير.

عمل المشرع الجزائري على مواكبة التطور الحاصل في مجال المعاملات الإلكترونية بإصدار قوانين تنظم المعاملات و رافقها بنصوص لحماية المعطيات الشخصية؛ فلم يكتفي بوضع الجزاءات المترتبة عن الاعتداء على المعطيات الشخصية في قانون العقوبات، و القانون رقم: 18-07 ، بل أقر أيضا آليات وقائية لحماية البيانات عموماً والمعطيات ذات الطابع الشخصي خصوصاً، وهو ما تضمنه القانون رقم : 15-04، المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين[3]، و هو مجال دراستنا.

حيث جاء القانون المذكور أعلاه بعدة نصوص تعمل على توفير الحماية اللازمة للمحرر و التوقيع الإلكترونيين الذي يتضمنا البيانات الشخصية، فلا يخفى على أحد أهمية ودور هذين الأخيرين الذين أصبحا بديلاً عن الكتابة التقليدية و التوقيع التقليدي على التوالي في اثبات التصرفات و العقود القائمة على الدعامة الإلكترونية و المساهمة في إعطاء الثقة لهذا النوع من التعاملات.

انتشار العقود و التعاملات الإلكترونية يبقى رهين بمدى توفير الحماية التقنية والقانونية الكافية لنظام التعامل الإلكتروني، لإعطاء ضمانات تُشجع المتعاملين على الولوج إلى العالم الافتراضي وهم مطمئنين على معلوماتهم و معطياتهم الشخصية 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، نصوغه كما يلي: **ما هو دور و أهمية الآليات التقنية و القانونية التي أقرها المشرع الجزائري، في تحقيق الحماية الكافية للمعطيات ذات الطابع الشخصي؟**

انطلاقا من هذا التساؤل سندرس الموضوع بالاستعانة بالمنهج التحليلي والوصفي في مطلبين:

نتناول تقنية التشفير في المطلب الأول، و دور جهات التوثيق الإلكتروني في حماية المعطيات الشخصية في المطلب الثاني.

المطلب الأول: تقنية التشفير

الكتابة و التوقيع الإلكترونيين موجودين ضمن محرر على وسيط إلكتروني، يمكن للقراصنة اختراق أنظمة المعلومات الشخصية والتقاط صورة للمحرر والتوقيع، أو فك شفرة هذا الأخير ، ثم استخدامه بدون علم صاحبه، و كذا ظهور حالات عديدة لتزوير بطاقات الائتمان، زيادة على ذلك ظهور الفيروسات التي تهدد بإتلاف الملفات المحفوظة، مما يؤدي إلى اضطراب التعامل على الوسائط الالكترونية[4]؛ وعدم توفير الحماية اللازمة للمعطيات ذات الطابع الشخصي.

وبالرجوع إلى نص المادة 38، من القانون رقم: 07/18، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، التي تقضي بما يلي " يجب على المسؤول عن المعالجة وضع التدابير التقنية والتنظيمية الملائمة لحماية المعطيات ذات الطابع الشخصي من الإتلاف العرضي أو غير المشروع أو الضياع العرضي أو التلف أو النشر أو الولوج غير المرخصين"، نجد أن المشرع أكد في نفس المادة الفقرة الثانية، على أن هذه التدابير يجب أن تضمن مستوى ملائمًا من السلامة بالنظر إلى المخاطر التي تمثلها المعالجة و طبيعة المعطيات الواجب حمايتها.

و بناء على ما تقدم وُضِعت آلية لحماية المعطيات ذات الطابع الشخصي والتوقيع الإلكتروني من أجل تأمين المعاملات الإلكترونية والتجارة الإلكترونية وتجاوز هذه الصعوبات، حيث تم اعتماد آلية التشفير لكبح مرتكبي جرائم الاختراق والتجاوزات و الاحتيال الإلكتروني قصد المساس بالبيانات الالكترونية و بالأخص المعطيات ذات الطابع الشخصي.

الفرع الأول- المقصود بالتشفير: لم يتطرق المشرع الجزائري في قانون التجارة الإلكترونية إلى تعريف التشفير، واكتفى بتعريف مفتاح التشفير الخاص ومفتاح التشفير العمومي[5] في القانون رقم: 15-04، المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق 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 تغييرها[6]، 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."[7]

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، فتنصب 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 وفكه[8]، 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 مفتاحاً سرياً بأن يحول رسالة مقروءة إلى رسالة غير مقروءة و بالعكس، أي أن يستخدم المفتاح السري بفك الشفرة و إعادة الرسالة المشفرة إلى وضعيتها الأصلية".[9]

و يتضح من خلال التعريف الأخير أن التشفير يعتمد على عمليات رياضية يتم بها تحويل النص المراد إرساله إلى رموز و إشارات لا يتاح فهم محتواها إلا بواسطة فك الشفرة و تحويل هذه الرموز والإشارات إلى نصوص مقروءة ومفهومة عن طريق استعمال مفاتيح التشفير العامة و الخاصة، و بالتالي لا يمكن أن تتم هذه العملية إلا إذا كان مُستقبل الرسالة يملك مفتاح التشفير الذي يعيد الإشارات و الرموز إلى نصه الأصلي.[10]

و بناء 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.[11]

و لا يقتصر دور التشفير على وظائف الحماية و الأمن و السرية في المعلومات الشخصية 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 المُوَقَّع عليه إلكترونيا والتأكد من سلامته، ويقصد بذلك التثبت من عدم تغييره في أثناء عبور داخل شبكة الاتصال.[12]

الفرع الثاني- ضوابط التشفير: أقر المشرع الجزائري بضرورة تشفير البيانات والمعلومات، كما نص على العمل من أجل الحفاظ على سرية البيانات و المعلومات المشفرة، بالإضافة إلى اعتباره أن النص المشفر محرراً إلكترونياً، وسوف نتناول كل هذه الضوابط بأكثر تفصيل فيما يلي:

أولا: 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، وعرف التشفير الخاص والعام، و أجاز استخدامه في المراسلات الإلكترونية و التعاملات الإلكترونية التجارية.

و أكد حماية البيانات المشفرة والعناصر المستخدمة في عملية التشفير و فكها 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.[13]

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 تناولا عملية التشفير بشكل مباشر من خلال نصوص خاصة تجنبا لاختلاف التفاسير و الاجتهادات الفقهية بشأنها.[14]

ثانيا: الحق في الحفاظ على سرية البيانات و المعلومات المشفرة: اعتبر المشرع الجزائري من خلال القانون رقم : 15- 04، على أن الاعتداء على البيانات المرسلة بين طرفي العقد عبر الوسائط الإلكترونية هو اعتداء على خصوصية وسرية البيانات و المعلومات المرسلة بين طرفي العلاقة.

حيث نص المشرع على أنه لا يمكن للغير الاطلاع على المعطيات ذات الطابع الشخصي الخاضعة للمعالجة إلا من أجل انجاز الغايات المرتبطة مباشرة بمهام المسؤول عن المعالجة و المرسل إليه، ولا يشترط موافقة الشخص المعني إذا كانت المعالجة ضرورية لتنفيذ عقد يكون الشخص المعني طرفًا فيه أو من أجل تنفيذ إجراءات سابقة للعقد اتخذت بناءً على طلبه[15]؛ 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 والمعلومات المتعلقة بشهادات التصديق الإلكتروني الممنوحة.[16]

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 الغير [17] ، أو من طرف مؤدي خدمات التصديق الإلكتروني.[18] أو من طرف الشخص المكلف بالتدقيق.[19]

و يبقى أن نشير و في ما تعلق بتقنية التشفير، ضرورة مواكبة التطور السريع للتكنولوجيا، فما يبدوا 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 محرراً إلكترونياً: نتيجة إقرار المشرع للنص المشفر وحجيته 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.[20]

الفرع الثالث– طرق التشفير: يمكن تصنيف تقنيات التشفير في مجال المعلوماتية إلى فئتين رئيسيتين بالنظر إلى نوعية المفتاح المستخدم في التشفير.

أولا: المفتاح الخصوصي (تقنية التشفير المتماثل): هو نظام الكتابة المشفرة بالمفتاح الخصوصي، يعمل بواسطة مفتاح واحد يُعْرفُ بالخصوصي يمتلكه كل من مُرسِل الرسالة و مُتلقيها، و بالتالي 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 الأخر ولكي يتمكن

من قراءتها لا بد من إزالة الغموض وبيان الرسالة على شكلها الأصلي عن طريق استخدام كلمة المرور التي تمت بها عملية التشفير.[21]

يعاب على هذه التقنية استعمال المفتاح ذاته من قبل شخصين مختلفين (المُرسِل و المُرسَل إليه)، وهذا قد يضُعِف من حجية المستندات الرقمية و التوقيع الإلكتروني و قوتها الثبوتية، على أساس الخطر الدائم في أن يكون المفتاح الخصوصي قد سُرب 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 مُتلقي الرسائل المشفرة القادمة من مصادر مختلفة، عليه أن يقتني عددا من المفاتيح الخصوصية يوازي عدد الرسائل الواردة من هذه المصادر و هو ما يعتبر أمرا مرهقًا.[22]

ثانيا: المفتاح العمومي(التشفير غير المتماثل): خلافا للتشفير بالمفتاح الخصوصي لا يستعمل المفتاح ذاته من أجل تشفير الرسائل، بحيث أنه يُستعمل مفتاحين سريين مختلفين من أجل فك تشفيرها، الأول خصوصي يملكه مُستخدم معين لمستعمل الوسائط الإلكترونية و يبقيه سريا وخاصا به، أما الثاني عمومي يوزعه إلى المتعاملين الآخرين الذي يود تَلقي رسائل مشفرة منهم.[23]

و بالتالي يتم الاستعانة بمفتاحين مختلفين 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 بالمُوقِع و استعماله في التعرف على محتوى الرسالة، و المفتاح الخاص يكون

معروفا لدى جهة واحدة فقط و هو المُرسِل و يستعمل لتشفير الرسالة أو فك تشفيرها ، أما المفتاح العام فعادة ما يكون معروفا لدى أكثر من جهة أو شخص.[24]

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 تَلقاها. و رغم 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 و مستقلة تتثمل في جهة التصديق الإلكتروني.[25]

المطلب الثاني: دور جهات التوثيق الإلكتروني في حماية المعطيات الشخصية

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

استحداث جهة التوثيق الإلكتروني لم يكن بغرض تسهيل ومراقبة التعاملات الإلكترونية فحسب، بل يعتبر من أولوياتها ضمان الأمن القانوني وحماية التعاملات الإلكترونية وخاصة التوقيع الإلكتروني و المعطيات ذات الطابع الشخصي من الأخطار التي قد تواجهه بسبب طبيعة هذه المعاملات التي تتم عبر وسائط إلكترونية وبين اشخاص و متعاملين يجمعهما مجلس عقد افتراضي، و هو ما نص علية المشرع في القانون رقم:18-07، بالقول: إذا أدت معالجة المعطيات ذات الطابع الشخصي في شبكات الاتصال الإلكترونية المفتوحة للجمهور إلى إتلافها أو ضياعها

أو افشائها أو الولوج غير المرخص إليها، وجب أن يُعلِم مُقدم الخدمات فوراً السلطة الوطنية و الشخص المعني، إذا أدى هذا إلى المساس بحياته الشخصية، ما لم ترى السلطة الوطنية أن الضمانات الضرورية لحماية المعطيات قد تم اتخاذها من طرف مؤدي الخدمات.[26]

و يعتبر من أهم الضمانات القانونية لحماية و المحافظة على سلامة المحرر المتضمن المعطيات ذات الطابع الشخصي و التوقيع الإلكتروني هي اصدار شهادة التصديق الإلكتروني التي تثبت ذلك، و العمل على التحقق من هوية الشخص المُوقِع، بالإضافة إلى اثبات مضمون البيانات الإلكترونية وإصدار مفاتيح التشفير.

الفرع الأول: اصدار شهادة التصديق الإلكتروني

ميز المشرع الجزائري بين الشهادة الإلكترونية البسيطة و الشهادة الإلكترونية الموصوفة في نص المادة 3 مكرر من المرسوم التنفيذي رقم : 162/07[27]، وعَرَّفَ الأولى بأنها : " وثيقة في شكل إلكتروني تثبت الصلة بين معطيات فحص التوقيع الإلكتروني و المُوقِع." أما الثانية فهي" شهادة إلكترونية تستجيب للمتطلبات المحددة"؛ ثم عاد المشرع الجزائري في القانون رقم : 15-04، ليبين 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 تُمنح من قبل طرف ثالث موثوق أو من قبل مُؤدي خدمات تصديق إلكتروني طبقا لسياسة التصديق الإلكتروني الموافق عليها.

2- أن تُمنح للمُوقِع دون سواه.

3- يجب أن تتضمن على الخصوص:

أ- اشارة 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 المُصدِر لشهادة التصديق الإلكتروني، و كذا البلد الذي يقيم فيه.

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

د- امكانية ادراج صفة خاصة للمُوقِع 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 و نهاية مدة صلاحية شهادة التصديق الإلكتروني.

ز- رمز تعريف شهادة التصديق الإلكتروني.

ح- التوقيع الإلكتروني الموصوف لمُؤدي 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.[28]

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 بوجوب ارتباط التوقيع الإلكتروني بشهادة إلكترونية والتي تصدر حصريًا من جهة تصديق إلكتروني معتمدة ؛ و من ثم فلا بد من توافر شهادة التصديق الإلكتروني لكي يكون التوقيع الإلكتروني موصوفاً.

اشترط المشرع في القانون رقم: 18-07، المذكور أعلاه، أن يتم الحصول على المعطيات ذات الطابع الشخصي التي يتم جمعها قِبَل مؤدي خدمات التصديق

الالكتروني لأغراض تسليم و حفظ الشهادات المرتبطة بالتوقيع الإلكتروني من الأشخاص المعنيين بها مباشرة، ما عدا في حالة موافقتهم الصريحة، كما لا يجوز معالجتها لأغراض غير تلك التي جمعت من لأجلها.[29]

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 تُبين أن المُوقِع المحدد بالشهادة حائزا للمفتاح الخاص المناظر للمفتاح العام الوارد في الشهادة، الأمر الذي يجعل مُتلقى الشهادة يستخدم المفتاح العام المذكور فيها للتأكد من أن التوقيع الإلكتروني أُسْتحدث من المفتاح الخاص المقابل له، وأن الرسالة لم يصبها أي تغيير منذ التوقيع عليها.[30]

الفرع الثاني- التحقق من هوية الشخص المُوقِع: ينص المشرع الجزائري في القانون رقم:15-04، على أنه يجب على مُؤدي 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 المُستعمل للتوقيع المتعلق بشهادة التصديق الإلكتروني الموصوفة، بحيث يمكن تحديد هوية الشخص الطبيعي عند كل استعمال لهذا التوقيع الإلكتروني.[31]

تعمل جهة التصديق أو مُقدم أو مُزود خدمات التصديق عبر إصدارها شهادة التصديق الإلكتروني من تحقيق الثقة لدى الغير بصحة البيانات التي تحتويها، وخاصة ما تعلق بهوية المُوقِع و نسبة التوقيع الإلكتروني إليه، مما يدفع المُطلِع عليها إلى التعاقد بثقة و اطمئنان.[32]

كما تختص جهة التوثيق بأن توفر لمن يُعول 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.[33] فضلاً عن هذا، نص القانون رقم:18-07، على ضرورة قيام كل مُقدم خدمات بمسك جرداً محيناً حول الانتهاكات المتعلقة بالمعطيات ذات الطابع الشخصي و الإجراءات التي اتخذها بشأنها.[34]

الفرع الثالث- إثبات 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 اثبات وجوده ومضمونه، حيث تعمل جهة التوثيق على تعقب المواقع التجارية و التأكد من وجودها

الفعلي ومصداقيتها[36] ، 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 و مضمونه و محله و تاريخه.[37]

الفرع الرابع- إصدار المفاتيح الإلكترونية: من بين مهام جهة التوثيق الإلكتروني اصدار 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]

الخاتمة:

عملت من خلال هذا البحث تسليط الضوء على الوسائل التقنية و القانونية التي أقرها المشرع في القانون رقم : 15-04، المدعمة لحماية البيانات والمعطيات الشخصية من القرصنة الإلكترونية و الاختراقات ومنع الغير من الدخول و التقاط رسائل البيانات التي يتم تبادلها من خلال شبكة الإنترنت أو تعديلها أو تحريفها والتحايل 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 المعطيات الشخصية للمتعاملين و المحرر و التوقيع الإلكتروني الذين يتطلبان بنية أساسية و عالمية للمعلومات تتسم بالأمن لمنح المستخدمين الثقة و الأمان 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 : 15-04، حاول مواكبة التطور الحاصل في حماية المعاملات الإلكترونية و المعطيات الشخصية وإضافة الأمان القانوني على مستعملي المحرر و 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 الآمن و الحماية 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 المُوَثَّقة الذي ينفذه طرف ثالث لتأكيد أن العميل الحقيقي هو الذي يتعامل مع المُوقِع من خلال اصدار شهادات إلكترونية تبين فيها نسبة التوقيع الإلكتروني لصاحبه

والتأكد من هوية المُوقِع 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 و التصديق- ضمان سرية البيانات الشخصية و المعاملات التجارية وحماية المحرر و التوقيع الالكتروني من اجل عقد صفقات آمنة.

وفي الأخير نذكر **أهم التوصيات** التي خرجنا بها فيما يلي:

1- حبذ لو ينص المشرع على آلية التشفير و أنواعه وطرق العمل به من أجل إضفاء الصبغة القانونية على هذه التقنية المهمة في ضمان سلامة المعطيات الشخصية و المعاملات الإلكترونية.
2- توعية المتعاملين بأهمية أخذ الحيطة و الخذر في تعاملاتهم الإلكترونية وضرورة الاستعانة بالتوقيع الإلكتروني الموصوف الذي يتميز بحماية أكبر من التوقيع الإلكتروني البسيط.
3- ضرورة تكوين القضاة في مجال المنازعات الإلكترونية، وتنظيم ندوات و أيام تكوينية خاصة في ما تعلق بحماية البيانات الإلكترونية والمعطيات الشخصية للمتعاملين في البيئة الإلكترونية.

قائمة المصادر و المراجع:

أولا: المصادر

1- المرسوم التنفيذي رقم :07-162، المؤرخ في 30 ماي 2007 ، يعدل و يتمم 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 ج، العدد 37، المؤرخة في 07 جوان 2007.

2- القانون رقم : 15-04، المؤرخ في أول فيفري2015، **يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين**، ج ر ج ج، العدد 06، المؤرخة في 10 فيفري2015.

3- القانون رقم: 18-07، المؤرخ في 10 يونيو سنة 2018، **المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي**، ج ر ج ج، العدد 34 المؤرخة في 10 يونيو سنة 2018.

ثانيا: المراجع

أ-الكتب

1- سلطان عبد الله محمود الجواري، 2010،"**عقود التجارة الإلكترونية و القانون الواجب التطبيق، دراسة مقارنة**"، منشورات الحلبي الحقوقية، الطبعة الأولى، بيروت.

2- فادي محمد عماد الدين توكل، 2010،"**عقد التجارة الإلكترونية**"، منشورات الحلبي الحقوقية، الطبعة الأولى، بيروت.

3- محمد فواز المطالقة، 2008، "**الوجيز في عقود التجارة الإلكترونية**"، دار الثقافة للنشر والتوزيع، الطبعة الأولى، الإصدار الثاني، عمان.

4- محمود عبد الرحيم الشريفات، 2011،" **التراضي في تكوين العقد عبر الانترنت**"، دار الثقافة للنشر والتوزيع، الطبعة الثانية، عمان.

5- نضال إسماعيل برهم، 2005، "**أحكام عقود التجارة الالكترونية**"، دار الثقافة للنشر والتوزيع، الطبعة الأولى، عمان.

6- لزهر بن سعيد، 2012، "**النظام القانوني لعقود التجارة الالكترونية**"، دار هومة للطباعة والنشر والتوزيع، الجزائر.

ب - الرسائل العلمية

1- آلاء أحمد محمد حاج علي، 2013، "**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- بلقاسم حامدي، 2015،" **ابرام العقد الإلكتروني**"، أطروحة مقدمة لنيل درجة دكتوراه العلوم في العلوم القانونية، تخصص قانون أعمال، كلية الحقوق والعلوم السياسية، جامعة باتنة.

3- 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.

ج- المقالات العلمية

1- أسامة بن غانم العبيدي، (دون ذكر سنة النشر)"حجية التوقيع الإلكتروني في الإثبات "، **المجلة العربية للدراسات الأمنية والتدريب**، المجلد 28، العدد 56، المملكة السعودية.

2- زهيرة كيسي، جوان 2012،" النظام القانوني لجهات التوثيق (التصديق) الالكتروني"، **دفتر السياسة والقانون**، العدد السابع.

3- سمير سعد رشاد سلطان، (عدم ذكر العدد و سنة الشر)،" التصديق الإلكتروني دراسة مقارنة"، **مجلة كلية الحقوق**، جامعة المنصورة.

4- هلا الحسن، 2010،" تصديق التوقيع الالكتروني"، **مجلة جامعة دمشق للعلوم الاقتصادية والقانونية**، المجلد 26، العدد الأول.

الهوامش:

[1] – القانون رقم : 16-01 المؤرخ في 06 مارس 2016، **يتضمن التعديل الدستوري**، ج ر ج ج ، العدد 14 المؤرخة في 7 مارس 2016.

[2] – القانون رقم: 18-07، المؤرخ في 10 يونيو سنة 2018، **المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي**، ج ر ج ج، العدد 34 المؤرخة في 10 يونيو سنة 2018.

[3] – القانون رقم : 15-04، المؤرخ في أول فيفري2015، **يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين**، ج ر ج ج، العدد 06، المؤرخة في 10 فيفري2015.

[4] – هناك العديد من طرق الاحتيال و التعدي على البيانات الإلكترونية، أنظر نضال إسماعيل برهم، 2005، "**أحكام عقود التجارة الالكترونية**"، دار الثقافة للنشر والتوزيع، الطبعة الأولى، عمان، ص127-129.

[5] – تنص المادة 8/2 من القانون رقم : 15-04، على ما يلي :" مفتاح التشفير الخاص، هو عبارة عن سلسلة من الأعداد يحوزها حصريا المُوقِّع 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 سلسة من الأعداد تكون موضوعة في متناول الجمهور بهدف تمكينهم من التحقق من الإمضاء الإلكتروني و تدرج في شهادة التصديق الالكتروني."

[6] – الفصل الأول من مشروع **قانون التجارة الإلكترونية المصري**، التعريفات، راجع نصوص مشروع القانون لدى محمد أمين الرومي ، التعاقد الالكتروني عبر الانترنت ، دار المطبوعات الجامعية ، الطبعة الأولى، 2004.

[7]– المادة الثانية من القانون رقم: 83 لسنة 2000، المؤرخ في 09 أوت 2000، المتعلق **بالمبادلات التجارية الإلكترونية التونسي**، منشور بجريدة الرائد الرسمي في تونس، بتاريخ 11 أوت 2000، أنظر الموقع الإلكتروني: www.c-justice T.n/fleadmin.

[8] – محمد فواز المطالقة، 2008، "**الوجيز في عقود التجارة الإلكترونية**"، دار الثقافة للنشر و التوزيع، الطبعة الأولى، الإصدار الثاني، عمان، ص 159.

[9] – سلطان عبد الله محمود الجواري، 2010،"**عقود التجارة الإلكترونية و القانون الواجب التطبيق، دراسة مقارنة**"، منشورات الحلبي الحقوقية، الطبعة الأولى، بيروت، ص202.

[10]– محمد فواز المطالقة، مرجع سابق ، ص 159.

[11]– 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.

[12] – سلطان عبد الله محمود الجواري، مرجع سابق، ص201.

[13] – 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 158و 159.

[14] – محمد فواز المطالقة، مرجع سابق، ص 161.

[15] – المادة 7 من القانون رقم: 18- 07، مصدر سابق.

[16] – أنظر كلا من المادة 1/11/أ، و المادة 42 من القانون رقم: 15-04، مصدر سابق.

[17] – أنظر المادة 68 من القانون رقم : 15-04، نفس المصدر.

[18] – أنظر كلا من المادة 70و 71 من القانون رقم : 15-04، نفس المصدر.

[19] – أنظر المادة 73 من القانون رقم: 15-04، نفس المصدر.

[20] – أسامة بن غانم العبيدي، مرجع سابق، ص 160.

[21] – محمد فواز المطالقة، مرجع سابق، ص 163 و164.

[22] – سلطان عبد الله محمود الجواري، مرجع سابق، ص 203 و204.

[23] – محمد فواز المطالقة، مرجع سابق، ص 165.

[24] – أسامة بن غانم العبيدي، مرجع سابق، ص 160و 161.

[25] – فادي محمد عماد الدين توكل، 2010،"**عقد التجارة الإلكترونية**"، منشورات الحلبي الحقوقية، الطبعة الأولى، بيروت، ص155.

[26]– أنظر الفقرة الأولى من المادة 43، من القانون رقم: 18-07، مصدر سابق.

[27] – المرسوم التنفيذي رقم :07-162، المؤرخ في 30 ماي 2007 ، يعدل و يتمم 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 ج، العدد 37، المؤرخة في 07 جوان 2007.

[28] – المادة 15 من القانون رقم : 15-04، مصدر سابق.

[29] – أنظر المادة 42، من القانون رقم: 18-07، مصدر سابق.

[30] – آلاء أحمد محمد حاج علي، 2013، "**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، ص 57.

[31] – المادة 44 من القانون رقم : 15-04، مصدر سابق.

[32] – هلا الحسن، 2010،" تصديق التوقيع الالكتروني"، **مجلة جامعة دمشق للعلوم الاقتصادية والقانونية**، المجلد 26، العدد الأول، ص 531.

[33] – زهيرة كيسي، جوان 2012،" النظام القانوني لجهات التوثيق (التصديق) الالكتروني"، **دفتر السياسة والقانون**، العدد السابع، ص216.

[34] – الفقرة الثانية من المادة 43، من القانون رقم: 18-07، مصدر سابق.

[35] – المادة 45 من القانون رقم : 15-04، مصدر 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، 2012، "**النظام القانوني لعقود التجارة الالكترونية**"، دار هومة للطباعة والنشر والتوزيع، الجزائر، ص 177.

[39] – محمود عبد الرحيم الشريفات، 2011،" **التراضي في تكوين العقد عبر الانترنت**"، دار الثقافة للنشر والتوزيع، الطبعة الثانية، عمان، ص 204.