# دور التشفير وشهادات المصادقة الإلكترونية في حماية الدفع الإلكتروني

# The role of encryption and electronic authentication certificates in protecting electronic payment

**الدكتورة حسينة عبد الحميد شرون**
جامعة محمد خيضر. بسكرة.الجزائر
مخبر الاجتهاد القضائي

**الدكتورة صـونيا مقـــري**
جامعة محمد خيضر. بسكرة. الجزائر
مخبر الاجتهاد القضائي

**تاريخ استلام المقال** : 2021-11-02 **تاريخ القبول** : 2022-04-21 **المؤلف المراسل** : **حسينة عبد الحميد شرون**

**الملخص:**

يمكن أن يتعرض استعمال وسائل الدفع الإلكتروني لعدد من المخاطر ذات الطابع الأمني، مما يترك أثراً بالغاً في ثقة المتعاملين بهذه الوسائل. ومن شأن إغفال معالجة هذه المخاطر أن يشجع أكثر على تعريض هذه الوسائل للضرر، وهو ما يجعل مستقبل العمل بوسائل الدفع الإلكتروني مهدداً.

ولا يقتصر الأمر على تطوير تقنيات جديدة لمواجهة هذه المخاطر، بل يلتزم كذلك إيجاد ضمانات كفيلة بإرساء الأمان القانوني للتعامل بوسائل الدفع الإلكتروني، وقد تكون هذه الضمانات من الجهة نفسها التي توفر هذا الأمان، لكن غالباً ما تكون من جهة ثالثة.

لذلك سيتم التطرق خلال هذا البحث لتشفير البيانات كوسيلة لتأمين الدفع الإلكتروني، ليتسنى لنا البحث عن دور جهات المصادقة الإلكترونية في حماية الدفع الإلكتروني، من خلال البحث عن الدور الذي تؤديه شهادات المصادقة الإلكترونية في هذا المجال.

**الكلمات المفتاحية:** التشفير الإلكتروني- شهادة المصادقة الإلكترونية- الدفع الإلكتروني- جهة المصادقة الإلكترونية- التشفير المتماثل.

**Abstract**

The use of electronic payment methods may be exposed to a number of security-related risks, which shakes the confidence of dealers in these means. Ignoring these risks will encourage further exposure to these ways of harm, the

fact that threatens the future of e-payment methods. It is not only limited to developing new technologies to address these risks, but is also committed to finding guarantees that can establish legal security for dealing with e-payment methods. These guarantees may come from the same party that provides this security, but they often come from a third party. Therefore, during this research, we will discuss data encryption as a means to secure e-payment, so that we can search for the role of electronic authenticators in protecting electronic payment, by researching the role that electronic authentication certificates play in this field.

**Keywords**: Electronic Encryption - Electronic Authentication Certificate - Electronic Payment - Electronic Authentication Bodies - Symmetric Encryption.

**مقدمة**

أدى الانتشار الواسع الذي شهدته التكنولوجيا الإلكترونية الحديثة ومنها الحاسب الآلي والإنترنت، إلى ازدهار التجارة الإلكترونية التي اعتمدت هذه الوسائل إلى حد كبير، مما استتبع ذلك ظهور وسائل دفع في صورتها الإلكترونية، هذه الأخيرة لها دور كبير في إطار التجارة الإلكترونية، إلا أنه يمكن اعتبار أن هذه التكنولوجيا سلاح ذو حدين، فبالإضافة إلى مزاياها ووظائفها المتعددة، إلا أنه يمكن لمستعمليها أن يصيبوا البيئة الإفتراضية بعدة اختلالات جراء تدخلاتهم التي تشكل خطراً على استمرارية هذه الوسائل والثقة المطلوب توافرها لإقناع المستهلكين باستخدامها.

وتتعدد المخاطر التي تهدد مستخدمي وسائل الدفع الإلكتروني، فيمكن أن تكون من طرف الأشخاص المتدخلين في الصفقات أو من الغير، كما قد تنجم عن طبيعة هذه الوسائل التي يمكن أن تكون عبارة عن خدمات مالية تعتمد التكنولوجيا الحديثة في أداء مهامها والتي تكون في الكثير من الأحيان في بيئة مفتوحة كالإنترنت.

وإزاء هذه المخاطر الناجمة عن استعمال وسائل الدفع الإلكترونية، فإنه يجب ألا تبقى مجردة من أي ضوابط تحد من استمرارها، لذلك تتجه الهيئات المنظمة الراعية لقطاعات وسائل الدفع الإلكترونية ومن وراءها المشرعين إلى وضع القوانين والمعايير والوسائل التكنولوجية التي يجب مراعاتها والعمل بموجبها في سبيل الحد من هذه المخاطر، وإذا أمكن الأمر العمل على تلافي حدوثها، ومن بين هذه الوسائل التكنولوجية التي وجدت لمحاولة الحد من أساليب الغش والاحتيال والاعتداء عليها، هي التشفير الإلكتروني وشهادات المصادقة الإلكترونية (المصادقة الإلكترونية).

وبالتالي فالإشكالية التي يثيرها هذا الموضوع تتعلق **بمدى فعالية هذه الوسائل التكنولوجية في حماية الدفع الإلكترونية؟**

ويتفرع عن الإشكالية الرئيسية إشكاليات فرعية والمتمثلة في:

1- ما معنى تشفير البيانات؟ وماهي أنواعه؟

2- ماهي الجهات المختصة بإصدار شهادات المصادقة الإلكترونية؟

3- ماهي أنواع شهادات المصادقة الإلكترونية؟

ومن أجل الإحاطة بكل الجوانب القانونية للموضوع، فقد اعتمدت في هذه الدراسة على:

**المنهج الوصفي التحليلي**: وذلك من خلال مناقشة النصوص القانونية التي تناولت موضوع التشفير الإلكتروني وتحليلها. إضافة الى مناقشة الآراء الفقهية المتعددة ذات العلاقة سواء تلك الواردة في الكتب المتخصصة أو التي نوقشت في الدراسات والأبحاث.

**المنهج المقارن**: وذلك بعرض ومقارنة بعض النصوص القانونية المنظمة لهذا الموضوع لبعض تشريعات العديد من الدول والمنظمات الدولية والإقليمية.

للإجابة على كل التساؤلات المطروحة قمت بتقسيم الدراسة إلى مطلبية أساسيين:

**المطلب الأول: تشفير البيانات كوسيلة لتأمين الدفع الإلكتروني**

**المطلب الثاني: دور شهادات المصادقة الإلكترونية في حماية الدفع الإلكتروني**

## المطلب الأول: تشفير البيانات كوسيلة لتأمين الدفع الإلكتروني

إن التشفير ليس حديثا، فالكتابة المشفرة واستخدام الشيفرات في الرسائل موجود منذ زمن طويل حيث كانت تستعمل للأغراض العسكرية والاستخبارية أو الدبلوماسية وغيرها من الأغراض، التي[1] كانت تقدرها الدول بالنظر إلى أمن وسلامة وسرية المعلومات المتبادلة. وتعود عمليات التشفير تاريخيا إلى عصر يوليوس قيصر الذي استخدم رمزاً للتشفير يتضمن إزاحة أحرف النص المراد تشفيره عددا محدداً من الخانات، وعلى مدار التاريخ دار صراع بين مطوري علم التشفير وبين أولئك الذين يسعون لكسره واختراعه وقد تطور هذا العلم من شكله البسيط حتى وصل إلى تقنيات غاية في التعقيد والقوة بحيث يصعب كسرها أو اختراقها الأمر الذي أدى إلى ظهور عملية التوقيع الرقمي كتطبيق لتقنيات التشفير عالية التقنية من ناحية الأمن والسرية [2].

وفي مجال الإنترنت، لم يعد التشفير مقتصرا على الأغراض العسكرية أو الدبلوماسية فعالمية الشبكة استوجبت إطلاق هذا النوع من أساليب التأمين لخدمة الأغراض الشخصية للناس حتى أصبحت وظائفها تتعدى ذلك فتمتد لتشمل مختلف المراسلات العادية المتبادلة عبرها فتعمل على ابراز هوية مرسلها والمصادقة على مضمونها والتأكيد على مدى سلامتها وعدم المساس بها [3]. وقد وردت العديد من التعاريف للتشفير من قبل الفقه والتشريعات المقارنة، نبدئها أولاً بالتعريف الفقهي في (**الفرع الأول**) ثم بالتعريف القانوني في (**الفرع الثاني**)، وإلى دراسة أنواعه في (**الفرع الثالث**).

**الفرع الأول: التعريف الفقهي للتشفير الإلكتروني**

يعرف التشفير بأنه: «آلية يتم بمقتضاها ترجمة معلومة مفهومة إلى معلومة غير مفهومة عبر تطبيق بروتوكولات سرية قابلة للانعكاس، أي يمكن ارجاعها إلى حالتها الأصلية» [4].

كذلك عرف على أنه: «عملية حسابية معقدة يتم بمقتضاها تحويل النص المقروء إلى رموز واشارات غير مقروءة على نحو يحقق أمن المعلومات وسريتها» [5]. أو أنه: «تحويل للكتابة من نمطها التقليدي المقروء إلى كودات سرية أي في شكل رموز وعلامات غير مقروءة» [6].

ومن هنا يمكن القول إن مبدأ التشفير يقوم على تحويل بيانات المحرر الإلكتروني إلى صيغة غير مقروءة، لذلك فهي تدعى أيضا عملية الترميز والتي تتضمن تطبيقات لمعادلات رياضية يتم بها تحويل النص المراد تحويله إلى رموز وإشارات لا يمكن فهمها باستخدام التشفير [7]. ويقوم التشفير على الضوابط التالية:

1-إباحة تشفير البيانات والمعلومات التي يتم تدوينها أو التعامل فيها من خلال الوسائط الإلكترونية.

2-احترام سرية البيانات المشفرة والاعتراف بحق مالكيها في سريتها بتجريم الاعتداء عليها.

3-استخدام التشفير كوسيلة معتبرة قانونا، في شأن تحرير البيانات والمعلومات بواسطة الجهات المختصة [8].

**الفرع الثاني: التعريف القانوني للتشفير الإلكتروني**

عرف قانون المبادلات والتجارة الإلكترونية التونسي في الفصل الثاني من الباب الأول على أنه: «إما استعمال رموز أو إشارات غير متداولة تصبح بمقتضاها المعلومات المرغوب

تمريرها أو ارسالها غير قابلة للفهم من قبل الغير أو استعمال رموز أو إشارات لا يمكن الوصول إلى المعلومة بدونها»[9] .

أما المشرع المصري فقد أباح تشفير البيانات والمعلومات التي يتم تدوينها أو التعامل عليها من خلال الوسائط الإلكترونية، وذلك كأسلوب يحقق تأمين المعاملات التجارية وبالتالي ازدهارها رغم أن قانون التوقيع الإلكتروني المصري رقم 15 لسنة 2004 جاء خاليا من تعريف التشفير، إلا أنه ترك هذه المسألة ليتم تنظيمها بأحكام اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري رقم 109 لسنة 2005 وذلك بوضع القواعد والضوابط الخاصة بتشفير المحررات والبيانات الإلكترونية، وكذلك وضع القواعد الخاصة بتشفير التوقيع الإلكتروني وبيانات الائتمان وغيرها من البيانات التي يتم تحريرها أو نقلها على وسائط إلكترونية، وفقا للمعايير الفنية والتقنية المنصوص عليها في اللائحة التنفيذية للقانون والمشار إليها في الملحق الفني والتقني لهذه اللائحة [10].

وفي الجزائر، فقد صدر المرسوم التنفيذي رقم 09-410[11]، إذ بينت المادة الأولى منه الهدف من هذا المرسوم، وهو تحديد قواعد الأمن المطبقة على النشاطات المتعلقة بالتجهيزات الحساسة وكذا شروط وكيفيات ممارسة هذه النشاطات. ولقد أطلق المشرع في صلب المرسوم على التشفير مصطلح " **الترميز**" الذي أخضعه لنظام الرخصة من قبل سلطة ضبط البريد والمواصلات. ولقد أصدرت سلطة ضبط البريد والموصلات في 2012/06/11قرار حدد المدة القانونية لرخصة استغلال تقنيات التشفير المصنفة في القسم الفرعي 3 من القسم أ من المرسوم التنفيذي رقم 09-410 الذي يحدد قواعد الأمن المطبقة على النشاطات المتعلقة بالتجهيزات الحساسة السالف ذكره، والتي تم تحديديها بثلاث سنوات، ويمكن تجديدها بطلب صريح عبر البريد مع اشعار بالوصول في أجل أقصاه 30 يوما قبل انتهاء أجل الرخصة ويتم تجديدها في أجل أقصاه سنتين[12].

**الفرع الثالث: أنواع التشفير**

يتمثل التشفير من الناحية الفنية في إعادة كتابة رسالة البيانات قبل تصديرها باستخدام رمز أو مفتاح معين، يفرض الربط بين البيانات والأرقام، على أن تتوفر لدى المرسل إليه القدرة على إستعادة الرسالة في صورتها الأصلية قبل تشفيرها، وقد يكون الرمز أو المفتاح متماثلاً أو غير متماثل [13].

**1-التشفير المتماثل (المفتاح العام)**: وهو التشفير الذي غالباً ما يعتمد فيه على (شفرة القيصر) التي تقوم على أساس استبدال النص بأحرف تقابله وهذا بالمرور على عدة مراحل للوصول إلى النص المشفر. ويستخدم فيه صاحب الرسالة المفتاح الخاص ذاته لإنشاء التوقيع ولفكه بعد الاتفاق المسبق مع المرسل إليه على كلمة السر بينهما[14]. ويتضمن المفتاح الذي تم إنشاؤه للمرور حروف كبيرة وصغيرة ورموز أخرى بحسب ما ينتج عن الخوارزمية التي تم انشاؤها وعقب ذلك تحول برمجيات التشفير كلمة المرور الى عدد ثنائي ليتم بعد ذلك إضافة رموز أخرى لزيادة طولها، ويشمل العدد الثنائي مفتاح تشفير الرسالة التي تمت والذي سوف يستخدم في المستقبل لفك الشفرة نفسها[15].

**2-التشفير اللامتماثل (المفتاح العام والخاص)**: في هذا النوع من التشفير يتم استخدام نوعين من المفاتيح المفتاح الخاص والمفتاح العام، فالأول يكون معروفا فقط لدى الشخص القادر على تشفير المعلومة وفك شفرتها ويبقى سريا، أما الثاني فيكون معروفا لدى أكثر من جهة ويستطيع فك شيفرة الرسالة التي شفرها المفتاح الخاص[16]. وهنا بإمكان جميع الحائزين على المفتاح العام استخدامه في تشفير الرسائل وارسالها إلى المستخدم الحائز على مفتاح خاص[17]. ويعتمد التشفير اللامتماثل على إرسال الرسالة المشفرة بالمفتاح الخاص وتكون غير قابلة للقراءة ولا يمكن فك تشفيرها، ويجب على متلقي الرسالة أن يحتفظ بالمفتاح الخاص بأمان وألا ينشره وهو الذي يملك صلاحية فك تشفير الرسالة، وبالتالي فإن التشفير اللامتماثل يضمن الخصوصية والسرية[18].

**3- التشفير المزدوج**: يعد نظاماً خليطاً بين المتماثل وغير المتماثل وفيه يتم تشفير الرسالة بمفتاح خاص ثم تشفير المفتاح الخاص بمفتاح عام وإرسال كل من الرسالة المشفرة والمفتاح الخاص المشفر إلى المرسل إليه باستخدام شبكة للاتصالات [19]. ولقد أخذ المشرع الجزائري من خلال المادة 8/02 من القانون رقم 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين[20]، بنظام التشفير المزدوج من خلال نصه على مفتاحي التشفير الخاص والتشفير العمومي، وبذلك يكون المشرع قد تجنب سلبيات نظام التشفير بالمفتاح المتماثل.

**المطلب الثاني: دور شهادات المصادقة الإلكترونية في حماية الدفع الإلكتروني**

لا يستلزم التطور الذي تعرفه التجارة الإلكترونية، تطوير تقنيات جديدة للكتابة الإلكترونية والتوقيع الإلكتروني وكذا الاعتراف القانوني بهما فقط، بل يلتزم كذلك إيجاد

ضمانات كفيلة بإرساء الأمان القانوني ووضع الثقة فيهما، وقد تكون هذه الضمانات من الجهة نفسها لكن غالباً من جهة ثالثة. ولدراسة دور شهادات المصادقة الإلكترونية في حماية الدفع الإلكتروني، أولا يجب بحث الحصول على الترخيص بالاستعمال في (الفرع الأول)، لكي يمكن الحديث عن شهادات المصادقة الإلكترونية في (الفرع الثاني).

**الفرع الأول: الحصول على الترخيص بالاستعمال**

وهو عبارة عن طلب يقدم إلى الجهة المصدرة لوسائل الدفع الإلكتروني خاصة في مجال النقود الإلكترونية، حيث يقوم المستخدم بعمليات الدفع التي تتم على شبكة الإنترنت، وكذا اجراء الصفقات بواسطة هذه النقود. ففي أنظمة النقود ذات البطاقة، فإن الترخيص يطلب عادة في مرحلة التخزين في الحساب المصرفي للمستخدم، وهذا ما يتطلب استخدام رقم تعريفي شخصي PIN.

ويطلب الترخيص أيضاً بين التاجر والمشغلين لضمان عدم الدفع لذات الصفقة أكثر من مرة، ويكون ذلك عبر نظام مركزي. وكذلك الأمر بالنسبة للنقود ذات البرمجيات إذ يفترض الحصول على مثل هذا الترخيص أثناء إجراء هذه الصفقات لتلافي إعادة استخدام النقود مرات متعددة. إضافة إلى ماسبق ذكره فإن أنظمة النقود الإلكترونية يمكن أن تؤمن مستويات إضافية من الأمن في مواجهة الأعمال غير المشروعة، فإجراء الصفقات قد يتطلب عدداً من الإثباتات على صحتها مثل: تاريخ الصلاحية، عدد الصفقات المبرمة بواسطة وسيلة الدفع، الأرصدة الموجودة على البطاقة والحد الأعلى للرصيد المسموح به في الصفقات[21].

**الفرع الثاني: شهادات المصادقة الإلكترونية**

يعتبر عنصري الثقة والأمان ضروريان لتطوير التجارة الإلكترونية، التي تعتمد على شبكة الاتصال المفتوحة، إذ لا توجد ضمانات بوجود الشركة صاحبة الموقع التي يزودها العميل بالمعلومات عن البطاقة الائتمانية، مما يقتضي وجود خدمة محايدة تتضمن هذه الموثوقية، والتي تعرف بشهادات المصادقة الإلكترونية، حيث يمكن استخدام هذه التقنية في تحديد هوية مستخدمي الشبكة وأهليتهم القانونية للتعاقد، والتحقيق في مضمون التعامل وسلامته، وكذلك تقوم بإصدار المفاتيح الإلكترونية سواء المفتاح الخاص بالتشفير أو العام بفك التشفير، كما تقوم بإصدار شهادات المصادقة الإلكترونية [22].

كما تقوم بالتأكد من جدية الإرادة في التعاقد بين الأطراف وبعدها عن الغش والنصب، إضافة إلى تحديد مضمون الإرادة تحديداً دقيقاً، وكذا مدى صحتها ونسبتها إلى من صدرت

عنه، لذلك كان من الضروري التطرق لهذا الموضوع من خلال تحديد تعريف جهة المصادقة الإلكترونية، وبيان مهامها وكذلك الحديث عن شهادات المصادقة الصادرة عنها.

**أولا: تعريف جهة المصادقة الإلكترونية**

لقد اختلفت التشريعات الدولية والداخلية في التسمية التي تطلق على القائم بمهمة المصادقة الإلكترونية بين مقدم خدمات التصديق أو التوثيق، أو سلطات التصديق، أو سلطات الإشهار، أو الطرف الثالث المصادق أو مزود خدمات التصديق، وكذلك في المفهوم حيث عرف التوجيه الأوروبي رقم 93/99 المتعلق بالتوقيعات الإلكترونية في المادة 11/2 مقدم خدمة التصديق الإلكتروني بأنه: «كل شخص قانوني طبيعي أو معنوي يصدر شهادات توثيق التوقيع الإلكتروني، أو يوفر الخدمات الأخرى المتعلقة بالتوقيعات الإلكترونية[23] » .

كماعرفها قانون الأونسترال النموذجي لسنة 2001 والمتعلق بالتوقيعات الإلكترونية في المادة 2/ه بأنها: «شخص يصدر شهادات، ويجوز أن يقدم خدمات اخرى ذات صلة بالتوقيعات الإلكترونية »[24].

أما بالنسبة للمشرع التونسي فقد استخدم مصطلح مزود خدمات المصادقة الإلكترونية، وتناولها بمزيد من التفصيل في القانون رقم 83 لسنة 2000 بشأن المبادلات والتجارة الإلكترونية، ووفقا لأحكام هذا القانون، فإنه يقصد بمزود خدمات المصادقة الإلكترونية: «كل شخص طبيعي أو معنوي يحدث ويسلم ويتصرف في شهادات المصادقة ويسدي خدمات أخرى ذات علاقة بالإمضاء الإلكتروني»[25].

أما بالنسبة للمشرع الجزائري فقد أطلق مصطلح مؤدي خدمات التصديق الإلكتروني على الجهات المختصة بإصدار شهادات التوقيع الإلكتروني وعرفه بموجب المادة 12/2: «**مؤدي خدمات التصديق الإلكتروني**: شخص طبيعي أو معنوي يقوم بمنح شهادات تصديق إلكتروني موصوفة، وقد يقدم خدمات أخرى في مجال التصديق الإلكتروني »[26].

لم يخرج المشرع الجزائري عما جاء به القانون النموذجي الخاص بالتوقيعات الإلكتروني لسنة 2001 ولم يخرج كذلك عن التوجيه الأوروبي، إذ أن ذلك لا يعتبر عيبا حيث أن قانون الأونسترال النموذجي هو قانون استرشادي يمكن لمختلف الدول الرجوع إليه عند تنظيم القواعد المتعلقة بالتوقيع والتصديق الإلكترونيين، لذلك نجد أن المشرع الجزائري

لم يخرج عن السياق العام للتعاريف كون هيئة التصديق شخصي طبيعي أو معنوي يقدم خدمة التصديق أو خدمات أخرى متعلقة بالتوقيع الإلكتروني[27].

بالإضافة إلى ما سبق ذكره، نجد أن المشرع الجزائري في نص المادة 11/2 من قانون 15-04 السالف الذكر، نص على نوع آخر من جهات المصادقة الإلكترونية وهو(**الطرف الثالث الموثوق**) وعرفه بأنه:« شخص معنوي يقوم بمنح شهادات تصديق إلكتروني موصوفة، وقد يقدم خدمات أخرى متعلقة بالتصديق الإلكتروني لفائدة المتدخلين في الفرع الحكومي» .

الشيء الملاحظ على المادة 2 بفقرتيها 11و12 أن هناك تذبذب في موقف المشرع الجزائري فيما يخص صفة الأشخاص الذين يؤدون نشاطات التصديق فمرة يفتح المجال للأشخاص الطبيعية والمعنوية الخاصة بصريح العبارة ومرة أخرى يقتصر النص على الأشخاص المعنوية فقط ولعل ذلك راجع لطبيعة الخدمات التي يؤدونها والإمكانيات المادية والفنية اللازمة.

وما يلاحظ على جل التعاريف التي نصت عليها التشريعات العربية أنها قد استقتها من قانون الأونسترال النموذجي طبقا للمادة 11/2، كما أنها لم تجتمع على مصطلح واحد للقائم بخدمات التصديق الإلكتروني، لكنها تتفق علىكونها: «هيئة أو مؤسسة يتولى إدارتها شخص طبيعي أو معنوي، تعمل بترخيص من إحدى مؤسساتالدولة، وظيفتها إصدار شهاداتالتصديق الإلكترونية التي تربط ما بين شخص طبيعي أو معنوي ومفتاحه العام، أو أي مهمة أخرى تتعلق بالتوقيع الإلكتروني » [28].

**ثانيا: إلزامية إنشاء جهة مختصة بالمصادقة الإلكترونية**

ألزم المشرع التونسي في قانون المبادلات والتجارة الإلكترونية التونسي على من يرغب في ممارسة مهنة المصادقة الإلكترونية شرط الحصول على ترخيص مسبق، حيث حدد الجهة المخولة بمنح الترخيص بالوكالة الوطنية للمصادقة الإلكترونية[29]، وهي مؤسسة عامة تتمتع بالشخصية المعنوية ولها استقلال مالي يخولها القيام بالمهام والمسؤوليات المسندة لها ولقد نظمت الفصول من 08 إلى 10 من قانون المبادلات والتجارة الإلكترونية التونسي الأحكام الخاصة بها. أما المشرع الإماراتي فقد خول صلاحية ترخيص وتصديق ومراقبة أنشطة

مزودي خدمات التصديق والاشراف عليها لمراقب خدمات التصديق، الذي يتم تعيينه بقرار من رئيس سلطة منطقة دبي الحرة للتكنولوجيات والتجارة الإلكترونية والاعلام [30].

ولقد عرف القرار الوزاري المشترك رقم 1 لسنة 2008 بشأن مزودي خدمات التصديق الالكتروني **"المراقب"** في المادة 1 بأنه: «الهيئة العامة لتنظيم قطاع الاتصالات » [31].

بالنسبة للمشرع الجزائري فقد منح صلاحية إصدار الترخيص للسلطة الاقتصادية للتصديق الإلكتروني، والتي تعينها السلطة المكلفة بضبط البريد والمواصلات السلكية واللاسلكية [32]، وتكلف السلطة بمتابعة ومراقبة مؤدي خدمات التصديق الإلكتروني الذين يقدمون خدمات التوقيع والتصديق الإلكترونيين لصالح الجمهور.

وتقوم السلطة الاقتصادية للتصديق الإلكتروني بعدة مهام أهمها:

1- إعداد سياستها للتصديق الإلكتروني وعرضها على السلطة الوطنية للتصديق الإلكتروني للموافقة عليها والسهر على تطبيقها.

2- منح التراخيص لمؤدي خدمات التصديق الإلكتروني بعد موافقة السلطة.

3- إعداد دفتر الشروط الذي يحدد شروط وكيفية تأدية خدمات التصديق الإلكتروني وعرضه للسلطة للموافقة عليه.

وتخضع جهات المصادقة الإلكترونية لإشراف الدولة التي تقوم بتحديد القواعد والإجراءات التي تنظم عملها، وتقوم هذه الجهات بإصدار شهادات المصادقة الإلكترونية وفق الترخيص الصادر لها من الجهات المسؤولة في الدولة. كما يحقق وجود هذه الجهات أهداف التجارة الإلكترونية خاصة من حيث تدعيم الثقة بين المتعاقدين بما يحقق الثقة والأمان بالتعاقد عبر شبكة الإنترنت وكذا إمكانية الصفقات التجارية التي تتم عن بعد [33].

**ثالثا: مهام جهات المصادقة الإلكترونية**

يكمن الهدف الأساسي من انشاء هيئات المصادقة الإلكترونية من خلال التحقق من هوية الشخص الموقع (المرسل) وصلاحية توقيعه وتحديد أهليته القانونية للتعامل والتعاقد[34]، وكذا التحقق من مضمون هذا التعامل أو التبادل الإلكتروني وسلامته، وكذلك جديته وبعده عن الغش والاحتيال[35]. بالإضافة إلى إصدار التوقيع الرقمي وإصدار المفاتيح الإلكترونية سواء المفتاح الخاص الذي يتم بواسطته تشفير البيانات والمعاملات الإلكترونية أو المفتاح

العام الذي يتم بمقتضاه فك التشفير[36]. وبالتالي فلجهات المصادقة الإلكترونية عدة وظائف يمكن تلخيصها فيما يلي:

**أولا: التحقق من هوية الشخص الموقع**

يتمثل الدور الرئيسي لجهات المصادقة الإلكترونية في القيام بالتحقق من هوية الشخص الموقع، فإذا قام أحد الأطراف بوضع توقيعه الإلكتروني على رسالة البيانات الإلكترونية، وقامت جهة التصديق بتأكيد صحتها، فإن هذا يؤكد صدور التوقيع من صاحبه، ويستتبع التحقق من هوية الموقع من طرف هيئة التصديق تحديد الأهلية القانونية للمتعاقد [37].

فعندما يضع أحد الأطراف توقيعه الإلكتروني على محرر إلكتروني ويقوم بإرساله إلى شخص آخر، فإن جهة المصادقة الإلكترونية تصدر شهادة إلكترونية تقوم بالربط بين الموقع ومفتاحه العام، حيث تتضمن هذه الشهادة البيانات الخاصة بصاحبها كاسمه وسلطته في التوقيع، فمن خلال هذه البيانات التي تحتويها الشهادة تمكن المرسل إليه من معرفة هوية المرسل (المُوَقع)، وبعد أن يتأكد المرسل إليه من صلاحية الشهادة الإلكترونية المرسلة له من خلال الجهة التي أصدرتها، يعول على المحرر الإلكتروني، وهكذا يتم التبادل بين المرسل والمرسل إليه حتى يتم التوصل إلى الاتفاق النهائي [38].

**ثانيا: إثبات مضمون التبادل الإلكتروني**

تتولى جهة المصادقة كذلك التحقق من مضمون التبادل الإلكتروني بين الأطراف المتعاقدة وكذلك التيقن من سلامته وجديته وبعده عن الغش والاحتيال، إضافة إلى إثبات وجوده ومضمونه، وذلك تجنبا لحدوث أي غش تجاه المتعاملين عبر الإنترنت، ويجوز اللجوء إلى هذه الهيئات قبل إبرام العقد للتحقق من أمر الشركة التي سيتم التعاقد معها [39] ولتأكيد سلامة البيانات الإلكترونية المتداولة يجب أن تضمن منظومة أمن إحداث التوقيعات الإلكترونية لجميع أطراف التعامل الإلكترونية، إقامة البيانات الخاصة بالتحقق من التوقيعات الإلكترونية [40]، مع وجوب الاستعانة بأنظمة مؤمنة لحفظ شهادات التصديق الإلكتروني على أي حامل إلكتروني تتيح امكانية الاطلاع عليها عند الحاجة، بالشكل الذي أنشئت أو أرسلت أو استلمت به[41].

**ثالثا: تحديد لحظة إبرام العقد**

إن تحديد لحظة إبرام العقد مؤشرا لتحديد موعد ترتيب الآثار القانونية لهذا العقد. وتظهر هذه الأهمية بشكل رئيسي في عقود المدة، مثلا في عقد الايجار هناك نص يقضي

بتجديد العقد بشكل تلقائي ما لم يستعمل أحد الطرفين حقه في طلب إنهاء العقد قبل نهايته بمدة معينة [42]. ولتحديد تاريخ إبرام التصرفات القانونية أهمية أخرى تتجلى في مدة التقادم التي يمكن أن ترد على مثل هذه التصرفات وما يرد أثناءها من اجراءات قاطعة أو موقفة لهذا التقادم.

وحتى لا نكون أمام تعارض بين التواريخ، فإنه يفضل الرجوع إلى جهات تتولى تحديد تاريخ منضبط بحيث أنه يضمن تحديد تاريخ واحد للتصرف القانوني الذي يبرم عبر وسائط إلكترونية. لذلك تضاف مثل هذه الخدمة للهيئات التي تقوم بخدمات التصديق على الشهادات لتسهيل الحل وتبسيط الإجراءات[43].

**رابعا: إصدار المفاتيح الإلكترونية**

تقوم جهات المصادقة الإلكترونية بالإضافة إلى الوظائف الأخرى، بإصدار مفاتيح التشفير الإلكتروني، سواء المفتاح الخاص الذي يتم بواسطته تشفير المعاملة الإلكترونية الذي يكون خاصا بصاحبه ولا يعلمه غيره، أو المفتاح العام الذي يتم بواسطته فك هذه الشفرة ويكون متاحا للكافة [44].

كما تتولى جهات المصادقة الإلكترونية إصدار التوقيع الرقمي والذي تبدأ إجراءات إصدار هذا التوقيع بتقديم البيانات اللازمة من طالب تصديق التوقيع إلى جهة المصادقة، مع بيان الأشخاص المخولين ليصدر كل واحد منهم مفتاح خاص. وبعد هذا الإجراء يتم اصدار المفتاح الخاص بحيث يتم تثبيت نصف هذا المفتاح بجهاز الحاسب الآلي لطالب تصديق التوقيع الإلكتروني، أما النصف الآخر من المفتاح فيتم تثبيته ببطاقة إلكترونية ذكية، لذلك فإن المفتاح الخاص الذي يتم استخدامه في التوقيع لا يمكن العمل به إلا من جهاز حاسب آلي واحد فقط، حتى يمكن التأكد من أن التوقيع الرقمي صادر بالفعل من صاحبه، ويحتفظ الموقع بالمفتاح الخاص لديه ولا يطلع عليه أي شخص بحيث يكون سريا لا يعلمه إلا صاحبه، أما المفتاح العام والذي تحتفظ به عادة جهة المصادقة، فتقوم هذه الأخيرة بإرساله عن طريق البريد الإلكتروني إلى كل من يرغب في التعامل مع صاحب التوقيع الإلكتروني، وبذلك يمكن التحقق من صحة التوقيع [45].

هذا بالإضافة إلى الدور الذي تلعبه جهات المصادقة الإلكترونية في تعقب المواقع التجارية على الإنترنت للتحري عن جديتها ومصداقيتها، فإذا تبين لها عدم أمن هذه المواقع، فإنها تقوم بتوجيه رسائل تحذيرية للمتعاملين تبين عدم مصداقية هذه المواقع، وهذا ما يمثل

المجال الأوسع الذي يتجلى فيه دور جهات المصادقة الإلكترونية في توفير الحماية للمستهلك في مجال المعاملات الإلكترونية، ذلك أن أغلب المعاملات تتوزع على عمليات البيع والشراء عبر المواقع التجارية على الإنترنت، خاصة في ظل كثرة الغش والاحتيال في هذا النطاق [46].

**رابعا: أنواع شهادات المصادقة الإلكترونية**

تتنوع الشهادات التي يمكن أن تصدرها جهات المصادقة الإلكترونية، حيث توفر كل واحدة منها مستوى مختلفا من الموثوقية والمصداقية، فتقسم إلى شهادات تصديق بحسب قيمتها القانونية أو بحسب وظيفتها والغرض المرجو منها كالآتي:

**1-حسب قيمتها القانونية**: تنقسم إلى شهادة التصديق الإلكتروني العادية (البسيطة) وشهادة التصديق الإلكتروني المعتمدة (المؤهلة):

**أ- شهادة التصديق الإلكتروني البسيطة (العادية)**: عرف المشرع الجزائري وفق المرسوم التنفيذي 07-162 السالف الذكر، عرف الشهادة الإلكترونية وفق المادة 3 مكرر/8، بقوله: «**الشهادة الإلكترونية**: وثيقة في شكل إلكتروني تثبت الصلة بين معطيات فحص التوقيع الإلكتروني والموّقع »[47]. وهو نفس التعريف الذي جاء به القانون رقم 15-04 السالف الذكر، ضمن المادة 7/02[48].انطلاقا من محتوى هذا النص، نستنتج أن شهادة التصديق الإلكتروني البسيطة تصنف على هذا النحو من خلال بياناتها فهي خاصة بصاحبها فقط.

**ب- شهادة التصديق الإلكتروني المعتمدة (المؤهلة)**: عرفها المشرع الجزائري في المادة 3 مكرر 9 من المرسوم التنفيذي رقم 07-162 السالف الذكر، بأنها: «الشهادة الإلكترونية الموصوفة شهادة إلكترونية تستجيب لمتطلبات محددة ».

يلاحظ أن المشرع الجزائري من خلال المادة المذكورة لم يبين المتطلبات المحددة ولكنه جاء بالقانون رقم 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين السالف الذكر وبين من خلاله هذه المتطلبات ضمن المادة 11.

**2- حسب وظيفتها أو الغرض منها**: تتعدد أنواع شهادات التصديق الإلكتروني بحسب الوظيفة التي تؤديها والغرض من إصدارها إلى:

**أ- شهادة موزع ويب**: الصادرة عن سلط التصديق الأعلى درجة على مستوى مرفق المفتاح العمومية والتي تمكن من تحديد هوية موزع الويب والتصديق على مضمونه، وذلك عن طريق اتفاق بين سلطة التصديق وموزع الويب (Serveur) حلو قبول والاعتراف بشهادة التصديق الرئيسية، والتي تسمح بتبادل البيانات الإلكترونية بين الموزع وعملائه وذلك من خلال ربط هوية الموزع بمفتاح عمومي، حيث يقوم المتعامل الإلكتروني بتثبيت (Installer) الشهادة على حاسوبه من أجل تأمين عمليات البيع والشراء أو الدفع الالكتروني أو الدفع، وذلك من خلال موقع تجاري من دون إطلاق الموزع لرسائل تحذير على جهاز الحاسوب[49].

**ب- شهادة الإذن**: بمقتضى هذه الشهادات يتم تقديم معلومات إضافية عن صاحبها مثل محل إقامة الشخص وعمره وعمله ومؤهلاته والترخيصات التي يملكها [50]، وفيما إذا كان عضوا في إحدى المنظمات أو النقابات المهنية كنقابة المحاميين. كما تلعب هذه الشهادة أدواراً أخرى عندما تعرف بالباحثين والدكاترة الباحثين، كما تساهم في تسهيل التعارف بين هؤلاء الأشخاص وذلك بتبادل الأبحاث وأسئلة الامتحان وغيرها من الجوائي العلمية [51].

**ت- شهادة البيان**: وهي الشهادة التي توثق وتشهد بصحة واقعة معينة[52]، وهي تختلف عن باقي الشهادات الأخرى من حيث أنها لم تنشأ لربط شخص معين بمفتاح أو رمز معين وإنما نشأت لبيان وقوع حدث ما وقع وقوعه[53].

**ث- شهادة خاتم الوقت الرقمي**: وتعرف بأنها مستند رقمي غير قابل للتزوير، يشهد بأن الوثيقة موجودة في وقت محدد، وأنه ليس من الصعب إثبات فيما إذا كانت الوثيقة موجودة قبل أو بعد حادث معين، ويعتبر هذا النوع من الشهادات ذا أهمية كبيرة حيث أن هناك حالات يكون فيها من المهم بيان متى وقعت الواقعة، وإثبات تاريخ وقوعها، وتمثل هذه الشهادة مصداقية للتوقيع الرقمي وذلك من خلال إمكانيتها على تقديم الدليل على الوقت الذي جرى فيه التوقيع الرقمي للوثيقة[54].

**ج- شهادة الإمضاء الإلكتروني**: تمكن من تحديد هوية صاحب الشهادة وارتباطها بعناصر التدقيق في إمضائه[55]، إذ يعول عليها الموقع في إثبات هويته وتأكيد صحة ونسبة بيانات إحداث توقيعه الإلكتروني، كما يعول الطرف المستقبل للرسالة الإلكترونية على الشهادة من أجل التعرف على هوية كل من الموقع والمصدر لها، والتأكد من وجود صلة بين بيانات إنشاء التوقيع الإلكتروني وصاحبه [56].

ح- **شهادة (Digital time stamp)**: التي توثق تاريخ، ووقت إصدار التوقيع الرقمي حيث يقوم صاحب الرسالة بعد التوقيع عليها بإرسالها إلى جهة المصادقة التي تقوم بتسجيل التاريخ عليها وتوقيعها من جهتها ثم تعيدها إلى مرسلها [57].

خ- **شهادة التوقيع الرقمي**: تتلخص تقنيتها فيما يلي: يقوم من يرغب في الحصول على توقيع إلكتروني موثق بطلب شهادة تصديق من جهة المصادقة معتمدة، حيث تحتوي على المفتاح العام الذي يقابل المفتاح الخاص الذي بحوزته أو الذي ستعطيه له هيئة التصديق إذا وافقت على طلبه، حيث يتم تقديم الطلب إلى هيئة التصديق مباشرة أو إلى أحد وكلائها، وفي حال ما إذا وافقت هيئة المصادقة على الطلب فإنها تصدر توقيعا رقميا خاصا بالعميل وشهادة تصديق تحتوي على هذا التوقيع، التي تشهد بمقتضاها على صحة التوقيع ونسبته إلى من صدر عنه [58].

إذا نستنتج من خلال ما تم عرضه عن أنواع شهادات التصديق الالكتروني، نلاحظ أن المشرع الجزائري لم يتطرق من خلال القانون 15-04 السالف الذكر، إلى تصنيف شهادات التصديق الالكتروني بحسب الأغراض التي تؤديها، إلا أن الصفحة الرسمية لسلطة ضبط البريد والمواصلات السلكية واللاسلكية أشارت إليها دون أن تحدد السند القانوني في ذلك [59]. وغالبا ما تصدر شهادة التصديق لفترة محدودة، وبمجرد انتهاء مدتها فإنها تصبح غير قابلة للاستعمال، حيث ترفض وبصفة تلقائية من قبل برمجيات موجودة على مستوى جهة المصادقة، لذا تقوم هذه الجهات غالبا بإعداد ونشر قائمة بالشهادة الصالحة للاستعمال، وأخرى للشهادات التي تنتهي فترة صلاحيتها أو تصبح غير صالحة للاستعمال لأسباب أخرى، كما يمكن أن يتم في بعض الحالات إبطال مفعول الشهادة أو إلغاؤها، كأن يفقد صاحب الشهادة السيطرة على مفتاحه الخاص أو يتم كشفه، إذ يتعين عليه في هذه الحالة إبلاغ سلطة التصديق أو الجهة المزودة بالتوقيع الرقمي حيث يتم نشر وإعلان ذلك بصفة إلكترونية من خلال سلطة التصديق، مع تحمل المقصر المسؤولية تجاه أي متعامل حسن النية الذي يعتمد على شهادة تصديق لم يتم إلغاؤها بعد [60].

**خاتمة**: بعد التطرق لكل الجوانب الرئيسية في الموضوع توصلت إلى نتائج وتوصيات:

**أولا: النتائج**

- يعتبر التشفير من أحدث الوسائل التقنية الخاصة بتأمين وسائل الدفع الإلكترونية، والذي أثبت فعاليته إلى حد بعيد في تأمين الدفع الإلكتروني، إلا أنه من المستحيل أن يوفر

نظام أمني فعال مئة بالمئة، وهذا ما يستوجب تدعيم الحماية التقنية بحماية قانونية صارمة في مجال حماية البيانات الإلكترونية ما سيشكل بالتالي حماية كاملة ومتكاملة لوسائل الدفع الإلكتروني.

- حاول المشرع الجزائري من خلال القانون رقم 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين، وضع أرضية قانونية من شأنها حماية المتعاملين في مجال التكنولوجيا الرقمية بصفة عامة والدفع الإلكتروني بصفة خاصة.

- إن نجاح الدفع مرهون بمدى إقرار واقبال أطراف المصادقة الإلكترونية بالتعويل على خدمات طرف ثالث محايد معتمد من طرف الجهات الرسمية لمزاولة نشاطات المصادقة الإلكترونية، وكذا بقوة المفتاح العمومي المستخدم في خدمات المصادقة الإلكترونية الموثوق بها.

- يتم تأمين المواقع الإلكترونية وبالخصوص مواقع التجارة الإلكترونية ( البيع والشراء والدفع الإلكتروني) واثبات هويتها عن طريق شهادات المصادقة الإلكترونية.

**ثانيا: التوصيات**

- بعد صدور القانون رقم 15-04 يتوجب على الجهات المعنية الإسراع إلى تكييف ومطابقة الأنظمة الخاصة بالتعاملات الإلكترونية مع أحكام هذا القانون وسن تشريع لحماية البيانات والخصوصية على الإنترنت وردع المخالفات المتعلقة بهما.

- كما يجب وضع استراتيجية وطنية شاملة لتعميم استخدام المعاملات الإلكترونية في جميع المجالات، سيما منها التجارة والقيام بحملات تحسيسية حول فوائد المعاملات الإلكترونية مثل الدفع الإلكتروني إلى جانب التوعية في مجال أساليب الاختراق والقرصنة والغش وسرقة المعلومات الشخصية.

- كما يتوجب على الدولة الجزائرية الاهتمام بمسألة الأمن المعلوماتي لوسائل الدفع الإلكتروني لأن الأمن المعلوماتي يعتبر اليوم من المستلزمات لتحقيق أمن الدولة بمفهومه الحديث.

- كما يجب وضع سياسات تعليمية وتكوينية قصد تلبية حاجيات سوق العمل من قوى عاملة متخصصة ومؤهلة في مجال المصادقة الإلكترونية، وكذا دعم الدولة للأنشطة البحث العلمي في مجال تكنولوجيا الاعلام والاتصال مع الحرص على التأهيل والتدريب المتواصل للمورد البشري في مجال المعاملات الإلكترونية.

## الهوامش

1عمر خالد رزيقات، **عقد التجارة الإلكترونية عقد البيع عبر الإنترنت (دراسة تحليلية)**، الطبعة الأولى، دار الحامد للنشر والتوزيع، عمان – الأردن، 2007، ص 269.

2عمر حسن المومني، **التوقيع الإلكتروني وقانون التجارة الإلكترونية دراسة قانونية وتحليلية مقارنة**، الطبعة الأولى، دار وائل للنشر،عمان- الأردن، 2003، ص 54 و55.

3عمر رزيقات، المرجع السابق، ص 269.

4عبد الصمد حوالف، "**دور التوقيع والتصديق الإلكتروني في تأمين وسائل الدفع الإلكتروني**"، مجلة كلية القانون الكويتية العالمية، كلية الحقوق والعلوم السياسية، جامعة تلمسان، العدد الأول، الجزائر، سبتمبر 2017، ص 367.

5علاء فرج طاهر، **الحكومة الإلكترونية (بين النظرية والتطبيق)**، الطبعة الأولى، دار الراية للنشر والتوزيع، عمان، 2009، ص 80.

6كمال فتحي دريس، "**آلية التصديق الإلكتروني كضمانة للتعاملات التجارية بالوسائل الحديثة في التشريع الجزائري**"، مجلة البحوث والدراسات، كلية الحقوق والعلوم السياسية، جامعة الوادي، العدد 24، السنة (14)، 2017، ص 162.

7 علاء فرج طاهر، المرجع السابق، ص 80.

8ممدوح محمد الجنيبهي، منير محمد الجنيبهي، **تزوير التوقيع الإلكترونيي**، دار الفكر الجامعي، الأزرايطة– الإسكندرية، 2006، ص 138 وما بعدها.

9 الفصل الثاني من القانون رقم 83 لسنة 2000، المتعلق بالمبادلات والتجارة الإلكترونية التونسي، المنشور في الرائد للجمهورية التونسية، عدد 64 الصادر في 09 أوت 2000.

10أنظر الفقرة (أ) و(ب) من الملحق الفني والتقني للائحة التنفيذية للقانون رقم 15 لسنة 2004، الصادر في 22 أفريل 2004 المتعلق بتنظيم التوقيع الإلكتروني وانشاء هيئة تنمية صناعة تكنولوجيا المعلومات، المنشور في الجريدة الرسمية عدد 17، الصادرة في 22 أفريل 2004.

11المرسوم التنفيذي رقم 09-410 المؤرخ في 23 ذي الحجة عام 1430 الموافق لـ 10 ديسمبر 2009، يحدد قواعد الأمن المطبقة على النشاطات المنصبة على التجهيزات الحساسة، الجريدة الرسمية عدد 73 المؤرخة في 26 ذي الحجة عام 1430هـ الموافق لـ 13 ديسمبر سنة 2009.

12القرار رقم 16/س خ/ رم/ س ض ب م المؤرخ في 2012/06/11، المتضمن مدة صلاحية رخصة استغلال تجهيزات وبرمجيات التشفير، منشور على موقع سلطة ضبط البريد والمواصلات السلكية واللاسلكية:www.arpt.dz، بتاريخ: 2018/01/11.

13نايت أعمر علي، "**الملكية الفكرية في إطار التجارة الإلكترونية**"، مذكرة في القانون، فرع: القانون الدولي للأعمال، كلية الحقوق والعلوم الساسية، جامعة مولود معمري – تيزي وزو، 2014/03/15، ص 63.

14حليتيم سراح، " **خصوصية التوقيع الرقمي في توثيق العقود الإلكترونية**"،مجلة الباحث للدراسات الأكاديمية، جامعة مستغانم، العدد الثالث عشر، جويلية 2018، ص 740.

15ابتهال زيد علي،" **التنظيم القانوني للتوقيع الإلكتروني ومدى حجيته في الإثبات** "، مجلة كلية العلوم السياسية، جامعة بغداد، العدد 20، د.س.ن، ص 149.

16بمعنى آخر أن المفتاح الذي يقوم بشفير الرسائل ليس هو نفسه الذي يقوم بفك تشفيرها.

- LE DUC BAO « **Authentification des empreintes digitales dans un système BioPKI** », travail d'intérêt personnel encadré, l'institut de la Francophonie pour l'informatique, Hanoi le 20 janvier 2007, p 6.

17 Cabinets FANTANEAUX, **La Signature électronique**, **revue Fiscalité européen et droit international des affaires**, n° 125, paris, 2001, disponible sur le site:www.fontaneaux.com

18 Maxime Wack, Nathanael Cottin, Bernard Mignot et Abdallah Elmoudni, « **certification et archivage légal de dossiers numériques** », Document Numériques, 2002/1 vol.6, p 145-158, article Disponible sur le site:https://www.cairn.inforevue – document – numérique – 2002 – 1 – page 145. Htm.

19 MaximeWack, Nathanael Cottin, Bernard MignotetAbdallahElmoudni, Op cit.

20القانون رقم 15-04 المؤرخ في 11 ربيع الأول عام 1436 الموافق لـ 1 فبراير سنة 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، الجريدة الرسمية عدد 06 الصادرة في 20 ربيع الثاني عام 1436هـ الموافق لـ 10 فبراير سنة 2015 م.

21عبد الصمد حوالف، المرجع السابق، ص 372 و373.

22المرجع نفسه، ص 374.

23Art 2/11 de laDirective 1999/93/CE du parlement européen et du conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques. J.O.C.E, n° L 13, du 19 janvier 2000, p 0012-0020, disponible sur le site:http://www.eur_lesc_europa.eu: « prestataire de service de certification toute entité ou personne physique ou morale qui délivre des certificats ou fournit d'autres services liés aux signature électronique ».

24Art2/e:« le terme prestataire de services de certification désigne une personne qui émet des certificats, et peut fournir d'autres services lies aux signatures électroniques ». www.unictiral.org

25القانون رقم 83 لسنة 2000 يتعلق بالمبادلات والتجارة الإلكترونية التونسي، المرجع السابق.

26القانون رقم 15-04، المتعلق بالتوقيع والتصديق الإلكترونيين، المرجع السابق.

27 المادة 12/2 من القانون رقم 15-04، المتعلق بالتوقيع والتصديق الإلكترونيين، المرجع السابق.

28أيمن أحمد الدلوع، **التنظيم القانوني للتوثيق الإلكتروني**، دار الجامعة الجديدة، الإسكندرية، 2016، ص 46.

29الفصل 11 من القانون رقم 83 سنة 2000، المتعلق بالمبادلاتوالتجارة الإلكترونية التونسي، المرجع السابق.

30المادة 1/23 من القانون رقم 02 لسنة 2002، المتعلق المعاملات والتجارة الالكترونية لإمارة دبي،المؤرخ في 30 ذي القعدة 1422هـ الموافق لـ 12فبراير 2002، المتعلق بالمعاملات والتجارة الإلكترونية لإمارة دبي، نقلا عن الموقع الإلكتروني لتعذر الحصول على الجريدة الرسمية: www.dc.gov.ae،تاريخ الاطلاع: 2017/12/10، على الساعة: 14:39.والمادة 20 من القانون الاتحادي رقم 01 لسنة 2006، بشأن المعاملات والتجارة الإلكترونية لدولة الإمارات العربية المتحدة، الصادر بتاريخ 30 ذي الحجة 1426، الموافق لـ 30 يناير 2006م، الجريدة الرسمية عدد 442 الصادرة بتاريخ 2006/1/31.

31القرار الوزاري رقم 1 لسنة 2008 (الامارات العربية المتحدة) بشأن إصدار لائحة مزودي خدمات التصديق الإلكتروني المنشور على الموقع الالكتروني: http://www.qistas.com/legislations/ude/view، تاريخ الاطلاع: 2018/10/24، على الساعة 16:44.

32المادة 29 من القانون رقم 15-04، المتعلق بالتوقيع والتصديق الإلكترونيين، المرجع السابق.

33عبد الصمد حوالف، المرجع السابق، ص 378 و379.

34سعيد السيد قنديل،**التوقيع الإلكتروني (ماهيته – صوره - حجيته في الاثبات بين التدويل والاقتباس)**، دار الجامعة الجديدة للنشر، الإسكندرية – مصر، 2004، ص 75.

35لينا إبراهيم يوسف حسان،**التوثيق الإلكتروني ومسؤولية الجهات المختصة به (دراسة مقارنة)**، الطبعة الأولى، دار الراية للنشر والتوزيع، عمان – الأردن، 2009،ص 47.

36 راضية لالوش،"**أمن التوقيع الإلكتروني**"، مذكرالماجستير في القانون، فرع: القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، مدرسة الدكتوراه للقانون الأساسي والعلوم السياسية، تيزي وزو، 2012، ص 112.

37لزهر بن سعيد، **النظام القانوني لعقود التجارة الإلكترونية**، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2012، ص 176.

38 راضية لالوش، المرجع السابق، ص 113.

39 لزهر بن سعيد، المرجع السابق، ص 177.

40 Éric A. CAPRIOLI, « **de l'authentification à la signature électronique quel cadre juridique pour la confiance dans les communications électroniques internationales** » ? p 8, Article sur le site électronique:https://www. Unictral.org , Op cit, pp5,6.

41-Valérie Sédallian, « **preuve et signature électronique** », article disponible sur le site:www.internet-juridique.net, Op cit.

42سعيد السيد قنديل، المرجع السابق، ص 105.

43المرجعنفسه، ص 106.

44المادة 01/ 13 من قرار رقم 109 لسنة 2005،، المؤرخ في 15 ماي 2005، المتعلق بإصدار اللائحة التنفيذية لقانون التوقيع الإلكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات، المرجع السابق.

45إبراهيم الدسوقي أبو الليل،**توثيق التعاملات الإلكترونية ومسؤولية جهة التوثيق تجاه الغير**،بحث مقدم في مؤتمر الأعمال المصرفية بين الشريعة والقانون، الذي نظمته جامعة الإمارات العربية المتحدة كلية الشريعة والقانون بالتعاون مع غرفة تجارة وصناعة دبي في الفترة ما بين 10 و12 ماي 2003، المجلد الخامس، ص 1869و1870.

46نذير قورية، " **دور مؤدي خدمات التصديق الإلكتروني في حماية المستهلك على ضوء قانون رقم 15-04** "، مجلة العلوم القانونية والاجتماعية زيان عاشور بالجلفة، كلية الحقوق والعلوم السياسية، جامعة باجي مختار -عنابة، العدد العاشر، جوان 2018، ص 190.

47المرسوم التنفيذي رقم 07-162 المؤرخ في 13 جمادي الأولى عام 1428 الموافق لـ 30 مايو سنة 2007، يعدل ويتمم المرسوم التنفيذي رقم 01-123 المؤرخ في 15 صفر عام1422 الموافق لـ 9 مايو سنة 2001، المتعلق بنظام الاستغلال المطبق على مختلف خدمات المواصلات السلكية واللاسلكية، جريدة رسمية عدد 37 مؤرخة في 21 جمادي الأولى عام 1428هـ، الموافق لـ 7 يونيو 2007 م.

48 القانون رقم 15-04، المتعلق بالتوقيع والتصديق الإلكترونيين، المرجع السابق.

49عبد القادر سرحاني، مبارك بن الطيبي، " **شهادة التصديق الإلكتروني في النظام القانوني الجزائري** "، مجلة العلوم القانونية والاجتماعية، جامعة زيان عاشور بالجلفة – الجزائر، المجلد الخامس، العدد الثالث، سبتمبر 2020، ص 611.

50 عبد الحميد بادي، "**الايجاب والقبول في العقد الالكتروني**"،مذكرة ماجستير في الحقوق، فرع: العقود والمسؤولية، كلية الحقوق، بن عكنون جامعة الجزائر 1، 2012/2011، ص 88.

51 يوسف رحمان، " **الآليات القانونية للمسؤولية المدنية لمزود خدمات التصديق الإلكتروني في القانون المقارن**"، مجلة الدراسات الحقوقية، جامعة تلمسان، العدد الثامن، د. س. ن، ص 187.

52 عبد الحميد بادي، المرجع السابق، ص 88.

53لينا إبراهيم يوسف حسان، المرجع السابق، ص 78.

54المرجعنفسه، ص 79.

55 الفصل 07 في الباب الثالث من الأمر عدد 1667-2001 المؤرخ في 17 جويلية 2001، يتعلق بالمصادقة على كراس الشروط الخاص بممارسة نشاط مزود خدمات المصادقة الالكترونية، منشور في الرائد الرسمي للجمهورية التونسية، عدد60، الصادر في 27 جويلية 2001.

56سمير دحماني، "**التوثيق في المعاملات الإلكترونية (دراسة مقارنة)**"، مذكرة ماجستير في القانون، فرع القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، 2015، ص 43.

57 عبد الحميد بادي، المرجع السابق، ص 87.

58لينا إبراهيم يوسف حسان، المرجع السابق، ص 79.

59الموقع الرسمي لسلطة ضبط البريد والمواصلات السلطية واللاسلكية:www.arpc.dz، تاريخ الاطلاع: 2020/09/23، على الساعة: 17:11.

60 عمر حسن المومني، المرجع السابق، ص 66.