Journal of Economic, Administrative and Legal Sciences
Volume (5), Issue (10): 30 May 2021
P: 19 - 38
ISSN: 2522-3372
مجلة العلوم الاقتصادية والإدارية والقانونية
المجلد (5)، العدد (10): 30 مايو 2021 م
ص: 19 - 38

Electronic Authentication of E-commerce Contracts

Shady Ramadan Ibrahim
College of Sciences and Arts in Dhahran ALJOUNB || King Khalid University || KSA

Abstract: This research aimed at explaining the electronic authentication from a technical and legal point of view, and to explain the authentication mechanism represented in encryption and its types, and to clarify the role of electronic certification in electronic transaction. We also clarified the role of documentation in electronic editors and the scope of electronic documentation, as well as how to authenticate in the field of e-mail, and the role of trustworthy third parties in the process. The study also clarified the method and mechanism of electronic documentation in the field of electronic preservation services. Based on the nature of the research, a comparative approach was followed by presenting the position of more than one local and international legislation besides conducting an analytical study. The researcher also used the analytical method by addressing each section after analyzing it through jurisprudential opinions and national laws where the descriptive method is sued to clarify some concepts that include a careful analysis of information and facts about the subject of study.

After presenting the research material, several results were reached, including: that electronic authentication services are the legal means to send confidence and secure online dealings. Based on the results, the researcher made a set of recommendations, including the recommendation to issue a comprehensive legislation that regulates the role played by trustworthy third parties in terms of electronic signature, recommended e-mail, and electronic preservation.

Keywords: E-commerce – Electronic signature – Electronic authentication – Electronic writing – Encryption.

التوثيق الإلكتروني لعقود التجارة الإلكترونية

شادي رمضان إبراهيم
كلية العلوم والآداب بظهران الجنوب || جامعة الملك خالد || المملكة العربية السعودية

المستخلص: هدفَ البحثُ إلى بيان ماهية التوثيق الإلكتروني من الناحية الفنية والقانونية، وبيان آلية التوثيق المتمثلة في التشفير وأنواعه، وتوضيح دور الشهادة الإلكترونية في التعامل الإلكتروني. كما أوضحنا دور التوثيق في المحررات الإلكترونية ونطاق التوثيق الإلكتروني، وكيفية التوثيق في مجال البريد الإلكتروني ودور الغير محل الثقة في ذلك. كما أوضحت الدراسة كيفية التوثيق الإلكتروني في مجال خدمات الحفظ الإلكتروني وآليته، ولطبيعة البحث أُتُّبِعَ المنهج المقارن، وذلك بعرض موقف أكثر من تشريع محلي ودولي وإجراء دراسة تحليلية، كذلك استخدم الباحث المنهج التحليلي بتناول كل جزئية بعد تحليلها من خلال الآراء الفقهية والقوانين الوطنية، وذلك بتطبيق المنهج الوصفي عند إيضاح بعض المفاهيم التي تتضمن تحليلاً دقيقاً للمعلومات والحقائق عن موضوع الدراسة.

وقد خرج البحث بعد عرض مادته بعدة نتائج، منها: أن خدمات التوثيق الإلكتروني هي الوسيلة القانونية لبعث الثقة وتأمين التعامل عبر الإنترنت، واستناداً للنتائج قدم الباحث جملة من التوصيات منها التوصية بإصدار تشريع شامل ينظم الدور الذي يقوم به الغير محل الثقة في مجالات التوقيع الإلكتروني، والبريد الإلكتروني الموصي عليه، والحفظ الإلكتروني.

الكلمات المفتاحية: التجارة الإلكترونية – التوقيع الإلكتروني – التوثيق الإلكتروني – الكتابة الإلكترونية – التشفير.

مقدمة.

يعيش العالم اليوم في رحاب ثورة إلكترونية تحققت بفضل الشبكة العنكبوتية الدولية، ونتيجة لمساهمة هذه الشبكة في عولمة السوق التجاري؛ فقد أدى ذلك إلى بزوغ عقود التجارة الإلكترونية، والتي فرضت نفسها بقوة خلال الحقبة الأخيرة من القرن المنصرم، حيث استطاعت شبكة الإنترنت إزالة جميع القيود والحدود الجغرافية والسياسية القائمة بين الدول أمام الصفقات التجارية، والتي كانت تعوقها إلى وقت قريب. ومع تزايد الصفقات والتعاملات التجارية التي تتم إلكترونيا عبر شبكات الإنترنت، وما يستلزمه ذلك من تبادل الخطابات وإبرام العقود والتوقيع عليها إلكترونيا، أثيرت العديد من المشكلات والتحديات القانونية بشأن أنظمة الدفع الإلكتروني وضوابط إبرام العقود "الإيجاب والقبول"، وضمان الالتزام بتنفيذ شروط التعاقد، ومدى حجية التوقيع الإلكتروني في الإثبات، ولتدارك هذه المشكلات كان لا بد من وضع إطار قانوني واضح ومحدد للتعاملات التجارية الإلكترونية، وأن يتم تأمين تلك التعاملات، حتى لا تصبح هذه التعاملات عرضة للقرصنة وخرقًا لحرمة المعلومات الشخصية.

مشكلة الدراسة:

تتسم المعاملات القانونية في صورتها التقليدية بسمتين أساسيتين، تتمثل السمة الأولى في وجود محرر مكتوب على وسيط مادي ليس من السهل إنكاره أو التغيير في مضمونه، فضلا عن إمكانية الرجوع إليه، بحالته التي نشأ عليها، في أي وقت متى دعت الحاجة إلى ذلك، وتتعلق السمة الثانية بوجود توقيع يزيِّل به المستند يفيد الإقرار بصحة مضمونه ونسبته إلى من وقع عليه. هاتان السمتان، اللتان لا وجود لهما بخصوص المحررات الإلكترونية، تُثيران الكثير من الشكوك حول درجة الثقة والأمان المتوافرين في المستند الإلكتروني. وهو ما يضعنا أمام المشكلة الأكبر التي تتصل بمدى قيمة المستند الإلكتروني من الناحية القانونية، لاسيما في مجال الإثبات.

ونظرا لأهمية التعاملات الإلكترونية وتشجيعاً لانتشارها وبث الثقة فيها، فإن الآلية القانونية لتأمين التعاملات عبر الإنترنت هي " عمليات التوثيق الإلكتروني ". وهي عمليات تقوم بها في الوقت الحالي جهات متخصصة مهمتها تأمين سلامة المعاملات التي تتم عبر وسيط إلكتروني من حيث مضمونها ودقة نسبتها إلى من صدرت منه وحفظها، وإصدار شهادة إلكترونية بذلك يمكن الاعتماد عليها في إنجاز هذه النوعية من المعاملات.

والحقيقة أن المشكلات القانونية المرتبطة بتأمين التعامل الإلكتروني على شبكة مفتوحة كشبكة الانترنت لا تتعلق، بالدرجة الأولى، بصحة العقود التي يمكن التي تبرم عليها، انما تكمن المشكلة الحقيقية في تسهيل إثبات سلامة البيانات والرسائل المتبادلة، وتحديد هوية الطرفين، لذلك فالتوثيق الإلكتروني يعتمد على وسائل تكنولوجية حديثة للتوثيق.

أسئلة الدراسة:

ومن هنا نطرح الإشكالية التالية التي هي عصب هذا البحث وجوهره:

إلى أي مدي يُعَدُّ التوثيق الإلكتروني لعقود التجارة الإلكترونية سنداً في التعاملات الإلكترونية؟

أهداف الدراسة:

استنادًا إلى ما سبق تهدفُ هذه الدراسة إلى تحقيق الأهداف التالية:

1- إزالة ما قد يعتري التوثيق الإلكتروني لعقود التجارة الإلكترونية من غموض.
2- مدى الاعتراف بهذه العقود وكيفية التوثيق الإلكتروني لها.

أهمية الدراسة:

تكمن أهمية الدراسة في التالي: -

1- أنه يرتبط ارتباطًا وثيقًا بنوع جديد من العقود وهو عقود التجارة الإلكترونية والتي أصبحت تفرض نفسها بقوة على المجتمع، نظرًا لما تمتاز به التجارة الإلكترونية من إبرام للعقود عن بُعد دونما التقاء مادي للمتعاقدين في مجلس العقد، وعدم ارتكازها إلى أية مستندات ورقية.

2- إن تحقيق الأمن القانوني للمعاملات، بكل تأكيد، أحد أهم عوامل تحقيق الأمن الاقتصادي والاجتماعي، فضلا عن أن أنظمة التشفير وإخفاء البيانات، كأحد التطبيقات التقنية في مجال الأمن الوطني، هي أهم وسيلة لتحقيق أمن المعاملات التي تتم بوسائل الاتصال الحديثة لاسيما عبر شبكة الإنترنت.

3- أن جل مشاكل الإنترنت تتمحور حول مشكلتين أساسيتين هما أمن التعامل، وكيفية الإثبات.

وفى هذا المجال تأتى خدمات التوثيق الإلكتروني كأحد أهم الوسائل في تحقيق هذه الغاية. وتقوم الفكرة على وجود جهة محايدة تبث الثقة لدى المتعاملين وتؤّمن عملية الاتصال والتبادل بينهما بما تضعه تحت أيديهما من تقنيات التشفير التي تضمن تأمين ونسبة التوقيع إلى صاحبه من ناحية، وعدم إحداث أي تعديل أو تغيير في مضمون الرسائل المتبادلة، أيا كان موضوعها، منذ إنشائها وحتى وصولها إلى المرسل إليه وطوال فترة بقائها وحفظها من ناحية ثانية.

منهجية الدراسة:

نظرًا لأن موضوع البحث، هو نتاج التطور التقني في مجال تكنولوجيا المعلومات والاتصالات، فقد اعتمدنا على مناهج علمية تتكامل فيما بينها بغية التعرف على هذا النظام ومحاولة إلقاء الضوء على جوانبه وتفاصيله وقد تجلت هذه المناهج في المنهج التحليلي، القائم على تحليل وشرح طبيعة التوثيق الإلكتروني لعقود التجارة الإلكترونية، من خلال الآراء الفقهية والقوانين والتشريعات الوطنية. كما استند البحث إلى المنهج الوصفي لإيضاح بعض المفاهيم التي تتضمن تحليلاً دقيقًا، كافيًا للمعلومات، عن موضوع الدراسة وذلك من خلال المنهج المقارن لتوضيح موقف أكثر من تشريع. إضافة إلى مناقشة الآراء الفقهية المتعددة ذات العلاقة سواء تلك التي وردت في الكتب المتخصصة أو التي نوقشت في الأبحاث والدراسات المتخصصة، أو التي نشرت على المواقع الإلكترونية.

2. الدراسات السابقة:

اهتمت العديد من الدراسات العلمية بدراسة موضوع التوثيق الإلكتروني وكان من أهمها دراسة:

- **(المطالقة، 2004)** والتي عالجت العقد الإلكتروني من حيث تعريفه، تميزه عن العقود الأخرى، حماية هذا النوع من العقود، كما تطرقت إلى موضوع التوقيع الإلكتروني وماهيته، صوره، وماهية المحررات الإلكترونية ومدي حجيتها في الإثبات. وأوضحت دراسة (عبيدات، 2005) تعريف العقد الإلكتروني، خصائصه، كيفية انعقاده، بالإضافة إلى موضوع المحررات الإلكترونية والشروط الواجب توافرها بها وحجيتها في الإثبات، كما تطرقت إلى موضوع التوقيع الإلكتروني، تعريفه، شروطه، صوره، وظائفه، ومدي حجيته في الإثبات.
- **وأضافت دراسة (العوضي، 2005)** مفهوم البريد الإلكتروني وطبيعته القانونية، وحدود ملكيته، ومشروعية التعاقد بالبريد الإلكتروني، وإبرام العقد بالبريد الإلكتروني وحجيته في الإثبات. وبينت دراسة (جوبيرت، 2002) دور مقدم خدمات التصديق وكيفية تنظيم أنشطته، وآلية التشفير والتي تستخدم للتحقق من التوقيع

الإلكتروني، كما أوضحت الدراسة إصدار الشهادة الإلكترونية وحالات إلغائها، وطريقة توقيع المعاملات القانونية.

- **وتناولت دراسة (كايدي، 2002)** إثبات الكتابة، ومبدأ المعادلة الوظيفية بين الكتابة التقليدية والكتابة الإلكترونية، وهل الكتابة الإلكترونية دليل إثبات في مجتمع المعلومات وكيفية الاحتفاظ بها، ومدي ضمان سلامة الوثائق وأرشفة الكتابة في مجتمع المعلومات.

التعليق على الدراسات السابقة:

يُلاحظ أن الدراسات السابقة تناولت موضوع التوثيق وجهات التوثيق بشكل عام دون التعمّق في كيفية التوثيق الإلكتروني لعقود التجارة الإلكترونية، كما لم تتطرق- بالتفصيل- لتأصيل التشفير كآلية للتوثيق الإلكتروني، ولذا؛ سنتناول الدراسة الحالية جميع أوجه القصور في الدراسات السابقة، والمتمثلة في التركيز على الدور المباشر لعملية التوثيق الإلكتروني لعقود التجارة الإلكترونية ومدي الاعتراف بها.

هيكل البحث:

اقتضتْ طبيعة الدراسة أن تُقَسَّمَ إلى ثلاثة أقسام، القسم الأول ويتعلق بالإطار العام للبحث وتناول: (المقدمة، والمشكلة، أسئلة الدراسة، والأهداف، والأهمية، والمنهجية، الدراسات السابقة والتعليق عليها).

أما القسم الثاني، فتناول الإطار النظري للدراسة وتكون من ماهية التوثيق الإلكتروني، نطاق التوثيق الإلكتروني. وتناول القسم الثالث النتائج والتوصيات. ثم استعراض المراجع العربية والأجنبية المستخدمة في البحث.

ولعلّه من المفيد الإشارة إلى أنّ المراجع المستخدمة في البحث كانت للتأصيل، فنظراً لوجود كتابات كثيرة ومتعددة (عربية وأجنبية) عن التوثيق الإلكتروني، فقد اختار الباحث الكتابات والأبحاث التي تناولته – دون التأصيل والدراسة لتوثيق عقود التجارة الإلكترونية - وإنما دارت جميعها حول التوثيق الإلكتروني بشكل عام، واختيار تلك المراجع كان بهدف زيادة العمق والتأصيل القانوني لموضوع الدراسة.

التوثيق الإلكتروني لعقود التجارة الإلكترونية

ماهية التوثيق الإلكتروني:

نظرًا لما تتميز به المعاملات القانونية في صورتها التقليدية بميزتين رئيستين. من حيث وجود محرر مكتوب على وسيط مادي ليس من السهل إنكاره، أو التغيير في مضمونه، فضلا عن إمكانية الرجوع إليه بحالته التي نشأ عليها، في أي وقت متى دعت الحاجة إلى ذلك، ووجود توقيع يزيِّل به المستند يفيد الإقرار بصحة مضمونه، ونسبته إلى من وقع عليه. فهذا أمر لا وجود له في المحررات الإلكترونية (أبو الليل، 2003، 1845)، مما يثير الريبة حول درجة الثقة والأمان المتوافران في المستند الإلكتروني. وهنا تثور المشكلة التي تتصل بمدى قيمة المستند الإلكتروني من الناحية القانونية، لاسيما في مجال الإثبات (شمس الدين، 2003، 496).

والواقع أن فكرة المستند الإلكتروني وكذا التوقيع الإلكتروني فكرتان ما زالتا عرضة للتطور الفني والتقني، فلا يجوز التضحية باستقرار المعاملات قبل التأكد من أداء المستند الإلكتروني لدوره الذي يجب أن يرسمه له القانون فإن الآلية القانونية لتأمين التعاملات عبر الانترنت هي " عمليات التوثيق الإلكتروني ".

(GOBERT, 2002 pp 83 à 172) وهي عمليات تقوم بها جهات متخصصة منوط بها تأمين سلامة المعاملات التي تتم من خلال وسيط إلكتروني من حيث المضمون والدقة في نسبتها إلى من صدرت منه وحفظها، وإصدار شهادة إلكترونية بذلك.

تعريف التوثيق من الناحتين الفنية والقانونية

التوثيق، في معناه العام، يعنى التصديق والتأكيد، ومجاله الطبيعي هو التصرفات القانونية في شكلها التقليدي، أي المستندات الورقية، فالمحرر الذي يصدر من موظف عام أو شخص مكلف بخدمة عامة، في حدود سلطته واختصاصه، مراعيا في ذلك الأوضاع التي يتطلبها القانون لإبرامه، هو تصرف موثق، وهذا التوثيق هو الذي يُضفى عليه الصفة الرسمية ويكسبه، بالتالي الحجية التي نص عليها القانون.

وفى معناه القانوني فقد أعطت له القواميس اللغوية العديد من المعاني تدور بين التأمين والاشهاد والترخيص وكذا الضمان. وقد عرف الفقه الفرنسي التوثيق، بأنه " إجراء بمقتضاه يقدم طرف ثالث ضمانا بأن (مستند) أو منتج أو برنامج معين أو خدمة أو مؤسسة أو هيئة معينة يتوافق مع ضوابط ومعايير واشتراطات خاصة ". وإذا كان التوثيق، بهذا المعنى العام، فإن التوثيق في المجال الإلكتروني وتكنولوجيا المعلومات يعنى بشكل أخص ضمان " سلامة وتأمين " التعامل عبر الانترنت، سواء من حيث أطرافه، ومضمونه، ومحله، وتاريخه، لذلك فهو أهم الشروط الواجب توافرها لقيام المحرر الإلكتروني (عبيدات، 2005، 79وما بعدها) ولإعطائه الحجية الواجبة في الإثبات. فاذا كان المحرر التقليدي يقوم على دعامتين اثنين هما الكتابة والتوقيع، فان مقومات المحرر الإلكتروني هي الكتابة، والتوقيع، والتوثيق، والحفظ، والقدرة على الاسترجاع بالحالة التي نشأ عليها.

فالتوثيق، وهو إجراء يتم عن طريق شخص ثالث أو جهة معتمدة عن طريق اتباع بعض الاجراءات الفنية المعقدة، بهدف إلى تثبيت مضمون المحرر والبُعد به عن التلاعب والتغيير ودقة ما يحمله من توقيعات، وصحة نسبته إلى من صدر عنه. وهو بهذه المثابة " قوام المحرر الإلكتروني وسر وجوده ". وبعبارة أخرى يعنى التوثيق الإلكتروني خلق " بيئة إلكترونية آمنة " للتعامل عبر الانترنت. ولما كانت المشاكل في التعامل الإلكتروني تكمن في أنه يتم بين طرفين لا يعرف كلا منهما الآخر، وعبر وسيط مفتوح وغير آمن، وعن طريق التجول في متجر افتراضي قوامه الأشكال والصور، وبطريقة ينعدم فيها أي دليل مادي على حقيقة ما تم وهذا أمر يستوجب توفير الضمانات الكفيلة بتحديد هوية المتعاملين (أبو الليل، 177)، وتحديد حقيقة التعامل ومضمونه. ولتحقيق هذا الهدف فقد استلزم الأمر وجود طرف ثالث محايد موثوق به، يقوم بطرقه الخاصة بالتأكد من صحة صدور الإرادة التعاقدية الإلكترونية ممن تنسب اليه، والتأكد من جدية هذه الارادة وبُعدها عن الغش والاحتيال، لذا فقد باتت الحاجة ملحة إلى آلية تبعث الثقة والأمان، نوعا ما، في هذا الصنف المستحدث من التعامل.

وقد تحقق ذلك تشريعيا بالفعل من خلال آلية التوثيق أو التصديق وذلك من خلال إيجاد وسيلة تؤدى إلى تحقيق مجموعة الأهداف التالية:

1- تحديد هوية أطراف المعاملة سواء أكانوا أشخاصا طبيعيين أو اعتباريين، (أبو الليل، 1889) وتحديد أهليتهم للتعامل.
2- ضمان سلامة محتوى البيانات المتداولة عبر الشبكة، وهو ما يسمح بالتحقق من أن مضمون الرسالة (الإيجاب أو القبول) لم يتغير في الفترة ما بين إرسال الرسالة وتسلمها بل واثناء فترة حفظها كدليل إثبات عند النزاع.
3- ضمان السرية الكاملة للبيانات المتداولة بين البائع والمشترى.

4- ضمان عدم انكار رسالة البيانات الصادرة من قبل أي من الطرفين.

(Barbry,Bensoussan،2000),http://www.journaldunet.com/juridique/juridique18certification.shtml)

آلية التوثيق:

بدأت اللبنة الأولى، على المستوى الأوروبي، بالتوجيه الاتحادي الصادر في 13 ديسمبر1999، والذى عنى بوضع نظام قانوني اتحادي للتوقيع الإلكتروني، ويعد بحق نقطة تحول في مجال التوقيع الإلكتروني وتنظيم خدمات التوثيق. ثم توالت بعد ذلك التشريعات المحلية الأوروبية في السير في نفس الاتجاه. وكان أول المشرعين سبقا في هذا الخصوص هو المشرع البلجيكي. ففي 16 ديسمبر 1999، وضعت الحكومة البلجيكية مشروع القانون رقم 322 المتعلق بتنظيم انشطة مقدمي خدمات التوثيق الإلكتروني. وقد جاء هذا المشروع، متأثرا بما ورد في التوجيه. وتم تطويع المشروع ليأتي متناغما بالكلية مع التوجيه الأوروبي، وليُعمل به اعتبارًا من9أكتوبر2001م (,GOBERT) op.cit، ثم كانت فرنسا، فقد صدر بتاريخ 21يونيه 2004 أحدث التشريعات وأشملها في معالجة مشكلات التجارة الإلكترونية تحت عنوان معبر هو" الثقة في الاقتصاد الرقميla confiance dans l'économie numérique ""، ومن أهم الاضافات التي أتى بها هذا القانون أنه تجاوز كثيرا المفهوم القديم للتعاقد عن بُعد، ثم أنشأ نظاما للمسئولية بقوة القانون بموجب المادة 1/15 على عاتق كل شخص طبيعي أو معنوي يمارس أنشطة التجارة الإلكترونية تجاه المشترى عن تنفيذ التزاماته الناتجة عن العقد سواء أكان هو نفسه القائم بالتنفيذ، أو شاركه في ذلك احد من الغير.

(ROJINSKY, TEISSONNIERE, http: //www.lex-electronica.org/articles/v10-1/rojinsky_teissonniere)

ويسرى هذا النظام من المسئولية على مقدمي خدمات التوثيق بطبيعة الحال. واثبت القانون هذه الحماية للمشترى سواء أكان محترفا أو مستهلكا، وجعل المشرع هذا النوع من المسئولية من النظام العام الذي لا يجوز الاتفاق على ما يخالفه. وفي مصر صدر القانون رقم15 لسنة 2004 الخاص بالتوقيع الإلكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات، وباستقراء التشريعات المختلفة التي تدخلت صراحة في هذا المجال نجد أن هذه الآلية تتجسد في وجود شخص محايد ذا إمكانات فنية وتكنولوجية خاصة يسمى أحيانًا بالغير محل الثقة، وأحيانًا أخرى بمقدمي خدمات التوثيق، وبالتالي بث الثقة لدى مستعملي الشبكات المفتوحة من خلال اتباع مجموعة من الوسائل والاجراءات الفنية اللازمة لتأمين ما يجري بينهم من تعاملات أو صونها من العبث طوال فترة حفظها، وتقديم شهادة إلكترونية معتمدة تثبت كل ذلك وتؤمنه وتبعث الثقة فيه. (رشدي، 2006، 124، PENNEAU،P.2065)، والآلية الأساسية التي تتبعها جهات التوثيق الإلكتروني في عملها تتمثل حتى الآن في آلية التشفير (أبو الليل، 1856). والتشفير La cryptographieهو عبارة عن عملية يتم فيها تحويل الرسالة وكذا التوقيع عليها من صورتها العادية إلى صورة أرقام أو رموز غير مفهومة، (الدكاني، وأحمد، د. ت، 119)، وهي عملية تستخدم فيها مفاتيح سرية وطرق حسابية معقدة " لوغاريتمات " لا يمكن فهمها الا بفك تشفيرها ممن يملك مفتاح ذلك التشفير وتعتمد قوة وفعالية التشفير على عاملين أساسيين: الخوارزمية، وطول المفتاح مقدرًا بالبت (bits)، وقد عرفته المادة الأولى من اللائحة التنفيذية للقانون المصري رقم 15 لسنة 2004م الخاص بتنظيم التوقيع الإلكتروني في فقرتها التاسعة بأنه " منظومة تقنية حسابية تستخدم مفاتيح خاصة لمعالجة وتحويل البيانات والمعلومات المقروءة إلكترونيا بحيث تمنع استخلاص هذه البيانات والمعلومات الا عن طريق استخدام مفتاح أو مفاتيح فك الشفرة ".كما عرفه المشرع التونسي في المادة 5/2 من قانون المبادلات والتجارة الإلكترونية التونسي 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 ". كما عرفه الفقه بأنه عملية تحويل النص إلى اشارات غير مفهومة تبدو غير ذات معنى لمنع الغير من الاطلاع عليها، وترتكز على القيام بتحويل النصوص العامة إلى نصوص مشفرة، مع امكانية إعادة النص المشفر إلى نص عادى بعد فك التشفير بمفتاح التشفير الذي تم إنشاؤه. وقد ظهر، في هذا الخصوص، نوعان من التشفير، ويسمى الأول بالتشفير المتماثل والثاني بالتشفير غير المتماثل.

أولا- التشفير المتماثل (المفتاح السري):

وفيه يتم الاعتماد على مفتاح سرى واحد بمقتضاه يتم تشفير المعاملة وكذا فكها.

(Sèdallian, 2000 ، www.juriscom.net/chr/2/fr20000 509.htm)

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..(Bitan, 2000 P. 10) فمرسل الرسالة ومستقبلها يستخدمان المفتاح نفسه، فهو مفتاح تم اعداده بين طرفي العلاقة ليتم التشفير وفكه من خلاله، فهو باختصار مفتاح ثنائي الوظيفة مع اختلاف وظيفته بالنسبة لكل منهما (عبيدات، 140). فالأول يستخدمه في التشفير والثاني لفك هذا التشفير، ويتفق الطرفان (المرسل والمستقبل) في البداية على عبارة المرور التي سيتم استخدامها. وتحتوي تلك العبارة على حروفا ورموزا متعددة يتم تحويلها، بموجب برمجيات التشفير إلى عدد ثنائي، يتم إضافة رموز أخرى لزيادة طولها. ويشكل العدد الثنائي الناتج مفتاح تشفير الرسالة. وبعد استقبال الرسالة المشفرة يستخدم المستقبل عبارة المرور نفسها من أجل فك شيفرة النص المشفر، إذ تترجم البرمجيات مرة أخرى عبارة المرور لتشكيل المفتاح الثنائي الذي يتولى اعادة تحويل النص المشفر إلى شكله الأصلي المفهوم (الدكاني، وأحمد، 120). وإذا كانت هذه الطريقة تتميز بالبساطة إلا أنه يعيبها ما يلي:

1- أنها تفترض سبق معرفة أطراف المعاملة لبعضهم البعض وهو ما يتنافى مع الواقع في كثير من الأحيان، بل ومع الطبيعة العالمية والمفتوحة لشبكة الانترنت (العوضي، 2005، 171)، تلك الشبكة التي لا تظهر فائدتها الحقيقية إلا في التعامل بين أطراف تفصل بينهما الحدود والمسافات وقد لا يعرف بعضهما بعضا.
2- أنه لا توجد وسيلة آمنة لتبادل المفتاح الوحيد المستخدم بين المرسل والمرسل إليه لأنه لو كانت هذه الوسيلة موجودة فعلا، فلماذا لم تُستخدم في التعاقد منذ البداية!!

ولا شك أن ذلك قد يغرى الغير بالتسلل واقتحام البيانات التي تم إرسالها. وهو ما يعنى التأثير سلبًا على عامل الثقة الذي (عبيدات، 141)، هو أساس نجاح عمليات التجارة عامة والتجارة الإلكترونية خاصة. فأهم عيوب هذا النظام تكمن في تبادل المفتاح السري نفسه بين الطرفين من خلال ارساله عبر هذه الشبكة المفتوحة مما يسهل فرص التقاطه من قبل القراصنة ومن ثم اقتحام ومهاجمة البيانات التي تم ارسالها لدوافع كثيرة اقلها التلصص والاعتداء على الخصوصية، ولذا فلابد من تدبير وسيلة اتصال عالية الأمان والسرية يتم عبرها تبادل المفتاح.

3- أنها تقنية تفترض وجود مفتاح لكل معاملة بما يعنى تعدد المفاتيح بتعدد المعاملات وتعدد المرسل إليهم.

وفضلا عما يؤدى إليه ذلك من تعقيد وتكلفة عالية، فإنه يقضى على عامل السرعة التي تتميز به المعاملات التجارية عامة (العوضي، 172) وتلك التي تتم عن طريق وسائل التقنية الحديثة بصفة خاصة.

ثانيا- التشفير غير المتماثل:

ولكثرة عيوب التشفير المتماثل، كان لا بد من البحث عن بديل أخر يحل محله ويؤدى 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 (أبوزيد، 46، 2002)، 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.

وعليه فإذا أراد (أ) إرسال عرض أو إيجاب بالتعاقد إلى (ب) ما عليه إلا أن يوقع الرسالة بمفتاحه الخاص الذي يحتفظ به سرا مكنونا لا يطلع عليه سواه ويرسلها إلى (ب) وبصحبتها مفتاحه العام للتحقق (أبو زيد، 190) من نسبتها إلى من صدرت عنه. وعندما يتحقق المرسل إليه من أصل الرسالة ونسبتها إلى الموقع بالمفتاح العام فانه يكون قد قطع نصف الطريق وبقى امامه 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، ويتم هذا التحقق بأن يقوم المرسل اليه بحل شفرة التوقيع الرقمي مستخدما في ذلك المفتاح العام للمرسل وذلك بإعادة الرمز أو العلامة المشفرة إلى حالتها الأولى قبل التشفير، فان نجحت العملية فهذا هو الدليل على أن الرسالة موقعة بالمفتاح الخاص للمرسل، وبالتالي منسوبة إليه، فالمفتاح الخاص هو، ببساطة، يساوى القلم الذي يوقع به الشخص في الوضع التقليدي للتعاقد وكل ما هنالك من فارق بين القلم كوسيلة تقليدية للتوقيع وبين المفتاح الخاص كوسيلة إلكترونية مستحدثة هو في الطريقة الفنية التي يُؤلف بها التوقيع في الحالة الثانية، ويتم التوقيع وفقا لهذه الطريقة باتباع إجراءات عالية التقنية والتعقيد تسمح لمنشئ المحرر الإلكتروني بأن يحول بيانات ومضمون المحرر الذي يريد توقيعه إلكترونيا إلى قيمة عددية يدرجها مع بيانات المحرر الإلكتروني لتمثل توقيعه الرقمي، بحيث لا يمكن لأحد الكشف عن المضمون اللغوي لهذه القيمة العددية إلا الموقع والمرسل إليه الذي يحوز مفتاح فك التشفير، أي المفتاح العام المقابل للمفتاح الخاص للمرسل. والسبب في ذلك يكمن كما هو معروف من ان المفتاحين مرتبطين ببعضهما البعض ارتباطا له هذ الدلالة. إما أن فشلت العملية بأن استعصى على المرسل إليه فك عملية التشفير فهذا يعنى إما ان المفتاح العام الذي بحوزة المرسل اليه ليس هو المفتاح العام للمرسل، وإما أن الرسالة ليست موقعة بمفتاحه الخاص. ويتم التحقق من أن مضمون الرسالة لم يتغير أثناء ابحارها عبر الشبكة باتباع الخطوات التالية:

1- يقوم المرسل اليه بفك شيفرة التوقيع الرقمي باستخدام المفتاح العام للمرسل، وذلك بأن يعيد الرمز المصاحب للرسالة إلى حالته الأولى قبل التشفير على نحو ما سلف البيان.
2- يقوم المرسل إليه بعمل خلط جديد واختزال للرسالة مستخدما في ذلك نفس برنامج الخلط والاختزال الذي سبق للمرسل أن استخدمه، والفرض أنه مبين في الشهادة الإلكترونية التي وصلته والصادرة من جهة التوثيق.
3- يقارن المرسل اليه بين العلامة أو الرمز الناتج عن عملية الخلط والاختزال التي قام بها وبين العلامة أو الرمز الناتجة عن عملية الخلط والاختزال الذي قام بها المرسل عن التوقيع على الرسالة فاذا لم يوجد اختلاف بين الرمزين أو العلامتين فهذا يعنى التطابق التام بين الرسالة كما صدرت من المرسل والرسالة كما وصلت إلى المستقبل، أما ان وجد اختلاف فهذا دليل على أن الرسالة قد شابها التعديل والتحريف، ذلك انه من المعطيات العلمية المؤكدة أنه يستحيل أن ينتج عن نصين مختلفين، ولو في شذرة واحدة، نفس الاختزال، أي نفس الرمز .(Bitan, op.cit P. 11) أو العلامة 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 يبق بإمكان أي شخص استخدام المفتاح العام في فك تشفير الرسالة والاطلاع على مضمونها وإن بقي عاجزًا 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. (Sèdallian, art Prèc)..

ويُدعى نظام التشفير الذي يستخدم المفاتيح العامة بنظام RSA ورغم أنه أكثر أمنا من نظام DESإلا أنه أعقد وأبطأ إذ أن جلسة التشفير وجلسة فك التشفير يجب أن تكونا متزامنتين تقريبا، فضلا عن أنه نظام ليس عصيا على الاختراق متى توافر الوقت والمال، ولذا فقد تم تطويره بنظام (PGP (Pretty Good Privacy الذي يستخدم مفتاحا طوله 128 بت إضافة إلى استخدام البصمة الإلكترونية للرسالة ولا يزال هذا النظام منيعا على الاختراق حتى الآن (عيسى، 2000، 204). والمفتاحان، عبارة عن متتالية رقمية متولدة، في الوقت نفسه من عمليات حسابية معقدة، أومن معطيات بيومترية وهي معطيات تتيح التحقق من هوية الإنسان عن طريق سماته الخلقية ومرتبطين ببعضها البعض ارتباطًا فنيًا على درجة عالية من الدقة، ومع ذلك فإن معرفة تركيبية أحد المفتاحين لا تتيح معرفة أو فك تركيبة المفتاح الآخر.

الشهادة الإلكترونية ودورها في التعامل الإلكتروني:

إذا كانت آلية التشفير الغير متماثل تقدم للمرسل إليه يقينا بأن الرسالة التي وصلته موقعة من المرسل، أي من صاحب المفتاح الخاص الذي اشتق منه المفتاح العام الذي استخدم في فك التشفير، وبالتالي فهي منسوبة إليه (أبوزيد، 200)، إلا أنها لا تحدد " ذاتية " هذا المرسل ولا تعين شخصيته على وجه الدقة. وبعبارة أوضح فإن آلية التشفير الغير متماثل وإن كانت تقيم علاقة بين شخص (افتراضي) ومفتاحه العام، إلا أنه يبقى التساؤل قائما 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 [(1)] بـ" شهادة التوثيق الإلكتروني" وهي شهادة معتمدة تصدر عن أحد مقدمي خدمات التوثيق الإلكتروني المرخص لها من قبل الجهات الرسمية في الدولة لتربط المفتاح العام (أبو زيد، 202) الذي استخدم في فك التشفير بشخص بعينه. فهي على حد تعبير المشرع الفرنسي

(*) وقد تكلم المرسوم الفرنسي الصادر في 30 مارس 2001 على نوعين من الشهادات: الأولى: الشهادة الالكترونية البسيطة le certificat électronique simple وهي عبارة عن مستند يظهر في شكل الكتروني ويشهد بوجود علاقة بين بيانات التحقق من التوقيع الالكتروني وشخصية الموقع، والثانية الشهادة الالكترونية المعتمدة certificat qualifié وهي تلك التي ينبغي أن تستوفى مجموعة من الضوابط والمعايير التي ورد النص عليها المرسوم. ووفقا لما ورد النص عليه في المادة السادسة من هذا المرسوم فانه يجب أن تسلم الشهادة المعتمدة من مقدم خدمة توثيق مؤهل لتسليم هذا النوع من الشهادات، وتتضمن البيانات المحددة التالية:

1. بيان يشير إلى أن هذه الشهادة مسلمة كشهادة الكترونية معتمدة.
2. هوية مقدم خدمة التصديق الالكتروني وحالته التي تأسس فيها.
3. اسم الموقع أو الاسم المستعار.
4. وعند الضرورة بيان صفة الموقع بحسب الاستعمال التي خُصصت الشهادة له.
5. بيانات ومعطيات التحقق من التوقيع الالكتروني.
6. بداية ونهاية مدة صلاحية الشهادة الالكترونية.
7. كود التعامل مع الشهادة الالكترونية.
8. التوقيع الالكتروني المؤمن لمقدم خدمة التوثيق الالكتروني الذي يُسلم شهادات معتمدة.
9. شروط استعمال الشهادة الالكترونية لا سيما بيان الحد الأقصى لمبلغ الصفقة التي تُستخدم الشهادة في إبرامها.

وهي نفس البيانات التي نص عليها التشريع الفيدرالي السويسري المتعلق بخدمات توثيق التوقيع الإلكتروني الصادر في 19 ديسمبر 2003م في مادته السابعة.

في المادة الأولى من الفقرة 9 من المرسوم رقم 272 لسنة 2001 م، مستند في شكل إلكتروني يقيم صلة دقيقة بين البيانات المستخدمة في التحقق من التوقيع وشخص الموقع ذاته، بحيث يمكن للمرسل اليه الاطمئنان إلى أن مصدر الرسالة هو ذات الشخص المحدد في هذه الشهادة، وبالتالي يتحول المرسل من شخص افتراضي إلى شخص محدد الهوية. وفي السياق ذاته عرفت المادة الثالثة من التوجيه الأوروبي شهادات التوثيق الإلكتروني بأنها تلك التي تربط بين أداة التوقيع وبين شخص معين، وتؤكد شخصية الموقع من خلال استيفاء الشروط الواردة في الملحق رقم (2). فضلا عن اشتمالها على تأكيد بأن التوقيع المعنى قد استوفى كافة الشروط والضوابط المطلوبة فيه باعتباره دليل إثبات يُعول عليه، وبهذه التكملة الضرورية توفر آلية التشفير غير المتماثل الأمان الكامل للرسائل المتبادلة ليس فقط من حيث مضمونها، (أبو الليل، 183) وإنما من حيث هوية أطرافها.

ولذا فقد نصت مختلف التشريعات على وجوب تضمين الشهادة المعتمدة بيانات معينة تساعد على تحقيق هذا الغرض، كما ورد في المادة (20) من اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري. وتتعدد شهادات التوثيق بحسب استخداماتها والغرض منها، فإلى جانب شهادة توثيق التوقيع الرقمي توجد شهادات أخرى مثل شهادة توثيق تاريخ الإصدارر، وهي شهادة توثق تاريخ ووقت اصدار التوقيع الإلكتروني، حيث يقوم صاحب الشهادة بعد التوقيع عليها بإرسالها إلى جهة التوثيق التي تقوم بتسجيل التاريخ عليها وتوقيعها من جهتها ثم تعيدها إلى مرسلها مرة أخرى، وأيضا شهادة الإذن، وبمقتضاها يتم تقديم معلومات اضافية عن صاحبها مثل عمله ومؤهلاته والتراخيص التي يملكها، وشهادة البيان، وهي شهادة تفيد بيان صحة واقعة أو حدث ما ووقت وقوعه. فالشهادة الإلكترونية هي، إذن، حقيقة معلوماتية تسمح بما لا يدع مجالا لأي شك، بربط هوية كائن معين (شخص أو هيئة) بمجموعة معينة من السمات المميزة له.

دور التوثيق في مجال المحررات الإلكترونية

إن مهنة الموثق الإلكتروني تتشابه كثيرًا في بعض وظائفها مع مهنة الموثق المعروفة في فرنسا ومصر والعديد من الدول، على اعتبار أن كلا منهما يعد شاهدًا محايدًا ومستقلًا عن العقد المبرم بين الأطراف (إبراهيم، 2006، 156)، يلجأ إليه هؤلاء بغرض تأمين معاملاتهم ومنحها الثقة الواجبة حتى تكون صالحة لإثبات ما تتضمنه من تصرفات قانونية. ولهذا السبب يُطلق عليهم" وكلاء الإثبات" (فايد، د.ت، 69). هذا وإذا كان كل ما للتوثيق من دور بالنسبة للكتابة المثبتة على دعامة ورقية يتمثل في مجرد تقوية حجيتها وقيمتها القانونية ليس إلا، فإن التوثيق بالنسبة للمحررات الإلكترونية هو الذي يُنشئ هذه الحجية من الأساس، وعلى ذلك فلا تصح التسوية التامة والمطلقة بين وظيفة ودور التوثيق التقليدي الذي يقوم به موظف عام مختص وبين التوثيق الإلكتروني الذي يتم في عالم افتراضي وتقوم به جهات خاصة.

ولذا فيمكن القول بأن التوثيق هو" سر وجود المحرر الإلكتروني من الناحية القانونية " أو هو، بالأحرى"، مكون أساسي من مكونات القيمة القانونية للكتابة الإلكترونية ". فبدون تقنيات التوثيق الإلكتروني تفقد الكتابة الإلكترونية أي دور قانوني لها، والدليل المبدئي على ذلك أن الحديث عن حجية الكتابة الإلكترونية والتوقيع الإلكتروني، وعمليات الحفظ والوفاء الإلكتروني لم يبدأ، ولم يكن له أن يبدأ، إلا بعد ظهور ما يسمى بتقنيات التوثيق الإلكتروني. ويمكن أن نقدم العديد من الأدلة التشريعية والفقهية على صدق هذه الحقيقة:

باستقراء التشريعات التي اهتمت بتنظيم المعاملات الإلكترونية يتبين بجلاء أنها لم تُسلم للتوقيع الإلكتروني والكتابة الإلكترونية بأية قيمة قانونية إلا بعد استيفائها للعديد من الاشتراطات التي أُنيط تحقيقها بتدخل شخص محايد هو الموثق الإلكتروني ويتضح ذلك في التشريع الفرنسي، من نص المادتين 1316-1، 1316-4 من القانون المدني

ووجه الاستدلال أن المادة الأولى ربطت مساواة الكتابة الإلكترونية بالكتابة الورقية من حيث الحجية بإمكانية تحديد شخص من صدرت عنه من ناحية وبقيامها وحفظها في ظروف من شأنها ضمان سلامتها من ناحية أخرى. كما ربطت المادة الثانية (1316-4) حجية التوقيع الإلكتروني في الإثبات بمدى قدرته على تحديد هوية الموقع من ناحية، وضمان صلته بالمحرر الذي وقع عليه من ناحية ثانية، وأقامت من هذين الأمرين قرينة قانونية بسيطة على صحة هذا التوقيع طالما أنه تم وفقا للشروط التي يحددها مرسوم يصدر من مجلس الدولة لتطبيق هذا النص، ولم يتوانى المشرع الفرنسي فقد صدر تلبية لهذ الاحالة، المرسوم رقم272-2001 م محددًا في مادته الأولى الفقرة الثانية أن التوقيع الإلكتروني المؤمن: هو ذلك الذي يستوفى، بجانب الضوابط المنصوص عليها في الفقرة الأولى من المادة1316-4 من التقنين المدني الشروط التالية:

أ- أن يكون خاصا بصاحبه.

ب- ان تكون وسائل انشاؤه تحت سيطرة الموقع وحده.

ج- أن يرتبط بالتصرف الذي وضع عليه برابطة تقود إلى اكتشاف أي تعديل لاحق يدخل عليه.

وطبيعي ألا يتحقق للتوقيع الإلكتروني هذه الدرجة من الأمان إلا إذا كانت أداة إنشاؤه لا يمكن اختراقها، ولن يتحقق ذلك، في نظر المشرع الفرنسي، إلا إذا استوفت تلك الأداة الضوابط المنصوص عليها في الفقرة الأولى من المادة الثالثة من المرسوم نفسه المشار إليه، وتم توثيقها طبقا للمقتضيات التي تضمنتها الفقرة الثانية من نفس المادة. وبالرجوع إلى الفقرة الأولى نجدها تشترط الضمان الكامل، بكافة الوسائل والإجراءات الفنية الممكنة، للضوابط الأربعة التالية في الأداة التي تُستخدم في وضع التوقيع الإلكتروني:

1- انعدام أية إمكانية لصدور هذه الأداة لأكثر من مرة واحدة مع الحفاظ على سريتها الكاملة، بمعنى عدم امكانية تكرار أداة التوقيع أو أحد مكوناتها، وهو ما يعنى بعبارة مختصرة عدم تصور وجودها إلا مع من صدرت لصالحه.

2- انعدام أية إمكانية للوصول إليها عن طريق الاستنتاج أو الاستنساخ أو التخمين مهما تعددت المحاولات وتكررت، فضلا عن حمايتها ضد أي تزوير أو تزييف.

3- ضمان سيطرة الموقع، وحده، على أداة إنشاء التوقيع وعدم وجود أية فرصة لاستعمالها من قبل الغير.

4- ألا تؤدى هذه الأداة، عند استعمالها أو حتى بعد ذلك، إلى إحداث أي تعديل أو تغيير في مضمون التصرف محل التوقيع من ناحية، وألا تحول، بأية طريقة، بين الموقع وبين معرفته التامة لهذا المضمون قبل التوقيع عليه من ناحية ثانية. لا يكفي كل ما سبق، لكي يُعد التوقيع الإلكتروني " مؤمنًا "، بل تطلبت الفقرة الثانية من نفس المادة وجوب أن تكون الضمانات المنصوص عليها في الفقرة الأولى ضمانات موثقة، سواء من قبل أجهزة تأمين أنظمة المعلومات التابعة لرئيس الوزراء، أومن قبل مؤسسة توثيق معنية بهذا الأمر في أي دولة من الدول الأعضاء في الاتحاد الأوروبي.

ومن التشريعات العربية التي أخذت بهذا القرينة في الإثبات قانون التجارة الإلكترونية البحريني لسنة 2002م

وقد جرى مجرى القانون الفرنسي، من التشريعات الأجنبية، القانون السويسري، إذ بعد أن عددت الفقرة (b) من المادة الثانية من القانون الفيدرالي السويسري الصادر في 2003م . السمات الخاصة بالتوقيع الإلكتروني (وهي تقريبا نفس سمات التوقيع التقليدي) مؤكدة على وجوب أن يأتي التوقيع الإلكتروني مرتبطا وحسب بشخص صاحبه، دالا على شخصيته، ناشئا بوسائل تحت السيطرة المطلقة له، مرتبطا بمضمون التصرف بطريقة تجعل بالإمكان كشف أي تغيير أو تعديل لاحق، أضافت الفقرة (C) أن هذا التوقيع لا يكون معتمدا إلا إذا استخدمت أداة

مؤمنة في انشائه طبقا لنص الفقرتين الأولى والثانية من المادة السادسة من ذات القانون، ومستندا على شهادة توثيق صحيحة وسارية المفعول وقت وضعه. وهما نفس الشرطين تقريبا الذي ورد النص عليهما في القانون الفرنسي. وبالرجوع إلى المادة 6 / 1، 2 المشار اليها وجدناها تشترط حتى تكون أداة إنشاء التوقيع مؤمنة الشروط الثلاثة التالية:

1- ضمان عدم تكرار مفتاح التوقيع من الناحية العملية مع الحفاظ التام على سريته.
2- الضمان التام والكامل، بكافة الوسائل الممكنة، على انعدام أية إمكانية للوصول إلى المفتاح المستخدم في التوقيع عن طريق الاستنساخ أو الاستنتاج.
3- الضمان التام على حماية مفتاح التوقيع من قبل صاحبه الشرعي وانعدام أية فرصة لاستخدامه استخداما غير مشروع من قبل الغير.

ومن التشريعات العربية، قانون المعاملات الإلكترونية الأردني رقم 85 لسنة2001م لاسيما مادتيه الثامنة التي علقت الاعتراف بصحة " السجل الإلكتروني " على توافر مجموعة من الشروط والضوابط شبيهة إلى حد ما بتلك الواردة في التشريعات الأجنبية، كذا مادته العاشرة التي ربطت صحة التوقيع الإلكتروني ونسبته إلى صاحبه باتباع آلية لتحديد هوية صاحب التوقيع، وقانون المبادلات والتجارة الإلكترونية التونسي الذي الزم كل من يرغب في إمضاء وثيقة إلكترونية إحداث إمضاء إلكتروني بواسطة منظومة موثوق بها يتم ضبط مواصفاتها التقنية بقرار من الوزير المكلف بالاتصالات. وكذا قانون المعاملات والتجارة الإلكترونية لإمارة دبى رقم 2 لسنة 2002م. وقانون التجارة الإلكترونية البحريني الذي ربطت مادته الخامسة في فقرتيها الثالثة والرابعة، حجية المحرر الإلكتروني والتوقيع الإلكتروني في الإثبات بضرورة توافر مقتضيات وضوابط معينة تستلزم بالضرورة دورا محوريا لجهات التوثيق الإلكتروني، وقانون المعاملات الإلكترونية العُماني لسنة 2008م وهو يعد أحدث التشريعات العربية في هذا الخصوص وهو، كسابقيه، لا يعطى للمحرر أو التوقيع الإلكتروني أية قيمة إذا لم يكن موثقا.

والحقيقة أن المقتضيات التي تطلبتها كل التشريعات السابقة وغيرها لا يمكن أن تتحقق، بصريح النص، إلا من خلال اتباع تقنيات التوثيق الإلكتروني. إذن فالتوثيق الإلكتروني أصبح الأن حقيقة لا يستقيم معنى المحرر الإلكتروني إلا بها، وكان من أوضح التشريعات العربية تجسيدا لهذه الحقيقة قانون المعاملات الإلكترونية الأردني في مادته 32 / ب إذ نفت هذه المادة أية قيمة قانونية للمحرر الإلكتروني والتوقيع الإلكتروني إذا لم يكن موثقًا. بل يمكن القول بأنه أصبح التزاما على عاتق من يختار طريق التعامل الإلكتروني أن يلجأ إلى مقدمي خدمات التوثيق. وقد كرس المشرع المصري هذا الالتزام بنصه في المادة (15) من قانون التوقيع الإلكتروني لسنة 2004م على أن الكتابة الإلكترونية لا تتمتع بذات الحجية المقررة للمحررات الورقية (رسمية كانت أم عرفية) إلا إذا استوفت الشروط المنصوص عليها في هذا القانون والضوابط الفنية والتقنية التي تحددها اللائحة التنفيذية الصادرة لتنفيذه. وهو ما يعنى بالأخير وجوب اللجوء إلى خدمات التوثيق الإلكتروني.

نطاق التوثيق الإلكتروني:

لقد حرص المشرع الأوروبي على تبنى نظاما قانونيا خاصا يُطبق على أنشطة مقدمي خدمات التوثيق الإلكتروني، وذلك بالتوجيه الصادر فى13ديسمبر 1999م. وهو التوجيه الذي نقله، في نظامه الداخلي، كل من المشرع البلجيكي والفرنسي وكذلك المشرع الإيطالي وقد تبنى المشرع السويسري هذا النظام بموجب المرسوم الصادر في 12 أبريل2000م. وغيرهما من مشرعي الدول الأوروبية. ويبدو أن الفقه، في معالجاته لهذه التشريعات، قد حصر عمليات التوثيق الإلكتروني في نطاق الخدمات المرتبطة بالتوقيع الإلكتروني فقط. فهل هذا، فعلا، هو المجال الوحيد الذي يعمل فيه الموثق الإلكتروني أو الغير محل الثقة؟ أم أن هناك مجالات أخرى يمكن أن يمتد إليها نشاطه؟ أن ما أثار

هذا التساؤل هو أن المشرع الفرنسي، ومعه غالبية مشرعي الدول الأوروبية، لم ينظم عمليات التوثيق الإلكتروني إلا بمناسبة تنظيمه لخدمات التوقيع الإلكتروني، فهل هذا هو ما أراده المشرع بالفعل أم أنه وضع، في هذا المجال، القاعدة العامة وترك للقضاء إمكانية مد العمل بها إلى مجالات أخرى؟

نعتقد مع البعض أن مجال التوقيع الإلكتروني ليس هو المجال الوحيد الذي يعمل فيه الغير محل الثقة أو مقدم خدمة التوثيق، وإنما توجد مجالات أخرى يمكن أن يمتد إليها نشاط هذا الأخير مثل البريد الإلكتروني المصحوب بعلم الوصول وكذا عمليات الحفظ الإلكتروني.

(GOBERT، www.droit technolgie.org/dossiers/goberttiersconfiancedossier.pdf)

وإذا كان المشرع لم يتكلم عن خدمات التوثيق الإلكتروني إلا بمناسبة تنظيم التوقيع الإلكتروني فلا يعنى ذلك ربط هذه الخدمات بهذا المجال وحده. وسوف نعطى لمحة مختصرة عن الدور الذي يؤديه الغير محل الثقة في كل مجال من هذه المجالات.

التوثيق في مجال خدمات البريد الإلكتروني

أهمية البريد الإلكتروني:

البريد التقليدي المصحوب بعلم الوصول هو خدمة قوامها تأمين الرسالة ضد خطر الفقد أو السرقة أو التلف أو الضياع، وهي خدمة يُقدم فيها، مكتب البريد، للمرسل، بناء على طلبه إيصال استلام الرسالة، وكذا إيصال يفيد علم وتاريخ وصولها إلى المرسل إليه (العوضي، 70). وقد أشار جانب من الفقه إلى أن البريد التقليدي المصحوب بعلم الوصول(MONTERO, 2003 p. 79) رغم الثقة الموضوعة فيه هو نظام متواضع نسبيًا من حيث الضمانات التي يقدمها، إذ كل ما يُتيحه إيداع رسالة مصحوبة بعلم الوصول في مكتب بريد هو إثبات تاريخ الايداع، دون أي تأكيد على أن الرسالة المرسلة قد وصلت بالفعل إلى علم المرسل إليه، وإذا دل إيصال الاستلام على وصول الرسالة، فلا يمكن التأكيد على أن المستقبل قد اطلع عليها بالفعل، ولذا وجدنا القضاء يستعين في هذا الخصوص، بفكرة القرائن بحيث يكون تسلم الرسالة قرينة على علم المستقبل بما ورد فيها، ويقدم البريد الإلكتروني المصحوب بعلم الوصول، الذي يقوم به شخص من الغير محل ثقة والمصحوب بآلية التوقيع الإلكتروني المعتمد، مزايا تفوق البريد التقليدي الموصى عليه، إذ يضمن البريد الإلكتروني ليس فقط واقعة الارسال وواقعة تسلم الرسالة إلى المرسل إليه، وإنما كذلك إثبات محتواها (العوضي، 74)، وكذا هوية طرفيها (المرسل والمستقبل). فتقنية البريد الإلكتروني الموصى عليه تسمح بالتحقق من أن المحتوى الذي تلقاه المستقبل يتوافق تماما مع المحتوى الذي يدعيه المرسل، بل إن هذه التقنية تسمح بالقول بأن المستقبل قد قرأ بالفعل الرسالة أو على الأقل فتحها(GOBERT, art Prèc) ، هذا ويتم اللجوء إلى الرسالة الإلكترونية إما بدافع الرغبة في إعداد دليل للإثبات تجنبا للنزاع في المستقبل، وإما لأنها مطلوبة، لصحة إجراء معين، بموجب نص في قانون أو لائحة. ومن المعلوم أن البريد الإلكتروني الموصى عليه يلعب دورًا كبيرًا في عمليات التعاقد عن بُعد، وهي عمليات تُبرم وتنفذ عن طريق تبادل الرسائل. وفى هذه الحالة تشتد حاجة كل طرف إلى أن يكون بيده دليل يمكنه، عند الضرورة، من إثبات حقه في مواجهة الطرف الأخر، ولا يوجد خير من البريد الإلكتروني الموصى عليه للقيام بهذا الدور.

وإزاء هذه الأهمية فقد بدأت الكثير من التشريعات الأوروبية في الاعتراف بخدمة البريد الإلكتروني. وقد تمثل أول اعتراف تشريعي بالبريد الإلكتروني في التوجيه الأوروبي الصادر فى15 ديسمبر1997م، وقد أقر المشرع البلجيكي هذه الخدمة بالمرسوم الملكي الصادر في 9 يوليه 1999م في مادته (21) حيث ورد بها ما معناه أن خدمة البريد الموصى عليه، في المجالات القضائية والادارية، تقوم بها مكاتب البريد التقليدية أيا كانت الدعامة التي

استخدمت في إنشائها. وإذا كان هذا النص قد فتح، من الناحية القانونية، الباب أمام البريد الإلكتروني الموصى عليه، فإنه قد قصر القيام به، في المجالات القضائية والإدارية (MONTERO, op.cit, pp. 81-83)، على مكاتب البريد التقليدية فقط متعللا في ذلك بضرورة المحافظة على النظام العام وبما تملكه هيئة البريد من خبرة في هذا المجال، هذا (العوضي، 75) ولم يكن بإمكان المشرع البلجيكي أن يبقى طويلا على موقفه غير المبرر هذا، فصدر قانون 2 أغسطس 2002م مقررا الاعتراف بالبريد الإلكتروني دون أي قيد أو شرط. وفى فرنسا اعترف المرسوم رقم 674 الصادر في 16 يونيه لسنة2005م بإمكانية استخدام وسيلة التراسل الإلكتروني في عمليات التعاقد (http: //www.journaldunet.com/juridique/juridique050621.shtml، ABDELLi).

وإزاء تحرير خدمة البريد الإلكتروني، على هذا النحو، وفتحها أمام أي جهة أو شخص من الغير يتوافر له مقومات القيام بتلك الخدمة من الناحية الفنية، فلم يبق سوى التساؤل عن قيمتها القانونية كبديل عن البريد التقليدي الموصى عليه، في الحالات التي يوجد فيها نص قانوني أو لائحي يستوجب الإرسال أو التبليغ في صورة خطاب مسجل مصحوب بعلم الوصول؟ ويتجه الرأي بشكل عام إلى صلاحية البريد الإلكتروني الموصى عليه للقيام بهذا الدور أيا كان موضوعه وأيا كان شخص القائم به، وذلك رغما عن أن القانون قد استعمل مصطلح خطاب موصى عليه في مكتب البريد. والقول بغير ذلك يكرس عملية احتكار البريد العادي لأداء مثل هذه الخدمات رغم التطور الحاصل في مجال تكنولوجيا الاتصال، والاعتراف بقيمته على أكثر من صعيد، وهو ما يضر، بالتالي، بقواعد المنافسة. ومع ذلك فإننا نتمنى أن نرى هذه الصلاحية محلا لنص صريح، في تشريعاتنا المحلية، يُعطى البريد الموصى عليه بالطريق الإلكتروني نفس قيمة البريد الموصى عليه بالطريق التقليدي قطعا لأي جدل أو غموض حول هذه المسألة (MONTERO, op.cit., p. 92). وهذا ما فعله المشرع المصري في قانون الضرائب رقم 91 لسنة 2005م، فهذا التشريع على الرغم من أنه أغفل النص على كيفية سداد الضرائب على المعاملات التجارية الإلكترونية، إلا أنه تناول الحجية القانونية للإعلان الضريبي عن طريق الانترنت، حيث نص في المادة 116 من الباب السادس على أنه " يكون للإعلان المرسل بكتاب موصى عليه مصحوبا بعلم الوصول، أو بأي وسيلة إلكترونية لها الحجية في الإثبات، وفقا لقانون التوقيع الإلكتروني الصادر بالقانون رقم 15 لسنة 2004م يصدر بتحديدها قرار من الوزير، ذات الأثر المترتب على الاعلان الذي يتم بالطرق القانونية ".

حجية الرسالة الإلكترونية في الإثبات:

فَرَّقَ التقنين المدني الفرنسي في الفقرتين السابعة والثامنة من المادة 1369، المضافة إلى القانون المدني الفرنسي، بين الرسالة الإلكترونية البسيطة والرسالة الإلكترونية الموصى عليها. ففيما يتعلق بحجية الرسالة الإلكترونية البسيطة، أقرت الفقرة السابعة من المادة المذكورة بإمكانية استخدامها، طبقا لمبدأ سلطان الإرادة، في إبرام وتنفيذ العقود، وتعتبر حجة على ما ورد فيها مالم ينكرها أو ينكر تاريخها من تنسب إليه، شأنها في ذلك شأن الورقة العرفية في نظام الإثبات التقليدي، وبالمقابل فإن الفقرة الثامنة من نفس المادة اعترفت للرسالة الإلكترونية الموصى عليها بحجية كاملة في الإثبات، سواء بالنسبة لمضمونها أو لتاريخ إرسالها أو استقبالها، شريطة أن يكون الذي أشرف على إعدادها ونقلها شخص من الغير محل الثقة مستخدمًا في ذلك آلية توثيق يكون من شأنها:

(1) تحديد هوية الغير محل الثقة الذي أشرف على توصيل الرسالة. (2) تحديد هوية المرسل.

(3) تحديد هوية المستقبل. (4) تحديد ما إذا كان الرسالة قد سُلمت إلى المرسل إليه أم لا؟.

آلية التوثيق في مجال البريد الإلكتروني:

ونحن نري وجوب ارتكاز آلية التوثيق في مجال التوثيق الإلكتروني، على غرار آلية التوثيق في مجال التوقيع الإلكتروني، على أمرين أساسيين: الأول: وجود شخص من الغير محل ثقة يتوسط بين المرسل والمستقبل في توصيل الرسالة وتأمينها ضد الاختراق، وتحديد تاريخ الإرسال، والاستقبال، بالإضافة إلى هوية الطرفين المتراسلين. والثاني: النص على قرينة " موثوقية البريد الإلكتروني الموصى عليه " متى اتبعت في ممارسة الخدمة ضوابط واجراءات معينة وذلك على غرار القرينة المنصوص عليها في مجال خدمات التوقيع الإلكتروني، وهي القرينة المقررة بموجب نص الفقرة الثانية من المادة 4/1316 من القانون المدني الفرنسي المضافة بالقانون رقم 230-2000.

(1) وجود شخص من الغير محل ثقة:

لابد من وجود جهة أو شخص محل ثقة، يقوم بدور هيئة البريد التقليدية يتبع وسائل فنية على درجة عالية من الدقة في توصيل الرسالة من المرسل إلى المرسل إليه. ويتبع هذا الغير تقنية مشابهة لتلك التي يتبعها مقدمو خدمات توثيق المفاتيح المشفرة المستخدمة لأغراض التوقيع الإلكتروني (MONTERO, op.cit., p. 92) وعلى منوال هؤلاء فإنه من الواجب على مقدمي خدمات البريد الإلكتروني الموصى عليه أن يُقدموا ضمانات تتعلق بما يأتي: الاستقلال وسلامة الخدمة. إعلام صحيح ودقيق لمستعمل خدمة البريد الإلكتروني. استمرارية أداء هذه الخدمات. ضمان مالي. الكفاءة والخبرة للعاملين في مجال خدمة البريد الإلكتروني. ضوابط سلامة وموثوقية التقنيات المستعملة لاسيما في مجال تسليم شهادات التصديق وكذا علم الوصول. استعمال معايير معترف بها في مجال التوثيق. التسليم التلقائي لدليل إثبات واقعة الإرسال من قبل مصدر الرسالة، وكذا دليل إثبات تسلمها من قبل المستقبل عند الاقتضاء. استعمال آلية التوقيع الإلكتروني المعتمد.

(2) قرينة موثوقية خدمات البريد الإلكتروني:

أما فيما يتعلق بقرينة موثوقية خدمات البريد الإلكتروني فمؤداها أنه يفترض صحة واقعة الإرسال والاستقبال وتاريخ كل منهما متى كنا بصدد بريد إلكتروني معتمد. ويعتبر البريد الإلكتروني الموصى عليه بريد معتمد متى كان صادرًا عن مزود خدمة مستوفى للشروط والضمانات التي نص عليها القانون. وقوام هذه القرينة هو افتراض أن خدمة البريد الإلكتروني المعتمدة تؤدى ذات الوظائف المقررة للبريد التقليدي لاسيما إثبات واقعة الارسال، وتاريخها، وكذا تقديم ما يفيد تسلم المستقبل للرسالة (MONTERO, op.cit., p. 93). حقا يجوز لهذا الطرف أو ذاك مكنة إثبات عكس ما تقضى به هذه القرينة. ولكن هذا الإثبات سيكون عسيرا جدًا إذ سيكون صعبًا من الناحية العملية أن يقتنع القاضي بعكس هذه القرينة، وذلك بسبب الجودة العالية التي يبديها مقدم الخدمة في أدائه لخدماته. وبالمقابل فإذا قرر المستعمل المرور عبر مقدم خدمة غير خاضع لتطبيق النظام القانوني الخاص بمقدمي خدمات التوثيق، أي عبر مزود لبريد إلكتروني غير معتمد، فلا يُعمل بهذه القرينة، وإنما يقع على عاتق مقدم الخدمة عبء إثبات إقناع القاضي بأن الخدمة المقدمة تسمح بالثقة التامة في واقعة الإرسال، وتاريخه، وكذا واقعة وصول الرسالة إلى المرسل إليه. ولا شك في صعوبة هذا الإثبات لاسيما إذا لم يكن مقدم خدمة البريد الإلكتروني الموصى عليه يتوافر لديه الحد الأدنى من الضمانات الفنية (كالتوقيع الإلكتروني المعتمد، وشهادة التصديق).

ونحن نري أن انتفاء هذه القرينة لا يعنى عدم إمكان مسئولية مقدم تلك الخدمة إذ يمكن أن تنعقد مسئوليته، في هذه الحالة، وفقا للقواعد العامة بما يعنيه ذلك من ضرورة إثبات عناصر المسئولية الثلاث من خطأ وضرر وعلاقة سببية، دون أن تنطبق عليه قرينة المسئولية، تلك القرينة التي لا تنطبق إلا على مقدم خدمة معتمد.

التوثيق في مجال خدمات الحفظ الإلكتروني

أهمية الحفظ الإلكتروني:

حفظ المستندات والمحررات، سواء أكانت تقليدية أو إلكترونية، لا يمكن أن يشكك في أهميتها أحد. فالمستند الكتابي لا ينشأ لكى يتم التخلص منه بعد ذلك مباشرة، وإنما تفرض المصلحة، وأحيانا القانون، الاحتفاظ به مدة زمنية قد تطول وقد تقصر حسب الأحوال (CAÏD ، pp. 111-135) فالاعتراف بحجية قانونية لمستند ما يفترض ثباته على حالته التي نشأ عليها طوال فترة بقاؤه (زهرة، 205)، فبقدر ثباته وعدم قابليته للتغيير أو التغير بمرور الزمان، بقدر ما تزداد الثقة فيه. وهوما يستتبع حفظه بطريقة لا تمكن من إدخال أي تعديل أو تغيير في مضمونه، أو في التوقيعات التي يحملها(Sèdallian, art Prèc) ، ويُجمع الفقه على أن حجية الدليل الإلكتروني، بل والكتابة الإلكترونية بشكل عام، أمر متوقف على حفظه في ظروف تؤدى إلى ضمان سلامته وعدم العبث به، ويضيفون بأن حفظ المستند الإلكتروني هو (C. HUC, http: //www.archivesdefrance.culture.gouv.fr) أمر لا محيص عنه للحديث عن أي حجية لهذا المستند، بل إن المشرع، في الكثير من التشريعات المقارنة، قد اقر بان حجية المستند الإلكتروني في الإثبات تتوقف إلى حد بعيد على التقنيات المستخدمة في حفظه. من ذلك ما نص عليه المشرع الفرنسي بشأن التوقيع الإلكتروني بقوله أن " الكتابة في الشكل الإلكتروني تُقبل في الإثبات شأنها في ذلك شأن الكتابة على دعامة ورقية طالما أنها تعبر تماما عن شخص من صدرت عنه من ناحية، وتنشأ وتحفظ في ظروف من شأنها ضمان سلامتها من ناحية ثانية ".

وهذا بالفعل ما قررته المادة (11) من قانون المعاملات الإلكترونية العُماني، إذ ربط المشرع بهذا النص ربطا صريحا بين حجية المستند الإلكتروني في الإثبات وبين التقنيات المتبعة في حفظه بحيث يمكن استرجاعه بحالته الأصلية، مستقبلا، عند الضرورة (أبو زيد، 157) لاسيما ضرورة الإثبات أمام القضاء. فمسألة حفظ المحرر ترتبط، اذن، ارتباطا لا يقبل الانفصال بمسألة الإثبات وبالحاجات العملية. فحجية المحرر الإلكتروني في الإثبات تستلزم حفظه في ظروف تكفل سلامته طوال الفترة اللازمة للتمسك به كدليل أمام القضاء. ويختلف أسلوب حفظ المستند الإلكتروني، بطبيعة الحال، عن أسلوب حفظ المستند الورقي. ولعل أول تحدى، في هذا الخصوص، يتمثل في مدى بقاء وثبات ووضوح المستند والبيانات والمعطيات الرقمية الواردة فيه، وقابليتها للقراءة دون أي تأثير لمرور الزمن. وبقاء المستند الإلكتروني كما هو دون تغيير يمكن مواجهته من زاويتين:

الأولى: بجعله عصيا على ادخال أي تعديلات عليه، ويتحقق ذلك متى تمكنا من تثبيت مضمون هذا المستند نهائيا بطريقة لا يمكن معها تعديله أو تشويهه. ويمكن تثبيت المستند الإلكتروني على هذا النحو إما عن طريق التعامل مع الوسيط الذي يُحفظ عليه، وأما عن طريق الرجوع إلى بعض التقنيات المعلوماتية، لاسيما آلية التوقيع الإلكتروني، أو التشفير.

الثانية: للمحافظة على سلامة المستند أن نجعله قابلا لإدخال تعديلات عليه، وذلك متى ضمنا أن أي تعديل لاحق يمكن كشفه وتحديد تاريخه. وهذا امر يمكن الوصول إليه من الناحية الفنية اما عن طريق البرنامج المناسب في هذا الخصوص، أو عن طريق الاستفادة من خدمات الغير محل الثقة، ومصدر هذه المشكلة يكمن، حقيقة، في أن المستند الرقمي، على خلاف المستند الورقي، لا يمكن، فنيا، قراءته مباشرة من قبل الانسان، بل لا بد من الاستعانة بوسائل وأدوات تقنية في حالة تطور وتغير مستمر، فقابلية المستند الرقمي للاسترجاع هى مسألة مهددة بالزوال مع مرور الوقت، وذلك بسبب الخلل الذي يمكن أن يصيب الآلة أو البرامج المشغلة لها أو بسبب اختراق مفاتيح التشفير المحفوظة مع الكتابة الإلكترونية، فمن المتوقع أن تصبح التقنية المستعملة وقت اعداد

مفاتيح التوقيع الإلكتروني تقنية بالية جدا ومن السهل اختراقها بعد خمس أو عشر سنوات، كأن يصبح من الميسور مثلا معرفة المفتاح الخاص عن طريق المفتاح العام، حيث يهوى قراصنة الحاسب الآلي تنفيذ هذا الاختراق (أبو زيد، 164). وفى الحقيقة فإن قيمة المعلومة المخزنة رقميا تُقاس بمدى قدرة الإنسان على استرجاعها في صورة مقروءة مفهومة دون تأثير لمرور الزمان. فالمستند الرقمي لا قيمة له إذا لم يوجد برنامج يمّكن من قراءة الوسيط الذي يحمله. ويكمن التحدي الثاني لعمليات الحفظ الإلكتروني في أن المشكلة لا تنتهي بحفظ المستند الإلكتروني ذاته، وإنما لابد من حفظ مجموعة من البيانات اللازمة للتحقق من صحة توقيع هذا المستند واستدعائه عند الضرورة. وتتمثل هذه المجموعة من البيانات في المفاتيح والشهادات الرقمية التي تستخدم في توقيع المستند الإلكتروني أو تشفيره أو حفظه. فالحفظ لا يقتصر على المستند الإلكتروني ذاته، وإنما يشمل أيضا توابعه وملحقاته وإذا لم تكن مفاتيح التشفير (العامة والخاصة) والشهادات الرقمية وأدوات إنشاء التوقيع والتحقق من سلامته محفوظة بشكل جيد، فسيستحيل، مع مرور الوقت، التحقق من هوية الموقعين على المستند أو التأكد من سلامة مضمونه، بل وسيكون مستحيلا الدخول إليه واسترجاعه إذا كان التشفير قد تم لأغراض السرية، وهوما يُفقد المستند أي قيمة قانونية له.

آلية الحفظ الإلكتروني:

ومن هنا يأتي الدور الهام الذي يمكن أن يلعبه شخص أو جهة محايدة تتوافر لها إمكانات فنية عالية تتخصص في عمليات الحفظ الإلكتروني سواء على سبيل الانفراد، أو بمناسبة قيامها بخدمات التوثيق في مجال التوقيع الإلكتروني، أو البريد الموصى عليه. فمهمة الغير محل الثقة تتمثل، إذن، في حفظ المستند الإلكتروني في ظروف وبطريقة آمنة تضمن صحته وسلامة مضمونه، وكذا ضمان بقائه في حالة مقروءة خلال عدد معين من السنوات، تختلف، بطبيعة، الحال باختلاف الغرض من المستند المطلوب وتقدم وسائل الحفظ، ونصوص القانون التي تحدد مدد معينة يجب أن يبقى فيها المستند محفوظًا. ونلاحظ بداية عدم انطباق القانون الخاص بمقدمي خدمات التوثيق في مجال التوقيع الإلكتروني، سواء في دول أوروبا أو منطقتنا العربية، على مقدمي خدمات الحفظ إلا عندما تؤدَى هذه الخدمات الأخيرة بمناسبة القيام بالأولى. والقول بغير ذلك معناه إفتئات على إرادة المشرع الذي لم تتجه إرادته إلا إلى عمليات التوثيق في مجال التوقيع الإلكتروني. أما في خارج هذه الحالة فإننا نسجل فراغا تشريعيا يجب العمل على سده في أسرع وقت ممكن وحتى في الحالة المشار إليها فإن نصوص القانون الخاص بالتوقيع الإلكتروني يعتريها الكثير من الشك والغموض عند محاولة تطبيقها على عمليات الحفظ الإلكتروني. ولذا فلا مناص من الإسراع في إصدار قانون خاص بعمليات الحفظ الإلكتروني، ومع ذلك فيمكن، كنقطة بداية، وإلى أن يصدر تشريع شامل في هذا الخصوص، أن نستوحى عدد معين من الضوابط من بين تلك المنصوص عليها في التشريع الخاص بمقدمي خدمات توثيق التوقيع الإلكتروني، ومحاولة تطبيقها، مع بعض المواءمات البسيطة، على أنشطة الغير القائم بعملية الحفظ.

ويمكن تلخيص هذه الضمانات فيما يلي:

1- استعمال أنظمة وبرامج وأدوات موثوق بها.
2- يلتزم الغير مقدم خدمة الحفظ كذلك، باعتباره ملتزما بالسر المهني، بضمان سرية المعلومات التي وقف عليها وعدم نقلها إلا إلى الأشخاص المرخص لهم صراحة بمعرفتها.

3- يلتزم مقدم خدمة الحفظ كذلك ليس فقط باتخاذ الاجراءات اللازمة لمنع أي تزوير أو تزييف أو تغيير في المستند المحفوظ، وإنما كذلك باستعمال أنظمة موثوق منها بحيث يكون المستند المحفوظ وفقا لها إلكترونيا تحت الرقابة الكاملة سواء من حيث أصالته أو فيما يتعلق بمضمونه.

4- يجدر بمقدم خدمة الحفظ كذلك أن يزود أي نظام يستخدمه في الحفظ ببرنامج لاستعادة المعلومات على المواقع المختلفة حتى يمكنه أن يكون جاهزًا لاسترجاع أي حذف أو اختفاء للمستندات المحفوظة.

5- ويجب فوق ذلك أن تتوافر لمقدمي خدمة الحفظ موارد مالية كافية لممارسة أنشطته، وضمان دوامها واستمرارها.

6- يجب على مقدم خدمة الحفظ كذلك أن يقدم ضمانات تتصل باستمرارية أنشطته.

7- الإعلام الدقيق لمستعملي خدمات الحفظ الإلكتروني.

8- وأخيرًا، تقديم الغير مقدم الخدمة ضمانات تفيد استقلاله عن مستعملي هذه الخدمة سواء من الناحية المالية أو من الناحية القانونية.

خلاصة النتائج:

1. خدمات التوثيق الإلكتروني، هي الوسيلة القانونية المتاحة لبعث الثقة وتأمين التعامل عبر وسائل الاتصال الحديثة لا سيما الإنترنت.
2. كشفت الدراسة كذلك عن أن المجال الأساسي لخدمات التوثيق هو مجال التوقيع الإلكتروني.
3. معظم الدول العربية قد حاكت الدول الأوروبية في إصدار تشريعات لتنظيم خدمات التوثيق في المجال الإلكتروني، إلا أن الواقع قد كشف عن عدم توافر إمكانات ممارسة هذا النشاط في الدول العربية على غرار ما هو متاح في الدول الأوروبية، سواء في ذلك الإمكانات المادية أو الفنية أو الكوادر البشرية.
4. الأهمية الكبرى للتوثيق الإلكتروني، كونه يربط ما بين شخص المتعاقد وبيانات الرسالة الإلكترونية، وبالنتيجة التأكيد على أن التوقيع الإلكتروني الوارد على الرسالة يعود للموقّع نفسه دون غيره.

التوصيات والمقترحات.

1. نوصي بإصدار تشريع شامل ينظم الدور الذي يقوم به الغير محل الثقة في مجالات، التوقيع الإلكتروني والبريد الموصى عليه وكذا خدمات الحفظ الإلكتروني.
2. نوصي كذلك بضرورة تهيئة البيئة العربية لاستقبال هذا الوافد الجديد والتعامل معه، بجانب التثقيف العام بأهمية هذه التقنيات في تطوير التجارة الإلكترونية وبالتالي في تنمية الاقتصاد الوطني.
3. نوصي بإنشاء صندوق قومي لتعويض الأضرار التي تنتج عن الخطأ في عمليات التوثيق تساهم الدولة بنسبة في تمويله بجانب نسبة أخرى تخصم من المقابل التي تحصله جهات التوثيق من المتعاملين.

هذا البحث تم دعمه من خلال البرنامج البحثي العام بعمادة البحث العلمي
جامعة الملك خالد – المملكة العربية السعودية (بالرقم G.R.P-116-1441)

قائمة المراجع

أولا- المراجع بالعربية:

- إبراهيم، خالد ممدوح (2006): إبرام العقد الإلكتروني دراسة مقارنة، ط1، دار الفكر الجامعي، القاهرة، مصر.

- أبو الليل، إبراهيم الدسوقي (2003): الجوانب القانونية للتعاملات الإلكترونية، دراسة للجوانب القانونية للتعامل عبر أجهزة الاتصال الحديثة " التراسل الإلكتروني "، مطبوعات مجلس النشر العلمي، جامعة الكويت.
- أبو زيد، محمد محمد (2002): تحديث قانون الإثبات، مكانة المحررات الإلكترونية بين الأدلة الكتابية، (د.ت).
- الدكاني، إبراهيم، وأحمد، حسام الدين (2005): المدخل إلى العلوم الهندسية، (د.ت).
- رشدي، أحمد (2006): التجارة الإلكترونية، مكتبة الأسرة، القاهرة، مصر.
- زهرة، محمد المرسي. (2008): الحاسب الإلكتروني والقانون، دراسة حول حجية مخرجات الحاسب الإلكتروني في الإثبات في المسائل المدنية والتجارية، دراسة مقارنة، دار النهضة العربية- القاهرة، مصر.
- شمس الدين، أشرف توفيق: الحماية الجنائية للمستند الإلكتروني، بحث مقدم بمؤتمر "الأعمال المصرفية الإلكترونية بين الشريعة والقانون" المنعقد بدولة الإمارات العربية المتحدة، غرفة تجارة وصناعة دبي، في الفترة من 10-12 مايو 2003، الجزء الثاني.
- عبيدات، لورانس محمد (2005): إثبات المحرر الإلكتروني، ط مكتبة دار الثقافة للنشر والتوزيع، عمان، الأردن.
- العوضي، فوزي عبد الهادي (2005): الجوانب القانونية للبريد الإلكتروني، دار النهضة العربية، القاهرة، مصر.
- عيسى، طوني ميشال (2000): التنظيم القانوني لشبكة الانترنت، دراسة مقارنة في ضوء القوانين الوضعية والاتفاقيات الدولية، رسالة دكتوراه، كلية الحقوق والعلوم السياسية والإدارية، الجامعة اللبنانية، الفرع الثاني.
- فايد، عابد (د.ت): الكتابة الإلكترونية، دار النهضة العربية.
- المطالقة، محمد فواز: النظام القانوني للعقود الإلكترونية المبرمة عبر الإنترنت، دراسة مقارنة، رسالة دكتوراه، مقدمة لمعهد البحوث والدراسات العربية، القاهرة، 2004م.
- وتوثيق التعاملات الإلكترونية ومسئولية جهة التوثيق تجاه الغير المتضرر، بحث منشور في مؤتمر " الأعمال المصرفية الإلكترونية بين الشريعة والقانون" المنعقد في الفترة من 9-11 ربيع الأول 1424هـ الموافق 10 - 12 مايو 2003م. الجزء الخامس.

ثانياً- المراجع بالفرنسية:

- ABDELLi, M, (2005), Courrier électronique et contrats en ligne Depuis le 16 juin 2005, une ordonnance précise les conditions d'usage du courrier électronique en matière de formalités contractuelles. Le point sur les implications de ce texte en matière de preuve, http: //www.journaldunet.com/juridique/juridique050621.shtml
- Barbry, E, Bensoussan،A. (2000),Le Contrat de certification de sites internet, http: //www.journaldunet.com/juridique/juridique18certification.shtml
- Bitan, H, (2000), La signature électronique, Comment la technique répond-t-elle aux exigence de la loi? Gaz. Pal. 19-20 Juillet.
- C. HUC, « La pérennité des documents électroniques – Points de vue alarmistes ou réalistes ? », Bulletin des Archives de France sur l'archivage à long terme des documents électroniques, n°7, oct. 2001, disponible à l'adresse http: //www.archivesdefrance.culture.gouv.fr.

http: // www.droit.fundp.ac.be/e-justice /documents.htm)

- CAÏD, S, (2002), La preuve et la conservation de l'écrit dans la société de l'information, Mémoire présenté à la Faculté des études supérieures en vue de l'obtention du grade Maîtrise en droit (L.L.M.)
- GOBERT, D , (2002), Cadre juridique pour les signatures électroniques et les services de certification: analyse de la loi du 9 juillet 2001 , Publié in La prévue, Formation permanenté CUP, Volume 54, mars.
- GOBERT, D, (2004),Commerce électronique: vers un cadre juridique général pour les tiers de confiance publié in Revue du Droits des Technologies de l'Information , n° 18, avril 2004, pp. 33-56 www.droit-technolgie.org/dossiers/goberttiersconfiancedossier.pdf
- MONTERO, E, (2003) Du recommandé traditionnel au recommandé électronique: vers une sécurité et une force probante renforcées, in Commerce électronique: de la théorie à la pratique, Cahiers du CRID, n° 23 ،Bruxelles, Brulant.
- PENNEAU, A, (2002), La certification des produits et systèmes permettant la réalisation des actes et signatures électroniques (à propos du décret N° 2002-535 du 18 avril 2002) Rec. Dalloz
- ROJINSKY, C, T EISSONNIERE, G, (2005), L'encadrement du commerce électronique par la loi française du 21 juin 2004 » pour laconfiance dans l'économie numérique« http: // www.lex-electronica.org/articles/v10-1/rojinsky_teissonniere.htm
- Sèdallian, V, (2000),Preuve et signature électroniqu disponebl sur le site www.juriscom.net/chr/2/fr20000 509.htm