تصديق التوقيع الالكتروني لجهة التوثيق الالكتروني

الدكتورة هلا الحسن

قسم القانون الخاص

كلية الحقوق

جامعة دمشق

الملخص

هَدَفَ هذا البحث إلى بيان مفهوم التوقيع الالكتروني الخاص بجهة التصديق الالكتروني وأهميته وطرائق التحقق من عائديته لجهة التصديق، كما يظهر الخطر الناجم عن ذلك التوقيع وسبل الوقاية منه، وتعتمد هذه الدراسة على توضيح أهم الطرائق المتبعة في التحقق من التوقيع الالكتروني مع بيان الطريقة الفُضلى التي ننصح باعتمادها لدى جهات التصديق الالكتروني في سورية، وضرورة اتخاذ الإجراءات اللازمة لتطبيقها بأسرع وقتٍ ممكنٍ، وذلك عبر إزالة العقبات التي تمنع تنفيذها، مع أهمية إصدار تشريعات مناسبة لتجاوز الخطر الذي يثيره ذلك التوقيع .

المقدمة:

يؤدي التوقيع الالكتروني الخاص بجهة التصديق الالكتروني دوراً مهماً جداً في مجال التعاقد الالكتروني من ناحية تأكيد بيانات الموقعين المسجلين لديها، وتعدُّ تلك الجهة طرفاً وسيطاً في التعاقد الالكتروني بين المتعاقدين سواء كانت جهة عامة أم خاصة، بحيث تتولى مهمة تأكيد بيانات الموقعين وخاصة فيما يتعلق بتواقيعهم الالكترونية ونسبتها إليهم، وذلك عبر إصدارها شهادة التصديق الالكترونية المدرجة فيها تلك البيانات كلّها الممهورة بتوقيعها الالكتروني[1]، وتختلف الطرائق المتبعة من قبل المتعاقدين في التأكد من صحة التوقيع الالكتروني ونسبته فعلاً إلى جهة التصديق الالكتروني، إلا أنها تثير بعض المشكلات والصعوبات، مما يدفعنا لدراسة أفضل طريقة من وجهة نظرنا في التحقق من صحة ذلك التوقيع، وكذلك قد يتعرض التوقيع الالكتروني لجهة التصديق الالكتروني لمشكلة خطيرة تتجلى في الاستيلاء عليه من قبل المتطفلين وما ينجم عن ذلك من أخطار كثيرة، وتتجلى أهمية بحثنا في أنه يبيّن قصور قانون التوقيع الالكتروني السوري عن معالجة كيفية التحقق من نسبة التوقيع لالكتروني لجهة التصديق الالكتروني، لذا عمدنا إلى تقسيم البحث إلى قسمين، أُفْرِدَ الأول منهما لبيان مفهوم التوقيع الالكتروني الخاص بجهة التصديق الالكتروني والخطر الناجم عن هذا التوقيع وطرائق الوقاية منه، أمَّا القسم الثاني فخُصِّصَ لتوضيح وسائل التحقق من صحة التوقيع الالكتروني الخاص بجهة التصديق الالكتروني ومدى فائدة استخدامها في الجمهورية العربية السورية، وذلك وفق المنهج الآتي:

المبحث الأول: التوقيع الالكتروني الخاص بجهة التصديق الالكتروني:

المطلب الأول: مفهوم التوقيع الالكتروني الخاص بجهة التصديق الالكتروني، وأهميته:

الفرع الأول: ماهية التوقيع الالكتروني العائد لجهة التوثيق الالكتروني .

الفرع الثاني: أهمية التوقيع الالكتروني الخاص بجهة التوثيق الالكتروني .

المطلب الثاني: المخاطر التي يثيرها التوقيع الالكتروني الخاص بجهة التصديق الالكتروني والوقاية منها:

الفرع الأول: خطر الاستيلاء على التوقيع الالكتروني العائد لجهة التصديق الالكتروني .

الفرع الثاني: طرائق الوقاية من مخاطر الاستيلاء على التوقيع الالكتروني العائد لجهة التصديق.

المبحث الثاني: التحقق من صحة التوقيع الالكتروني لجهة التصديق الالكتروني:

المطلب الأول: طرائق التأكد من عائدية التوقيع الالكتروني لجهة التصديق الالكتروني:

الفرع الأول: إنشاء عدة مراتب لجهات التصديق الالكتروني

الفرع الثاني: إنشاء مكتب حكومي للتصديق الالكتروني

المطلب الثاني:تصديق التوقيع الالكتروني لجهة التوثيق الالكتروني في سورية وعقبات تطبيقه:

الفرع الأول: الآلية الواجب تطبيقها للتأكد من صحة التوقيع الالكتروني لجهة التصديق .

الفرع الثاني: معوّقات تطبيق الطريقة المقترحة وسبل إزالتها .

---

1 ــ راجع في ذلــك: Froomkin Michael ,The Essential Role of Trusted Third Parties in Electronic Commerce , 75 Oregon Law Review , 1996 , p5 .

المبحث الأول

التوقيع الالكتروني الخاص بجهة التصديق الالكتروني

بدايةً لابدَّ من تعرّف مفهوم التوقيع الالكتروني بشكل عام، ومن ثم تطبيقه على جهة التصديق الالكتروني، كما ينبغي إيضاح الدور المهم الذي يؤديه ذلك التوقيع الخاص بتلك الجهة، وما الخطر الذي يثيره وكيف يُحَلُّ، وعليه بيّنا ذلك في المطلبين الآتيين:

المطلب الأول: مفهوم التوقيع الالكتروني الخاص بجهة التصديق الالكتروني وأهميته
المطلب الثاني: المخاطر الذي يثيرها التوقيع الالكتروني الخاص بجهة التصديق الالكتروني والوقاية منها .

المطلب الأول

مفهوم التوقيع الالكتروني الخاص بجهة التصديق الالكتروني وأهميته

يبرز دور التوقيع الالكتروني بشكل خاص في التعاملات التجارية لميزاته الكثيرة،مما يدفعنا لبيان المفهوم العام للتوقيع الالكتروني، ومن ثم تطبيق ذلك المفهوم على التوقيع الخاص بجهة التصديق الالكتروني، كما لابدّ من إظهار الفائدة العملية من اعتماد جهة التصديق الالكتروني على توقيع الكتروني خاص بها، وذلك وفق التقسيم الآتي:

الفرع الأول

ماهية التوقيع الالكتروني العائد لجهة التوثيق الالكتروني

يعرّف التوقيع الالكتروني بأنه: "مجموعة من الإجراءات التقنية التي تمكن من تحديد شخصية من تصدر عنه هذه الإجراءات وقبوله بمضمون التصرف الذي يصدر التوقيع بشأنه"[(2)]، ويبدو واضحاً من هذا التعريف أن التوقيع الالكتروني عبارة عن إجراءات تقنية تختلف عن الإجراءات التقليدية المتبعة في التوقيع الخطي[(3)]، ومن ثمَّ لم يحدد التعريف شكلاً معيناً لهذا التوقيع، استناداً إلى أن للتوقيع الالكتروني صوراً متعددة، ولكن المهم أن تحقق تلك الصور وظائف التوقيع في تحديد

2 ــ لورنس محمد عبيدات، إثبات المحرر الالكتروني، دار الثقافة للنشر والتوزيع، عمان، 2005، ص 126 .

3 ــ راجع في ذلــك: Allen Tom , Can Computers Make Contracts?, Harvard Journal of Law and Technology , U.S.A ,vol 9 , No 1 ,1996, p25 .

شخصية الموقع وتأكيد قبوله بمضمون التصرف القانوني الذي وقّع عليه، كما أن هذا التعريف وغيره من التعريفات القانونية يشمل التوقيع الالكتروني العائد للموقع سواء كان فرداً أم جهة عامة أم خاصة، ومنها جهة التصديق الالكتروني[4] التي تعدُّ طرفاً ثالثاً محايداً وموثوقاً به تقوم بدور الوسيط بين أشخاص يتعاملون عن بعد ولا يعرفون بعضهم بعضاً[5]، وهذا الوسيط يؤمن أعلى درجات الضمان من ناحية تحديد هوية المتعاملين، كما أنَّه يمارس دوراً مهماً في تأكيد صدور التوقيع الالكتروني من قبل صاحبه وعدم حدوث أي تبديل أو تعديل على ذلك التوقيع أو على المحرر الالكتروني الموقع عليه الكترونياً[6]، أي تتولى جهة التصديق توثيق التوقيع الالكتروني الخاص بالموقع، وذلك عبر إصدارها شهادة التصديق الالكتروني التي تحقق الثقة لدى الغير بصحة البيانات التي تحتويها وخاصة ما يتعلق بهوية الموقع ونسبة التوقيع الالكتروني إليه، مما يدفع المطلع عليها إلى التعاقد بثقةٍ واطمئنان مع ذلك الموقع [7]، ومن ثمَّ يستطيع المتعاقد التأكد من هوية الموقع عبر اللجوء إلى تلك الجهة التي تؤكد نسبة التوقيع بالفعل إلى الموقع المسجل لديها وذلك بإصدارها شهادة التوثيق الالكتروني[8].

إذْ إنَّ التوقيع الرقمي يعدّ من أكثر أنواع التوقيع الالكتروني انتشاراً، إذْ يستخدم الموقع مفتاحاً خاصاً به لتشفير الرسالة لتصبح في صورة مختزلة وغير مفهومة، فينتج عن ذلك التوقيع الرقمي للمرسل، وبعدها يرسل المرسل الرسالة إلى المرسل إليه الذي يقوم بفك شفرة الرسالة الالكترونية

---

4 ــ عملت القوانين الناظمة للتوقيع الالكتروني على تعريف ذلك التوقيع، ومنها القانون السوري الخاص بالتوقيع الالكتروني الصادر عام 2009 الذي عرفت مادته الأولى التوقيع الالكتروني بأنه:"جملة بيانات تدرج بوسيلة الكترونية على وثيقة الكترونية وترتبط بها، وتتخذ شكل حروف أو أرقام أو رموز أو إشارات أو أي شكل آخر مشابه، ويكون لها طابع متفرد يسمح بتحديد شخص الموقع ويميزه عن غيره وينسب إليه وثيقة الكترونية بعينها".

5 - خالد ممدوح إبراهيم، التوقيع الالكتروني، بحث منشور على الموقع الآتي:

www.kenanaonline.com/users/khaledMamdouh/posts/77870 آخر زيارة 10 -5 - 2013 .

6 ــ محمد سعيد أحمد إسماعيل،أساليب الحماية القانونية لمعاملات التجارة الالكترونية، منشورات الحلبي الحقوقية، بيروت، 2009، ص 275

7 ــ فاروق محمد الأباصيري، عقد الاشتراك في قواعد المعلومات عبر شبكة الإنترنت، دار الجامعة الجديدة للنشر، مصر، 2002، ص 84 .

8 ــ لمزيد من المعلومات عن دور جهة التصديق الالكتروني راجع:إيمان مأمون أحمد سليمان،إبرام العقد الالكتروني وإثباته، دار الجامعة الجديدة للنشر، الإسكندرية،2008، ص 314 .

في صورتها المختزلة (التوقيع الرقمي الملحق بالرسالة) عبر استخدام المفتاح العام للمرسل الذي تتولى جهة التصديق مهمة تسليمه من المرسل إلى المرسل إليه [9]، أي تقوم جهة التصديق بمنح المفتاح الخاص والعام للموقع، بحيث يلجأ المتعاقد الذي يريد القيام بعملية التوقيع الرقمي إلى جهة التصديق التي تمنحه مفتاحين مترابطين ببعضهما بعضاً بحيث يستخدم الموقع المفتاح الخاص في تشفير المعاملة الالكترونية التي يرغب بإرسالها، في حين يستخدم المرسل إليه المفتاح العام المذكور في شهادة التصديق الالكتروني الصادرة عن جهة التصديق في فك شفرة المعاملة الالكترونية المرسلة إليه[10]، ومن ثمَّ تتولى تلك الجهة إصدار شهادات تثبت ملكية شخص لتوقيعه الالكتروني[11] التي تؤكد صدور التوقيع ممن نسب إليه، كما أنها تبيّن أن المعلومات الموقّع عليها هي معلوماتٌ وبياناتٌ صحيحةٌ صادرة عن الموقع ولم يُتَلاعَبْ فيها، وذلك عبر استخدام المفتاح العام الذي يذكر في الشهادة، أي إنَّها تؤكد نسبة المفتاح العام المستخدم إلى صاحبه الفعلي[12] .

هذا، ويجب أن تكون شهادة التصديق الالكتروني موقعة الكترونياً من قبل جهة التصديق الالكتروني[13]، بحيث تستخدم تلك الجهة مفتاحها الخاص في توقيع الشهادة، ولاشك أن الغير سيتأكد من صحة ذلك التوقيع باستخدام المفتاح العام لجهة التصديق الذي يتوافق مع مفتاحها الخاص، ويدفعنا ذلك للتساؤل عن أهمية توقيع جهة التصديق الالكتروني للشهادات الصادرة عنها والدور الذي يؤديه وما يترتب على غيابه من أثر .

---

9 ــ يتم أولاً في التوقيع الرقمي إنشاء بصمة الكترونية للرسالة ثم تشفر تلك البصمة باستخدام المفتاح الخاص للموقع فينتج عن ذلك التوقيع الرقمي يلحق بالوثيقة المرسلة،وللتأكد من صحة التوقيع يقوم مستقبل الرسالة بفك شيفرة التوقيع مستخدماً المفتاح العام _ لمزيد من المعلومات عن آلية التوقيع الرقمي راجع: أمجد دخل الله،العقود الالكترونية، مجلة المحامون، العددان 9

ــ10 عام 2004، ص 841 وكذلك وسام أبو عمره، البصمة الالكترونية والتوقيع الرقمي منشور على الموقع الآتي (www.al3ez.net/vb/showthread.php?2770-%...) آخر زيارة في 5 /6/ 2012وكذلك راجع: بروس شناير،التعمية التطبيقية،منشورات الجمعية المعلوماتية السورية،2006،ص 4 -5 .

10- سامح عبد الواحد التهامى، التعاقد عبر الإنترنت (دراسة مقارنة)، دار الكتب القانونية، مصر،2008 ، ص 414 .

11 ــ ياسر إمام الغندور، حجية التوقيع في المعاملات التجارية الالكترونية، منشور على الموقع الالكتروني: www.okaz.com.sa/okaz/osf/20060801/Con20060801136011.htm آخر زيارة 5 /2012/6 .

12 ــ راجع:عمرو عيسى الفقي، وسائل الاتصال الحديثة وحجيتها في الإثبات،المكتبة القانونية،مصر ،2006،ص 46 ــ 47.

13 ــ إيمان مأمون أحمد سليمان، المرجع السابق، ص 323 .

الفرع الثاني

أهمية التوقيع الالكتروني الخاص بجهة التصديق الالكتروني

تصدر جهة التصديق الالكتروني شهادة التصديق التي تحتوي المعلومات الضرورية عن الموقع ومنها المفتاح العام العائد له، ولكن كيف السبيل إلى التأكد من أنَّ هذه الشهادة بما تتضمنه من بيانات هي صادرة بالفعل عن تلك الجهة ؟

في الحقيقة يتمُّ التأكد من صحة الشهادة فيما يتعلق بكل من محتواها ومصدرها عبر توقيع جهة التصديق الالكتروني عليها[14]، ومن ثمَّ يعدُّ توقيعها على الشهادة الصادرة عنها مسألة" حاسمة" في تأكد الشخص الذي يعتمد على تلك الشهادة أهي صادرة بالفعل عن جهة التصديق الالكتروني أم لا؟.

إذاً ، يؤدي التوقيع الرقمي الخاص بجهة التوثيق الالكتروني دوراً مهماً في تأكيد صحة الشهادة بكل ما تحتويه من بيانات وخاصة تأكيد هوية الموقعين ونسبة التواقيع الالكترونية إليهم، ومن دون توقيع جهة التصديق على شهاداتها لا يمكن للغير التأكد من نسبة المفتاح العام للموقع الذي يتعاقد معه، أي يعزز توقيع الجهة الوسيطة على الشهادات الصادرة عنها الثقة لدى الغير في سلامة المعلومات المذكورة فيها، مما يؤدي إلى مصداقية الشهادات لدى العامة .

لذا، يعدُّ توقيع جهة التصديق الالكتروني على شهاداتها من البيانات الإلزامية التي يجب أن تشتملها تلك الشهادات، إذْ يجب أن تذيل بالتوقيع الالكتروني الخاص بتلك الجهة، ولا يجوز أن يتخلف ذلك التوقيع لأنه من البيانات الإلزامية التي لا غنى عنها في شهادات التصديق جميعها لكي تتمتع بالقيمة القانونية الكاملة في الإثبات [15] .

المطلب الثاني

المخاطر التي يثيرها التوقيع الالكتروني الخاص بجهة التصديق الالكتروني والوقاية منها

رغم الدور المهم الذي يؤديه التوقيع الالكتروني الخاص بجهة التصديق الالكتروني، إلا أنه يثير مشكلة خطيرة جداً قد تهز الثقة في ذلك التوقيع وفاعليته؛ ممَّا يستدعي وضع عدة إجراءات وقائية

14 ــ محمد خالد جمال رستم، التنظيم القانوني للتجارة والإثبات الالكتروني في العالم، منشورات الحلبي الحقوقية، بيروت، 2006، ص 46 .

15 ــ راجع في ذلك: إيمان مأمون أحمد سليمان، المرجع السابق، ص 322 ــ 323

بهدف إزالة تلك المشكلة والقضاء عليها. لذا بيَّنا المخاطر التي تنجم عن ذلك التوقيع وآلية حلها، وذلك وفق التقسيم الآتي:

الفرع الأول

خطر الاستيلاء على التوقيع الالكتروني العائد لجهة التصديق الالكتروني

يتعرض التوقيع الالكتروني لجهة التصديق لمشكلة خطيرة تتجلى في احتمال سيطرة القراصنة عليه، ويمكن أن نعرّف القراصنة بأنهم أشخاص ينصب جلّ اهتمامهم على التوصل إلى المعلومات كلّها في حواسب الآخرين بصورةٍ غير مشروعة[16]، إذْ قد يستولون على النظام المعلوماتي الخاص بجهة التصديق عبر دخولهم غير المشروع إليه؛ مما يترتب عليه السيطرة على التوقيع الالكتروني الخاص بها[17]، وذلك بغرض الفضول أو الحقد والانتقام من جهة التصديق أو بقصد بيع توقيعها الالكتروني أو استغلاله لتحقيق مآرب خاصة بالقرصان[18]، ومن ثمَّ يقوم القرصان باختراق مفاتيح التشفير المتعلقة بالتوقيع الالكتروني العائد لجهة التصديق وفكها، مما ينجم عنه كشف البرامج الخاصة بتشفير التوقيع الالكتروني،أي كشف آلية تحويله من صورةٍ مكتوبةٍ إلى صورةٍ رقميةٍ ليكون مجرد إشارة أو رمزاً، فبمجرد اختراق مفاتيح التشفير المتعلقة بالتوقيع الالكتروني الخاص بجهة التصديق الالكتروني وفكها، فإن القرصان يكون قد استولى على نظام التوقيع الالكتروني الخاص بتلك الجهة[19] .

هذا، وبمجرد أن تتمَّ سيطرة القراصنة على النظام المعلوماتي لجهة التصديق فإنهم يقومون مباشرةً بإصدار شهادات تصديق الكتروني خاطئة تخدم مصالحهم،وذلك عبر استخدام المفتاح الخاص لجهة التصديق في إصدار العديد من شهادات التصديق الخاطئة والممهورة بتوقيع جهة التصديق، إذْ يتم فوراً وبسرعةٍ كبيرةٍ إصدار شهادات توثيقٍ خاطئةٍ دون معرفة جهة التصديق بذلك،ولاشك أنَّ هذا الأمر يؤثر سلباً في سمعة جهة التصديق الالكتروني عند العامة، وسيكون أثره عظيماً،خاصةً عند إلغاء شهادات

16 ــ أ . أمجد دخل الله، القرصنة الالكترونية، مجلة المحامون ، سورية، العددان 3-4 ، 2007، ص 322 .

17 ــ سامح عبد الواحد التهامى، المرجع السابق، ص 451 .

18 ــ لمزيد من المعلومات عن أسباب القرصنة راجع: حسن مظفر الرزو، المفاهيم المعلوماتية لجرائم الفضاء الافتراضي بالحاسوب، مجلة الشريعة والقانون، جامعة الإمارات العربية المتحدة، العدد16 ،2002، ص 243 ــ244.

19 ــ عبد الفتاح بيومي حجازي، النظام القانوني للتوقيع الالكتروني (دراسة تأصيلية مقارنة)، دار الكتب القانونية، مصر، 2007، ص 500 .

التوثيق الخاطئة وإصدار شهادات توثيق صحيحة[20]، وماينجم عن ذلك من تعرض جهة التصديق الالكتروني لمسؤولية قانونية كبيرة تجاه عدد كبير من المتضررين من تلك الشهادات الخاطئة.

الفرع الثاني

طرائق الوقاية من مخاطر الاستيلاء على التوقيع الالكتروني العائد لجهة التصديق

إن الخطر السابق ذكره يهز بموثوقية جهة التصديق الالكتروني، مما يتطلب اتباع عدة إجراءات للوقاية من تلك المشكلة، وتتمثل تلك الطرائق في ضرورة تأمين جهة التصديق الالكتروني للإطار الوظيفي المحترف القادر على منع أي اختراق لتوقيعها أو لمفتاحها الخاص، أي ضرورة توظيفها الأشخاص الذين يملكون المؤهلات العلمية المناسبة لأداء المهام الملقاة على عاتقهم[21]، والذين يستطيعون كشف أي اختراق قد يقع على التوقيع الالكتروني الخاص بها وتمييزه.

هذا، ولا يقتصر دور موظفي جهة التصديق على حماية توقيعها الالكتروني من خطر الاختراق والقرصنة، بل يمتد دورهم إلى ملاحقة أثر الاختراق في حال حصوله وعرقلة نشاطه وتدارك آثاره بالسرعة القصوى[22]، والحيلولة دون إفادة ذلك المخترق القرصان من توقيع جهة التصديق الالكتروني في إصدار شهادات توثيق خاطئة بما يضر بمصلحة تلك الجهة ويعرضها إلى مسؤولية قانونية كبيرة.

وكذلك يجب على جهة التصديق عدم الاكتفاء بنظم الحماية المتداولة التي يسهل اختراقها، بل عليها الاعتماد على أحدث برامج نظم الحماية لتأمين توقيعها الالكتروني على شهادات التوثيق مهما كان

---

20 ــ راجع في ذلك: Al-ghadyan (A) , Digital Signatures and Liability Issues Arising Out of Their Certification , Law Magazine , Kuwait, No 2 , 2004 ,p83

21 ــ د. صالح بن محمد المسند وعبد الرحمن بن راشد المهيني ،جرائم الحاسب الآلي: الخطر الحقيقي في عصر المعلومات المجلة العربية للدراسات الأمنية والتدريب ،جامعة نايف العربية للعلوم الأمنية ،الرياض، العدد 29، 2000، ص192.

22 ــ د. نعيم مغبغب، مخاطر المعلوماتية والإنترنت، من دون دار نشر،1998، ص 225 .

ثمنها[23]، مما يعني أن دور جهة التصديق الالكتروني لا يقف عند حد توفير النظام الأمني المبين قانوناً، بل يمتد إلى درجة استخدام أحدث الإنجازات التقنية التي تخدم مهمتها في تأمين توقيعها الالكتروني، بحيث تعدّ جهة التصديق مهملة إن لم تزود نظم المعلوماتية لديها بأحدث البرامج الأمنية، ومن ثمَّ تقوم مسؤوليتها المدنية في حال استولى القراصنة على توقيعها الالكتروني[24]كما يمكن لها الاعتماد على خبرات بعض محترفي القرصنة في سبيل تطوير نظم حماية توقيعها الالكتروني ضد المتسللين [25] .

لذا، يجب على جهة التصديق الالكتروني اختيار برامج أمن المعلومات الناجحة والمجربة لتحقيق حماية مثلى لمفتاحها الخاص من خطر الاختراق حتى لو كانت غالية الثمن، لأن ذلك يعدُّ أمراً هيناً مقارنة بالأخطار التي تنجم عن الاستيلاء على مفتاحها الخاص، ومن ثمَّ يجب أن تؤمن نظم الحماية المستعملة من قبل جهة التصديق عدم تعديل الشفرة المستخدمة من قبلها أو اكتشافها في توقيع الشهادة الرقمية .

المبحث الثاني

التحقق من صحة التوقيع الالكتروني لجهة التصديق الالكتروني

لا بدَّ من أن يتم تصديق التوقيع الالكتروني العائد لجهة التصديق حتى يتأكد المتعامل مع جهة التصديق من أن التوقيع الالكتروني يعود بالفعل لجهة التصديق التي يتعامل معها، فكما أن الموقع يصدق توقيعه لدى جهة التصديق التي تصدر شهادة تثبت فيه نسبة التوقيع إلى الموقع مما يجعل

23 ــ تكاثفت جهود الخبراء في مجال تصميم البرامج المضادة للفيروسات والاختراقات على تطوير نوعين من برامج نظم الحماية، الأول، وصل عمره إلى نحو خمس سنوات، وتقوم فكرته الأساسية على مراقبة هذا البرنامج لسلوك البرامج المحملة على البرامج الموجودة على جهاز الحاسب الآلي، ففي حالة قيام أيّ برنامج محملٍ على الجهاز بالتعامل مع البيانات السرية الموجودة في برنامج التشغيل، فعندها يبدأ برنامج الحماية مباشرة في العمل بطريقة الحجر على البرامج والملفات حتى يتمكن من تحليل طبيعة البرنامج الذي تم تحميله . أمَّا النظام الثاني فما زال حتى تاريخه تحت نطاق التجربة ويطلق عليه اسم " تحليل السمعة "، إذْ إنّه مصممٌ على أساس تحليل مصادر الشفرات التي تصل للجهاز، فإذا صادف هذا البرنامج موقعاً الكترونياً أو شفرة ليست معروفة لديه يبدأ على الفور بتأمين برامج الجهاز . راجع في ذلك:أ. إبراهيم فرغلي، توابع الفيس بوك، مجلة العربي، الكويت، العدد 601، 2008، ص 154 ــ 155 .

24 - راجع في ذلك: عزة أحمد خليل، مشكلات المسؤولية المدنية في مواجهة فيروس الحاسب، رسالة دكتوراه، جامعة القاهرة،1994، ص 312 -313 . وكذلك راجع: عايد رجا الخلايلة،المسؤولية التقصيرية الالكترونية،دار الثقافة للنشر والتوزيع،عمان، الطبعة الأولى، 2009، ص 173 .

25 ــ محمد عبد الله منشاوي، جرائم الإنترنت من منظور شرعي وقانوني ، بحث منشور على موقع الدكتور عايض المري للأبحاث القانونية (www.dralmarri.com/show.asp ? Field=res- a&id=221)، ص14 .آخر زيارة في10 /2012/6.

الغير يتعامل مع الموقع بثقة، كذلك يجب على المتعامل أن يتأكد من نسبة التوقيع الالكتروني العائد لجهة التصديق والمذكور في شهاداتها الالكترونية فعلاً لتلك الجهة التي يتعامل معها، ومن ثمَّ درسنا في المطلبين التاليين طرائق التأكد من صحة التوقيع الكتروني العائد لجهة التصديق الالكتروني وكيفية تطبيق ذلك في سورية وذلك وفق الآتي:

المطلب الأول: طرائق التأكد من عائدية التوقيع الالكتروني لجهة التصديق الالكتروني .

المطلب الثاني: تصديق التوقيع الالكتروني لجهة التوثيق الالكتروني في سورية وعقبات تطبيقه.

المطلب الأول

طرائق التحقق من عائدية التوقيع الالكتروني لجهة التصديق الالكتروني

يقوم توقيع جهة التصديق الالكتروني على الشهادات الصادرة عنها على إضفاء الثقة والمصداقية على جملة البيانات المدرجة في تلك الشهادات لدى الغير المطلع عليها، إلا أن ذلك يطرح استفساراً عن الوسيلة التي يتحقق بموجبها الغير من صحة التوقيع الالكتروني لجهة التصديق الالكتروني ونسبته إليها، فإذا كان بالإمكان التأكد من هوية من يتمّ التعاقد معه ونسبة التوقيع الالكتروني إليه عبر الاستعانة بالشهادة الالكترونية الصادرة عن جهة التصديق الالكتروني التي تؤكد صحة ذلك بتوقيعها الكترونياً على شهاداتها، فكيف يمكن لنا التأكد من صحة التوقيع الالكتروني لجهة التصديق الالكتروني على الشهادة الالكترونية؟

للإجابة عن هذه المعضلة،فإن الحل يكمن عبر اقتراح وسيلتين يمكن عن طريق استخدام أي منهما التأكد من نسبة التوقيع الالكتروني لجهة التصديق،وسنتعرف في الفرعين القادمين كلتا الوسيلتين وذلك وفق ما يأتي:

الفرع الأول

إنشاء عدة مراتب لجهات التصديق الالكتروني

يجري وفق هذا الحل التأكد من صحة التوقيع الالكتروني لجهة التصديق على الشهادة باستخدام المفتاح العام العائد لجهة التصديق الالكتروني المذكور بدوره في شهادة أخرى من قبل جهة تصديق الكتروني أخرى التي غالباً ما تكون في مستوى أعلى فيما يتعلق بالرتبة، وتلك الشهادة الأخرى يمكن

توثيقها بدورها عبر المفتاح العام المبيّن في شهادة أخرى، وهكذا إلى أن يتثبت الشخص المعتمد على التوقيع الالكتروني من صحته[26].

هذا، ويؤدي اتباع الحل السابق إلى تشكيل سلسلة من الثقة إذْ إنَّ جهة التصديق التي هي على رأس التسلسل الهرمي توقع شهادات جهات التصديق الالكتروني التابعة لها أو التي تأتي في مرتبة أدنى منها،وجهات التصديق تلك توقع بدورها شهادات جهات التصديق الالكتروني التي يكون ترتيبها أدنى منها وهكذا ...[27] .

لكن يؤخذ على الطريقة السابقة عدم حلها للمشكلة، بل إنها تحركها من مستوى إلى آخر لأن سلطة الشهادة الثانية تحتاج إلى سلطة أبعد لتوثيق مفتاحها العام وهكذا..، ومن ثمَّ فكلما زادت سلطات الشهادة في المنظومة (السلسلة) زادت حاجة الغير إلى فحص الشهادات واختبارها، مما يؤدي إلى ضياع وقته في التأكد من صحة التواقيع كلّها الصادرة عن الجهات جميعاً، ومما لا شك فيه أن هذا التتبع كلّه سيكون مكلفاً من الناحية المادية أيضاً[28] ، لذا لا يمكن من وجهة نظرنا الاعتماد على تلك الطريقة في التحقق من التوقيع الالكتروني لجهة التصديق الالكتروني، بل لا بدَّ من اتباع حل آخر، مما يدفعنا لمناقشة الحل الثاني.

الفرع الثاني

إنشاء مكتب حكومي للتصديق الالكتروني

يتجلى هذا الحل في أن يكون أصل جهة التصديق الالكتروني التي توقع على الشهادة الالكترونية أو أساسها مكتباً حكومياً يتولى مهمة تصديق المفاتيح العامة العائدة لجهات التصديق، ومن ثمَّ يمكن التأكد من صحة توقيع جهة التصديق الالكتروني على الشهادة الالكترونية عبر اللجوء إلى المكتب الحكومي الذي وثق المفتاح العام لتلك الجهة، وبهذا الشكل يمكن التخلص من ضياع الوقت الذي يصيب من يعتمد على تلك الشهادة والناجم عن تتبعه صحة التوقيعات الالكترونية الصادرة عن مختلف جهات التصديق وذلك وفق الخيار الأول .

---

26 ــ لمزيد من المعلومات راجع الموقع الآتي:

www.qun- engineer.org.sy/ar-files/index.php?page=3&sub-page=175 آخر زيارة في 5 -6 -2012

27ــ محمد خالد جمال رستم، المرجع السابق، ص 46 .

28 ــ راجع في ذلك: Al-ghadyan (A),op. cit,p78 .

وكذلك يؤدي استخدام هذه الوسيلة إلى سهولة معرفة صحة توقيع جهة التصديق على الشهادة الرقمية عبر استخدام المفتاح العام العائد لهذه الجهة الموثق لدى مكتب تابعٍ للدولة، وقد تبنى مشروع قانون التجارة الالكترونية المصري هذا الاتجاه بشكلٍ قوي، إذْ نصت المادة الثامنة من المشروع على ما يأتي: "ينشأ بالجهة التي يصدر بتحديدها قرار من السلطة المختصة مكتب للتشفير يكون جهة إيداع لمفاتيح الشفرات التي يحتاج استخدامها إلى الحصول على ترخيص مسبق".

يتضح من النص السابق أنْ لابدّ من إخضاع التشفير للرقابة المسبقة،لذا قررت لجنة صياغة المشروع وضع هذا النص لتمكين الجهة المختصة من وضع الضوابط الخاصة بالترخيص بالتشفير مع تأكيد ضرورة تمكينها من حيازة مفاتيح التشفير في هذه الحالات [29]، ومن ثمَّ قرر المشروع إنشاء مكتب للتشفير تودع لديه مفاتيح الشفرات الخاصة بجهات التصديق الالكتروني [30] .

وفي الواقع فإننا نرى أن الحل السابق أفضل وذلك لسهولته وبساطته ولضمانه نزاهة وسلامة التوقيع الالكتروني لجهة التصديق نظراً إلى توثيقه لدى مكتب حكومي تابع للدولة وليس تابعاً لأيّ جهة أو مؤسسة خاصة، مما يضمن حياده ومصداقية عملية التوثيق، كما قد يتولى المكتب الحكومي أيضاً مهمة توزيع المفاتيح العامة لجهات التصديق على الشهادات الالكترونية بأسس وضوابط منتظمة في أنحاء الدولة كلّها[31] .

المطلب الثاني

تصديق التوقيع الالكتروني لجهة التوثيق الالكتروني في سورية وعقبات تطبيقه

نُوقِشَتْ في هذا المطلب الطريقة الفُضلى للتأكد من صحة التوقيع الالكتروني الخاص بمزود خدمة التصديق الالكتروني في سورية وكيفية تطبيقها على أرض الواقع، وما المصاعب التي تحول دون تنفيذها فعلاً مما يؤدي في نهاية الأمر إلى عدم الإفادة منها على الإطلاق، إذْ بيَّنا ذلك في الفرعين الآتيين وفق ما يأتي:

---

29 - راجع الموقع الآتي:

www.f-law.net/law/threads/13243 آخر زيارة 10 -5- 2013

30 ــ راجع: د . بلال الصنديد، مداخلة حول حجية التوقيع الالكتروني، في الحلقة النقاشية عن مشروع قانون التجارة الالكترونية المنعقدة في جامعة الكويت في2005/4/5، منشورة في مجلة الحقوق، الكويت، ملحق العدد 3، 2005، ص174 .

31 ــ راجع في ذلك: . Al Ghadyan , Ahmad ,op.cit ,p78

الفرع الأول

الآلية الواجب تطبيقها للتأكد من صحة التوقيع الالكتروني لجهة التصديق الالكتروني

توصلنا من خلال المطلب السابق إلى نتيجة مفادها أن أفضل طريقة للتأكد من صحة التوقيع الالكتروني العائد لجهة التصديق الالكتروني هي إيجاد مكتب حكومي يتولى مهمة تصديق التوقيع الالكتروني الخاص بجهات التصديق الالكتروني،بحيث يقوم المكتب الحكومي بتوثيق المفتاح العام العائد لجهة التصديق الالكتروني؛ مما يؤدي إلى التأكد من صحة توقيع جهة التصديق الالكتروني على الشهادة الرقمية الصادرة عنها .

هذا، وقد نصّ صراحة قانون التوقيع الالكتروني السوري رقم 4 الصادر عام 2009 على أن الهيئة الوطنية لخدمات الشبكة هي الجهة الوحيدة والمخولة حصراً بمنح التراخيص للجهات الراغبة بمزاولة مهمة التصديق الالكتروني[32]، إلا أنّ القانون لم يوضح من يتولى تصديق المفاتيح العامة العائدة لجهات التصديق الالكتروني، وهل تستطيع الهيئة الوطنية لخدمات الشبكة تولي ذلك الأمر؟

بالمقابل وبالعودة إلى الضوابط الانتقالية الخاصة بالتوقيع الالكتروني الصادرة بالقرار رقم 190 تاريخ 2011/8/10، نجد أنها في الفقرة الثانية الخاصة بشروط تقديم خدمة إصدار شهادات التصديق للتوقيع الالكتروني قد أوجبت على أي جهة ترغب بتقديم خدمة إصدار شهادات التصديق الالكتروني أن تعلم الهيئة الوطنية لخدمات الشبكة بالمفتاح العلني الرئيس الخاص بها[33]، ومن ثمَّ يمكن التوسع في تفسير ذلك النص بأنه يمكن التأكد من صحة التوقيع الالكتروني العائد لجهة التصديق الالكتروني عبر استخدام المفتاح العام العائد لجهة التصديق الموثق والمبين لدى الهيئة الوطنية لخدمات الشبكة، إذْ لا حاجة لإنشاء مكتب حكومي يتولى هذه المهمة لأنه يمكن ببساطة أن تتولى الهيئة الوطنية

32 _ نصت المادة 15 /4 من قانون التوقيع الالكتروني السوري على مهام الهيئة الوطنية لخدمات الشبكة ومن أبرزها منح التراخيص لمزاولة خدمات التوقيع الالكتروني .

33 _ نصت تعليمات الفترة الانتقالية للعمل بالتوقيع الالكتروني في سورية على أنه : يجب على أي جهة ترغب بتقديم خدمة إصدار شهادات التصديق للآخرين،سواء كانت شهادات التصديق مولدة محلياً أو بالوكالة عن مزودين خارجيين أن تلتزم بما يأتي: 2-إعلام الهيئة ورقياً بالمفتاح العلني الرئيسي لسلطة التصديق،في حال إنشائها محلياً .

للاطلاع على التعليمات الانتقالية لقانون التوقيع الالكتروني السوري راجع الموقع الآتي:

nans.gov.sy/images/stories/doc/controls-transition-digitalsignature.pdf آخر زيارة 10 -5 -2013

لخدمات الشبكة تصديق التوقيع الالكتروني لجهة التصديق كونها هي المخولة حصراً بمنح الترخيص لجهة التصديق فلا مانع من أن توثّق التوقيع الالكتروني العائد لجهة التصديق الالكتروني لأنها تمتلك المتطلبات التقنية التي تؤهلها لهذا الأمر .

كذلك واستناداً إلى المادة 14/ب من قانون التوقيع الالكتروني السوري يمكن للهيئة الوطنية لخدمات الشبكة إقامة مكتب أو مركز تخصصي تابع لها يتولى عنها مهمة تلقي المفتاح العام العائد لجهة التصديق الالكتروني[34] .

هذا، ونرى أنه يجب منح الهيئة الوطنية لخدمات الشبكة الحق في توزيع المفاتيح العامة لجهات التصديق الالكتروني وفق أسس معينة، وذلك لأنه يفترض بالهيئة الوطنية أن تمتلك تقنيات عالية تزيد على التقنيات المستخدمة من قبل جهات التصديق الالكتروني لأنَّها تمارس رقابة على تلك الجهات،لذا فمن المنطقي أن تتولى منح المفاتيح العامة لجهات التصديق الالكتروني .

الفرع الثاني

معوقات تطبيق الطريقة المقترحة وسبل إزالتها

يبدو أنه من السهولة نظرياً تطبيق تصديق التوقيع الالكتروني وفق التصور السابق الذكر، إذْ تودع المفاتيح العامة العائدة لجهات التصديق الالكتروني لدى الهيئة الوطنية لخدمات الشبكة، إلا أنّ المسألة على أرض الواقع ستكون عديمة الفائدة، ذلك لأن جهات التصديق الالكتروني لم تتشكل بعد في سورية رغم صدور التعليمات الانتقالية لقانون التوقيع الالكتروني السوري،لعدم قدرتها على امتلاك المتطلبات التقنية والمادية المطلوبة منها، ومن ثمَّ كان يجب توفير البنية التحتية الكاملة اللازمة لتنفيذ قانون التوقيع الالكتروني قبل صدور القانون وليس محاولة تأمينها بعد صدور القانون، إذْ أقرّت التعليمات الانتقالية الخاصة بالتوقيع الالكتروني في سورية أن الجهات الراغبة بإصدار شهادات التصديق الالكتروني لا تمتلك التقنيات اللازمة لتلك المهمة،كما أنها لا تستطيع تغيير آلية عملها،مما يدفعنا للمطالبة بتوفير المستلزمات التقنية جميعها قبل نهاية مدة السنة المقررة لتلك التعليمات الانتقالية حتى لا يُمدَّدُ العمل بها إلى أجل غير مسمى، ومن ثمَّ عدم الإفادة من قانون التوقيع الالكتروني؛ مما يعني تجميد دور الهيئة الوطنية لخدمات الشبكة .

34 _نصت المادة 14 /ب من قانون التوقيع الالكتروني السوري على: " يجوز للهيئة بقرار من الوزير إقامة مراكـز تخصـصية تسند إليها بعض المهام التي تقوم بها الهيئة " .

كذلك نجد في تعليمات المرحلة الانتقالية أنه قد أُوقِفَ العمل بقانون التوقيع الالكتروني فيما يتعلق بحجية التوقيع الالكتروني، إذْ ينصّ القانون على ضرورة توافر شروط خاصة في التوقيع الالكتروني حتى يتمتع بالحجية القانونية، ومن أهم تلك الشروط وجود جهة التصديق الالكتروني لإصدار شهادات التصديق المعتمدة، لكن جاءت التعليمات الانتقالية وبيّنت أنه يجب على جهة التصديق الالكتروني إعلام المستفيدين من خدماتها بأن التوقيع الالكتروني لا يتمتع بأي حجية خلال الفترة الانتقالية، ومن ثمَّ نظراً إلى أنّ التوقيع الالكتروني لا يتمتع بأي حجية فلا فائدة من تصديق التوقيع الالكتروني الخاص بجهة التوثيق الالكتروني لدى الهيئة الوطنية، كما لا فائدة ترجى من وجود جهات التصديق الالكتروني على أرض الواقع لأنه مع كونها مرخصة و توقيعها موثق من قبل الهيئة الوطنية لخدمات الشبكة إلا أن التواقيع الالكترونية الخاصة بالموقعين المسجلين لديها ليس لها أي حجية قانونية إذْ أوجبت التعليمات الانتقالية على جهات التصديق أن تبين كتابة للمستفيدين من خدماتها عدم وجود أي حجية قانونية للتوقيع الالكتروني الموثق لديها[35]، وهو ما يعني عدم لجوء أحد إلى جهات التصديق الالكتروني في حال إنشائها لأنه سيتوجب عليه دفع مبلغ من المال مقابل أن تمنحه جهة التصديق شهادة التصديق الالكتروني المبينة لتوقيعه الالكتروني الذي لا يتمتع بأي حجية قانونية [36] .

هذا، ونرى أن عدم تمتع التوقيع الالكتروني بأي حجية يجب أن يكون خاصاً بجهات التصديق الالكتروني غير المعتمدة من قبل الهيئة الوطنية لخدمات الشبكة رغم أن القانون نصّ صراحة على أنه لا يمكن مزاولة خدمات التصديق دون الحصول على ترخيص من قبل الهيئة الوطنية ، لذا يجب أن يتم التوفيق بين قانون التوقيع الالكتروني والتعليمات الانتقالية بحيث تعدل تلك الأخيرة في أسرع وقت ممكن وقبل انتهاء مدة السنة المحددة لها بحيث تنصّ على تمتع التوقيع الالكتروني الصادر عن جهات التصديق المرخص لها بكامل حجيته القانونية،مع ضرورة الإفادة من الوقت في إيجاد البنية التحتية المناسبة لتنفيذ قانون التوقيع الالكتروني السوري وتطويرها على أرض الواقع .

35 - نصت تعليمات الفترة الانتقالية على: يجب على أي جهة ترغب بتقديم خدمة إصدار شهادات التصديق للآخرين أن تلتزم بما يأتي:5- إعلام المستفيدين من خدماتها كتابة وبشكل واضح وصريح بعدم وجود أي حجية قانونية للتوقيع الالكتروني المستخدم خلال هذه المدة .

36- تبدو فائدة اللجوء إلى جهة التصديق الالكتروني من الناحية التقنية فقط المتمثلة بحصول الموقع على توقيع الكتروني خاص به .

الخاتمة:

حاولنا في هذه الدراسة أن نتناول موضوعاً مهماً هو تصديق التوقيع الالكتروني الخاص بجهات التصديق الالكتروني إذْ بينّا مفهوم ذلك التوقيع وأهميته الكبيرة كما أوضحنا طرائق التحقق من صحته، كما ناقشنا آلية التحقق منه في سورية وعقبات تطبيق ذلك فعلياً، ونخلص من البحث السابق إلى عدة نتائج وتوصيات تتجلى في:

1- ضرورة تصديق التوقيع الالكتروني الخاص بجهة التصديق الالكتروني في مكتبٍ حكومي دائم يحوي الشفرة الخاصة بها، وذلك للتأكد من صحة التوقيع الالكتروني ونسبته إلى جهة التصديق الالكتروني .

2- يجب اتباع الإجراءات المبينة لتفادي خطر الاستيلاء على توقيع جهة التصديق الالكتروني من قبل القراصنة . لذلك يجب على الدول العربية تهيئة الأساليب والتقنيات الضرورية للوقاية من هذا الخطر، وكذلك الإفادة من النصوص القانونية التي تجرم الاستيلاء والحصول على التوقيع الالكتروني، فإذا كانت هذه النصوص قد صدرت بالأصل لتجريم من يستولي على التوقيع الالكتروني الخاص بالموقع وعقابه إلا أنها جاءت شاملة وعامة بحيث تجرم حتى من يعتدي على التوقيع الالكتروني الخاص بجهة التصديق الالكتروني .

3- ضرورة تفعيل قانون التوقيع الالكتروني السوري على أرض الواقع ومنح التوقيع الالكتروني المستجمع لشروطه القانونية الحجية القانونية الكاملة جميعها في الإثبات خلال المرحلة الانتقالية رغم تعارض التعليمات الانتقالية مع القانون؛ وذلك لأن القانون هو الأولى بالتطبيق .

4- استغلال المرحلة الانتقالية التي نصت عليها التعليمات الانتقالية الخاصة بالتوقيع الالكتروني في سورية، وذلك بتوفير التقنيات الخاصة بتطبيق التوقيع الالكتروني على أرض الواقع.

5- تولي الهيئة الوطنية لخدمات الشبكة السورية مهمة تصديق التوقيع الالكتروني الخاص بجهات التوثيق الالكتروني مع إمكانية قيامها بمنح المفاتيح العامة لتلك الجهات، وذلك بالنص صراحةً على هذه المهمة في الضوابط والتعليمات الخاصة بالتوقيع الالكتروني .

المصادر والمراجع

أولاً ــ المراجع العربية:

- أ .إبراهيم فرغلي، توابع الفيس بوك، مجلة العربي، الكويت، العدد 601، 2008 .
- أ.أمجد دخل الله:
- العقود الالكترونية، مجلة المحامون، العددان 9 ــ10 عام 2004 .
- القرصنة الالكترونية، مجلة المحامون ، سورية، العددان 3-4 ، 2007 .
- د.إيمان مأمون أحمد سليمان، إبرام العقد الالكتروني وإثباته، دار الجامعة الجديدة للنشر، الإسكندرية، 2008 .
- بروس شناير،التعمية التطبيقية،منشورات الجمعية المعلوماتية السورية،2006
- د.بلال الصنديد، مداخلة حول حجية التوقيع الالكتروني، في الحلقة النقاشية حول مشروع قانون التجارة الالكترونية المنعقدة في جامعة الكويت في 2005/4/5، منشورة في مجلة الحقوق، الكويت، ملحق العدد 3، 2005 .
- حسن مظفر الرزو، المفاهيم المعلوماتية لجرائم الفضاء الافتراضي بالحاسوب، مجلة الشريعة و القانون، جامعة الإمارات العربية المتحدة، العدد16 ،2002 .
- خالد ممدوح إبراهيم، التوقيع الالكتروني، بحث منشور على الموقع:
- www.kenanaonline.com/users/khaledMamdouh/posts/77870
- د.سامح عبد الواحد التهامى، التعاقد عبر الإنترنت (دراسة مقارنة)، دار الكتب القانونية، مصر،2008 .
- د.صالح بن محمد المسند وعبد الرحمن بن راشد المهيني ،جرائم الحاسب الآلي: الخطر الحقيقي في عصر المعلومات المجلة العربية للدراسات الأمنية والتدريب، جامعة نايف العربية للعلوم الأمنية، الرياض، العدد 29، 2000 .
- عايد رجا الخلايلة، المسؤولية التقصيرية الالكترونية،دار الثقافة للنشر والتوزيع،عمان، الطبعة الأولى، 2009
- د.عبد الفتاح بيومي حجازي، النظام القانوني للتوقيع الالكتروني (دراسة تأصيلية مقارنة)، دار الكتب القانونية، مصر، 2007 .
- عزة أحمد خليل، مشكلات المسؤولية المدنية في مواجهة فيروس الحاسب، رسالة دكتوراه، جامعة القاهرة، 1994

- **د.عمرو عيسى الفقي، وسائل الاتصال الحديثة وحجيتها في الإثبات، المكتبة القانونية، مـــصر 2006 .**
- **د.فاروق محمد أحمد الأباصيري،عقد الاشتراك في قواعد المعلومات عبر شبكة الإنترنت، دار الجامعة الجديدة للنشر،مصر ،2002 .**
- **لورنس محمد عبيدات، إثبات المحرر الالكتروني، دار الثقافة للنشر والتوزيع، عمان، 2005 .**
- **أ.محمد خالد جمال رستم، التنظيم القانوني للتجارة والإثبات الالكتروني في العالم، منـــشورات الحلبي الحقوقية، بيروت، 2006 .**
- **د.محمد سعيد أحمد إسماعيل، أساليب الحماية القانونية لمعاملات التجارة الالكترونية منشورات الحلبي الحقوقية، بيروت، 2009.**
- **أ.محمد عبد الله منشاوي، جرائم الإنترنت من منظور شرعي وقانوني، بحث منشور على موقع الدكتور عايض المري للأبحاث القانونية**

(www.dralmarri.com/show.asp?Field=res- a&id=221) .

- **د . نعيم مغبغب، مخاطر المعلوماتية والإنترنت، من دون دار نشر،1998 .**
- **وسام أبو عمره،البـــصمة الالكترونيـــة والتوقيـــع الرقمـــي منـــشور علـــى الموقـــع الآتـــي:** (www.al3ez.net/vb/showthread.php?..)
- **ياسر إمام الغندور، حجية التوقيع في المعاملات التجارية الالكترونية، منـــشور علـــى موقـــع** .www.okaz.com.sa/okaz/osf/20060801/Con2006080136011.htm
- www.qun- engineer.org.sy/ar-files/index.php?page=3&sub-page=175
- www.f-law.net/law/threads/13243
- nans.gov.sy/images/stories/doc/controls-transition-digitalsignature.pdf

ثانياً ــ المراجع الأجنبية:

- Al-ghadyan (A), Digital Signatures and Liability Issues Arising Out of Their Certification, Law Magazine , Kuwait, No 2 , 2004 .
- Allen Tom, Can Computers Make Contracts? , Harvard Journal of Law and Technology, U.S.A ,vol 9, No 1 ,1996.
- Froomkin Michael ,The Essential Role of Trusted Third Parties in Electronic Commerce, 75 Oregon Law Review , 1996.

تاريخ ورود البحث إلى مجلة جامعة دمشق 2012/8/15