

جامعة المنصورة

كلية الحقوق

مجلة الكلية

التصديق الإلكتروني

"دراسة مقارنة"

بحث مقدم من الباحث

سمير سعد رشاد سلطان

المدرس المساعد بقسم القانون المدني

كلية الحقوق – جامعة المنصورة

إشراف

الأستاذ الدكتور / ثروت عبد الحميد عبد الحليم عمر

أستاذ القانون المدني بكلية الحقوق – جامعة المنصورة

ووكيل الكلية لشؤون الطلاب والتعليم

مقدمة

تتمتع المعاملات الإلكترونية في صورتها التقليدية بالأمن والأمان القانوني من حيث وجود محرر مكتوب على وسيط مادي ليس من السهل إنكاره أو التغيير في مضمونه وإمكانية الرجوع إليه في أي وقت عند الحاجة إليه، وكذلك الإقرار بصحة ومضمون المحرر ونسبته إلى من وقع عليه إلا أن الأمر مازال مختلفاً بخصوص المحررات الإلكترونية من حيث إثارة الشكوك حول درجة الثقة والأمان الواجب توافرها في المستند الإلكتروني مما يثير الجدل حول القيمة القانونية للمستند الإلكتروني في مجال الإثبات.

ونظراً لأهمية المعاملات الإلكترونية التي لا تقف عند مجرد الحصول على موقع على الانترنت وإنما هي أكبر من ذلك بكثير إذ توجد تطبيقات كثيرة للتعامل عبر الانترنت فمن السوق الإلكتروني لبيع وشراء السلع والمنتجات وتبادل الخدمات إلى تسهيل وتدفق المعلومات والاتصالات والتعاون بين الشركات والبريد الإلكتروني وغيرها الكثير من المعاملات التي يستخدم بصددها وسائل الاتصال الحديثة^(١).

وإذا كان التقدم العلمي قد ظهر في العديد من الأنشطة منذ زمن بعيد ، فقد ظهر حديثاً في مجال مهم هو مجال الاتصالات والمعلومات وأدى لتطور وتقدم مذهل بشأنها فالمعلومات تعد - بلا شك- عنصراً جوهرياً في كافة الأنشطة الحياتية وقيل إن المعلومات أظهرت نوعاً ثالثاً من الذهب هو الذهب الرمادي إلى جانب الذهب الأبيض "القطن" والذهب الأسود "البتروول"^(٢).

وتشجيعاً لانتشار هذه المعلومات وبث الثقة فيها والوصول للتطور الفني والتكنولوجي، فإن الآلية القانونية التي تواتر الحديث عنها في مجال الفقه المقارن لتأمين التعاملات التي تتم عبر شبكة الانترنت هي عمليات التوثيق الإلكتروني وتقوم بها جهات متخصصة مهمتها تأمين سلامة المعاملات

(١) انظر:

MICHON (Ch.) & ANDRÉANI (J.- C.), Le Marketeur: Fondements et nouveautés du marketing, Pearson Education France, 2010, P. 127.

(٢) د. إبراهيم الدسوقي أبو الليل، الجوانب القانونية للتعامل عبر وسائل الاتصال الحديثة، مؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون، الإمارات، ٢٠٠٠، المجلد الثاني، ص ٩٩٣.

التي تتم عبر وسيط إلكتروني من حيث مضمونها ودقة نسبتها إلى من صدرت منه وحفظها وإصدار شهادات الكترونية بذلك يمكن الاعتماد عليها في انجاز هذه النوعية من المعاملات الإلكترونية^(١).

ونظراً للطبيعة الخاصة للمعاملات الإلكترونية حيث إنها لا تقوم على وسيط مادي ملموس ، وتحتمل في ذاتها الخطأ والغش ، وإمكانية اقتحامها والعبث في محتواها ، ولما تتعرض له المعاملات الإلكترونية من قرصنة واعتداءات غير مشروعة ، فمن شأن ذلك التأثير السلبي على هذه الأعمال من أمن وسرية، مما يوجب معه ضرورة توافر الضمانات الخاصة لحماية هذه المعاملات ، ويوفر الثقة للمتعاملين عبر شبكة الانترنت من تمتع هذه المعاملات بتلك الضمانات ، الأمر الذي يؤدي معه لازدهار المعاملات الإلكترونية^(٢).

ومسايرةً لهذا التقدم الهائل فقد أنشأ المشرع المصري وفقاً لأحكام قانون التوقيع الإلكتروني هيئة ذات شخصية اعتبارية وتعتبر هي السلطة العليا في مجال التصديق الإلكتروني في الدولة وهي التي ترخص لمن يريد مزاولة نشاط التصديق الإلكتروني مقابل رسم نص عليه القانون.

ووفقاً لما جرى عليه العمل في الواقع لم تثر مسألة التوثيق في معناها أو مضمونها العام إشكالية بقدر ما تواجهه المحررات والكتابة والتوقيع الإلكتروني، قد يكون لحدثة الأمر على مجتمعنا، مما أثار العديد من التساؤلات التي يمكن الإجابة عنها من خلال هذه الدراسة.

ونعرض في هذه الدراسة لمبحثين، وهما: المبحث الأول ويتعلق ببيان ماهية عملية التصديق الإلكتروني، ونستعرض من خلاله لثلاثة مطالب الأول منه لبيان المقصود بالتصديق الإلكتروني وبيان أهميته، وفي المطلب الثاني نستعرض بياناً لجهات التصديق الإلكتروني، وفي المطلب الثالث نبين آلية التصديق الإلكتروني وتلك المبادئ التي تحكم عملية التصديق. أما المبحث الثاني فنستعرضه من خلال مطلبين أيضاً أولهما ماهية شهادات التصديق الإلكتروني، والمطلب الثاني يتعلق بالحجية القانونية للشهادات الإلكترونية الأجنبية.

(١) انظر:

LAUDON (K.) & LAUDON (J.), Management des systèmes d'information, Pearson Education France, 2010, P. 306.

(٢) د. ممدوح عبد الحميد عبد اللطيف، جرائم استخدام شبكة المعلومات العالمية، مؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون، الإمارات، ٢٠٠٠، المجلد الأول، ص ٢٢٨.

وهكذا ستكون خطة الدراسة على النحو التالي:

المبحث الأول: ماهية عملية التصديق الإلكتروني.

المبحث الثاني: شهادات التصديق الإلكتروني.

المبحث الأول ماهية التصديق الإلكتروني

نعرض في هذا المبحث لماهية التصديق الإلكتروني وذلك من خلال مطلبين أساسيين نوضح في أولهما المقصود بالتوثيق الإلكتروني، وفي المطلب الثاني نعرض للجهات القائمة على عملية التصديق الإلكتروني، ثم نبين آلية التوثيق الإلكتروني والمبادئ التي تحكم عملية التصديق الإلكتروني وذلك في المطلب الثالث.

المطلب الأول المقصود بالتصديق الإلكتروني وأهميته

في إطار التوجه المصري نحو النهضة التكنولوجية وتنمية صناعة تكنولوجيا المعلومات والاتصالات على المستوى الحكومي والمؤسسي ومن جانب الأفراد كذلك، ولمواكبة التطور المتلاحق في استخدام تكنولوجيا الاتصالات والمعلومات في مختلف الأنشطة الاقتصادية والاجتماعية، ومن أجل دعم وتنمية المعاملات الإلكترونية التي أصبحت لا تقل وزناً أو أهمية عن المعاملات التقليدية، فقد أصدر المشرع المصري القانون رقم ١٥ لسنة ٢٠٠٤م بشأن التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات^(١)، ولائحته التنفيذية رقم ١٠٩ لسنة ٢٠٠٥م بقرار وزير الاتصالات وتكنولوجيا المعلومات^(٢).

وفي هذا القانون فقد كفل المشرع للتوقيع والكتابة الإلكترونية الحجية في الإثبات كما هو مقرر في التوقيع والكتابة في الشكل التقليدي وفقاً لقواعد واشتراطات معينة. وبهذا الاعتراف علينا أن نتعرض لكيفية حماية الكتابة والمحركات الإلكترونية وإقرار المسؤولية القانونية لتلك الجهات القائمة على عملية التصديق على المحركات والكتابة الإلكترونية.

(١) الجريدة الرسمية، العدد ١٧ تابع (د) في ٢٢ إبريل سنة ٢٠٠٤م.

(٢) الوقائع المصرية، العدد ١١٥ تابع في ٢٥ مايو ٢٠٠٥م.

الفرع الأول المقصود بالتصديق الإلكتروني

يقصد بالتصديق في معناه العام التأكيد، وبالنسبة للتصرفات القانونية فيقصد به أن يضع موظف عام مختص تأكيده على صحة ما ورد بالمستند المقدم للتوثيق وصحة نسبته إلى من وقع عليه، وقد نص قانون التوثيق رقم ٦٨ لسنة ١٩٤٧م ولائحته التنفيذية على إجراءات التوثيق والتصديق على التوقيعات^(١).

ويقصد بالتصديق في قانون الإثبات في المواد المدنية والتجارية وفقا لنص المادة العاشرة منه على أن المحرر الرسمي هو الذي يثبت فيه موظف عام أو شخص مكلف بخدمة عامة ما تم على يديه أو ما تلقاه من ذو الشأن وذلك طبقا للأوضاع القانونية وفي حدود سلطته واختصاصاته.

ويقابل ذلك نص المادة ١٣١٧ من التقنين المدني الفرنسي التي نصت على أنه "الورقة الرسمية هي التي تلقاها، وفقا للأوضاع الشكلية المطلوبة، موظف عام له حق التوثيق في الجهة التي كتبت فيها الورقة"^(٢).

ويعتبر التصديق هنا في مجال هذا النص القانوني هو التصرفات القانونية في شكلها التقليدي أي المستندات الورقية، وإذا كان الأمر يكتفه الغموض والغرابة حول مضمون وإجراءات والجهات التي تقوم على عمليات التصديق الإلكتروني، فكان ذلك لطبيعة البيئة الإلكترونية، حيث تخلو من أية عناصر مادية يمكن أن تستجيب لقواعد وإجراءات التوثيق في الشكل التقليدي.

ويتميز التصديق الإلكتروني بضمان سلامة وتأمين التعامل عبر شبكة الانترنت سواء من حيث أطرافه ومضمونه ومحلّه وتاريخه أي خلق بيئة الكترونية آمنة للتعامل عبر الانترنت ويتم ذلك عن طريق شخص ثالث عن أطراف التعامل الإلكتروني، أو جهة معتمدة عن طريق إتباع بعض

(١) من ذلك ما نصت عليه المادة ٢٦ من اللائحة التنفيذية لقانون التوثيق رقم ٦٨ لسنة ١٩٤٧م بقولها "أن تقوم مكاتب التوثيق بعد أداء الرسم المقرر بإثبات تاريخ المحررات العرفية بكتابة محضر يثبت فيه تاريخ تقديم المحرر ورقم إدراجه في الدفتر المعد لذلك، ويختم بخاتم المكتب، ويوقعه الموثق".

(٢) انظر:

"L'acte authentique est celui qui a été reçu par officiers publics ayant le droit d'instrumenter dans le lieu où l'acte a été rédigé, et avec les solennités requises".

الإجراءات الفنية بهدف التثبت من مضمون المحرر والبعد عن التلاعب فيه وحماية التوقيعات الواردة عليه وصحة نسبتها إلى من صدرت عنه^(١).

ولتحقيق هذا الهدف استلزم الأمر وجود طرف ثالث محايد موثوق فيه يقوم بطرقه الخاصة بالتأكد من صحة صدور الإرادة التعاقدية ممن تنسب إليه والتأكد من جدية هذه الإرادة وبعدها عن الغش والاحتيال بالإضافة لتحديد مضمون الإرادة تحديدا دقيقا يمكن التعامل والاعتماد عليه ولكن يلاحظ أن دور جهات التصديق الإلكتروني لا يقتصر فحسب على تحديد هوية المتعاملين في المعاملات الإلكترونية وتحديد أهليتهم لإتمام التعامل الإلكتروني وإنما يمتد أيضا للتحقق من مضمون هذا التعامل وسلامته وجديته وبعده عن عمليات الغش والاحتيال فيوفر الثقة والأمان للمتعاملين^(٢).

ويضيف البعض بأن هدف التوثيق في المجال الإلكتروني وتكنولوجيا المعلومات هو ضمان سلامة وتأمين التعامل عبر شبكة الانترنت سواء من حيث أطرافه ومضمونه ومحلّه وتاريخه^(٣).

ويستوجب الأمر هنا توفير الضمانات الكفيلة بتحديد هوية المتعاملين، وتحديد حقيقة التعامل ومضمونه. فإذا تمثل التوقيع الإلكتروني في إبرام عقد ما فيلزم التيقن من إرادة التعاقد وصحتها ونسبتها إلى من صدرت منه لذا فقد تطلب الأمر وجود طرف ثالث محايد موثوق به يقوم بدوره وبطرق خاصة يتبعها للتأكد من صحة صدور الإرادة التعاقدية الإلكترونية ممن تنسب إليه والتأكد من جدية هذه الإرادة وبعدها عن الغش والاحتيال^(٤).

ولذا فإن التوثيق هو أهم الشروط الواجب توافرها لقيام المحرر الإلكتروني ولإعطائه الحجية الواجبة في الإثبات فإذا كان المحرر التقليدي يقوم على دعامين هما الكتابة والتوقيع، فإن مقومات

(١) انظر:

CARPENTIER (J.- F.), La sécurité informatique dans la petite entreprise: état de l'art et bonnes pratiques, Editions ENI, 2009, P. 105.

(٢) د. مصطفى أبو مندور موسى، خدمات التوثيق الإلكتروني "تدعيم للنقطة وتأمين للتعامل عبر الانترنت"، دراسة مقارنة، ندوة الجوانب القانونية للمعاملات الإلكترونية، مسقط، ٢٣/١١/٢٠٠٨م، ص ١٨.

(٣) انظر:

THIERRY (P.- C.), Certification électronique: Pratique et modélisation, Voir à: <http://www.e-betobe.com/texteece.htm>, 13-2-2009.

(٤) د. إبراهيم الدسوقي أبو الليل، الجوانب القانونية للمعاملات الإلكترونية، مرجع سابق، ص ١٧٧.

المحرر الإلكتروني هي الكتابة والتوقيع والتوثيق والحفظ والقدرة على الاسترجاع بالحالة التي نشأ عليها^(١).

ويدل على ذلك أن التوثيق هو قوام المحرر الإلكتروني وسر وجوده ولم يجرؤ أحد على الحديث عن أي حجية لرسائل البيانات المتداولة عبر الشبكة إلا بعد ظهور فكرة وتقنيات التوثيق الإلكتروني رغم أسبقية الكتابة الإلكترونية في الظهور^(٢).

وقد وضعت القوانين تنظيمياً خاصاً بمقتضاه يتاح التحقق من صدور الإرادة ممن تنسب إليه من ذلك ما نصت عليه المادة الثالثة عشر الفقرة الأولى من القانون الاتحادي للإمارات رقم ١ لسنة ٢٠٠٦ في شأن المعاملات والتجارة الإلكترونية من نسبة الإرادة للمتعاقد ليس فقط إذا كان هو الذي أرسلها باستخدام وسيلة الكترونية سواء بنفسه أو بواسطة نائب عنه وإنما افتراض في بعض الحالات إسناد هذه الإرادة للمتعاقد إذا توافرت ظروف معينة منها قيام المرسل إليه بتطبيق أو إجراء توثيق سبق أن وافق عليه الطرف الآخر - المرسل - بقصد التأكد من صدور الرسالة عن هذا الأخير.

وتقوم جهات التوثيق الإلكتروني أيضاً بتعقب المواقع التجارية عبر شبكة الانترنت للتحري عنها وعن جديتها ومصداقيتها فإذا تبين لها أن أحد المواقع غير آمن فتقوم بتوجيه رسائل تحذيرية للمتعاملين توضح فيها عدم مصداقية الموقع ويتم ذلك كثيراً عن طريق استخدام البريد الإلكتروني بتوجيه رسائل لأصحابه.

وكان الغرض من إنشاء هيئة تنمية صناعة تكنولوجيا المعلومات هو إحداث نقلة نوعية لصناعة تكنولوجيا المعلومات في مصر، ولكي تدعم بناء القدرة التنافسية اللازمة لوضع مصر على خريطة تصدير تكنولوجيا المعلومات وتطبيقاتها^(٣).

ويأتي هذا الدور من كيفية قيام الهيئة بحماية المعاملات الإلكترونية ومن ابسط وسائل حماية المحررات الإلكترونية المنشئة لتلك المعاملات الإلكترونية من خلال عملية التصديق الإلكتروني لفوائده الكثيرة والتي نعرض لها الآن.

(١) انظر:

MONTERO (E.), Les contrats de l'informatique & de l'Internet, Larcier, 2005, P. 212.

(٢) د. مصطفى أبو مندور موسى، خدمات التوثيق الإلكتروني، مرجع سابق، ص ٢٠.

(٣) د. تامر محمد سليمان الدمياطي، إثبات التعاقد الإلكتروني عبر الانترنت، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، ٢٠٠٨، ص ٢٩٢.

الفرع الثاني أهمية التصديق الإلكتروني

أولاً:- التصديق الإلكتروني تدعم الثقة:

تتمثل السمة المميزة لشبكة الانترنت في كونها شبكة عالمية مفتوحة فالانترنت هو أفضل سوق عالمية يمكنك فيها مقارنة الأسعار بدلاً من الخروج إلى الشارع، والبحث في المحلات، حيث يمكنك شراء كل شيء دون أن تغادر منزلك. فضلاً عن الحرية الكاملة في التعرف على السلع المعروضة ومقارنتها دون أي ضغط من صاحب المحل أو العاملين فيه كما يحدث في الأوضاع العادية^(١).

وفي الحقيقة فإن غياب إدارة تؤدي دور المراقب لما يتم على شبكة الانترنت من مبادلات ومعاملات من حيث سلامتها ودرجة دقتها، تؤدي ذلك انعدام أو نقص في الثقة لدى العديد من المتعاملين من خلال تلك الشبكة العالمية ولذا جاء دور التوثيق الإلكتروني لتوفير الثقة والاطمئنان بين المتعاملين. وبهذا يتحدد دور الموثق أو المصدق بأنه يقوم بدور هام لمنح الثقة في المحررات حتى يمكن استخدامها لإثبات ما تتضمنه من تصرفات قانونية وانبعث الثقة والطمأنينة للمتعاملين بها^(٢).

وواقع أن الشك يظل قائماً حتى مع تطبيق نظم التشفير الإلكتروني من حيث قدرة القائم على عملية التوثيق الإلكتروني على الوفاء بالتزاماته.

والخلاصة أن جهات التوثيق الإلكتروني تقوم " بدور الوسيط المؤتمن بين المتعاملين في التعاملات والمراسلات الإلكترونية"^(٣).

(١) د. مصطفى أبو مندور موسى، خدمات التوثيق الإلكتروني، مرجع سابق، ص ٢٥ .

ISAAC (H.) & VOLLE (P.), E-commerce: De la stratégie à la mise en oeuvre opérationnelle, Pearson Education France, 2008, P. 238.

(٢) د. عابد فايد، الكتابة الإلكترونية في القانون المدني: الفكرة والوظائف، دار النهضة العربية، القاهرة، ٢٠٠٧، ص ٦٩.

(٣) د. إبراهيم الدسوقي أبو الليل، الجوانب القانونية للتعاملات الإلكترونية، مطبوعات مجلس النشر العلمي، جامعة الكويت، ٢٠٠٣، ص ١٧٧.

ويأتي هذا الدور من توثيق لهذه التعاملات والتصديق على توقعات أصحاب الشأن عليها، وتصدر شهادات الكترونية معتمدة لا تفيد فقط صحة التوقعات الإلكترونية ونسبتها إلى أصحابها، وإنما كذلك سلامة البيانات والمعلومات التي يتضمنها المستند الإلكتروني^(١).

بالإضافة إلى ذلك يتم التأكد من صحة صدور الإرادة التعاقدية ممن تنسب إليه، والتأكد من جدية هذه الإرادة وبعدها عن الغش والاحتيال، حيث يتم تحديد مضمون الإرادة تحديدا واضحا مما يمكن المتعامل من الاعتماد عليها في معاملاته^(٢).

ثانياً: - فوائد التصديق بالنسبة للمستهلكين:

مع التطور التقني للشركات الصناعية تعددت السلع في ظل تدفق إنتاجي غير مسبوق وتتنوع الخدمات مع سباق محموم للحصول عليها، بحيث أصبح الاستهلاك فلسفة الحياة المعاصرة^(٣).

وتفتح التجارة عبر الانترنت للمستهلك أفقا هامة للغاية، فهي تقدم له أبعاداً وتصورات مستقبلية جديدة سواء فيما يتعلق بأسلوب التعاقد أو بمحله من السلع والخدمات.

فلا شك أن اختيارات المستهلك تتسع كثيرا كلما زاد عدد التجار وكلما زادت الفرص المعروضة والخدمات المقدمة، وكذلك تسهيل عملية الوصول إلى السلع والخدمات، إذ في ظل شبكة الانترنت وثورة الاتصال لا يكلف الشخص سوى تصفح المواقع التجارية على هذه الشبكة ليعرف كل ما هو معروض في كل أنحاء العالم من السلعة أو الخدمة التي يبحث عنها ويرغب في التعاقد عليها. وتحدث هذه المعرفة في زمن قياسي وبتكلفة زهيدة^(٤).

وتعتبر شبكة الانترنت المنتشرة حول العالم بمثابة نافذة مفتوحة أمام الملايين، وصالة عرض لكافة المنتجات والخدمات، فضلا عن البريد الإلكتروني الذي يقدم للمستهلك أنواعاً متباينة من

(١) انظر:

LAUDON (K.) & LAUDON (J.), Op. Cit., P. 331; JACQUET (J.- M.) & DELEBECQUE (Ph.) & CORNELOUP (S.), Droit du commerce international, Dalloz, 2007, P. 423.

(٢) انظر:

MOUGENOT (D.), La prévue, Larcier, 2002, P. 322.

(٣) د. أسامة احمد بدر، حماية المستهلك في التعاقد الإلكتروني، دراسة مقارنة، دار الجامعة الجديدة للنشر، الإسكندرية، ٢٠٠٥، ص ١٧.

(٤) د. مصطفى أبو مندور موسى، خدمات التوثيق الإلكتروني، مرجع سابق، ص ٤٢.

المنتجات والخدمات، الأمر الذي يفرض على مقدمي الخدمات الإلكترونية التزاما باحترام القواعد الحمائية لجمهور المستهلكين.

ومن جانب آخر يعطى الانترنت دائما إحساسا بأننا في عالم مجهول يصعب ضبطه أو الرقابة عليه، ولذا فإن التوثيق يقدم للمستهلك أفضل تأمين سواء فيما يتعلق بجودة المنتجات والخدمات المقدمة من ناحية، أو فيما يتعلق بشخصية المتعاقد وسلامة المعاملة من ناحية ثانية.

وبجانب التأمين يؤدي التوثيق إلى المساعدة في تنوير إدراك المستهلك بخصوص الصفقات التي تبرم عبر الإنترنت، وذلك من خلال توفير إعلام حقيقي صادر عن جهة محايدة هي جهة التوثيق، وهو ما يؤدي في النهاية إلى القضاء على كل عوامل الخوف والقلق لدى المتعامل، ويدفعه بالتبعية إلى الإقدام على استخدام هذه الوسيلة الحديثة في تعاملاته مما يؤدي لمزيد من الثقة والطمأنينة في التعاملات الإلكترونية^(١).

(١) انظر:

GUERRIER (C.) & MONGET (M. -Ch.), Droit et sécurité des télécommunications, Springer, 2000, P. 378.

المطلب الثاني جهات التصديق الإلكتروني

كان لزاما على المشرع عند الحديث على التوقيع الإلكتروني وكيفية التأكد من سلامته وصحته ونسبة صدوره ممن وقعه وكذا توثيقا للكتابة الإلكترونية وبصدد الحديث عنها أن ينشأ الجهة المنوط بها القيام بعملية التوثيق.

وبالنسبة للمادة العاشرة من قانون الإثبات في المواد المدنية والتجارية المصري فتشترط لتوثيق المحررات وإضفاء الطابع الرسمي عليها الرسمي أن تصدر من موظف عام أو شخص مكلف بخدمة عامة في حدود سلطته واختصاصه مع مراعاة الأوضاع القانونية في ذلك^(١).

والجدير بالذكر أن قانون التوقيع الإلكتروني المصري جاء خاليا من تعريف جهات التصديق الإلكتروني ولكن جاءت اللائحة التنفيذية لهذا القانون الصادرة بالقرار رقم ١٠٩ لسنة ٢٠٠٥ وعرفت بها "الجهات المرخص لها بإصدار شهادة التصديق الإلكتروني وتقديم خدمات تتعلق بالتوقيع الإلكتروني"^(٢).

وإزاء هذا القصور يتعين علينا محاولة التعرف على جهات التصديق الإلكتروني من خلال تتبع القوانين في دول أخرى .

فقد عرفها القانون النموذجي للتوقيعات الإلكترونية سنة ٢٠٠١ بأنها "الشخص الذي يصدر الشهادات الإلكترونية ويمكن أن يقدم خدمات أخرى مرتبطة بالتوقيع الإلكتروني"^(٣).

وقد عرفها كذلك التوجيه الأوروبي الصادر في ١٣ ديسمبر ١٩٩٩ بأنها "كل شخص طبيعي أو اعتباري يسلم شهادات التصديق الإلكتروني أو يقدم خدمات أخرى مرتبطة بالتوقيعات الإلكترونية"^(٤).

(١) انظر في شرح تلك الشروط: د. محسن البيه، قانون الإثبات في المواد المدنية والتجارية، مكتبة الجلاء الجديدة، المنصورة، ٢٠٠١-٢٠٠٢، ص ٨٤.

(٢) المادة الأولى الفقرة السادسة من اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري.

(٣) المادة الثانية من قانون الأونسترال النموذجي بتاريخ ١٠/١/٢٠٠١ م.

(٤) المادة الثانية من التوجيه الأوروبي الصادر في ١٣ ديسمبر ١٩٩٩ الخاص بالتوقيع الإلكتروني.

وفي ذات السياق فقد عرفها المرسوم الفرنسي الصادر في ٣٠ مارس ٢٠٠١ بشأن تطبيق المادة ١٣١٦ - ٤ من التقنين المدني الفرنسي والمتعلق بالتوقيع الإلكتروني^(١) بمقتضى المادة الأولى فقرة (١١) منه بأنها "كل شخص يصدر شهادات تصديق إلكتروني أو يقدم خدمات أخرى تتعلق بالتوقيعات الإلكترونية"^(٢).

ويقصد بالخدمات المرتبطة بالتوقيع الإلكتروني، التقنيات التي تسمح بإصدار توقيع مؤرخ أو خدمات النشر والخدمات المعلوماتية الأخرى كالحفظ في الأرشيف^(٣).

أما القانون رقم ١ لسنة ٢٠٠٦ بشأن المعاملات والتجارة الإلكترونية بدولة الإمارات العربية المتحدة في مادته الأولى بأنه " أي شخص أو جهة معتمدة أو معترف بها تقوم بإصدار شهادات تصديق الكترونية أو أي خدمات أخرى أو مهمات متعلقة بها وبالتوقيعات الإلكترونية والمنظمة بموجب أحكام القانون.

وقد عرفه القانون التونسي وأطلق عليه مسمى مزود خدمات التصديق الإلكتروني وهو "كل شخص طبيعي أو معنوي يحدث ويسلم ويتصرف في شهادات المصادقة ويسدي خدمات أخرى ذات علاقة بالإمضاء الإلكتروني"^(٤).

وقد عرفه القانون البحريني الخاص بالمعاملات والتجارة الإلكترونية وأطلق عليه مسمى مزود خدمة الشهادات بأنه "الشخص الذي يصدر شهادات إثبات الهوية لأغراض التوقيعات الإلكترونية أو الذي يقدم خدمات أخرى تتعلق بهذه التوقيعات".

ومزود خدمة شهادات معتمد: مزود خدمة شهادات يتم اعتماده لإصدار شهادات معتمدة طبقاً لأحكام المادتين (١٦) و(١٧) من هذا القانون".

(١) انظر:

Décret N° 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique.

(٢) انظر:

"Prestataire de services de certification électronique: toute personne qui délivre des certificats électroniques ou fournit d'autres services en matière de signature électronique".

(٣) د. ثروت عبد الحميد، التوقيع الإلكتروني، دار الجامعة الجديدة، الإسكندرية، ٢٠٠٧، ص ١٦٣.

(٤) الفصل الثاني من قانون عدد ٨٣ لسنة ٢٠٠٠ مؤرخ في ٩ أوت ٢٠٠٠ يتعلق بالمبادلات والتجارة الإلكترونية.

ويتضح من التعريفات سالفه الذكر أن جميعها تجعل المهمة الأولى لجهات التصديق الإلكتروني هي إصدار الشهادات الإلكترونية وكذلك القيام بأية خدمات تتعلق بتلك الشهادات أو تكون متعلقة بالتوقيع الإلكتروني.

وفي مصر فقد أقر قانون التوقيع الإلكتروني المصري ١٥ لسنة ٢٠٠٤ إنشاء هيئة عامة ذات شخصية اعتبارية و تتبع وزير الاتصالات وتكنولوجيا المعلومات، وتسمى "هيئة تنمية صناعه تكنولوجيا المعلومات"^(١).

وهي سلطة التصديق الإلكتروني العليا ولها أن ترخص في مزاوله نشاط خدمات التصديق الإلكتروني وفقا لأحكام القانون ولأحتته التنفيذية وكذلك اعتماد الشهادات الإلكترونية الأجنبية.

ويستفاد من ذلك أن القانون قد عنى بتسمية الهيئة فى صلب القانون وقرر اعتبارها هيئة عامة مشيرا إلى تمتعها بالشخصية الاعتبارية العامة، الأمر الذي يترتب عليه أن تصبح الهيئة قابلة لأن تكتسب الحقوق وان تتحمل بالالتزامات^(٢).

ويتولى إدارة الهيئة مجلس إدارة يشكل بقرار من رئيس مجلس الوزراء، برئاسة الوزير المختص وعضوية أربعة عشر عضوا^(٣).

وتعمل هذه الهيئة على إدارة و تنظيم و تحديد معايير التوقيع الإلكتروني و إصدار و تجديد التراخيص اللازمة لمزاولة الأنشطة في مجال المعاملات الإلكترونية، كما تعمل علي تنمية صناعه تكنولوجيا المعلومات والاتصالات بهدف تنمية الصادرات الوطنية من البرمجيات وتسويقها محلياً وعالمياً.

ذلك إلى جانب تقييم الجهات العاملة في مجال تكنولوجيا المعلومات وتقديم المشورة الفنية لمثل هذه الجهات، وخاصة بشأن المنازعات التي قد تنشأ بين الأطراف المعنية بأنشطة التوقيع الإلكتروني و المعاملات الإلكترونية، كما تختص الهيئة أساساً بإصدار التراخيص اللازمة لمزاولة نشاط خدمات التوقيع الإلكتروني وغيرها من الأنشطة الأخرى في مجال المعاملات الإلكترونية وتكنولوجيا المعلومات.

Information Technology Industry Development Agency (ITIDA)

(١)

(٢) د. تامر الدمياطي، مرجع سابق، ص ٤٧٩.

(٣) راجع: المادة ٨ من قانون التوقيع الإلكتروني المصري ١٥ لسنة ٢٠٠٤.

وقد أعطى القانون لهذه الهيئة الحق في إدارة وتنظيم قطاع المعاملات الإلكترونية بصفة عامة بل وفي رقابة المرخص لهم بالعمل في هذا القطاع واتخاذ الإجراءات اللازمة نحو ضمان حسن سير هذا القطاع بما يتفق مع الصالح العام وسياسة الدولة في هذا الشأن.

وحتى يكون مقدم خدمة التوثيق مؤهلاً لإصدار شهادات توثيق معتمدة، فإنه يلزم أن تتوفر فيه الشروط الكفيلة لتحقيق الحد الأدنى من الأمان في التوقيع الإلكتروني ووفقاً لمواصفات قياسية يتم فرضها، وأي إخلال بذلك يرتب مسؤوليته^(١).

وتخضع جهات التصديق الإلكتروني لإشراف الدولة التي تقوم بتحديد القواعد والإجراءات التي تحدد عملها كما تنشئ جهة حكومية عليا هي التي تقوم بمنح التراخيص لتلك الجهات الراغبة في القيام بعمليات التصديق الإلكتروني بعد التأكد من استيفائها للشروط التي تضعها مسبقاً وفقاً للتنظيم القانوني الساري في هذا الشأن.

وتصدر جهات التصديق الإلكتروني شهادات التصديق أو التوثيق الإلكتروني تشهد بان التوقيع الإلكتروني هو توقيع صحيح ينسب إلى من أصدره ويستوفي الشروط والضوابط المطلوبة فيه باعتباره دليل إثبات يعول عليه كما تؤكد الشهادة أن البيانات الموقع عليها بيانات صحيحة صادرة من الموقع ولم يتم التلاعب فيها فلم يطرأ عليها أي تغيير سواء بالحذف أو الإضافة أو التغيير.

وقد تدخل المشرع الفرنسي بإصدار المرسوم رقم ٥٣٥ - ٢٠٠٢ والصادر في ١٨ إبريل ٢٠٠٢ المتعلق بتقييم مستوى الأمان الذي توفره منتجات وأنظمة تكنولوجيا المعلومات والتصديق عليه^(٢).

وبناء على هذا المرسوم فيجوز وفقاً للمادة الأولى لمشغلي الأنظمة من (ناشري البرامج، مقدمي التقنيات، ٠٠٠٠) أن يسعوا لإجراء تصديق على منظومة ما تكفل إتاحة سلامة المعلومات أو سريتها التي تستخدم إزاء التهديدات التي تعود بصفة خاصة إلى سوء النية.

ووفقاً للمادة (٧) من هذا المرسوم (والمعدلة بالمرسوم رقم ٨٣٤ لسنة ٢٠٠٩)^(١) فإنه عقب إجازة الإدارة الوطنية لأمان أنظمة المعلومات لتقرير التقييم، فيتعين على الإدارة أن تعد خلال مهلة

(١) د. ثروت عبد الحميد، التوقيع الإلكتروني، مرجع سابق، ص ١٦٤.

(٢) انظر:

Décret n°2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.

تقدر بشهر واحد، تقرير التصديق الذي يحدد خصائص وأهداف الأمان المقترحة وفي أثناء ذلك تبت الإدارة الوطنية لأمان أنظمة المعلومات إما بتسليم شهادة للممول بمطابقة منتجاته وأنظمتها لشروط الأمان المطلوبة أو برفضها التصديق.

ووفقاً للمادة (٨) والمادة (١٢) من هذا المرسوم فإنه تصدر شهادة بهذه المطابقة من قبل رئيس الوزراء لمدة عامين، تشهد بأن منتجات وأنظمة المعلومات الخاضعة للتقييم تستوفي خصائص الأمان المحددة، وكذلك تثبت تلك الشهادة أن التقييم كان يسيراً طبقاً للقواعد والمعايير السارية، مع الاختصاص والنزاهة المطلوبة.

وقد صدر قرار وزير الصناعة الفرنسي الصادر في ٣١ مايو ٢٠٠٢ والمتعلق بالاعتراف بصلاحيات مقدمي خدمات التصديق الإلكتروني وبعتماد الهيئات المعنية بتقييمهم ولاعتبار مقدم خدمات التصديق مؤهلاً لتقديم خدمات التصديق الإلكتروني^(٢).

وينص هذا القرار على أنه يتم اعتماد الهيئات المعنية بتقييم مقدمي خدمات التصديق الإلكتروني من قبل اللجنة الفرنسية للاعتماد COFRAC أو من هيئات الاعتماد الموقعة على اتفاق أوروبي متعدد الأطراف يدخل في إطار التنظيم الأوروبي لهيئات الاعتماد.

ووفقاً للمادة (٤) من هذا القرار يتم منح الاعتماد لمدة عامين ويجوز إعادة تجديده لمدة مماثلة بناء على طلب الهيئة المستفيدة عقب تحقق مركز الاعتماد من أن تلك الهيئة تلبى دائماً مجموعة الشروط المطلوبة.

ويضيف جانب من الفقه بان هناك فارق جوهري بين سلطات التصديق الإلكتروني والموثق يتمثل في أن سلطات التصديق ليس من مهمتها أن تتدخل في إنشاء وتاريخ وحفظ المحررات القانونية طبقاً للإجراءات المنصوص عليها قانوناً ولكن مهمتها تقتصر فقط على فحص التصرفات القانونية

(١) انظر:

Décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé «Agence nationale de la sécurité des systèmes d'information».

(٢) انظر:

Arrêté du 31 mai 2002 relatif à la reconnaissance de la qualification des prestataires de certification électronique et à l'accréditation des organismes chargés de l'évaluation, J.O. , no 132 du 8 juin 2002, P. 10223.

الإلكترونية وإعطاء ذوى الشأن شهادة تفيد ذلك وتسمى شهادة التصديق الإلكتروني وإن كان ثمة التزامات تجمع بين الموثق وجهات التصديق الإلكتروني^(١).

هذا وإن كان طبيعة عمل الجهات القائمة على عملية توثيق التوقيع تقترب من مهمة الجهات القائمة على هذا الأمر من مهمة الموثق في النظام الفرنسي للتأكد من شخص المتعاقد ومن مضمون التصرف المراد توثيقه^(٢).

ويعتبر الشخص الذي يقوم بعملية التوثيق شخصاً محايداً ويسمى بمسميات كثيرة منها "مزودي خدمات المصادقة الإلكترونية"^(٣)، ويسمى كذلك "مراقبي خدمات التوثيق لإلكترونية"^(٤)، ويسمى "جهات التصديق الإلكترونية"^(٥).

ومن الجدير بالذكر أن هذه المسميات جميعها تتفق على حقيقة الدور الذي تقوم به وهو تأكيد وتوثيق المعاملات الإلكترونية وكذلك بث الثقة لدى مستخدمي شبكات الانترنت من خلال إتباع مجموعة الوسائل الفنية والتقنية لتأمين ما يجرى على الشبكة وحفظها وصونها من العبث والضياع.

وقد أعطى المشرع المصري حماية كبيرة من جانب آخر لشهادة التصديق الإلكتروني حيث قرر قانون التوقيع الإلكتروني المصري رقم ١٥ لسنة ٢٠٠٤ في المادة التاسعة عشر منه لا تجوز مزاوله نشاط إصدار شهادات التصديق الإلكتروني إلا بترخيص من هيئة تنمية صناعة تكنولوجيا المعلومات نظير مقابل يحدده مجلس إدارة الهيئة وفقاً للإجراءات والقواعد والضمانات التي تحددها اللائحة التنفيذية لقانون التوقيع الإلكتروني كما قرر القانون بعدم جواز التوقف عن مزاوله النشاط المرخص به أو الاندماج في جهة أخرى أو التنازل عن الترخيص للغير إلا بعد الحصول على موافقة كتابية مسبقاً من الهيئة.

(١) د. عابد فايد، الكتابة الإلكترونية في القانون المدني، مرجع سابق، ص ٧١ .

(٢) د. عبد الحميد عثمان الحفني، المسؤولية المدنية للموثق، دراسة مقارنة بين القانون الفرنسي والمصري، مجلة البحوث القانونية والاقتصادية، كلية الحقوق، جامعة المنصورة، العدد الثاني عشر، أكتوبر ١٩٩٢، ص ٢.

(٣) القانون التونسي رقم ٨٣ لسنة ٢٠٠٠ م في شأن المبادلات والتجارة الإلكترونية.

(٤) قانون المعاملات والتجارة الإلكترونية لإمارة دبي رقم ٢ لسنة ٢٠٠٢ المادة ١/٢٣.

(٥) المشرع المصري في إصدار اللائحة التنفيذية لقانون التوقيع الإلكتروني ١٥ لسنة ٢٠٠٤ ولائحته التنفيذية ١٠٩ لسنة ٢٠٠٥.

المطلب الثالث

آلية التصديق الإلكتروني ومبادئه

إن البحث في آلية التصديق الإلكتروني ومبادئه يقتضي أن نقسم هذا المطلب إلى فرعين نبيين في الأول آلية التصديق الإلكتروني، ونوضح في الثاني المبادئ الحاكمة لعملية التشفير.

الفرع الأول

آلية التصديق الإلكتروني

تتجسد عملية التصديق الإلكتروني في وسيلة تقنية تسمى بعملية التشفير ويعرف التشفير بأنه مجموعة من التقنيات التي تسمح بحماية المعلومات من أي تعديل غير مرغوب فيه أو الحفاظ على خصوصيتها من أي اختراق بفضل الاستعانة برموز خاصة يطلق عليها تسمية المفاتيح^(١).

ويتم تحويل المعلومات لسفريات غير مفهومة لمنع الأشخاص غير المرخص لهم من الإطلاع على تلك المعلومات أو فهمها أي يتم تحويل النصوص العادية إلى نصوص مشفرة. ويتم التشفير عن طريق استخدام صيغ رياضية معقدة (خوارزميات) لفك التشفير بإعادة تحويل البيانات إلى صيغتها الأصلية باستخدام المفتاح المناسب لفك الشفرة^(٢).

وقد عرفه قانون الاونسترال النموذجي بشأن التوقيعات الإلكترونية سنة ٢٠٠١ بأنه "فرع الرياضيات التطبيقية الذي يعنى بتحويل الرسالة لأشكال تبدو غير مفهومة ثم إعادتها إلى أشكالها الأصلية".

وبالنسبة لمصر فقد جاء قانون التوقيع الإلكتروني خاليا من الإشارة لتحديد المقصود بالتشفير وقد تم تدارك هذا الأمر من قبل اللائحة التنفيذية لهذا القانون فقد عرفته بأنه " منظومة تقنية حسابية

(١) انظر:

BOCHURBERG (L.), Internet et commerce électronique, DELMAS, 2001, P. 154.

(٢) انظر:

SHERIF (M.), Paiements électroniques sécurisés, PPUR presses polytechniques, 2007, 213;
ROHAUT (S.), Préparation à la certification LPIC-1: Linux, Editions ENI, 2009, P. 509.

تستخدم مفاتيح خاصة لمعالجة وتحويل البيانات والمعلومات المقروءة الكترونياً بحيث تمنع استخلاص هذه البيانات والمعلومات إلا عن طريق استخدام مفتاح أو مفاتيح فك الشفرة^(١).

وتنص المادة (١٨) من قانون التوقيع الإلكتروني المصري على المساواة في حجية الإثبات لكلا من التوقيع الإلكتروني والكتابة الإلكترونية والمحركات الإلكترونية شريطة إمكانية كشف أي تعديل أو تبديل في بيانات المحرر الإلكتروني أو التوقيع الإلكتروني.

وتقرر اللائحة التنفيذية لهذا القانون في المادة (١١) منه أنه يتم من الناحية الفنية والتقنية كشف أي تعديل أو تبديل في بيانات المحرر الإلكتروني الموقع الكترونياً باستخدام تقنية شفرة المفاتيح العام والخاص وبمضاهاة شهادة التصديق الإلكتروني بأصل هذه الشهادة وتلك البيانات أو بأي وسيلة مشابهة .

وقد عرف مشروع قانون التجارة الإلكترونية المصري التشفير في الفصل الأول منه بأنه "تغيير في شكل البيانات عن طريق تحويلها إلى رموز أو إشارات لحماية هذه البيانات من إطلاع الغير عليها أو من تعديلها أو تغييرها"^(٢).

كما عرفه المشرع التونسي في المادة ٥/٢ بأنه "استعمال رموز وإشارات غير متداولة تصبح بمقتضاها المعلومات المرغوب تحريرها أو إرسالها غير قابلة للفهم من قبل الغير أو استعمال رموز وإشارات لا يمكن وصول المعلومة بدونها"^(٣).

ويقوم التشفير بدور هام في المحافظة على سرية البيانات وكذلك سلامتها من أي تحريف أو اعتداء من أي شخص عليها، وكذلك خدمة هامة للغاية في مجال توثيق المعاملات الإلكترونية وتحديد هوية الأطراف وسلامة المعلومات وكذلك عدم إنكار أي طرف من الأطراف لأي التزام أو تصرف

(١) المادة ٩/١ من اللائحة التنفيذية ١٠٩ لسنة ٢٠٠٥ لقانون التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات.

(٢) مشروع قانون التجارة الإلكترونية المصري، صادر عن رئاسة مجلس الوزراء، مركز المعلومات لجنة التنمية التكنولوجية، سنة ٢٠٠٠، الفصل الأول.

(٣) مادة ٥/٢ من قانون المبادلات والتجارة الإلكترونية التونسي رقم ٨٣ لسنة ٢٠٠٠.

عند حصول نزاع بشأن المعاملات الإلكترونية وكذلك توفير أكبر قدر من الحماية والاطمئنان لمستخدمي الانترنت^(١).

ويضيف البعض بان التشفير لا يجب أن يفهم على انه مرادف للتوقيع الإلكتروني وذلك لسببين^(٢):-

أولاً:- أن نظام التشفير ما هو إلا وسيلة تقنية مستخدمة للحفاظ على التوقيع الإلكتروني والكتابة الإلكترونية.

ثانياً:- يعتبر التشفير نظام أمان للتبادل الرقمي يقوم بوظائف السرية والحفظ والتأريخ.

وقد ظهر، في هذا الخصوص، نوعان من التشفير يسمى الأول بالتشفير المتماثل والثاني بالتشفير غير المتماثل. وسوف نحاول فيما يلي إعطاء نبذة مختصرة عن كل منهما.

أولاً: التشفير المتماثل (المفتاح السري):-

وفيه يتم الاعتماد على مفتاح سرى واحد بمقتضاه يتم تشفير المعاملة وكذا فكها. فمرسل الرسالة يكتب رسالته ويوقع عليها ويقوم بتشفيرها وإرسالها إلى المرسل إليه مع ذات المفتاح الذي استخدمه في التشفير لأنه هو الذي سيستخدمه المستقبل في عملية فك التشفير^(٣).

فمرسل الرسالة ومستقبلها يستخدمان نفس المفتاح مع اختلاف وظيفته بالنسبة لكل منهما، فالأول يستخدمه في التشفير والثاني لفك هذا التشفير. يتم الاتفاق مسبقا بين المرسل والمستقبل على كلمة المرور التي سيتم استخدامها ويمكن أن تحوى حروفا كبيرة وصغيرة ورموزا أخرى وبعد ذلك

(١) د. تامر محمد سليمان الدمياطي، مرجع سابق، ص ٤٣٥.

(٢) انظر:

RENARD (I.), Vive la signature électronique, Dalloz, 2002, P. 19.

(٣) انظر:

BITAN (H.), La signature électronique, Comment la technique répond-t-elle aux exigences de la loi? Gaz. Pal. 19-20 Juillet 2000, P. 10; ATELIN (Ph.), Réseaux informatiques: Notions fondamentales, Editions ENI, 2009, P. 330; BITAN (H.), Droit des créations immatérielles, Editions Lamy, 2010, P. 232.

يتم تحويل عبارة المرور بواسطة برمجيات التشفير إلى عدد ثنائي ويشكل العدد الثنائي الناتج مفتاح تشفير الرسالة والتي تجعل من المستحيل تزويرها^(١).

وإذا كانت هذه الطريقة تتميز بالبساطة إلا أنه يعيبها ما يلي :

١- أنها تفترض سبق معرفة أطراف المعاملة لبعضهم البعض وهو ما يتنافى مع الواقع في كثير من الأحيان، بل ومع الطبيعة العالمية والمفتوحة لشبكة الانترنت، تلك الشبكة التي لا تظهر فائدتها الحقيقية إلا في التعامل بين أطراف تفصل بينهما الحدود والمسافات، وقد لا يعرف بعضهما بعضاً.

٢- أنه لا توجد وسيلة آمنة لتبادل المفتاح الوحيد المستخدم بين المرسل والمرسل إليه، لأنه لو كانت هذه الوسيلة موجودة، فعلاً، ولا شك أن ذلك قد يغري الغير بالتسلل واقتحام البيانات التي تم إرسالها.

ثانياً التشفير غير المتماثل:

ولكثرة عيوب التشفير المتماثل كان لابد من البحث عن بديل آخر يحل محله ويؤدي الغاية المرجوة منه فتوصل العلم إلى ما يسمى بتقنية التشفير غير المتماثل، وهي تقنية تقوم على وجود مفتاحين: الأول ويسمى بالمفتاح الخاص، وبه يوقع الشخص على الرسالة الإلكترونية التي تحمل إيجابه أو قبوله للطرف الآخر ويتم الاحتفاظ به على بطاقة ذكية مؤمنة، والثاني يسمى بالمفتاح العام، وبه يستطيع المستقبل فك شفرة الرسالة والتأكد من صحة التوقيع التي تحمله ونسبته إلى المرسل وعدم وجود أي تلاعب أو تغيير في مضمون الرسالة منذ إنشائها وحتى وصولها إلى المرسل إليه.. وعندما يتحقق المرسل إليه من أصل الرسالة ونسبتها إلى الموقع بالمفتاح العام فإنه يكون قد قطع نصف الطريق وبقي أمامه النصف الآخر المتمثل في التحقق من أن الرسالة تحتفظ بصورتها الأولى التي كُتبت بها قبل التشفير وأنه لم يدخل عليها أي تعديل أو تحريف أثناء رحلتها عبر الشبكة^(٢).

(١) د. عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الإلكترونية، الكتاب الأول، دار الفكر الجامعي، ٢٠٠٢، ص ٢١١.

(٢) انظر:

ISAAC (H.) & VOLLE (P.), E-commerce: De la stratégie à la mise en oeuvre opérationnelle, Pearson Education France, 2008, P. 135.

وهذا الأسلوب من أساليب التشفير وإن كان يضمن للمستقبل نسبة الرسالة إلى المرسل فضلا عن سلامتها من الناحية الموضوعية ، إلا أنه لا يحافظ على سريتها إذ يبقى بإمكان أي شخص استخدام المفتاح العام في فك تشفير الرسالة والإطلاع على مضمونها وإن بقي عاجزاً عن إدخال أي تعديل عليها ، بمعنى أن التشفير بهذه الطريقة يضمن فقط سلامة الرسالة من الناحية الموضوعية وصدق نسبتها إلى من صدرت عنه ولكنه لا يضمن سريتها.

ولذا فإن أسلوب التشفير الذي يؤمن سرية الرسالة، بجانب سلامتها ونسبتها إلى صاحبها هو أن يقوم المرسل بتشفير الرسالة بالمفتاح العام للمرسل إليه الذي سيستخدم مفتاحه الخاص، عندما تصله الرسالة، لفك شفرتها. فمالك المفتاح الخاص هو، وحده دون غيره، الذي يستطيع فك شفرة الرسائل التي شفرها المفتاح العام.

ويُدعى نظام التشفير الذي يستخدم المفاتيح العامة بنظام RSA ورغم أنه أكثر أمناً من نظام DES إلا أنه أعقد وأبطأ إذ أن جلسة التشفير وجلسة فك التشفير يجب أن تكونا متزامنتين تقريباً، فضلاً عن أنه نظام ليس عصياً على الاختراق متى توافر الوقت والمال، ولذا فقد تم تطويره بنظام PGP الذي يستخدم مفتاحاً طوله ١٢٨ بت إضافة إلى استخدام البصمة الإلكترونية للرسالة message digest ولا يزال هذا النظام منيعاً على الاختراق حتى الآن^(١).

وإذا كانت آلية التشفير غير المتماثل تقدم للمرسل إليه يقيناً بأن الرسالة التي وصلتته موقعة من المرسل، أي من صاحب المفتاح الخاص الذي اشتق منه المفتاح العام الذي استخدم في فك التشفير، وبالتالي فهي منسوبة إليه، إلا أنها لا تحدد ذاتية هذا المرسل ولا تعين شخصيته على وجه الدقة. وبعبارة أوضح فإن آلية التشفير غير المتماثل وإن كانت تقيم علاقة بين شخص (افتراضي) ومفتاحه العام، إلا أنه يبقى التساؤل قائماً عن ذاتية هذا الشخص وهويته. لذلك كان لابد من البحث عن وسيلة أخرى تسد هذا النقص وتكون بمثابة التكملة الضرورية لنظام التشفير غير المتماثل. وقد تجسدت هذه الوسيلة فيما يسمى بـ "شهادة التوثيق الإلكتروني".

وبهذه التكملة الضرورية توفر آلية التشفير غير المتماثل الأمان الكامل للرسائل المتبادلة ليس فقط من حيث مضمونها، وإنما أيضاً من حيث هوية أطرافها.

(١) د. مصطفى أبو مندور موسى، خدمات التوثيق الإلكتروني، مرجع سابق، ص ٢٧ .

الفرع الثاني المبادئ الحاكمة لعملية التشفير

المبدأ الأول: إباحة تشفير الرسائل الإلكترونية:-

أباح القانون المصري تشفير البيانات والمعلومات التي يتم تدوينها أو التعامل فيها من خلال الوسائط الإلكترونية. وذلك كأسلوب يحقق تأمين المعلومات التجارية وبالتالي ازدهارها وقد أحال القانون إلي اللائحة التنفيذية لوضع القواعد والضوابط الخاصة بتشفير المحررات والبيانات الإلكترونية وكذلك وضع القواعد الخاصة بتشفير التوقيع الإلكتروني وبيانات الائتمان وغير ذلك من البيانات التي يتم تحريرها أو نقلها أو تخزينها علي وسائط إلكترونية^(١).

المبدأ الثاني: إخضاع عمليات التشفير لرقابة مشددة:-

أخضع القانون ولائحته التنفيذية - عملية التشفير والقواعد المتعلقة باستيراد واستخدام أجهزته والبرامج التي تستخدم لإتمامه لضوابط تحددها الجهة المختصة^(٢).

ويرجع السبب في ذلك إلي أن استخدام التشفير في بعض الحالات وتحديد نوع الأجهزة التي تستخدم في إجرائه والترخيص باستيرادها أو تصنيعها يتعلق بمصالح عليا لا بد من تنظيمها تنظيمياً خاصاً، وفي ظل رقابة الجهة التي ينعقد لها الاختصاص بذلك، وبهذا يكون القانون قد واعم بين حماية الشخص لخصوصياته وأسراره، وبين متطلبات تحقيق السلامة العامة والأمن القومي حتى لا يتمكن المجرمون والإرهابيون من استخدام التشفير للحد من مقدرة أجهزة الأمن علي تتبع اتصالاتهم وكشف جرائمهم.

المبدأ الثالث: احترام الخصوصية:-

يقصد بهذا المبدأ احترام سرية البيانات المشفرة والالتزام بحق أصحاب هذه البيانات والمعلومات في الخصوصية، ورغم أن المشرع المصري قد قرر خضوع عملية تشفير البيانات لرقابة

(١) راجع المادة ١٨ من قانون التوقيع الإلكتروني، والمادة ١١ من اللائحة التنفيذية لهذا القانون.

(٢) نصت المادة (١١) من اللائحة التنفيذية علي الآتي: "مع عدم الإخلال بما هو منصوص عليه في المواد (٤، ٣، ٢) من هذه اللائحة يتم من الناحية الفنية والتقنية، كشف أي تعديل أو تبديل في بيانات المحرر الإلكتروني الموقع الكترونياً باستخدام تقنية شفرة المفاتيح العام والخاص، وبمضاهة شهادة التصديق الإلكتروني وبيانات إنشاء التوقيع الإلكتروني بأصل هذه الشهادة وتلك البيانات، أو بأي وسيلة مشابهة".

جهة يرخص لها بذلك، إلا أنه اهتم أيضاً بتأكيد سرية المعلومات المشفرة واعتبرها معلومات خاصة بصاحبها لا يجوز فضها أو نسخها إلا بموافقة كتابية منه أو بناء علي أمر قضائي^(١).

وتطبيقاً لهذا المبدأ نصت المادة ٢١ من قانون التوقيع الإلكتروني المصري رقم ١٥ لسنة ٢٠٠٤، علي أن: "بيانات التوقيع الإلكتروني والوسائط الإلكترونية والمعلومات التي تقدم إلي الجهة المرخص لها بإصدار شهادات التصديق الإلكتروني سرية، ولا يجوز لمن قدمت إليه أو اتصل بها بحكم عمله إفشاؤها للغير أو استخدامها في غير الغرض الذي قدمت من أجله".

ومن ناحية التجارة الإلكترونية فإن إحاطة البيانات الشخصية بسرية أمر يساعد على نمو وازدهار التجارة سواء تعلقت بالمستهلك أو البائع أو صفقة البيع ذاتها وبيانات وسيلة الدفع وغيرها، واعتبار المركز المالي للشركات المتعاملة في مجال التجارة الإلكترونية يعول عليه كثيراً فكلما كانت القدرة المالية لهذه الشركات عالية كانت قدرتها على تحمل التكاليف الخاصة بتأمين المعلومات على شبكة الانترنت كبيرة^(٢).

المبدأ الرابع: قانونية عملية التشفير:

حرصت اللائحة التنفيذية لقانون التوقيع الإلكتروني، الصادرة بالقرار الوزاري رقم ١٠٩ لسنة ٢٠٠٥، بتاريخ ٢٠٠٥/٥/١٥^(٣)، علي إضفاء القانونية علي عملية التشفير، وقد استهلكت ذلك بالبند (٩) من المادة الأولى الذي عرف التشفير بأنه: "منظومة تقنية حسابية تستخدم مفاتيح خاصة لمعالجة وتحويل البيانات والمعلومات المقروءة الكترونياً بحيث تمنع استخلاص هذه البيانات والمعلومات إلا عن طريق مفتاح فك الشفرة". ثم تولت البنود التالية ١٠ & ١٢ & ١٣ الحديث عن تقنية شفرة المفاتيح العام والخاص والجذري.

ويرجع الاهتمام بهذه المسألة إلي أن البيئة الإلكترونية قد أظهرت الحاجة إلي ضرورة تشفير البيانات والمعلومات حفاظاً علي سريتها وعدم تمكين الغير من الإطلاع عليها أو التلاعب فيها. وتبدو فائدة عملية التشفير في أنها تسمح بتحويل بيانات المحرر الإلكتروني من لغة مفهومة إلي رموز وعلامات وشفرات غير مفهومة، ثم إعادة تحويلها إلي الحالة الأولى التي كانت عليها. وهو تأكيد لما

(١) د. هدي حامد قشقوش، الحماية الجنائية للتجارة الإلكترونية عبر الانترنت، دار النهضة العربية، ٢٠٠٠، ص ٤١.

H. XUE, Cyber Law in China, Kluwer Law International, 2010, P. 84.

(٢) د. عبد الفتاح بيومي حجازي، مرجع سابق، ص ٢٧٤.

(٣) منشور الوقائع المصرية، العدد ١١٥ (تابع) في ٢٥/٥/٢٠٠٥.

قرره القانون من الاعتراف بصحة نقل البيانات بطريقة الكترونية، إذ أن عملية النقل تستلزم - إذا أردنا الحفاظ علي سريتها وحمايتها من التلاعب - أن يقوم المرسل بتحويل النص إلي شفرات ثم يقوم المرسل إليه بفك شفرته.

وهكذا، يتضح الدور الجوهرى الذى يلعبه تشفير البيانات والمعلومات فى مجال المحررات الإلكترونية وما تحمله من توقيع إلكترونى.

المبحث الثانى

شهادات التصديق الإلكترونية

شهادة التصديق الإلكترونية هى الشهادة التى تصدرها سلطات التصديق الإلكترونية المرخص لها من قبل الجهات المسؤولة فى الدولة بممارسة نشاطها، لتشهد بموجبها بأن التوقيع الإلكتروني هو توقيع صحيح وينسب إلى من صدر عنه، ويستوفى الشروط والمعايير المطلوبة فيه باعتباره دليل إثبات يعول عليه، وعليه فإن جهات التصديق الإلكترونية أثناء قيامها بهذا الدور عليها واجب اتخاذ الحيطة والحذر والدقة لما يترتب على الشهادة التى تصدرها بذلك من خطورة فى إنشاء التصرفات القانونية والتى قد توجب مسئوليتها عند حدوث أى خطأ أو تقصير من جانبها.

وعلى هذا النحو يكمن الغرض من إصدار الشهادات الإلكترونية فى تأكيد أن التوقيع الإلكتروني أو الرسالة الإلكترونية صادرة ممن نسبت إليه وأن توقيعه الإلكتروني صحيح، كما تؤكد بأن البيانات الموقع عليها صحيحة وصادرة عن الموقع، ولم يتم التلاعب فيها ولم يطرأ عليها أى تعديل أو تغيير، وعندئذ تصبح هذه البيانات موثقة ولا يمكن إنكارها.

ونعرض من خلال هذا المبحث لشهادات التصديق الإلكتروني من خلال بيان ماهيتها، وكذلك اعتمادها، وذلك على النحو التالى:

المطلب الأول: ماهية شهادات التصديق الإلكتروني.

المطلب الثانى: اعتماد شهادات التصديق الإلكتروني.

المطلب الأول

ماهية شهادة التصديق الإلكتروني

إن البحث في ماهية شهادة التصديق الإلكتروني يقتضي أن نعرض أولاً للمقصود بهذه الشهادة، ونوضح ثانياً البيانات الواجب توافرها في شهادة التصديق الإلكتروني، وأخيراً نتناول كيفية إيقاف شهادة التصديق الإلكتروني وإلغاؤها.

الفرع الأول

المقصود بشهادة التصديق الإلكتروني

يمكن تعريف الشهادة بوجه عام بأنها مستند يصدق على معلومات معينة مدرجة فيه أو ترتبط به ارتباطاً منطقياً^(١).

في هذا السياق عرفت المادة الثالثة من التوجيه الأوروبي شهادات التصديق الإلكتروني بأنها "تلك التي تربط بين أداة التوقيع وبين شخص معين، وتؤكد شخصية الموقع".

وقد عرفها قانون الاونسترال النموذجي بشأن لتوقيعات الإلكترونيات بأنها "تعنى رسالة بيانات أو سجلاً آخرأ يؤكد الارتباط بين الموقع وبيانات إنشاء التوقيع"^(٢).

كما عرف قانون التوقيع الإلكتروني المصري شهادة التصديق الإلكتروني بأنها "الشهادة التي تصدر من الجهة المرخص لها بالتصديق وتثبت الارتباط بين الموقع وبيانات إنشاء التوقيع"^(٣).

(١) انظر:

AGOSTI (P.), La signature: De la sécurité juridique et la sécurité technique, Thèse Montpellier, 2003, P. 84.

(٢) المادة الثانية، فقرة ب، قانون الاونسترال النموذجي بشأن التوقيع الإلكتروني ٢٠٠١ م.

(٣) المادة الأولى، فقرة (و)، قانون التوقيع الإلكتروني المصري ١٥ لسنة ٢٠٠٤ م.

وقد عرف القانون التونسي الخاص بالمبادلات و التجارية الإلكترونية شهادة المصادقة الإلكترونية "الوثيقة الإلكترونية المؤمنة بواسطة الإضاء الإلكتروني للشخص الذي أصدرها والذي يشهد من خلالها اثر المعاينة، على صحة البيانات التي تتضمنها"^(١).

وقد عرفها قانون الإمارات الخاص بالمعاملات والتجارة الإلكترونية شهادة المصادقة الإلكترونية – شهادة يصدرها مزود خدمات التصديق يفيد فيها تأكيد هوية الشخص أو الجهة الحائزة على أداة توقيع معينة، ويشار إليها في هذا القانون بـ «الشهادة»^(٢).

وأما التوجيه الأوروبي رقم ٩٣ لسنة ١٩٩٩ فقد عرف في المادة التاسعة منه الشهادة الإلكترونية بأنها "كل شهادة إلكترونية أو إقرار إلكتروني يربط المعلومات المتعلقة بالتأكد من توقيع شخص ما بشخص معين كما تؤكد هوية هذا الشخص".

وتعرف كذلك شهادة التصديق الإلكتروني بأنها "وثيقة صادرة عن سلطة التصديق أو طرف ثالث موثوق به تم التوقيع عليها بمفتاحه الخاص، وتصاحب رسالة مشفرة، بهدف التصديق على صاحب الرسالة وتقديم المفتاح العام، وتحتوى هذه الوثيقة على اسم سلطة التصديق ومدة صلاحية الشهادة واسم صاحب الشهادة ومفتاحه العام لفك التشفير، وخوارزمية وإعدادات التشفير"^(٣).

وقد عرفها جانب من الفقه المصري بأنها شهادة تصدر أثناء عملية التوقيع الإلكتروني ومن شأنها إثبات هوية الموقع، ولذلك يطلق عليها أيضاً: بطاقة إثبات الهوية الإلكترونية، وعادة تختص جهة معينة بإصدار هذه الشهادة. هذه الجهة تختص أيضاً في نفس الوقت بالتصديق علي التوقيع الإلكتروني. وبمقتضى هذه الشهادة يمكن للجهة المختصة أن تشهد بصحة التوقيع وأن تحدد هوية الموقع^(٤).

وقد عرفها البعض من الناحية الفنية بأنها عملية الكترونية تربط بين شخص معين (طبيعي أو

(١) الفصل الثاني، المفاهيم ، القانون التونسي الخاص بالمبادلات والتجارية الإلكترونية رقم ٨٣ لسنة ٢٠٠٠.

(٢) المادة الثانية، الفصل الأول (التعريفات)، قانون رقم (٢) لسنة ٢٠٠٢ بشأن المعاملات والتجارة الإلكترونية للإمارات.

(٣) انظر:

GUALINO (J.), Dictionnaire pratique informatique, Internet et nouvelles technologies de l'information et de la communication, Paris, 2005, P. 85.

(٤) د. محسن البيه، دور المحررات الإلكترونية في الإثبات، مرجع سابق، ص ٥٦ .

(معنوي) بخصائص معينة تسمح بتمييزه عن غيره^(١).

ويتم التحقق من تلك المعلومات الموجودة في الشهادة عن طريق استخدام المفتاح العام لمن صدرت عنه الشهادة الإلكترونية، حيث تتضمن هذه الشهادة مفتاحاً عاماً وتفاصيل أخرى تؤكد أن الموقع المحدد في الشهادة هو حائز للمفتاح الخاص المناظر للمفتاح العام الوارد في الشهادة، أي أنها تقوم بربط مفتاح مزدوج بمشترك معين الأمر الذي يمكن متلقي الشهادة بان يستخدم المفتاح العام المذكور فيها للتأكد من أن التوقيع الإلكتروني استحدث من المفتاح الخاص المناظر وان الرسالة لم تتغير منذ التوقيع عليها^(٢).

وتنشئ شهادة التصديق الإلكتروني علاقة ثلاثية بين كل من جهة التصديق ، والموقع والمرسل إليه وتفرض هذه العلاقة الثلاثية بعض الالتزامات على عاتق كل طرف من أطرافها فتلتزم جهات التصديق باستخدام أنظمة ومعدات وموارد بشرية جديرة بالثقة ، وبذل العناية اللازمة ، واتخاذ الإجراءات المعقولة لضمان دقة وسلامة المعلومات الواردة في الشهادات التي تصدرها ، وأن تضع تحت تصرف المرسل إليه الوسائل المعقولة التي تمكنه من التحقق من سيطرة الموقع على وسيلة التوقيع وأنها كانت تحت سيطرته بالفعل وقت التوقيع ، والتعرف على الطريقة المتبعة لتحديد هوية الموقع^(٣).

وقد حرص المشرع الفرنسي على تعريف شهادة التصديق الإلكتروني في المرسوم رقم ٢٧٢ - ٢٠٠١ والصادر في ٣٠ مارس ٢٠٠١ في المادة الأولى الفقرة التاسعة منه بأنها "مستند في شكل إلكتروني تثبت توافر الرابطة بين بيانات التحقق من صحة التوقيع الإلكتروني وبين الموقع"^(٤).

وفي الفقرة التي تليها فقد أورد المشرع الفرنسي تعريفاً أيضاً لشهادة التصديق المؤهلة بأنها

(١) د. أيمن سعد سليم، التوقيع الإلكتروني، دراسة مقارنة، دار النهضة العربية، القاهرة، ٢٠٠٤، ص ٣٣.
BITAN (H.), Droit des créations immatérielles, Editions Lamy, 2010, P. 233.

(٢) د. طارق كميل، مقدمو خدمات المصادقة الإلكترونية (التنظيم القانون واجباتهم ومسئولياتهم)، مجلة جامعة الشارقة للعلوم الشرعية والقانونية، المجلد ٥، العدد ٣، ٢٠٠٨، ص ٢٤٥.

(٣) د. خالد عبد الفتاح محمد، التنظيم القانوني للتوقيع الإلكتروني، دراسة مقارنة، المركز القومي للإصدارات القانونية، الطبعة الأولى، ٢٠٠٩، ص ١٩٥.

(٤) انظر:

"Certificat électronique: un document sous forme électronique attestant du lien entre les données de vérification de signature électronique et un signataire".

"شهادة تصديق إلكتروني تلبى الاشتراطات المحددة في المادة السادسة من المرسوم الفرنسي"^(١).

والجدير بالذكر أن المادة السادسة من المرسوم الفرنسي قد اشترطت من أجل أن تكون شهادة التصديق الإلكتروني مؤهلة ضرورة أن تتضمن بعض العناصر المحددة في الفقرة الأولى وان تصدر بواسطة مقدم خدمات تصديق إلكتروني يستوفى الاشتراطات المنصوص عليها في الفقرة الثانية من هذا المرسوم.

ويلاحظ أن المشرع الفرنسي قد سار على نفس النهج الذي اتبعه التوجيه الأوربي في ١٣ ديسمبر ١٩٩٩ بشأن التوقيعات الإلكترونية ، حين أشار هذا التوجيه في المادة ٩/٢ إلى أن مصطلح الشهادة يقصد به " شهادة الكترونية تربط بين بيانات التحقق من صحة توقيع شخص معين وتؤكد هوية هذا الشخص"، وكذلك فقد عرف هذا التوجيه الشهادة المؤهلة بأنها "الشهادة التي تلبى الاشتراطات الواردة في الملحق رقم (١) والتي يوفرها مقدم خدمة تصديق يستوفى الاشتراطات الواردة في الملحق رقم (٢)".

الفرع الثاني

البيانات الواجب توافرها في شهادة التصديق الإلكتروني

من الجدير بالذكر أن قانون الأونسترال النموذجي للتوقيعات الإلكترونية لسنة ٢٠٠١ قد أشار لضرورة أن تتضمن شهادة التصديق الإلكترونية بعض البيانات الأساسية حتى توفر الثقة فيها ، كما بين أن الغرض من إيراد تلك البيانات هو إتاحة الفرصة للتحقق من ارتباط الموقع بالمفتاح العام وكذلك بالتبعية بالمفتاح الخاص^(٢).

وفقا لقانون الأونسترال النموذجي تقوم جهات تزويد خدمات التصديق الإلكتروني بتوفير قدر معقول من وسائل التدخل التي تمكن جهة التوثيق الإلكتروني من التأكد حيثما تراه ضرورياً من وجوب تضمين الشهادة العناصر الآتية^(٣):-

١- الطريقة المستخدمة في تحديد هوية صاحب التوقيع.

(١) انظر:

"Certificat électronique qualifié: un certificat électronique répondant aux exigences définies à l'article 6".

(٢) دليل إشتراع قانون الأونسترال النموذجي بشأن التوقيعات الإلكترونية عام ٢٠٠١، ص ٧٨.

(٣) المادة ٩/د من قانون الأونسترال النموذجي للتوقيعات الإلكترونية لسنة ٢٠٠١.

٢- حدود الغرض والقيمة التي تستخدم شهادة المصادقة الإلكترونية من أجلها.

٣- البيانات اللازمة لإنشاء توقيع الكترونية صحيحة.

٤- حدود المسؤولية القانونية لمقدم خدمات التوثيق الإلكتروني.

ويتضح من ذلك انه يجب أن تتضمن شهادة التصديق الإلكتروني وفقا للقانون النموذجي البيانات الضرورية التي تتيح للأفراد تحديد هوية مقدم خدمة التصديق الإلكتروني مع ضمان أن الشخص المحدد هويته في الشهادة كان مسيطرا على إتمام التوقيع الإلكتروني وقت إصدار الشهادة وان أداة التوقيع صالحة للاستخدام في هذا الوقت.

أما بالنسبة للتوجيه الاوربي رقم ٩٣ لسنة ١٩٩٩ فقد اعترف بالقيمة القانونية لشهادات التصديق الإلكتروني إذا تضمنت البيانات التالية:-

١- تحديد شخصية مقدم خدمة التصديق والدولة التي أنشأ بها لممارسة اختصاصاته.

٢- اسم الموقع الفعلي أو اسمه المستعار الذي يمكن التحقق من خلاله على شخصيته.

٣- المفتاح العام الذي يمكن من خلاله الوصول للمفتاح الخاص للموقع والذي يخضع لرقابته.

٤- تحديد مدة صلاحية الشهادة من بدايتها وحتى نهايتها.

٥- الرقم المسلسل الخاص بالشهادة.

٦- التوقيع الإلكتروني لمقدم خدمة التصديق الإلكتروني بتسليم الشهادة.

٧- عند الاقتضاء حدود استخدام الشهادة.

وقبل اكتمال الشهادة يجب على مقدم خدمة التصديق الإلكتروني أن يتحقق عن طريق الوسائل المناسبة من صفة الشخص الذي ستسلم إليه الشهادة، يجب أن يتحقق من صحة البيانات التي تحتويها الشهادة، ويجب كذلك على مقدم خدمة التصديق اتخاذ الوسائل التي تكفل عدم تزوير الشهادة وكذلك يجب عليه تحديد الوقت وبكل دقة الذي من خلاله يستطيع اي من أطراف التعاقد تعديل أو فسخ

الصفحة محل الشهادة الإلكترونية وكذلك إمكانية تقديم الشهادة من قبل جهات التوثيق الإلكتروني لأصحاب المصلحة في طلبها ولكن بشروط خاصة^(١).

ويوجب المرسوم الفرنسي ٢٧٢ - ٢٠٠١ سالف الذكر أن تتضمن الشهادة ما يفيد بأنها صادرة بوصفها شهادة تصديق إلكتروني مؤهلة وهو بيان جوهري ليس فقط لأصاحب الشهادة بل للغير الذي يعول على تلك الشهادة.

وهذا ما أقدم المشرع المصري على توضيحه في المادة ٢/٢٠ من اللائحة التنفيذية لقانون التوقيع الإلكتروني حين تطلب ضرورة أن تشتمل نماذج شهادات التصديق الإلكتروني التي يصدرها مقدم الخدمات على ما يفيد صلاحية تلك الشهادة للاستخدام في التوقيع الإلكتروني، واشتمالها كذلك على موضوع الترخيص الصادر لمقدم الخدمات المرخص له، موضحاً فيه نطاقه ورقمه وتاريخ إصداره وفترة سريانه.

وقد تناول القانون الإماراتي الخاص بالتجارة الإلكترونية في المادة ٢٤ منه التزامات وواجبات وبيانات يجب على جهة التصديق الإلكتروني مراعاتها عند إصدار شهادات التوثيق الإلكتروني فيجب أن تتضمن الشهادة ما يلي^(٢):-

- ١- هوية مزود خدمات التصديق.
- ٢- أن الشخص المعينة هويته في الشهادة لديه السيطرة في الوقت المعني على أداة التوقيع المشار إليها في الشهادة.
- ٣- الطريقة المستخدمة في تعيين هوية الموقع.
- ٤- وجود أية قيود على الغرض أو القيمة التي يجوز أن تستخدم من أجلها أداة التوقيع.
- ٥- ما إذا كانت أداة التوقيع صحيحة ولم تتعرض لما يثير الشبهة.
- ٦- ما إذا كان للموقع وسيلة لإعطاء إشعار بموجب المادة (٢٢) (١) - (أ)، (ب) من هذا القانون.

(١) د. سعيد السيد فنديل، التوقيع الإلكتروني، دار الجامعة الجديدة للنشر، الإسكندرية، ٢٠٠٤، ص ٨١.

(٢) المادة ٢٤ من قانون التجارة الإلكترونية الإماراتي رقم ٨٣ لسنة ٢٠٠٢.

٧- ما إذا كان هناك وسيلة مناسبة للإبلاغ عن الإلغاء.

أما بالنسبة للمشرع المصري فقد حددت اللائحة التنفيذية لقانون التوقيع الإلكتروني البيانات الواجب تضمينها لشهادات التصديق الإلكتروني وهي^(١):-

١- ما يفيد صلاحية هذه الشهادة للاستخدام في التوقيع الإلكتروني.

٢- موضوع الترخيص الصادر للمرخص له، موضعاً فيه نطاقه ورقمه وتاريخ إصداره وفترة سريانه.

٣- اسم وعنوان الجهة المصدرة للشهادة ومقرها الرئيسي وكيانها القانوني والدولة التابعة لها.

٤- اسم الموقع الأصلي أو اسمه المستعار أو اسم شهرته وذلك في حالة استخدامه لأحدهما.

٥- صفة الموقع.

٦- المفتاح الشفري العام لحائز الشهادة المناظر للمفتاح الشفرة الخاص به.

٧- تاريخ بدء صلاحية الشهادة وتاريخ انتهائها.

٨- الرقم المسلسل للشهادة.

٩- التوقيع الإلكتروني لجهة إصدار الشهادة.

١٠- عنوان الموقع الإلكتروني المخصص لقائمة الشهادات الموقوفة أو الملغاة.

وقد نصت اللائحة التنفيذية على بيانات يجوز إضافتها عند الحاجة إليها من قبل ذوى الشأن بناءً على طلبهم وهي:-

١- ما يفيد اختصاص الموقع والغرض من استخدام الشهادة.

٢- حدود قيمة التعاملات المسموح بها للشهادة.

٣- مجالات استخدام الشهادة.

(١) المادة ٢٠ من اللائحة التنفيذية ١٠٩ لسنة ٢٠٠٥ لقانون التوقيع الإلكتروني المصري ١٥ لسنة ٢٠٠٤.

ويلاحظ مما تقدم عرضه أن اغلب التشريعات على المستوى الدولي قد عملت على تنظيم الشهادات الإلكترونية ودور جهات التوثيق الإلكتروني بصددھا، ويتمثل دورھا بالفعل في التأكيد على صحة التوقيع الإلكتروني ونسبته إلى صاحبه من خلال التأكيد على صحة البيانات الواردة فيه^(١).

وتكمن قيمة هذه الشهادة في أنها تضمن أن الجهة الصادر عنها الشهادة قد ثبت لديها أن أداة التوقيع المستخدمة تكفل تحقق الشروط الواردة بالمادة ١٨ من قانون التوقيع الإلكتروني المصري. وذلك بالتنبث من الارتباط بين الموقع علي المحرر الإلكتروني وبيانات إنشاء التوقيع. إذا يمكن جمع البيانات الواجب توافرها في شهادة التصديق الإلكتروني المعتمدة أو المؤهلة في ثلاث طوائف وهم بيانات تتعلق بالشهادة نفسها وبيانات تتعلق بصاحب التوقيع وبيانات تتعلق بمقدم خدمات التصديق الإلكتروني.

ويضاف لما سبق ضرورة التأكيد على أن مقدم خدمة التصديق الإلكتروني يجب عليه أن يوقع على الشهادة ببيانات إنشاء التوقيع الخاصة به (المفتاح الشفري الخاص) حتى يطمئن الطرف الذي يعول على التوقيع الإلكتروني لمقدم الخدمة إلى صحة التوقيع الإلكتروني^(٢).

ويأتي ذلك للمحافظة والتأكيد على صحة الشهادة فيما يتعلق بكل محتواھا ومصدرھا ، وحتى يتسنى لصاحب الشهادة أو الغير الذي يعول على تلك الشهادة أن يتأكد من تصديق مقدم الخدمات (المحدد هويته في الشهادة) على المعلومات الواردة فيها والتيقن من المحافظة على سلامة تلك المعلومات^(٣).

الفرع الثالث

إيقاف شهادة التصديق الإلكتروني وإلغائها

تثار إشكالية عند تعرض المفتاح الخاص للموقع لما يثير الشبهة مثل حالة فقد الموقع لسيطرته على ذلك المفتاح، مما تفقد معه الشهادة جدارتها للثقة أو تصبح غير قابلة للتحويل عليها. وقد يعمد

(١) د. طارق كميل، مقدمو خدمات المصادقة الإلكترونية، المرجع السابق ص ٢٤٩.

(٢) دليل إشتراع قانون الأونسترال النموذجي بشأن التوقيعات الإلكترونية عام ٢٠٠١، ص ٣٤.

(٣) انظر:

مقدم خدمات التصديق الإلكتروني بناء على طلب الموقع أو حتى بدون موافقته وفقاً للظروف إلى إيقاف الشهادة مؤقتاً أو إلى إلغائها.

ولكن يوجد التزام يلقى على عاتق مقدم خدمات التصديق الإلكتروني في حالة القيام بتعليق العمل بالشهادة الإلكترونية أو حالة إلغائها فيجب عليه أن يعلن ذلك الأمر على عنوان الموقع الإلكتروني المخصص لقائمة الشهادات الموقوفة أو الملغاة والمبين في الشهادة، بما يؤدي إلى علم الأطراف المعولة على التوقيع الإلكتروني بان الشهادة قد فقدت جدارتها بالثقة أو أصبحت غير قابلة للتحويل عليها^(١).

أولاً: إيقاف شهادة التصديق الإلكتروني:-

ويقصد بذلك الوقف المؤقت لسريان الشهادة وتعطيل العمل بالأثر القانوني المترتب عليها تمهيداً لإلغائها^(٢). ويزيد البعض من القول بان إيقاف الشهادة أي اعتبارها كأن أم تكن تمهيداً لإلغائها أو استئناف سريانها متى ثبت عدم صحة السبب الذي تم بناء عليه وقف هذه الشهادة^(٣).

وقد حددت اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري حالات إيقاف شهادة التصديق الإلكتروني وهي^(٤):-

١- العبث ببيانات الشهادة أو انتهاء مدة صلاحيتها.

٢- سرقة أو فقد المفتاح الشفري الخاص أو البطاقة الذكية، أو عند حدوث شك في حدوث ذلك.

(١) المادة ٢٠ فقرة ١٠ من اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري ١٥ لسنة ٢٠٠٤ م، حيث فرضت التزاماً على عاتق مقدم خدمات التصديق الإلكتروني بأن ينشئ موقعاً إلكترونياً على شبكة الانترنت، يعلن من خلاله عن الشهادات الموقوفة أو الملغاة.

(٢) انظر:

VERBIEST (Th.) & WÉRY (E.), Le droit de l'internet et de la société de l'information: droits européen, belge et français, Larcier, 2002, P. 381.

(٣) د. تامر الدمياطي، مرجع سابق، ص ٥٦٧.

(٤) المادة ١٢ من اللائحة التنفيذية ١٠٩ لسنة ٢٠٠٥ لقانون التوقيع الإلكتروني المصري ١٥ لسنة ٢٠٠٤.

٣- عدم التزام الشخص المصدر له شهادة التصديق الإلكتروني ببند العقد المبرم مع المرخص له.

ويكون نظام إيقاف الشهادة وفقا للقواعد التي يضعها مجلس إدارة هيئة تنمية صناعة تكنولوجيا المعلومات، ولا شك أن هذه التصرفات غير المشروعة التي تؤدي لإيقاف الشهادة تزعزع الثقة في الشهادة وفي استقرار المعاملات الإلكترونية.

– حالات وقف العمل بالشهادة:-

١- بناء على طلب صاحب الشهادة:-

ويقصد بصاحب الشهادة هو كل شخص طبيعي مرخص له باستخدام الشهادة سواء كان ذلك بصفة أصلية أم باعتباره ممثلاً قانونياً لأحد الأشخاص المعنوية ، ويكون لمستخدم الخدمة الحق في إيقاف الشهادة في حالة إصدارها بصفته الشخصية، ويكون لجهة العمل والشخص المفوض فقط الحق في طلب الإيقاف لأي شهادة صادرة للعاملين بهذه الجهة^(١).

وينبغي أن يكون طلب الإيقاف له ما يبرره من سند واقعي ويقنع به مقدم الخدمة لاتخاذ إجراء الإيقاف، خاصة وان شهادة التصديق الإلكتروني فور صدورها واستعمالها يتعلق بها حقوق للغير^(٢).

٢- تغيير البيانات الواردة في الشهادة أو العبث بها:-

تفترض شهادة التصديق أن البيانات التي تتضمنها صحيحة لم تتغير وذلك خلال مدة سريان الشهادة ، الأمر الذي يتطلب معه ضرورة قيام صاحب الشهادة بإعلام مقدم الخدمة بأي تغيير يطرأ على بياناته المدونة في الشهادة ، ويجب على مقدم الخدمة في حالة علمه بتغيير البيانات المتعلقة بالشهادة أن يغير الشهادة ويخطر ذوى الشأن بذلك.

ويتعين على مقدم خدمات التصديق أن يوقف الشهادة متى علم بان تغييرا قد حدث في البيانات التي صدرت الشهادة بناء عليها، نتيجة العبث بتلك البيانات^(١).

(١) راجع: ترخيص تقديم خدمات التوقيع الإلكتروني الصادر من هيئة تنمية صناعة تكنولوجيا المعلومات رقم ١٠٣ لسنة ٢٠٠٦، ص ٤٥.

(٢) د. تامر الدمياطي، مرجع سابق، ص ٥٦٧.

ونحن نتفق مع ما ذهب إليه البعض من أن اللائحة التنفيذية لقانون التوقيع الإلكتروني لم تحدد صور "العبث" ببيانات الشهادة حتى يتم تفسير ذلك تفسيراً واسعاً للوقوف ضد أى محاولة لتعديل بيانات الشهادة أو المساس بها^(٢).

ويفرق بين حالة العبث بالشهادة وحالة تعديل أو تغيير البيانات ، أما العبث ببيانات الشهادة فيكون ذلك رغماً عن مقدم الخدمة أو صاحب الشهادة ، أما تعديل البيانات سواء بيانات تتعلق بصاحب الشهادة من بيانات شخصية أو بيانات موضوعية تتعلق بموضوع الشهادة ومجالات استعمالها فتكون بمحض إرادته.

٣- انتهاء مدة صلاحية الشهادة:-

كل شهادة الكترونية لها مدة صلاحية تسرى خلالها، ومدة الشهادة من البيانات الجوهرية التي يجب أن تتضمنها الشهادة.

وتوجب اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري على مقدم خدمات التصديق الإلكتروني التأكد من صلاحية الشهادة للعمل بها وأنها سارية، وعليه أن يصدر قراراً بإيقاف العمل بالشهادة متى انتهت مدة صلاحيتها.

٤- سرقة أو فقد المفتاح الشفري الخاص أو البطاقة الذكية، أو عند الشك في حدوث ذلك^(٣):-

حيث أوجبت اللائحة التنفيذية على مقدم الخدمة أن يسارع من تلقاء نفسه إلى إيقاف العمل بالشهادة متى ثبت سرقة أو فقد المفتاح الشفري الخاص بالموقع أو البطاقة الذكية التي تحتوى على عناصر متفردة وهى بيانات إنشاء التوقيع الإلكتروني وشهادة التصديق الإلكتروني، أو عند الشك في حدوث ذلك^(٤).

٥- عدم التزام الشخص المصدر له شهادة التصديق ببند العقد المبرم مع المرخص له:-

(١) راجع: المادة ١٢/ ط - ١ من اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري.

(٢) د. تامر الدمياطي، مرجع سابق، ص ٥٦٨.

(٣) راجع: المادة ١٢/ ط - ٢ من اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري.

(٤) راجع: المادة ٣ / د من اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري.

ويحكم المصدر له والمرخص له العلاقة التعاقدية الناشئة عن العقد المبرم بينهما مما يرتب ذلك المسؤولية العقدية حالة مخالفة أى بند من بنود الاتفاق ويتم وقف تلك الشهادة مؤقتاً^(١).

ثانياً: إلغاء شهادة التصديق الإلكتروني:-

لم يتعرض قانون التوقيع الإلكتروني المصري أو لائحته التنفيذية لقواعد وحالات إلغاء الشهادة ، على الرغم من تضمينه لبيانات الشهادة بيانا يقتضى وجود عنوان موقع إلكتروني مخصص لقائمة الشهادات الموقوفة أو الملغاة مما يسجل معه قصور تشريعي في هذا المجال وعلى الرغم من تعرضه لحالات إيقاف الشهادة وترك الأمر الأكثر خطورة وهو إلغاء الشهادة.

- حالات إلغاء شهادة التصديق الإلكتروني:-

١- طلب صاحب الشهادة الإلكترونية:-

حيث أن الشهادة تحمل صفة شخصية لصاحب الشهادة ذاته فيمكن إلغاؤها متى طلب صاحبها ذلك، ويكون لجهة العمل والشخص المفوض فقط الحق في إلغاء أية شهادة مصدرة للعاملين بهذه الجهة^(٢).

٢- وفاة الشخص الطبيعي وانتهاء الشخص المعنوي:-

لا يوجد داعي لوجود التوقيع الإلكتروني في حالة وفاة الشخص الطبيعي ويجب بناء عليه إلغاء الشهادة الإلكترونية ، وكذلك في حالة حل الشخص المعنوي أو انقضائه كحل الشركة أو تصفيتها أو إفلاسها أو إلغاء إحدى الهيئات أو المؤسسات العامة أو إعادة دمجها في هيئة عامة أخرى أو مؤسسة عامة أخرى ، وتلغى بناء عليه شهادة التصديق الإلكتروني الخاصة بالشخص المعنوي والتي تصدر باسم الممثل القانوني له^(٣).

٣- إلغاء الشهادة التي سبق إيقافها بصفة مؤقتة:-

(١) راجع: المادة ١٢ / ط - ٣ من اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري.

(٢) راجع: الترخيص رقم ١٠٣ / ٢٠٠٦ الصادر من هيئة تنمية صناعة تكنولوجيا المعلومات بشأن تقديم خدمات التوقيع الإلكتروني، ص ٤٥.

(٣) د. تامر الدمياطي، مرجع سابق، ص ٥٧٠.

بعد أن قام مقدم الخدمة بإيقاف الشهادة مؤقتاً في الحالات السابق ذكرها فعليه أن يتحرى بنفسه بواسطة وسائل مادية أو فنية عن مدى صحة سبب الإيقاف وإذا تحقق بالفعل من سبب الإيقاف فيمكن له إلغاء شهادة التصديق الإلكتروني بصفة نهائية.

ويجوز لصاحب الشهادة أو للغير المتعامل معه بمقتضى تلك الشهادة الاعتراض على القرار الصادر من مقدم خدمة التصديق الإلكتروني بإلغاء الشهادة ويكون ذلك الاعتراض منذ لحظة نشر القرار بالموقع الإلكتروني الخاص بقائمة الشهادات الموقوفة أو الملغاة^(١).

٤- توقف مقدم خدمات التصديق عن تقديم الخدمات المرخص بها:-

في حالة رغبة مقدم الخدمة المرخص له من قبل الهيئة عن التوقف عن تقديم الخدمات فإنه يلتزم بعد الحصول على الموافقة المسبقة من الهيئة بإلغاء كل شهادات التصديق الإلكتروني المصدرة منه لمستخدمي الخدمة المتعاملين معه، وذلك اعتباراً من تاريخ التوقف عن الخدمة.

ويستوي في ذلك التوقف عن تقديم الخدمة بمحض إرادته أو كنوع من العقاب بسحب الترخيص الممنوح له من قبل الهيئة مما يوجب معه التزامه بدفع التعويضات اللازمة لمستخدمي الخدمة أو دفع تكاليف إصدار شهادات جديدة لهم من مقدم خدمة آخر يختاره مستخدم الخدمة إذا دعت الضرورة ذلك، ويجب على مقدم الخدمة الذي يرغب في التوقف عن تقديم الخدمات أن يخطر مستخدم الخدمة مسبقاً عن طريق رسالة الكترونية قبل إجراء أي معاملة الكترونية تعتمد على توقيعه الإلكتروني بتاريخ إيقاف الخدمة^(٢).

(١) د. عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظم القانونية المقارنة، مرجع سابق، ص ١٨٥.

(٢) راجع: الترخيص رقم ١٠٣ / ٢٠٠٦ الصادر من هيئة تنمية صناعة تكنولوجيا المعلومات بشأن تقديم خدمات التوقيع الإلكتروني، ص ٣٣، ٣٤.

المطلب الثاني

اعتماد شهادات التصديق الإلكتروني

إن البحث في اعتماد شهادات التصديق الإلكتروني يتطلب أن نقسم هذا المطلب إلى ثلاثة فروع، نبحث في الأول أنواع شهادات التصديق الإلكتروني، بينما نعرض في الثاني لاعتماد شهادات التصديق الأجنبية، ونوضح في الثالث سلطة الموثق الإلكتروني في التأكد من الأهلية والهوية.

الفرع الأول

أنواع شهادات التصديق الإلكتروني

تجدر الإشارة هنا إلى وجود نوعين من شهادات التصديق الإلكتروني، وهما شهادات تصديق إلكتروني بسيطة أو عادية، وشهادات تصديق إلكتروني معتمدة أو موصوفة على حد تعبير البعض^(١).

النوع الأول: شهادة التصديق الإلكتروني البسيطة:-

شهادة التصديق الإلكتروني البسيطة هي وثيقة الكترونية تصدرها الهيئة المختصة بإصدار شهادات التصديق الإلكتروني وتتضمن بيانات بسيطة تتعلق بصحة بيانات التوقيع الإلكتروني ونسبته إلى الموقع، ولا تشمل بيانات غير ذلك وتستخدم في التأكيد من صحة البريد الإلكتروني^(٢).

وقد عرفها المرسوم الفرنسي رقم ٢٧٢ لسنة ٢٠٠١ على هذه الشهادات البسيطة في المادة الأولى منه بأنها عبارة عن مستند يظهر في شكل إلكتروني ويشهد بوجود علاقة بين بيانات التحقق من التوقيع الإلكتروني وشخصية الموقع.

ويقصد بهذه الشهادة رسالة بيانات أو محرر إلكتروني صادر من هيئة تنمية صناعة تكنولوجيا المعلومات، أو من الغير الذي تعهد له هذه الهيئة بتقديم هذه الخدمة تحت إشرافها وتفيد هذه الشهادة

(١) د. عابد فايد، الكتابة الإلكترونية في القانون المدني، المرجع السابق، ص ٧٧.

(٢) د. أيمن سعد سليم، التوقيع الإلكتروني، دراسة مقارنة، دار النهضة العربية، ٢٠٠٤، ص ٣٦.

BITAN (H.), Protection et contrefaçon des logiciels et des bases de données, Editions Lamy, 2006, P. 163.

تحقق الهيئة مما يأتي^(١):

(أ) سلامة شهادة التصديق الإلكتروني وتوافقها مع بيانات إنشاء التوقيع الإلكتروني.

(ب) إمكان تحديد مضمون المحرر الإلكتروني في الموقع بدقة.

(ج) سهولة العلم بشخص الموقع سواء في حالة استخدام اسمه الأصلي أم استخدامه لاسم مستعار أم اسم الشهرة.

ويجوز للهيئة أن تعهد للغير بتقديم هذه الخدمة تحت إشرافها وفي جميع الأحوال تصدر الهيئة شهادة فحص التوقيع الإلكتروني.

ولكن إذا لم يتمكن صاحب الشأن – وهو من يستند إلي المحرر الإلكتروني الموقع إلكترونياً – من تقديم الشهادة السابقة، فعليه أن يتقدم بشهادة فحص التوقيع الإلكتروني^(٢).

النوع الثاني: شهادة التصديق الإلكتروني المعتمدة:-

هي شهادة تصدرها الجهة المختصة بإصدار شهادات التصديق الإلكتروني وتهدف لتأكيد صحة بيانات التوقيع الإلكتروني ونسبته إلي صاحبه، وتتضمن الشهادة المعتمدة الكثير من البيانات التي تجعلها أكثر أماناً للمتعاملين^(٣).

وعرفها البعض بأنها شهادة معتمدة تصدر عن أحد مقدمي خدمات التوثيق الإلكتروني المرخص لها من قبل الجهات الرسمية في الدولة لتربط المفتاح العام الذي استخدم في فك التشفير بشخص بعينه، وبالتالي يتحول المرسل من شخص افتراضي إلي شخص محدد الهوية^(٤). فضلاً عن

(١) المادة (٧) من اللائحة التنفيذية لقانون التوقيع الإلكتروني.

(٢) تنص المادة (٦) من اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري علي أن: "تقدم الهيئة، بناء علي طلب كل ذي شأن، خدمة الفحص والتحقق من صحة بيانات إنشاء التوقيع الإلكتروني نظير مقابل يحدد فئاته مجلس إدارة الهيئة، ويجوز للهيئة أن تعهد للغير بتقديم هذه الخدمة تحت إشرافها ، وفي جميع الأحوال تصدر الهيئة شهادة فحص بيانات إنشاء التوقيع الإلكتروني".

(٣) د . عابد فايد، الكتابة الإلكترونية في القانون المدني، المرجع السابق، ص ٧٨.

CACHARD (O.), La régulation internationale du marché électronique, Librairie générale de droit et de jurisprudence, 2002, P. 378.

(٤) وفي هذا السياق عرفت المادة الثالثة من التوجيه الأوربي شهادات التوثيق الإلكتروني بأنها تلك التي تربط بين أداة التوقيع وبين شخص معين، وتؤكد شخصية الموقع.

اشتمالها على تأكيد بأن التوقيع المعنى قد استوفى كافة الشروط والضوابط المطلوبة فيه باعتباره دليل إثبات يُعول عليه^(١).

وقد تناول المرسوم الفرنسي رقم ٢٧٢ لسنة ٢٠٠١ عن الشهادة الإلكترونية المعتمدة وهي تلك التي ينبغي أن تستوفى مجموعة من الضوابط والمعايير التي ورد النص عليها في المرسوم. ووفقاً لما ورد النص عليه في المادة السادسة من هذا المرسوم فإنه يجب أن تسلم الشهادة المعتمدة من مقدم خدمة توثيق مؤهل لتسليم هذا النوع من الشهادات .

ويجب أن تتضمن هذه الشهادة البيانات المحددة التالية:

- ١- بيان يشير إلي أن هذه الشهادة مسلمة كشهادة الكترونية معتمدة.
- ٢- هوية مقدم خدمة التصديق الإلكتروني وحالته التي تأسس فيها.
- ٣- إسم الموقع أو الإسم المستعار.
- ٤- وعند الضرورة بيان صفة الموقع بحسب الإستعمال التي خصصت الشهادة له.
- ٥- بيانات ومعطيات التحقق من التوقيع الإلكتروني.
- ٦- بداية ونهاية مدة صلاحية الشهادة الإلكترونية.
- ٧- كود التعامل مع الشهادة الإلكترونية.
- ٨- التوقيع الإلكتروني المؤمن لمقدم خدمة التوثيق الإلكتروني الذي يُسلم شهادات معتمدة.

وطبقاً للمادة (٦) من المرسوم الفرنسي الصادر في ٣٠ مارس لسنة ٢٠٠١، فإن التوقيع المصدق عليه بشهادة التصديق المعتمدة يعتبر توقيعاً صادراً من صاحبه، وهو حجة في الإثبات، وعلي من يدعي العكس إثبات ما يدعيه. وبعبارة أخرى، فإن شهادة التصديق علي التوقيع الإلكتروني المعتمدة هي بمثابة قرينة بسيطة علي صحة التصرف القانوني المشمول على توقيع إلكتروني مصدق عليه^(٢).

(١) راجع في ذلك: د. إبراهيم الدسوقي أبو الليل، الجوانب القانونية للتعاملات الإلكترونية، المرجع السابق، ص ١٨٣.

(٢) د. محسن البيه، دور المحررات الإلكترونية في الإثبات، المرجع السابق، ص ٦٢ .

ولكن إعمال هذه القرينة يستلزم توافر الشروط الآتية^(١):

- ١- أن تكون وسيلة التوقيع الإلكتروني تحت سيطرة الموقع وحده دون غيره.
- ٢- أن يكون هذا التوقيع موثقاً فيه بناءً على أن النظام الإلكتروني الذي أنشأ هذا التوقيع يمكن الوثوق به.
- ٣- أن يكون فحص التوقيع الإلكتروني مستنداً على شهادة التوقيع الإلكتروني المعتمدة.

فهذه الشهادة الإلكترونية - على حد تعبير المشرع الفرنسي في المادة الأولى من المرسوم رقم ٢٧٢ لسنة ٢٠٠١ الصادر في ٣٠ مارس ٢٠٠١ - مستند في شكل إلكتروني يقيم صلة دقيقة بين البيانات المستخدمة في التحقق من التوقيع وشخص الموقع ذاته ، بحيث يمكن للمرسل إليه الاطمئنان إلي مصدر الرسالة هو ذات الشخص المحدد في هذه الشهادة وتأكيداً لذلك فقد كان هذا القانون رغبة من المشرع الفرنسي لتحديد الشروط اللازمة للتوقيع الإلكتروني الموثوق فيه^(٢).

فالشهادة الإلكترونية المعتمدة تؤدي ذات الدور الذي يؤديه جواز السفر الرسمي الذي تصدره الدولة أو البطاقة الشخصية التي يحملها المواطن. فكما أن جواز السفر أو البطاقة الشخصية وثيقة رسمية تقيم صلة بين الصورة الملتصقة فيه وبين شخص صاحب التوقيع الخطي أو اليدوي الموضوع عليه، فإن الشهادة المعتمدة تقيم صلة رسمية بين هوية الشخص المرسل ومفتاحه العام^(٣).

كما ربطت المادة (٤-١٣١٦) من التقنين المدني الفرنسي^(٤) حجية التوقيع الإلكتروني في الإثبات بمدى قدرته على تحديد هوية الموقع من ناحية، وضمان صلته بالمحرر الذي وقع عليه من

(١) انظر :

JOLY-PASSANT (E.), Le décret du 30 mars 2001 pris pour l'application de l'article 1316-4 du Code civil et relatif à la signature électronique, Revue Lamy Droit des affaires, Juillet 2001, N° 40, P. 21.

(٢) د. محمد محمد أبو زيد، تحديث قانون الإثبات، مكانة المحررات الإلكترونية بين الأدلة الكتابية، ٢٠٠٢، ص ٢٠٢.

(٣) د. مصطفى أبو مندور موسى، خدمات التوثيق الإلكتروني، مرجع سابق، ص ٣٦.

(٤) انظر :

Article 1316-4 : « Lorsqu'elle (la signature) est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature est créée.....dans des conditions fixées par décret en Conseil d'Etat. »

ناحية ثانية، وأقامت من هذين الأمرين قرينة قانونية بسيطة على صحة هذا التوقيع، شريطة أن يتم ذلك وفقاً للشروط التي يحددها مرسوم يصدر من مجلس الدولة لتطبيق هذا النص^(١).

ولذا فقد نصت مختلف التشريعات على وجوب تضمين الشهادة المعتمدة بيانات معينة تساعد على تحقيق هذا الغرض كاسم الحامل، أي صاحب الشهادة، ومفتاحه العام، واسم هيئة التوثيق، وفترة صلاحية الشهادة، والحد الأقصى لقيمة التعاملات التي تستخدم الشهادة في إبرامها... الخ^(٢)، فالشهادة الإلكترونية هي، إذن، حقيقة معلوماتية تسمح بما لا يدع مجالاً لأي شك، بربط هوية كائن معين (شخص أو هيئة) بمجموعة معينة من السمات المميزة له.

شروط إصدار شهادات التصديق على التوقيع الإلكتروني في مصر:

تنص المادة (١٩) من قانون التوقيع الإلكتروني رقم ١٥ لسنة ٢٠٠٤، على أنه: "لا تجوز مزاوله نشاط إصدار شهادات التصديق الإلكتروني إلا بترخيص من الهيئة، وذلك نظير مقابل يحدده مجلس إدارتها وفقاً للإجراءات والقواعد والضمانات التي تقررها اللائحة التنفيذية لهذا القانون ودون التقيد بأحكام القانون رقم ١٢٩ لسنة ١٩٤٧ بالتزامات المرافق العامة. ومع مراعاة ما يأتي: (أ) أن يتم اختيار المرخص له في إطار من المنافسة والعلانية. (ب) أن يحدد مجلس إدارة الهيئة مدة الترخيص بحيث لا تزيد على تسعة وتسعين عاماً. (ج) أن تحدد وسائل الإشراف والمتابعة الفنية والمالية التي تكفل حسن سير المرفق بانتظام واطراد.

ولا يجوز التوقف عن مزاوله النشاط المرخص به أو الاندماج في جهة أخرى أو التنازل عن الترخيص للغير إلا بعد الحصول على موافقة كتابية مسبقة من الهيئة".

وبناءً عليه فقد تطلب القانون لمزاوله نشاط إصدار شهادات التصديق الإلكتروني في مصر

شروطاً ثلاثة تتمثل في الآتي:-

(١) من أوضح التشريعات العربية التي أخذت بهذه القرينة في الإثبات، التشريع البحريني الخاص بالتجارة الإلكترونية الصادر بتاريخ ١٤ سبتمبر ٢٠٠٢م إذ ورد النص في الفقرة الثالثة من المادة السادسة على أنه "إذا عرض بصدد أية إجراءات قانونية توقيع إلكتروني مقرون بشهادة معتمدة، قامت القرينة على صحة ما يأتي ما لم يثبت العكس أو يتفق الأطراف على خلاف ذلك: ١- أن التوقيع على السجل الإلكتروني هو توقيع الشخص المسمى في الشهادة المعتمدة. ٢- أن التوقيع الإلكتروني على السجل الإلكتروني قد وضع من قبل الشخص المسمى في الشهادة المعتمدة بغرض توقيع هذا السجل. ٣- أن السجل الإلكتروني لم يطرأ عليه تغيير منذ وضع التوقيع عليه.

(٢) انظر على سبيل المثال المادة رقم ٢٠ من اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري الصادرة بالقرار رقم

١٠٩ لسنة ٢٠٠٥م بتاريخ ١٥/٥/٢٠٠٥م.

أولاً:- ضرورة حصول من يرغب في مزاولة نشاط إصدار شهادات التصديق الإلكتروني على ترخيص بذلك من هيئة تنمية صناعة تكنولوجيا المعلومات باعتبارها الجهة الوحيدة المنوط بها إصدار هذا الترخيص، وفقاً للشروط والإجراءات التي تقرها اللائحة التنفيذية لقانون التوقيع الإلكتروني.

ثانياً:- عدم جواز احتكار نشاط إصدار شهادة التصديق الإلكتروني إذ يتم اختيار المرخص له وفقاً لقواعد المنافسة والعلانية، منعاً لاحتكار هذا العمل والتحكم فيه.

ثالثاً:- عدم جواز توقف المرخص له بممارسة نشاط التصديق الإلكتروني عن نشاط التصديق أو الاندماج في جهة أخرى أو التنازل عن الترخيص للغير إلا بعد الحصول على موافقة كتابية من الهيئة، ومن يخالف ذلك يعرض جهة التصديق على التوقيع للعقوبات الوارد ذكرها في المادة ٢٣ من القانون ١٥ لسنة ٢٠٠٤ الخاص بالتوقيع الإلكتروني^(١).

الفرع الثاني

اعتماد شهادات التصديق الأجنبية

يتصف العقد الإلكتروني الذي يبرم عبر شبكة الإنترنت بأنه ذو طابع دولي عادةً، فهو عقد يتجاوز الحدود الإقليمية للدول التي أبرم فيها أو التي يقيم فيها أحد الأطراف، وذلك لأن التجارة الإلكترونية التي تتم عبر شبكة الإنترنت، هي تجارة تتم على مستوى عالمي من خلال شبكة المعلومات الدولية التي جعلت العالم بمثابة قرية صغيرة، حيث تمكن الأطراف من إبرام العقود فيما بينهم رغم المسافات البعيدة التي تفصل بينهم^(٢).

ويثير هذا الأمر التساؤل عن القيمة القانونية للتوقيعات الإلكترونية التي تصدر بناءً على شهادات إلكترونية صادرة عن مزودي خدمات تصديق يتبعون لدول وأنظمة مختلفة.

(١) تنص المادة ٢٣ من قانون التوقيع الإلكتروني المصري على أنه "مع عدم الإخلال بأية عقوبة اشد منصوص عليها في قانون العقوبات أو في أي قانون آخر، يعاقب بالحبس وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز مائة ألف جنيه أو بإحدى هاتين العقوبتين كل من: (أ) أصدر شهادة تصديق إلكتروني دون الحصول على ترخيص بمزاولة النشاط من الهيئة.....".

(٢) د. طارق كميل، مقدمو خدمات المصادقة الإلكترونية، مرجع سابق، ص ٢٥٠.

De ROECK (P.) & VERBIEST (Th.), Commerce électronique: Le nouveau cadre juridique: Publicité, contrats, contentieux, Larcier, 2004, P. 159.

تنص المادة ٢٢ من قانون التوقيع الإلكتروني المصري على أنه "تختص الهيئة باعتماد الجهات الأجنبية المختصة بإصدار شهادات التصديق الإلكتروني، وذلك نظير المقابل الذي يحدده مجلس إدارة الهيئة، وفي هذه الحالة تكون للشهادات التي تصدرها تلك الجهات ذات الحجية في الإثبات المقررة لما تصدره نظيراتها في الداخل من شهادات نظيره، وذلك كله وفقاً للقواعد والإجراءات والضمانات التي تقررها اللائحة التنفيذية لهذا القانون".

وقد حددت المادتان ٢١ و ٢٢ من اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري ١٥ لسنة ٢٠٠٤ حالات وإجراءات وضمانات اعتماد الهيئة للجهات الأجنبية المختصة بإصدار شهادات التصديق الإلكتروني في مصر.

ويلاحظ هنا من نص المادة (٢٢) من قانون التوقيع الإلكتروني المصري أن المشرع قد ربط الاعتراف بالجهات الأجنبية التي تصدر شهادات التصديق بالاعتداد بشهادة التصديق التي تصدرها أي أن الاعتراف بحجية الشهادات الأجنبية يأتي بالتبعية بالاعتراف – من قبل هيئة تنمية صناعة تكنولوجيا المعلومات – بتلك الجهات الأجنبية المصدرة لها.

أولاً: الإعراف بالجهات الأجنبية المختصة بإصدار شهادات التصديق الإلكتروني:-

تبين من قانون التوقيع الإلكتروني المصري أن المشرع أوكل لهيئة تنمية صناعة تكنولوجيا المعلومات مهمة اعتماد الجهات الأجنبية المختصة بإصدار شهادات التصديق الإلكتروني، نظير مقابل يحدده مجلس إدارة الهيئة.

ويترتب على اعتماد الجهات الأجنبية المختصة من قبل تلك الهيئة أن تتمتع الشهادات التي تصدرها بذات الحجية القانونية في الإثبات المقررة لتلك الشهادات التي تصدرها جهات التصديق الإلكتروني المرخص لها في مصر.

أي أن الشرط الجوهرى الذي نص عليه القانون لتمتع تلك الشهادات الأجنبية بالحجية في الإثبات هو اعتماد الجهة الأجنبية المصدرة لها من قبل هيئة تنمية صناعة تكنولوجيا المعلومات، ويستوي في ذلك أن تكون الجهة الأجنبية المصدرة لتلك الشهادات من مقدمي خدمات التصديق الأجنبية أو أية جهة أخرى مرخص لها بإصدار تلك الشهادات في البلد الأجنبي التابعة له.

وقد أثير خلطاً في الفقه المصري بين اعتماد الجهة الأجنبية من قبل الهيئة واعتماد الشهادة الأجنبية فذهب البعض لاعتبار أن المقابل الذي تدفعه الجهات الأجنبية هو مقابل لاعتماد شهادات التصديق الإلكترونية والتي تصدرها تلك الجهات^(١).

ويذهب جانب آخر – أويده – لإعتبار أن المقابل المنصوص عليه وفقاً لنص المادة ٢٢ من قانون التوقيع الإلكتروني هو لاعتماد الجهات الأجنبية المصدرة لتلك الشهادات وليس لاعتماد الشهادات نفسها لوضوح النص في عباراته ومعناه ومدلوله على ذلك ولربطه الشديد بين اعتماد تلك الجهات من قبل هيئة تنمية صناعة تكنولوجيا المعلومات وبالتبعية الاعتراف بحجية الشهادات التي تصدرها تلك الجهات الأجنبية^(٢).

ومن الجدير بالذكر عدم خضوع الجهات الأجنبية فيما يتعلق بإصدار الشهادات الإلكترونية لسلطات هيئة تنمية صناعة تكنولوجيا المعلومات أي أن هيئة تنمية صناعة تكنولوجيا المعلومات ينحصر دورها في اعتماد الترخيص الصادر للجهة الأجنبية فقط ولا يمتد لسلطة إصدار ترخيص لتلك الجهات الأجنبية إذ أن هذا الترخيص بإصدار الشهادات قد صدر لها من قبل الجهة المختصة في بلدها.

ويلاحظ أيضاً على نص المادة ٢٢ من قانون التوقيع الإلكتروني المصري أن النص قد عالج مسألة شهادات التصديق الإلكتروني الصادرة عن جهات أجنبية بيد أنه لم ينظم التوقيع الإلكتروني الصادر عن الجهات الأجنبية وما إذا كان يمكن التعويل عليه وإعطائه الحجية القانونية في الإثبات^(٣).

وقد أحالت المادة ٢٢ من قانون التوقيع الإلكتروني إلي اللائحة التنفيذية لهذا القانون بشأن تحديد قواعد وإجراءات و ضمانات اعتماد الجهات الأجنبية المختصة بإصدار شهادات التصديق وبيت المادة ٢٢ من اللائحة التنفيذية لقانون التوقيع الإلكتروني حالات اعتماد تلك الجهات من قبل الهيئة بشرط توافر إحدى الحالات الآتية:-

أ – أن يتوافر لدى الجهات الأجنبية المختصة بإصدار الشهادة القواعد والإشترطات المبينة في هذه اللائحة بالنسبة للجهات التي ترخص لها الهيئة بمزاولة نشاط إصدار شهادات التصديق الإلكتروني.

(١) د. أيمن سعد سليم، التوقيع الإلكتروني، مرجع سابق، ص ٤٤٤.

(٢) د. تامر الدمياطي، إثبات التعاقد الإلكتروني عبر الانترنت، مرجع سابق، ص ٥٧٢.

(٣) عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظم القانونية المقارنة، مرجع سابق، ص ٤٥٩.

وتتمثل هذه الإشتراطات فيما نصت عليه اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري في هذا الصدد في المواد ١٢، ١٣، ١٤، منها حيث ورد في نص المادة ١٢ من اللائحة التنفيذية المتطلبات اللازم توافرها لدى طالب الحصول على الترخيص بإصدار الشهادات، وتبين المادة ١٣ من اللائحة التنفيذية لالتزام المرخص له بعدم إبرام عقد مع العملاء إلا بعد اعتماد نموذج هذا العقد من قبل هيئة تنمية صناعة تكنولوجيا المعلومات، وتقر المادة ١٤ من اللائحة بالتزام طالب الترخيص أن يقدم الضمانات والتأمينات التي يحددها مجلس إدارة الهيئة لتغطية أى أضرار أو أخطار تتعلق بذوي الشأن في حالة إنهاء الترخيص أو حدث أي إخلال من جانبه بالتزاماته حين تقرر مسؤليته عن ذلك .

ب – أن يكون لدى الجهة الأجنبية وكيل في جمهورية مصر العربية مرخص له من قبل الهيئة بإصدار شهادات التصديق الإلكتروني، ويتوافر لديه كل المقومات المطلوبة للتعامل بشهادات التصديق الإلكتروني، وتكفل تلك الجهة فيما تصدره من شهادات تصديق إلكتروني وفيما هو مطلوب من اشتراطات وضمانات.

ويلاحظ أن كفالة الوكيل هنا للجهة الأجنبية يثير تساؤلات حول مدى تعلقه بالالتزامات المتعلقة بإصدار شهادات التصديق الإلكتروني وكذلك المسؤولية الملقاة على عاتق تلك الجهات بصدد إصدار الشهادات وهو ما لم يتم إيضاحه أو ينص عليه في القانون واللائحة التنفيذية لهذا القانون.

وفي اعتقادي أن مجمل الفقرة (ب) من المادة ٢٢ من اللائحة التنفيذية لقانون التوقيع الإلكتروني يتبين منها أن هذا الوكيل كفيلا لتلك الجهة الأجنبية المطلوب اعتمادها واشترط النص فيه كفالة تلك الجهة الأجنبية مما مقتضاه تحمله للمسؤولية بجانب تلك الجهات الأجنبية، وهذا ما نادى به البعض من أن كفالة الوكيل للجهة الأجنبية تمتد لتشمل الالتزامات والمسؤوليات على حد سواء^(١).

ج – أن تكون الجهة الأجنبية ضمن الجهات التي وافقت جمهورية مصر العربية بموجب اتفاقية دولية نافذة فيها على اعتمادها باعتبارها جهة أجنبية مختصة بإصدار شهادات التصديق الإلكتروني.

د – أن تكون الجهة الأجنبية ضمن الجهات المعتمدة أو المرخص لها بإصدار شهادات تصديق إلكتروني من قبل جهة الترخيص في بلدها، وبشرط أن يكون هناك اتفاق بين جهة الترخيص الأجنبية وبين هيئة تنمية صناعة تكنولوجيا المعلومات على ذلك.

(١) د. تامر الدمياطي، مرجع سابق، ص ٥٧٤.

ويتيح هذا النص من اللائحة التنفيذية لهيئة تنمية صناعة تكنولوجيا المعلومات عقد اتفاقات مع جهات الترخيص الأجنبية من أجل الموافقة على اعتماد مقدم الخدمات المرخص له بإصدار شهادات التصديق الإلكتروني من قبل تلك الجهات الأجنبية .

ويتطلب أن يقوم ذوى الشأن أو الجهات الأجنبية بتقديم طلب للهيئة لاعتماد جهات الترخيص الأجنبية ويكون ذلك على النماذج التي تعدها الهيئة، ومن حق الهيئة اعتماد تلك الجهات الأجنبية من تلقاء نفسها في الحالات المبينة في (أ، ج، د) .

ووفقاً لنص المادة ٢١ من اللائحة التنفيذية تنحصر سلطة الإعتقاد في مجلس إدارة الهيئة ويصدر قرار الاعتماد من المجلس بعد سداد المقابل الذي يحدده مجلس إدارة الهيئة للاعتماد، ويحدد في القرار مدة الاعتماد وأحوال تجديده، كما يكون للهيئة دائماً الحق في إلغاء الاعتماد أو وقفه وذلك بقرار مسبب، فضلاً عن أن مجلس إدارة الهيئة ينبغي له البت في طلب الاعتماد خلال مدة لا تتجاوز السنتين يوماً من تاريخ استيفاء الجهة الأجنبية لكافة الاشتراطات، وكل ما تحدده الهيئة، ويعتبر مضي السنتين يوماً دون إصدار القرار من الهيئة يعتبر ذلك قراراً ضمناً بالرفض على الطلب المقدم للاعتماد ما لم تخطر الهيئة الجهة طالبة الاعتماد بمد المهلة وفقاً للقانون.

ثانياً: اعتماد شهادات التصديق الإلكتروني الأجنبية:-

وبعد استعراض لكيفية اعتماد الجهات الأجنبية المصدرة لشهادات التصديق الإلكتروني من قبل هيئة تنمية صناعة تكنولوجيا المعلومات، فهذه الجهات أن تطلب من الهيئة اعتماد أنواع أو فئات شهادات التصديق الإلكتروني التي تصدرها وفقاً للقواعد والضوابط التي يضعها مجلس إدارة الهيئة فضلاً عن تحديد هذا المجلس لمقابل اعتماد تلك الشهادات كما يحدد مجلس إدارة الهيئة لأنواع وفئات شهادات التصديق الأجنبية ما يناظرها من شهادات تصديق إلكتروني صادرة من الجهات المرخص لها في مصر .

وتصدر هيئة تنمية صناعة تكنولوجيا المعلومات قراراً باعتماد الجهات الأجنبية المصدرة لشهادات التصديق الإلكتروني فضلاً عن اعتماد شهادات التصديق الإلكتروني النظرية للشهادات المصدرة داخل جمهورية مصر العربية.

ويرى البعض أن هناك توسعا من قبل اللائحة التنفيذية في شأن اختصاصات الهيئة وكذلك في منحها الاختصاص في وضع الضوابط والقواعد لاعتماد الشهادات الأجنبية ويبرر ذلك بالاعتبارات العملية وحدثة التجربة التشريعية في مجال المعاملات الإلكترونية^(١).

وإن كنت اعتقد بحقيقة الرأي السابق في التوسع في اختصاصات هيئة تنمية صناعة تكنولوجيا المعلومات فذلك من اقتناع أكيد بأنها السلطة العليا للتصديق الإلكتروني والجهة المركزية الوحيدة المنظمة والمراقبة لجهات التصديق الإلكتروني داخل جمهورية مصر العربية وكذلك من هذا المنطلق ضرورة منحها سلطات في تحديد مقابل الاعتماد للجهات الأجنبية والشهادات الإلكترونية الأجنبية من الاعتبارات العملية ووفقاً لما يستجد في النواحي العملية ومواكبة التطورات والمستجدات على الصعيد العملي.

وفي فرنسا بينت المادة التاسعة من المرسوم الفرنسي رقم ٥٣٥ - ٢٠٠٢ الصادر في ١٨ ابريل ٢٠٠٢ أسس الاعتراف بشهادات التصديق الإلكتروني الصادرة عن جهات تصديق أجنبية، وفقاً لقواعد التوجيه الأوروبي بشأن التوقيعات الإلكترونية. وقد فرق هذا المرسوم بين الشهادات الصادرة داخل إطار الاتحاد الأوروبي وتلك الصادرة خارجه^(٢).

وتعهد المادة ٢/٩ من المرسوم الفرنسي ٥٣٥ - ٢٠٠٢ والصادر في ١٨ ابريل ٢٠٠٢ إلي رئيس الوزراء بمهمة الإقرار لشهادات التصديق الصادرة من جهات الترخيص الأجنبية بدولة عضو في الاتحاد الأوروبي بذات الحجية المقررة لشهادات التصديق الصادرة تطبيقاً لأحكام هذا المرسوم، متى صدرت في إطار إجراءات مماثلة تتطوي على ضمانات مناظرة للشهادات الصادرة في فرنسا.

وقد وضعت المادة (١٢) من قانون الأونسترال النموذجي مبادئ للاعتراف بشهادات التصديق الإلكتروني الأجنبية وهي:-

أولاً:- تدعيم مبدأ عدم التمييز بين شهادات التصديق الإلكتروني الأجنبية والوطنية .

ويتطلب ذلك وجود معيار أساسي للتكافؤ بين شهادات التصديق بصرف النظر عن مكان إصدارها ، ولا ينبغي أن يكون مكان المنشأ في حد ذاته هو العامل الوحيد الذي يحدد ما إذا كان ينبغي

(١) د. تامر الدمياطي، مرجع سابق، ص ٥٧٤.

(٢) راجع: المادة ٩ من المرسوم الفرنسي رقم ٥٣٥ - ٢٠٠٢ الصادر في ١٨ ابريل ٢٠٠٢ بشأن "التقييم والتصديق على مستوى الأمان الذي تقدمه منتجات وأنظمة تكنولوجيا المعلومات".

والى أي مدى ينبغي الاعتراف بالشهادات أو التوقيعات الإلكترونية الأجنبية باعتبارها يمكن أن تكون سارية المفعول قانوناً في الدولة المصدرة لها^(١).

ثانياً: - ضرورة وضع معياراً عاماً للاعتراف بالشهادة الإلكترونية عبر الحدود، والذي يترتب على عدم توافره تحمل مقدم خدمات التصديق عبئاً غير معقول يتمثل في ضرورة الحصول على تراخيص دول متعددة.

ثالثاً: - تحدد الفقرة الرابعة من المادة (١٢) من القانون النموذجي العوامل التي ينبغي وضعها في الاعتبار عند البت في ما إذا كانت الشهادة الإلكترونية تتيح مستوى من قابلية الاعتراف حتى يكون للشهادة ذات المفعول القانوني والحجية في غير المكان الذي صدرت فيه ويرجع في ذلك للمعايير الدولية المعترف بها في المواد ٦ ، ٩ ، ١٠ من القانون النموذجي ٢٠٠١ أو أية عوامل أخرى ذات صلة.

وينبغي عند تفسير عبارة "معياري دولي معترف به" أن تفسر تفسيراً واسعاً ليشمل المعايير الدولية التقنية والتجارية وكذلك المعايير والقواعد التي اعتمدها هيئات حكومية ودولية ويمكن أن تكون أيضاً ممارسات تقنية أو قانونية أو تجارية مقبولة وضعها القطاع العام أو الخاص، وبصفة عامة فإن هذه المعايير الدولية، معايير قياسية فنية وتجارية ومالية هدفها انسياب المعاملات الإلكترونية الدولية^(٢).

وتعتبر العوامل الأخرى ذات الصلة منها مبدأ المعاملة بالمثل ما بين الدولة التي صدر فيها التوقيع الإلكتروني أو الشهادة الأجنبية وتلك الدولة المطلوب فيها التنفيذ ، ويكون له ذات الحجية والأثر القانوني خارج حدود الدولة التي صدر فيها شرط المعاملة بالمثل وتوافر الضوابط والشروط التي تثبت له الحجية في الدولة التي صدر فيها والدولة المطلوب التعويل عليه فيها^(٣).

(١) قانون الأونسترال النموذجي بشأن التوقيعات الإلكترونية مع دليل الاشتراع، ٢٠٠١، ص ٤٦.

(٢) قانون الأونسترال النموذجي بشأن التوقيعات الإلكترونية مع دليل الاشتراع، ٢٠٠١، ص ٨٧.

(٣) د. عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظم القانونية المقارنة، مرجع سابق، ص ٢٧٥.

الفرع الثالث

سلطة الموثق الإلكتروني في التأكد من الأهلية والهوية

من المعلوم قانوناً أن التعبير عن الإرادة حتى ينتج أثره قانوناً فلا بد من صدوره من شخص يعتد القانون بأهليته، ونظراً لانتشار والتوسع في وسائل وتقنيات الاتصال الحديثة والتعاقد عن بعد دون حضور مادي للمتعاقدين فإنه يصعب على كل متعاقد التأكد من شخصية المتعاقد الآخر خاصة فيما يتعلق بالأهلية القانونية.

ويرتكز تحديد الهوية على قيام الشخص بالتعبير عن هويته، وبدون هذا التعبير تصبح عملية تحديد الهوية في غاية الصعوبة وهو ما يتم مواجهته في حالة إخفاء الشخص لهويته على شبكة الانترنت أو تعمدته انتحال هوية أخرى أو غير حقيقية كما هو الحال أيضاً في كثير من الأحوال عند اللجوء للبريد الإلكتروني. ويضيف البعض بان القانون لا يهتم بتحديد هوية الأشخاص الطبيعيين، حيث أن القانون قد لا يهتم بتحديد هوية الشخص قدر اهتمامه بشبكة علاقاته التي تربطه بالآخرين^(١).

وعلى الرغم من أنه لا توجد حتى الآن وسائل تقنية حاسمة لتحديد الأهلية القانونية إلا أنه توجد وسائل احتياطية وتحذيرية يمكن استخدامها، وقد تتمثل تلك الوسائل في البطاقات الإلكترونية أو الاستعانة بوسيط إلكتروني أو استخدام وسائل تحذيرية^(٢)، حيث إن الوسيط الإلكتروني وهو طرف ثالث محايد يسند إليه مهمة تنظيم العلاقة بين أطراف العقد الإلكتروني ويلجأ إليه للتحقق من هوية المتعاقدين وأهليتهم القانونية وإصدار شهادة مصدق عليها تتعلق بأطراف العقد الإلكتروني.

كما يمكن إيجاد حل لهذه المسألة في الوقت الحاضر باللجوء إلى سلطات الإشهار التي تتمثل في قيام طرف ثالث محايد سواء كانت هيئة عامة أم خاصة، تنظم العلاقة بين الطرفين فنقوم بتحديد هوية الطرفين وأهليتهما القانونية عن طريق إصدار شهادات تثبت حقائق معينة متعلقة بالتعاقد الذي يجرى عبر شبكة الإنترنت^(٣).

(١) انظر:

BERNARD (A.), L'identité des personnes physiques en droit privé, Presses Universitaires de France, Paris, 1994, P. 128.

(٢) د. سمير حامد الجمال، التعاقد عبر تقنيات الاتصال الحديثة، دراسة مقارنة، دار النهضة العربية، القاهرة، ٢٠٠٦، ص ١٥٧.

(٣) د. محسن عبد الحميد البيه، النظرية العامة للإلتزامات، مرجع سابق، ص ٢٨٤.

وفي مجال الإثبات ذهب البعض للقول بأنه "ينبغي أن يتيح ما يتم تسطيره تحديد هوية الأشخاص الصادر منهم المحرر، وتاريخ وماهية المضمون الذي وافق عليه الأطراف"^(١).

ويقصد بتحديد الهوية هو تعيين الشخص الذي ينسب إليه المحرر الإلكتروني والذي يتحمل بالالتزامات الناشئة عنه، كما يقتضى الحقوق التي تثبت بمقتضى التصرف القانوني الذي يتضمنه المحرر^(٢).

وهذا ما أكده القانون الفرنسي في المادة ١٣١٦ - ١ بان الكتابة الإلكترونية تتمتع بنفس الحجية المعترف بها للمحررات الكتابية في الإثبات، شريطة أن يكون بالإمكان تحديد شخص مصدرها على وجه الدقة، وان يكون تدوينها وحفظها قد تم في ظروف تدعو إلى الثقة.

ويمكن أن يمتد نشاط جهات التوثيق إلى جوانب أخرى مهمة تساهم في تأمين التعامل وتعزيز الثقة بين الطرفين كذلك المتصلة بحالتهما المهنية وعملهما والمؤهلات التي يحملونها فهذه كلها بيانات قد لا يصدق المتعاقد في الإدلاء بها على الوجه الصحيح، وفي نفس الوقت يصعب على المتعاقد الاستعلام عنها بوسائله الخاصة، إذ جرى التعامل في بيئة الكترونية افتراضية يتلاقى فيها الطرفان لأول مرة وكل منهما في مكان جغرافي متباعد عن الآخر.

يضاف إلى ذلك أن القوائم بخدمة التصديق يسمح بجانب التحقق من هوية شخص الموقع بالتحقق أيضاً من سلطات هذا الشخص وأهليته القانونية وكذلك اختصاصاته الوظيفية^(٣).

وقد أفرد المشرع المصري في أحكام القانون المدني عدة نصوص تتعلق بأحكام الأهلية وان كان من أهم قواعدها تعلقها بالنظام العام فلا يجوز مخالفتها ويعتبر باطلاً بطلاناً مطلقاً كل اتفاق يتضمن نزول الشخص عن أهليته أو التعديل في أحكامها.

ويوجد نوعان لهوية الأشخاص عبر شبكة الانترنت وهما الهوية العارضة على الشبكة والهوية المحققة على شبكة الانترنت، ويقصد بتحديد الهوية العارضة على الشبكة تلك التي يتم تحديدها دون إقدام من جانب المتعاقد على تحديد الهوية، أي يتم بصورة عرضية حال استخدام الشبكة من جانب المستخدم أو لدى تصفح مواقع الانترنت، نظراً للتطور التكنولوجي في مجال تقنيات الانترنت، أما

(٤) انظر:

CAPRIOLI (E.A.), Traçabilité et droit de la preuve, Droit & Patrimoine 2001, P . 68.

(٢) د. ثروت عبد الحميد، التوقيع الإلكتروني، مرجع سابق، ص ١٧٨.

(٣) د. سعيد السيد قنديل، مرجع سابق، ص ٧٥.

تحقيق الهوية المحقق على شبكة الانترنت فجاء نتيجة التطور التقني حيث أوجد أنظمة حديثة لتحديد الهوية ، ومن خلالها يمكن التحقق من هوية الأشخاص والتعرف على مصادر البيانات عن طريق استخدام وسيلة من وسائل التوقيع الإلكتروني مثل التوقيع الرقمي وشهادة التصديق الإلكتروني^(١).

ويثير هذا الأمر مسألة التعرض للخصوصية وحماية الحياة الخاصة لمستخدمي شبكة الإنترنت، وقد وضع التوجيه الأوروبي رقم ٨٥ - ٢٠٠٢ الصادر في ١٢ يوليو ٢٠٠٢ والخاص بمعالجة البيانات ذات الطابع الشخصي وحماية الحياة الخاصة في قطاع الاتصالات الإلكترونية، حيث فرض على مزودي الخدمات على الانترنت التزاما مقتضاه أن يبصروا متصفح الشبكة باستخدامهم وسائل من شأنها أن تسمح بتخزين معلومات في الحواسيب الخاصة بهم أو الوصول لمعلومات مخزنة في حواسيبهم، وان يبينوا لمستخدم شبكة الانترنت أيضاً الوسائل الممكنة للاعتراض على استخدام هذه الأساليب^(٢).

ويشير تقرير مجلس الدولة الفرنسي بشأن الانترنت والشبكات الرقمية، إلي أن البيانات الخاصة بالاتصال تتعلق من جهة بعناوين الأشخاص المشتركين في شبكة الانترنت، وهي ما تعرف باسم (IP) وبخاصة عنوان كل من المرسل والمرسل إليه، متضمناً تاريخ وتوقيت الاتصال والمعلومات التقنية التي تبين نوعية الاستخدام مثل الدخول إلي مواقع الويب والوسائل الإلكترونية المستخدمة، وترتبط من جهة أخرى برغبة المستخدم للشبكة في طلب صفحة (Web site) التي يرغب في زيارتها أو الرسائل ويتولى مورد خدمات الدخول للانترنت جمع البيانات آلياً وإيداعها في ملف يطلق عليه اسم log^(٣).

وقد تعرض القانون التونسي رقم ٨٣ لسنة ٢٠٠٠ في المادة (٢٥) منه لهذا الأمر بالنص على أنه يلزم عند إبرام العقد الإلكتروني الإفصاح عن الهوية بطريقة واضحة ومفهومة.

وفي التوجيه الأوروبي ٩٧-٧ والصادر في ٢٠ مايو ١٩٩٧ بشأن البيع عن بعد فإنه وفقاً لنص المادة ٤-١ يلزم عند إبرام العقد عن بعد عبر تقنيات الاتصال تحديد هوية الأطراف المتعاقدة بما في ذلك بيان الأهلية القانونية.

(١) د. تامر الدمياطي، مرجع سابق، ص ٥٣٨.

(٢) JOCE, L. 201 du 31 juillet 2002, P. 37.

(٣) انظر :

Internet et les réseaux numériques: Etude adoptée par l'assemblée générale du Conseil d'État, section du rapport et des études, le 2 juillet 1998 , P. 32 .

ووصولاً لتأمين وسلامة التعامل عبر الانترنت فيما يتعلق بموضوع الأهلية يمكن اللجوء للقواعد العامة في أحكام القانون المدني لعدم ورود نص على ذلك في قانون التوقيع الإلكتروني حيث جاء حكم المادة ١١٤ / ٢ من القانون المدني المصري بصحة تصرفات المجنون أو المعتوه إذا كانت قد أبرمت قبل تسجيل قرار الحجر متى كانت حالة الجنون أو العته غير شائعة وغير معلومة للمتعاقد الآخر والذي قد لا يراه بصورة مادية بصدد التعاقد الإلكتروني.

وبناءً عليه فقد حرص المشرع المصري على إقرار صحة التصرف بالرغم من صدوره من ناقص الأهلية حرصاً منه على استقرار المعاملات.

وإن كان الحكم الوارد بالمادة ١١٩ من القانون المدني المصري يجيز لناقص الأهلية طلب إبطال العقد فإنه أورد بصددتها حق للمتعاقد الآخر بطلب التعويض إذا كان ناقص الأهلية قد لجأ إلي طرق احتيالية لإخفاء نقص أهليته وإن كان خير تعويض لذلك، وهو التعويض العيني بإقرار صحة العقد.

ويرى البعض هنا بإقرار نظرية الوضع الظاهر نظراً للطابع الخاص للعقد الإلكتروني لتوفير الثقة والأمان لدى المتعاقدين عبر تقنيات الاتصال وحفاظاً على استقرار التعامل وهذا أمر لا غنى عنه في مجال العقود الإلكترونية^(١).

(١) د. سمير حامد الجمال، التعاقد عبر تقنيات الاتصال الحديثة، دراسة مقارنة، دار النهضة العربية، ٢٠٠٦، ص ١٥٦، وراجع أيضاً:

PIETTE-COUDOL (Th.) , La signature électronique, Litec, Paris, 2001 , P. 15

خاتمة

من خلال هذه الدراسة تمت معالجة أحد أهم إنعكاسات التقدم العلمي والتقني في مجال الإتصالات وتكنولوجيا المعلومات وهو فكرة " التصديق الإلكتروني " .
وتهدف عملية التصديق الإلكتروني والتي تتم من خلال شخص محايد يعتبر طرف ثالث في العملية الإلكترونية وهو القائم بالتصديق الإلكتروني فتهدف لبث ونشر الثقة والأمان لدى المتعاملين بوسائل الإتصال الحديثة ولا سيما من خلال شبكة الإنترنت، والتي حولت العالم لمجرد قرية صغيرة ، يستطيع مستخدمي شبكة الإنترنت الإبحار في ساحتها وتتيح من الفرص الكثيرة لتقديم الخدمات وإبرام العقود وإتمام الكثير من الإجراءات في زمن قياسي، الأمر الذي إستتبع معه إدخال الكثير من التعديلات الجوهرية على أساليب وأشكال التعاقد .

ولم يأخذ المشرع في جميع دول العالم موقف المنقرج على ثورة الإنفتاح في عالم جديد من التكنولوجيا وتطور وسائل الإتصالات والتي ألفت بظلالها على إنعكاسات قانونية هامة وجديرة بالبحث لمواكبة التقدم العلمي والتقني والتكنولوجي ، الأمر الذي إستدعى معه إما تطويع القواعد التقليدية إن كانت نصوص تلك القواعد تسمح بذلك أو إستحداث قواعد جديدة كي يتم تقنين الإستفادة من ثمار التقدم العلمي ومواجهة مخاطره .

وأمام حتمية اللجوء لوسائل التقنية الحديثة في التعامل، ونظرا لضعف الأمان الذي توفره تلك الوسائل ، فكان لزاما الإحتكام لشخص ثالث موثوق به ليقوم بعملية التصديق على المعاملة من حيث أطرافها وموضوعها على حد سواء ويسمى هذا الطرف الموثوق به بمقدمي خدمات التصديق الإلكتروني في مجال التوقيعات الإلكترونية ، وقد يكون شخصا طبيعيا أو معنويا ، تتوافر لديه إمكانيات فنية وتقنية ومالية عالية .

ويقوم مقدمو خدمات التصديق الإلكتروني بالإعتماد على تقنية إعداد مفاتيح شفرية عامة وخاصة وكذلك تقنية التشفير لحماية الرسائل ولتأمين خدمات التوقيع الإلكتروني .

وقد نتج عن هذه الدراسة النتائج والتوصيات الآتية :-

أولاً :- تعتبر خدمات التصديق الإلكتروني الوسيلة القانونية المتاحة لتأمين وسلامة المعاملات التي تتم عبر وسائل الإتصالات الحديثة عامة وشبكة الإنترنت بصفة خاصة وما يمكن أن يسفر عنه التطور الدائم والمستمر في مجال تقنيات الإتصال الحديثة في المستقبل من وسائل أخرى ، وإن كان المجال

الخصب لعمليات التصديق يكون في مجال التوقيع الإلكتروني ولكنه ليس بالمجال الوحيد إذ يعمل به أيضا في مجال خدمات البريد الإلكتروني وكذلك عملية الحفظ الإلكتروني ، وإن كانت الدراسة قد إقتصرت على التصديق في مجال التوقيع الإلكتروني .

ثانياً :- ومسايرة للتقدم المذهل في مجال تكنولوجيا المعلومات فقد ساءرت معظم الدول العربية لمثيلتها الأوروبية في إصدار تشريعات لتنظيم خدمات التصديق الإلكتروني ، الأمر الذي أثبت عدم توافر إمكانيات ممارسة تلك الخدمة كما هو الحال في الدول الأوروبية سواء إمكانيات مادية أو فنية أو من حيث الكوادر البشرية .

ثالثاً :- ومن خلال إستعراض خدمات التصديق الإلكتروني في مصر فإنه ليس كافيا التنظيم القانوني الوارد بالقانون رقم ١٥ لسنة ٢٠٠٤ والخاص بالتوقيع الإلكتروني وإنما يمثل خطوة أولية سبقت الكثير من الدول مصر فيها والحاجة لإصدار تشريع شامل ينظم دور مقدم خدمات التصديق الإلكتروني وكل ما يتعلق بدوره لبث الثقة بين جمهور المتعاملين ومستخدمي خدمات التصديق مما يرتب أثره على إزدهار المعاملات الإلكترونية .

رابعاً :- ننضم للبعض فيما يوصى به من ضرورة إنشاء صندوق قومي لتعويض الأضرار الناتجة عن الخطأ في عمليات التصديق الإلكتروني وتساهم الدولة فيه بجانب جهات التصديق الإلكتروني .

قائمة المراجع

أولاً: المراجع العربية:—

- د. إبراهيم الدسوقي أبو الليل، الجوانب القانونية للتعامل عبر وسائل الاتصال الحديثة، مؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون، الإمارات، ٢٠٠٠.
- د. أسامة احمد بدر، حماية المستهلك فى التعاقد الإلكتروني، دراسة مقارنة، دار الجامعة الجديدة للنشر، الإسكندرية، ٢٠٠٥.
- د. أيمن سعد سليم، التوقيع الإلكتروني، دراسة مقارنة، دار النهضة العربية، القاهرة، ٢٠٠٤.
- د. تامر محمد سليمان الدمياطي، إثبات التعاقد الإلكتروني عبر الانترنت، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، ٢٠٠٨.
- د. ثروت عبد الحميد، التوقيع الإلكتروني، دار الجامعة الجديدة، الإسكندرية، ٢٠٠٧.
- د. خالد عبد الفتاح محمد، التنظيم القانوني للتوقيع الإلكتروني، دراسة مقارنة، المركز القومي للإصدارات القانونية، الطبعة الأولى، ٢٠٠٩.
- د. سعيد السيد فتديل، التوقيع الإلكتروني، دار الجامعة الجديدة للنشر، الإسكندرية، ٢٠٠٤.
- د. سمير حامد الجمال، التعاقد عبر تقنيات الاتصال الحديثة، دراسة مقارنة، دار النهضة العربية، القاهرة، ٢٠٠٦.
- د. طارق كميل، مقدمو خدمات المصادقة الإلكترونية (التنظيم القانون واجباتهم ومسئولياتهم)، مجلة جامعة الشارقة للعلوم الشرعية والقانونية، المجلد ٥، العدد ٣، ٢٠٠٨.
- د. عابد فايد، الكتابة الإلكترونية فى القانون المدني: الفكرة والوظائف، دار النهضة العربية، القاهرة، ٢٠٠٧.
- د. عبد الحميد عثمان الحفني، المسؤولية المدنية للموثق، دراسة مقارنة بين القانون الفرنسي والمصري، مجلة البحوث القانونية والاقتصادية، كلية الحقوق، جامعة المنصورة، العدد الثاني عشر، أكتوبر ١٩٩٢.
- د. عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الإلكترونية، الكتاب الأول، دار الفكر الجامعي، الإسكندرية، ٢٠٠٢.
- د. محسن البيه، قانون الإثبات في المواد المدنية والتجارية، مكتبة الجلاء الجديدة، المنصورة، ٢٠٠١-٢٠٠٢.
- د. محمد محمد أبو زيد، تحديث قانون الإثبات، مكانة المحررات الإلكترونية بين الأدلة الكتابية، ٢٠٠٢.

- د. مصطفى أبو مندور موسى، خدمات التوثيق الإلكتروني "تدعيم للثقة وتأمين للتعامل عبر الإنترنت"، دراسة مقارنة، ندوة الجوانب القانونية للتعاملات الإلكترونية، مسقط، ٢٣/١١/٢٠٠٨م.
- د. ممدوح عبد الحميد عبد اللطيف، جرائم استخدام شبكة المعلومات العالمية، مؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون، الإمارات، ٢٠٠٠.
- د. هدي حامد فشقوش، الحماية الجنائية للتجارة الإلكترونية عبر الإنترنت، دار النهضة العربية، القاهرة، ٢٠٠٠.

ثانياً: المراجع الأجنبية:-

- AGOSTI (P.)**, La signature: De la sécurité juridique et la sécurité technique, Thèse Montpellier, 2003.
- ATELIN (Ph.)**, Réseaux informatiques: Notions fondamentales, Editions ENI, 2009. **BITAN (H.)**, Droit des créations immatérielles, Editions Lamy, 2010.
- BERNARD (A.)**, L'identité des personnes physiques en droit privé, Presses Universitaires de France, Paris, 1994.
- BITAN (H.)**, La signature électronique, Comment la technique répond-t-elle aux exigences de la loi? Gaz. Pal. 19-20 Juillet 2000.
- BITAN (H.)**, Protection et contrefaçon des logiciels et des bases de données, Editions Lamy, 2006.
- BOCHURBERG (L.)**, Internet et commerce électronique, DELMAS, 2001.
- CACHARD (O.)**, La régulation internationale du marché électronique, Librairie générale de droit et de jurisprudence, 2002.
- CAPRIOLI (E.A.)**, Traçabilité et droit de la preuve, Droit & Patrimoine 2001.
- CARPENTIER (J.- F.)**, La sécurité informatique dans la petite entreprise: état de l'art et bonnes pratiques, Editions ENI, 2009.
- De ROECK (P.) & VERBIEST (Th.)**, Commerce électronique: Le nouveau cadre juridique: Publicité, contrats, contentieux, Larcier, 2004.
- GUALINO (J.)**, Dictionnaire pratique informatique, Internet et nouvelles technologies de l'information et de la communication, Paris, 2005.
- GUERRIER (C.) & MONGET (M. -Ch.)**, Droit et sécurité des télécommunications, Springer, 2000.
- H. XUE**, Cyber Law in China, Kluwer Law International, 2010.
<http://www.e-betobe.com/texteece.htm>, 13-2-2009.
- ISAAC (H.) & VOLLE (P.)**, E-commerce: De la stratégie à la mise en oeuvre opérationnelle, Pearson Education France, 2008.
- ISAAC (H.) & VOLLE (P.)**, E-commerce: De la stratégie à la mise en oeuvre opérationnelle, Pearson Education France, 2008.

JACQUET (J.- M.) & DELEBECQUE (Ph.) & CORNELOUP (S.), Droit du commerce international, Dalloz, 2007.

JOLY-PASSANT (E.), Le décret du 30 mars 2001 pris pour l'application de l'article 1316-4 du Code civil et relatif à la signature électronique, Revue Lamy Droit des affaires, N° 40, Juillet 2001.

LAUDON (K.) & LAUDON (J.), Management des systèmes d'information, Pearson Education France, 2010.

MICHON (Ch.) & ANDRÉANI (J.- C.), Le Marketeur: Fondements et nouveautés du marketing, Pearson Education France, 2010.

MONTERO (E.), Les contrats de l'informatique & de l'Internet, Larcier, 2005.

MOUGENOT (D.), La prévue, Larcier, 2002.

PIETTE-COUDOL (Th.) , La signature électronique, Litec, Paris, 2001.

RENARD (I.), Vive la signature électronique , Dalloz, 2002.

ROHAUT (S.), Préparation à la certification LPIC-1: Linux, Editions ENI, 2009.

SHERIF (M.), Paiements électroniques sécurisés, PPUR presses polytechniques, 2007.

THIERRY (P.- C.), Certification électronique: Pratique et modélisation, Voir à:

VERBIEST (Th.) & WÉRY (E.), Le droit de l'internet et de la société de l'information: droits européen, belge et français, Larcier, 2002.