دور التوقيع والتصديق الإلكترونيين في تأمين وسائل الدفع الإلكتروني

د. حوالف عبد الصمد

رئيس قسم القانون الخاص– أستاذ محاضر قسم «ب»
كلية الحقوق والعلوم السياسية– جامعة تلمسان– الجزائر

الملخص:

يؤدي التوقيع الإلكتروني دوراً مهماً كإجراء من إجراءات تأمين المعاملات الإلكترونية بصفة عامة، التي يمكن أن تطال الأجهزة والنظم الإلكترونية المستخدمة في مجال الدفع الإلكتروني والتجارة الإلكترونية، وهذا بفضل ما تحققه هذه التقنية من سرية وخصوصية المراسلات والبيانات والاتصالات المستخدمة في الصفقات. يضاف إلى ذلك، الاستخدامات المختلفة للتوقيع الإلكتروني في نظام التجارة الإلكترونية، والتي تهدف جميعها إلى توفير الثقة في المعاملات المصرفية والتجارة الإلكترونية. ولقد أدرك المشرع الجزائري الدور الذي يمكن أن تؤديه هذه التقنية في حماية وسائل الدفع الالكتروني، لذلك قام بإفراد قانون خاص بالتوقيع والتصديق الإلكترونيين من خلال القانون رقم 15–04.

فإلى أي مدى يمكن لهذا القانون تعزيز ثقة المتعاملين في حقل وسائل الدفع الإلكتروني وبذلك تعميم استخدام هذه الوسائل؟ هذا ما سأحاول إبرازه من خلال هذا البحث على ضوء التشريع الجزائري والمقارن.

المقدمة:

لقد أدى انتشار التكنولوجيا الإلكترونية الحديثة ومنها الحاسب الآلي والإنترنت، إلى ازدهار التجارة الإلكترونية التي اعتمدت هذه الوسائل إلى حد كبير، مما استتبع ذلك ظهور وسائل دفع في صورتها الإلكترونية؛ وهذه الأخيرة تؤدي مهام كبيرة في إطار التجارة الإلكترونية، إلا أنه يمكن اعتبار أن هذه التكنولوجيا تعد سلاحا ذو حدين، فهي إضافة إلى مزاياها أو وظائفها المتعددة، إلا أنه في الجانب الآخر يمكن لمستعمليها أن يصيبوا البيئة الافتراضية بعدة اختلالات جراء تدخلاتهم بتحويلها عن الأهداف المرسومة لها، هذه التدخلات تشكل خطراً على استمرارية هذه الوسائل والثقة المطلوب توافرها لإقناع المستهلكين باستخدامها. وتتعدد المخاطر التي تهدد مستخدمي وسائل الدفع الإلكتروني، فيمكن أن تكون من طرف الأشخاص المتدخلين في الصفقات أو من الغير، كما قد تنجم عن طبيعة هذه الوسائل التي يمكن أن تكون عبارة عن خدمات مالية تعتمد التكنولوجيا الحديثة في أداء مهامها، والتي تكون في الكثير من الأحيان في بيئة مفتوحة كالإنترنت.

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

فالتوقيع الإلكتروني[1]، هو التوقيع الناتج عن إتباع إجراءات محددة تؤدي

(1) التوقيع بالمعنى التقليدي هو الذي يتم على وسيط ورقي، ويعرَّف بأنه علامة شخصية ومميزة يضعها الشخص باسمه أو ببصمته أو أي وسيلة أخرى على مستند لإقراره والالتزام بمضمونه. كما تم تعريف التوقيع أيضا بأنه كل علامة شخصية توضع كتابة بحيث تتيح تحديد شخص محدثها على وجه لا يتطرق إليه أي شك وتنم عن إرادته التي لا يحيطها أي غموض، في قبول مضمون السند أو المحرر. ووفقا للتعريفين السابقين للتوقيع، فهما وإن اختلفا في طريقة التوقيع، حيث أجاز التعريف الأول أن يكون كتابيا أو باليد عن طريق البصمة أو بوسيلة أخرى كالختم، بينما اقتصر التعريف الثاني على الكتابة فقط للتوقيع، فقد أوجب كل منهما أن يتوافر أمران بالتوقيع، الأول أن يكون محدداً لصاحبه، والثاني أن يدل على انصراف إرادته للالتزام بما وقع عليه، ويمكن أن يتم التوقيع بالإمضاء أو بالختم أو ببصمة الإصبع.

Martin(S), Tessalonikos(A) Et Bensoussan(A), La Signature Électronique,Premières Réflexions Après La Publication De La Directive Du 13 Décembre 1999 Et La Loi Du 13mars 2000, Gaz. Pal., Recueil Juillet-Aout 2000, P. 1274.

في النهاية إلى نتيجة معينة معروفة مقدما[2]، أو هو معطى ينجم عن استخدام أسلوب عمل يستجيب للشروط المحددة في المادتين 323 مكرر و323 مكرر1 من القانون المدني الجزائري[3]، والقانون 15-04 الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين.

إن جوهر التوقيع هو أن يكون شخصيا، لذا فإن فكرة التوقيع الشخصي لا تقتصر فقط على فكرة التوقيع المخطوط باليد، وبالتالي فكل توقيع أو علامة مميزة وشخصية تسمح بتمييز من أجراها يمكن أن يسمى توقيعا شخصيا، وقد عرفت المادة 2 من القانون النموذجي للتوقيعات الإلكترونية «اليونيسترال» الصادر عام 2001[4] الموقِّع بأنه: «الشخص الحائز على بيانات إنشاء توقيع ويتصرف إما بالأصالة عن نفسه وإما نيابة عن الشخص الذي يمثله». لذلك ومن خلال ما تم التطرق له، نتساءل إلى أي مدى يمكن لهذا القانون من تعزيز ثقة المتعاملين في حقل وسائل الدفع الإلكتروني وبذلك تعميم استخدام هذه الوسائل؟

سوف يتم محاولة معالجة هذا الموضع من خلال المبحثين التاليين:

(2) محمد المرسي زهرة، الحماية المدنية للتجارة الإلكترونية (العقد الإلكتروني، الإثبات الإلكتروني، المستهلك الإلكتروني)، دار النهضة العربية، القاهرة، 2008، ص 163.

(3) بالإضافة إلى المادة 3 مكرر من المرسوم التنفيذي رقم 07/ 162 المؤرخ في 13 جمادى الأولى عام 1428 الموافق لـ 30 مايو سنة 2007، المعدل والمتمم للمرسوم التنفيذي 01/ 123 والمتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية (ج.ر. عدد 37).

(4) راجع هذا القانون على الموقع:
https://www.uncitral.org/pdf/arabic/texts/electcom/ml-elecsig-a.pdf

المبحث الأول
دور التوقيع الإلكتروني في تأمين وسائل الدفع الإلكتروني

لا تعد الكتابة سواء كانت في الشكل الإلكتروني أو على دعامة مادية دليلا كاملا في الإثبات إلا إذا كانت موقعة، فالتوقيع هو العنصر الثاني من عناصر الدليل الكتابي المعد أصلا للإثبات وهو شرط أساسي لصحة الوثيقة سواء كانت الكترونية أو ورقية[5]. فالتوقيع الإلكتروني لا يعد جزءاً من الوثيقة أو المحرر، وإنما يقوم بعملية حفظ في معنى ومنح مصداقية للوثيقة أو المحرر الإلكتروني، بحيث يمكن بمقتضى هذا الحفظ إكساب هذه الوثيقة أو المحرر مصداقية لدى الغير أو الطرف الآخر المستقبل لهذا المحرر أو الوثيقة[6]، ويعد العنصر الثاني من عناصر الدليل الكتابي المعد أصلا للإثبات، وهو شرط أساسي لصحة الوثيقة سواء كانت إلكترونية أو ورقية. كما يمثل وسيلة للتأكد من الأطراف المتعاقدة ونصوص العقد، فهو يسمح بالتأكد من شخصية الطرف الذي أرسل العرض أو الذي قبله ويميزه عن غيره[7]، كما يسمح بالتأكد من أن نفس الرسالة التي تم إرسالها هي نفسها الرسالة التي تم الرد عليها.

لكن ما يهم في هذا المقام، هو بحث الدور الذي يؤديه التوقيع الإلكتروني في تأمين وسائل الدفع الإلكتروني، وسيتم ذلك من خلال التطرق لمفهوم التوقيع الإلكتروني وعلاقته بوسائل الدفع الإلكتروني (المطلب الأول)، ثم دراسة استخدام التوقيع الإلكتروني وحجيته في الإثبات بالدفع الالكتروني (المطلب الثاني).

المطلب الأول
مفهوم التوقيع الإلكتروني وعلاقته بوسائل الدفع الالكتروني

تتعدد الأدوار التي يستعمل فيها التوقيع الإلكتروني لإضفاء مصداقية أكثر وأمان على وسائل الدفع الإلكتروني، سواء أكان ذلك لاستعمالها كدليل للإثبات أو لحمايتها

(5) عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظم القانونية المقارنة، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2005 ، ص 7.

(6) عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، القاهرة، مصر، 2004، ص 14.

(7) محمد حسين منصور، الإثبات التقليدي والإلكتروني، دار الفكر الجامعي، الإسكندرية، مصر، 2006، ص 279.

من الهجمات التي تتعرض لها لاختراقها. وسيتم التطرق من خلال ما يلي، للتوقيع الإلكتروني بالتعرف على مفهومه بشكل عام بتعريفه في التشريعات الدولية ثم الوطنية، ثم نبين أهم تطبيقاته وعلاقته بوسائل الدفع الالكتروني.

الفرع الأول

تعريف التوقيع الإلكتروني

انقسمت التشريعات في تحديد مفهوم التوقيع الإلكتروني، فركَّز بعضها على شكل التوقيع بينما ركز البعض الآخر على وظائفه. ولعل أول خطوة فعلية لميلاد التوقيع الإلكتروني تشريعيا، كانت بصدور القانون النموذجي للتجارة الإلكترونية الدولية لسنة 1996، إذ عرفت التوقيع الإلكتروني في المادة السابعة على أنه: "عندما يشترط القانون وجود توقيع من شخص يستوفي ذلك الشرط بالنسبة إلى رسالة البيانات إذا:

استخدمت طريقة لتعيين هوية ذلك الشخص والتدليل على موافقة ذلك الشخص على المعلومات الواردة في رسالة البيانات.

كانت تلك الطريقة جديرة بالتعويل عليها بالقدر المناسب للغرض الذي أنشئت أو أبلغت من أجله رسالة البيانات في ضوء كل الظروف بما في ذلك أي اتفاق متصل بالأمر».

يركز هذا التعريف على ضرورة قيام التوقيع الإلكتروني بالوظائف التقليدية للتوقيع وهي تمييز هوية الشخص، والتعبير عن رضائه الارتباط بالعمل القانوني، كما ركز أيضا على أنه يتعين أن تكون طريقة التوقيع الإلكتروني طريقة موثوق بها، ولم يحدد تلك الطرق أو الإجراءات التي يتعين اتباعها، وإنما تركها لكل دولة تحددها بطريقتها ووفقا لتشريعاتها. وجاء بعد ذلك قانون «اليونيسترال» للتوقيعات الإلكترونية لعام 2001، وتحديدا في نص المادة 2/أ التي عرَّفت التوقيع الإلكتروني بأنه: «بيانات في شكل إلكتروني مدرجة في رسالة بيانات، أو مضافة إليها أو مرتبطة بها منطقيا، يجوز أن تستخدم لتعيين هوية الموقع على المعلومات الواردة في رسالة البيانات».

ويظهر من خلال هذا التعريف أنه قد اهتم بمسألتين، هما تعيين هوية الشخص المُوقِّع وبيان موافقته على المعلومات الواردة في المحرر، وهو بذلك انسجم مع الأصل العام للتوقيع في الدلالة على شخص المُوقِّع، وللتأكيد على أن إرادته قد اتجهت للالتزام

بما وقع عليه. أما القانون الفيدرالي الأمريكي بشأن التجارة الإلكترونية والصادر في 30 يوليو 2000 فعرَّف التوقيع الإلكتروني[8] بأنه: "أصوات أو إشارات أو رموز، أو أي إجراء آخر يتصل منطقيا بنظام معالجة المعلومات إلكترونيا، ويقترن بتعاقد أو مستند أو محرر، ويستخدمه الشخص قاصداً التوقيع على المحرر»[9].

ومن ناحيته، فقد ميَّز التوجيه الأوروبي رقم 99/93 الخاص بالتوقيعات الإلكترونية[10]، في نصوصه بين نوعين من التوقيع الإلكتروني، النوع الأول ويعرف بالتوقيع الإلكتروني العادي، وهذا التوقيع حسب نص المادة الثانية من التوجيه يعرَّف بأنه: «معلومة تأخذ شكلا إلكترونيا تقترن أو ترتبط بشكل منطقي ببيانات أخرى إلكترونية، والذي يشكل أساس منهج التوثيق»[11]. أما النوع الثاني فهو التوقيع الإلكتروني المتقدم[12]، وهو توقيع يرتبط بالنص الموقع.

(8) Loi N°., 2000-230 du 13 mars 2000, J.O. 62, 14 mars 2000, p. 3968, JCP 2000, III, 20259.

(9) En France, comme aux Etats-Unis, une signature, traditionnellement définie comme un écrit ou une marque, vise à identifier son auteur et apparaît sur le document dans le but de l'authentifier ou d'en établir sa légalité.10 Dans un contexte juridique, elle manifeste également la volonté du signataire de consentir aux obligations contractuelles.

Autant en France qu'aux Etats-Unis, la signature électronique remplit la même fonction mais peut apparaître sous différentes formes telles que des sons électroniques, des symboles, ou encore des données électroniques jointes ou logiquement associées à un contrat ou fichier et dont l'utilisation par un individu reflète son intention de signer le document.11 Comme le souligne certains spécialistes de ce domaine, une signature électronique peut être simple et consister en un nom apposé à la fin d'un courrier électronique ou plus complexe et plus fiable en ayant recours à des technologies avancées de biométrique, telles que les empreintes digitales ou encore les scanners rétiniens.12Comme dans le cas des signatures traditionnelles, la fraude relative aux signatures électroniques reste une préoccupation majeure. Chacun des deux pays utilise l'authentification, la certification ou encore d'autres formes traditionnelles d'identification pour se prémunir contre la fraude. Laurence Birnbaum-Sarcyet Florence Darques, La signature électronique Comparaison entre les législations française et américaine, Revue du Droit des Affaires Internationales, Avril 2001, Disponible sur:
http://www.signelec.com

=

(10) DIRECTIVE 1999/93/CE DU PARLEMENT EUROPÉEN ET DU CONSEIL, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques. Disponible sur:

http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:31999L0093&from=FR

(11) Art. 2: Définitions: «Aux fins de la présente directive, on entend par:1) «signature électronique», une donnée sous forme électronique, qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification».

(12) Arti2 .: Définitions: «Aux fins de la présente directive, on entend par: 2) «signature électronique avancée» une signature électronique qui satisfait aux exigences suivantes:
a) être liée uniquement au signataire;

=

إن التعريف الذي أورده التوجيه الأوروبي أخذت به معظم التشريعات الأوروبية، ففي القانون المدني الفرنسي تم تناول التوقيع الإلكتروني بالمادة 1316/4 المضافة بقانون 13 مارس 2000 [13] حيث تنص على أنه: «عندما يتم التوقيع في شكل إلكتروني، فإنه يجب أن يتم باستخدام طريقة موثوق بها لتمييز هوية صاحبه، وضمان ارتباطه بالعمل القانوني المقصود.

من جهته أيقن المشرع الجزائري أهمية هذه التكنولوجيا الحديثة، فأصدر القانون رقم 15-04 [14] المتعلق بالتوقيع والتصديق الإلكترونيين، إذ وبالرجوع إلى المادة 02/01 من هذا القانون، نجده قد عرَّف التوقيع الإلكتروني بأنه: «بيانات في شكل إلكتروني، مرفقة أو مرتبطة منطقيا ببيانات إلكترونية أخرى، تستعمل كوسيلة توثيق». وتضيف الفقرة الثالثة من نفس المادة حول تعريف بيانات إنشاء التوقيع الإلكتروني: «بيانات فريدة، مثل الرموز أو مفاتيح التشفير الخاصة، التي يستعملها المُوقِّع لإنشاء التوقيع الإلكتروني».

فمن خلال هذين التعريفين، يظهر الاهتمام بمسألة موثوقية البيانات محل التوقيع دون الاهتمام بمسألة موافقة الشخص الموقع على المعلومات الواردة في المحرر، هو التأكيد على أن إرادته قد اتجهت للالتزام بما وقع عليه[15].

= b) permettre d'identifier le signataire;

c) être créée par des moyens que le signataire puisse garder sous son contrôle exclusif et

d) être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable.

(13) Art. 1316-4: Créé par Loi n°2000-230 du 13 mars 2000 - art. 4 JORF 14 mars 2000: La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte.

Lorsqu'elle 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 électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'Etat. Disponible sur:

http://legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006070721&idArticle=LEGIARTI

(14) المؤرخ في 11 ربيع الثاني 1436 الموافق لأول فبراير سنة 2015، ج.ر.عدد 06.

(15) أول نص تشريعي تطرق فيه المُشرِّع للتوقيع الإلكتروني كان المادة 327 من القانون المدني المعدل بالقانون رقم 05/10 والتي نصت على أنه: «... ويعتد بالتوقيع الإلكتروني وفق الشروط المذكورة في المادة 323 مكرر 1 أعلاه».

وتختلف أشكال وصور التوقيع الإلكتروني باختلاف الطريقة المتبعة في إظهاره، كما تتباين هذه الصور فيما بينها، من حيث الثقة ومستوى ما تقدمه من ضمان بحسب الإجراءات المتبعة في إصدارها وتأمينها والتقنيات التي تخرجها، فقد تتخذ شكل حروف أو أرقام أو أية رموز كانت يختارها الشخص من لوحة الطابع كما قد يكون مجرد نسخ للتوقيع العادي أو عبارة عن وحدات ضوئية أو رقمية أو كهرومغناطيسية[16].

يتضح من كل ما سبق أن التوقيع الإلكتروني وسيلة حديثة لتحقيق شرطي الرضا وهما تعيين صاحبه وانصراف إرادته نهائيا إلى الالتزام بمضمون ما وقع عليه، كل ما هنالك أنه ينشأ عبر وسيط إلكتروني وذلك استجابة لنوعية المعاملات التي تتم إلكترونيا، فحيث تبرم العقود والصفقات إلكترونيا وجب أن يتم التوقيع إلكترونيا، بما يسمح بالتالي باستبعاد فكرة التوقيع التقليدي بمفهومه الضيِّق[17].

الفرع الثاني

تطبيقات التوقيع الالكتروني وعلاقته بوسائل الدفع الالكتروني

لقد تزامن ظهور التوقيع الإلكتروني مع استعمال بطاقة الائتمان في عمليات سحب النقود أو إجراء المشتريات أو الحصول على الخدمات، ثم اتسعت بعد ذلك دائرة استخدامه لتشمل عمليات الشراء عن بعد؛ سواء عن طريق الهاتف أو شبكة الإنترنت، ثم لتمتد إلى القيام بالإجراءات الإدارية، وتسديد الرسوم والضرائب، كما أن التوقيع الإلكتروني مرشح للتغلغل في حياتنا أكثر وأكثر، من خلال مشروع الحكومة الإلكترونية الذي شرعت فيه معظم الدول من بينها الجزائر[18]، بهدف الوصول إلى

(16) بمراجعة الوسائل الإلكترونية التي تضمنت طرقاً تكنولوجية مختلفة، نجد أن التوقيع الإلكتروني يمكن أن يتخذ عدة صور أهمها:

- التوقيع بالقلم الإلكتروني (OP-PEN).
- التوقيع باستخدام البطاقة المغنطة المقترنة بالرقم السري أو الكودي.
- التوقيع بالحواس الذاتية (البيوميتري) Biométrique Signature.
- التوقيع الرقمي Signature Numérique.

ويمكن القول، أن هذه الصور تتباين فيما بينها من حيث درجة الثقة وذلك بحسب الإجراءات المتبعة في إصدارها وتأمينها والتقنيات التي تتيحها، ولا شك أن هذه التقنيات في تطور مستمر بهدف إيجاد نظام آمن يضمن الحفاظ على الحقوق.

(17) إيمان مأمون أحمد سليمان، الجوانب القانونية لعقد التجارة الإلكترونية، رسالة دكتوراه، كلية الحقوق، جامعة المنصورة، 2005/2006، ص253.

(18) مثلا القانون 15-03 المؤرخ في 11 ربيع الثاني 1436 الموافق لأول فبراير 2015 يتعلق بعصرنة العدالة، ج.ر.عدد 06.

إدارة بدون أوراق[19].

وسيتم التطرق من خلال التالي لتطبيقات التوقيع الإلكتروني وعلاقته بوسائل الدفع الإلكتروني[20]:

أولا- بطاقات الدفع الإلكتروني:

من أقدم المجالات التي يستخدم فيها التوقيع الإلكتروني هو مجال بطاقات الائتمان[21]، والتي بدأ استعمالها لدى محطات الوقود والمحلات التجارية الكبرى، وهناك سوق عريضة ومتزايدة بسرعة للمنتجات في مجال التقنية لتزويد أدوات الأمن للتسوق خاصة داخل شبكة الإنترنت. وتسارع أكثر الشركات لعرض الحلول التقنية، التي أصبحت اليوم تتحد استجابة لمتطلبات التوقيعات الرقمية المعترف بها حديثاً في التشريعات الوطنية، ومن هذه المنتجات من البطاقات:

1- البطاقات المغناطيسية[22] Cartes Magnétiques:

بطاقة الشريط المغناطيسية ليست بالضبط الأداة التقنية المتقدمة في الوقت الحاضر، بيد أنها لا تزال تؤدي دوراً مهماً ومركزياً في الملايين من الصفقات التجارية الإلكترونية اليومية، ومعظم الاستعمالات المألوفة للبطاقة المغناطيسية نجدها في بطاقة الائتمان، حيث إن المعلومات المخزنة باستخدام المعايير الدولية لتشفير البيانات الرقمية على شريط مغناطيسي مقروء من قبل جهاز الصراف الآلي، بطريقة تتيح فك الشفرة الموجودة على الشريط المغناطيسي المثبت على البطاقة.

(19) محمد المرسي زهرة، الدليل الكتابي وحجية مخرجات الكومبيوتر في المواد المدنية والتجارية، بحث مقدم إلى مؤتمر القانون والكومبيوتر والإنترنت، جامعة الإمارات العربية المتحدة، الجزء الثالث، المنعقد من 1-3 ماو 2000، ص 797.

(20) أيمن علي حسين الحوثي، التوقيع الإكتروني بين النظرية التطبيق، دار المطبوعات الجامعية، 2011، ص 103 وما بعدها.

(21) عمر خالد زريقات، عقد البيع عبر الإنترنت، دار الحامد للنشر والتوزيع، عمان، الأردن، 2007، ص 311.

(22) فياض ملفي القضاه، مسؤولية البنك عن استخدام الكومبيوتر كوسيلة وفاء، مؤتمر القانون والكومبيوتر والإنترنت، الذي نظمته كلية الشريعة الإسلامية والقانون في جامعة الإمارات العربية المتحدة، الجزء الأول،الطبعة الثالثة، دبي الفترة الممتدة من 1-3 مايو 2000 ، 2004، ص 95. سميحة القليوبي، الأوراق التجارية، دار النهضة العربية، القاهرة، مصر، 1992، ص 305.

2- البطاقات الذكية Cartes à Puce:

وهي تشبه بطاقات الصراف الآلي ذات الشريط المغناطيسي العادية، بيد أنها تحتوي وبشكل رائع على كمية كبيرة من المعلومات التي تتضمنها كل بطاقة ويتم معالجتها بشكل دقيق وتكاملي، حيث إنها يمكن أن تخزن تقريباً أي معلومة، ويمكن الولوج بهذه البطاقات إلى شبكة الإنترنت، واستعمال البرامج التلفزيونية المدفوعة الأجر، وأن من أمن البطاقات الذكية يكون نموذجاً بإتباع مجموعة من إجراءات السلامة، حيث تتضمن كلمات السر أو ما يسمى بالرقم السري كمعلومات المفتاح العام والمفتاح الخاص (التي سيتم التطرق إليها لاحقاً في المطلب الموالي). ويمكن أن تقسم البطاقات الذكية في هذا المقام إلى مجموعتين: الأولى هي البطاقة الذكية ذات الرقاقة الإلكترونية؛ وتتمتع هذه البطاقات بقوة حسابية لتزويد أكثر أمناً، وتسمح بالتحقق من حامل البطاقة بإدخال الرقم السري، وتعمل هذه البطاقات الذكية بنظام (Off-line) أي غير متصل أو الاتصال غير المباشر، حيث تتم إضافة المعلومات الجديدة بعد الانتهاء من المعاملات البنكية الإلكترونية. وأما المجموعة الثانية من البطاقات الذكية فإنها تلك التي تحتوي على وحدة معالجة مركزية؛ تتميز هذه البطاقات بقابليتها لإضافة ومعالجة المعلومات الجديدة، حيث تتم معالجة البيانات وتخزينها لتأخذ مكاناً في البطاقة نفسها، حيث إنها تعمل بنظام (On- line) الذي يمثل الاتصال المباشر[23]. ويبدو أن معظم المشاكل المتعلقة بالتواقيع الالكترونية لها حل في شكل البطاقات الذكية، وليس هناك شك بأن هذه الأخيرة يمكن أن تحمل مثل هذه الكمية من المعلومات، لذلك فإن عامل الثقة يجب أن يكون محل عناية مرضية للمستعملين، فالبطاقة الذكية هي المكان الآمن لأداء العمليات التي يرغب أصحابها في ألا تكون مكشوفة للآخرين على نطاق العالم الافتراضي.

يكون تطبيق التوقيع الإلكتروني على هذه البطاقات على النحو التالي[24]:

أ. إدخال البطاقة التي تحتوي البيانات الخانة بالعمل في الجهاز المخصص لها، وإذا كان التعامل بها عبر شبكة الإنترنت يكون التعامل بإدخال البيانات التي يتطلبها الجهاز (الحاسوب).

(23) عايض راشد عايض المري، مدى حجية الوسائل التكنولوجية الحديثة في إثبات العقود التجارية، رسالة دكتوراه، جامعة القاهرة، مصر، 1998، ص 93، 94.

(24) إبراهيم الدسوقي أبو الليل، توثيق التعاملات الإلكترونية ومسؤولية جهة التوثيق تجاه الغير المضرور، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، الجزء الخامس، دبي، جامعة الإمارات العربية المتحدة، المنعقد مابين 9-11 ربيع الأول 1424هـ الموافق 10-12 مايو 2003م، ص 32، 33.

ب. كتابة الرقم السري المخصص لصاحب البطاقة.
ج. إصدار الأمر للقيام بالعملية المراد إتمامها وبالضغط على المفتاح المخصص يكتمل التعبير عن الإرادة في قبول إتمام العملية.

يستعمل الرمز السري لتعريف وإمضاء العمليات الحسابية عبر شاشة الكومبيوتر دون طبعها على الورق، ثم صبها في دفاتر إلكترونية تتم معالجتها من طرف مصالح المحاسبة، فيتحصل البنك على ميزانية دقيقة تبين له المدفوعات والواردات على المدى القريب والمتوسط، كما يستعمل موظفو البنك البطاقة الذكية مع الرمز السري لإمضاء أوامر الدفع المالية للعملاء التي تمر على أكبر شبكة عالمية (Swift) لنقل الأوامر التي تربط أكثر من 90 % من بنوك العالم، وبناءً على ذلك فإن كل بطاقة بلاستيكية تعمل عن طريق إدخال الرقم السري الذي لا يعلم به سوى العميل الذي يلتزم به سراً، والذي يعد بديلاً عن التوقيع اليدوي.

ثانيا- التوقيع الإلكتروني على الشيكات وسندات الشحن الإلكترونية:

وهي من وسائل الدفع المطورة التي كانت موجودة، لكنها طوِّرت وأصبحت موجودة على دعامة إلكترونية، وحتى هي يمكن أن تؤمن عن طريق التوقيع الإلكتروني، وذلك على الشكل التالي:

1- التوقيع الإلكتروني على الشيكات الإلكترونية:

الشيكات الإلكترونية أو الآلية[25]، هي شيكات تصدرها الحاسبات الإلكترونية أو الآلية (الكومبيوتر)، يستغنى فيها عن التوقيع الكتابي الذي يضعه مصدرها، أي الآمر بسحبها وإحلال رقم سري محل هذا التوقيع، وبذلك يقوم هذا الأخير مقام

(25) حاولت بعض المؤسسات المالية تطويع كافة وسائل الدفع المعروفة لتتناسب مع مقتضيات التجارة الإلكترونية، وقد جرى تطوير استخدام الشيكات الورقية إلى نظام الشيكات الإلكترونية، ويعتمد تحويل الشيكات الورقية إلى الإلكترونية على أساس الدراسات التي تمت في الولايات المتحدة الأمريكية والتي أوضحت أن البنوك تستخدم سنوياً أكثر من 500 مليون شيك مع زيادة أعدادها بنسبة 3 % سنوياً، وعندما أجريت دراسة على إمكانية استخدام الشيكات الإلكترونية اتضح أن تكلفة التشغيل هي 25 سنتاً بدلاً من 79 سنتاً للشيكات الورقية، وهو ما يحقق وفراً يقدر بـ 250 مليون دولار سنوياً في الولايات المتحدة الأمريكية وحدها. للمزيد من التفصيل راجع؛ قاسم النعيمي، التجارة الإلكترونية بين الواقع والحقيقة، مقال منشور على الرابط التالي:

https://www.facebook.com/permalink.php?id=1701839133706 51&story_fbid=1923874684504905

التوقيع العادي، وبواسطته يمكن التعرف على مصدر الشيك[26]. ويعد الشيك الإلكتروني من أهم الأوراق التجارية التي تخضع للمعالجة الآلية إما كلياً أو جزئياً، وهو ملائم للأشخاص الذين لا يملكون بطاقات دفع إلكتروني[27].

2- التوقيع الإلكتروني على سندات الشحن الإلكترونية:

يعد سند الشحن الإلكتروني من أهم وثائق عقد النقل البحري، وظهرت مع انتشار استخدام الوسائل التكنولوجية في مجالات التجارة الدولية، وتتم باستعمال وسيط إلكتروني. لقد تم إقرار اتفاقية الأمم المتحدة لنقل البضائع بالبحر لعام 1978[28] بجواز استخدام الوسائل الإلكترونية، بحيث راعت هذه الاتفاقية دخول صورة جديدة للتوقيع بخلاف التوقيع بخط اليد، وذلك واضح من خلال المادة 14/ 2، حيث استلزمت أن يكون سند الشحن موّقعا، لكنها لم تشترط توقيعه من الحامل نفسه، بل اكتفت بأن يكون هذا التوقيع ممن يفوضه الناقل في ذلك، ومع أنها لم تشترط أن يكون هذا الشخص هو الربان، إلا أنه إذا وقَّع السند ربان السفينة التي يتم عليها الشحن، فالمفروض أن يوقعه لحساب الناقل. كما استلزمت الفقرة الثالثة من نفس المادة، أن يكون التوقيع بخط اليد أو بصورة مطبوعة أو بالتثقيب أو بالختم، أو بالرموز، أو بأي طريقة آلية أو إلكترونية أخرى شريطة ألا يتعارض ذلك مع قانون الدولة التي يصدر فيها سند الشحن، غير أن اتفاقية هامبورغ HAMBURG[29] قد تبنت صراحة التوقيع الإلكتروني في إصدار سندات الشحن لغرض مسايرة متطلبات التجارة الحديثة، التي تحتاج للسرعة أكثر من أجل زيادة وتيرة

(26) إبراهيم الدسوقي أبوالليل، المرجع السابق، ص 33.

(27) مصطفى كمال طه، وائل أنور بندق، الأوراق التجارية ووسائل الدفع الإلكترونية الحديثة، دار الفكر الجامعي، 2009، ص 350، 351.

(28) اتفاقية الأمم المتحدة للنقل البحري للبضائع، الموقعة بهامبورغ في 31 مارس 1978 والتي لم تنضم إليها الجزائر.

(29) والتي يصطلح على تسميتها قواعد هامبورغ، وهي اتفاقية تم التوقيع عليها في 31 مارس 1988، ودخلت حيز التنفيذ في الفاتح من يناير 1992. لمزيد من التفصيل؛ راجع، عايض راشد عايض المري، المرجع السابق، ص 348.

التبادل التجاري، وتجري عملية تحويل البضاعة عن طريق المفتاح الخاص، الذي هو عبارة عن شفرة تقنية مثل التأليف بين مجموعة من الحروف أو الأرقام تكفل صحة وسلامة الإرسال الإلكتروني، أما الناقل فيعطى المفتاح مقام سند الشحن الورقي، ويتم تغيير المفتاح الخاص مع كل تحويل للبضائع، وعلى حائز المفتاح الخاص إخطار الناقل اعتزامه نقل حق البضاعة لشخص آخر، فيقوم الناقل بعد تأكيد الإشعار بإرسال وصف وخصائص البضائع إلى الحائز الجديد المقترح، وعندما يقبل يعطى مفتاحاً خاصاً جديداً، وهذا في كل عملية تحويل للبضاعة، ويترتب عن إصدار مفتاح خاص جديد للحامل الجديد باعتباره في نفس الوضع كما لو كان حصل على سند الشحن الورقي.

يقوم الناقل بتسليم البضاعة للشخص الذي يكشف عن المفتاح الخاص الصحيح عند وجود حائزين لمفاتيح خاصة مخالفة لبعضها، أي يجعل كل حائز في وضع مماثل لحالة حصوله على سند شحن ورقي أصلي، وعليه فالمفتاح الخاص (التوقيع الإلكتروني) يحل محل التوقيع التقليدي في عملية إصدار سند الشحن وفي عملية تداوله[30].

وبذلك يظهر جلياً أهمية التوقيع الإلكتروني في تحديد قيمة المحررات بشكل عام ووسائل الدفع الإلكتروني بشكل خاص، والذي يتوفر على خصائص أخرى تميزه عن التوقيع التقليدي، كونه يقوم أحياناً بالمساهمة في إتمام العمليات التجارية في ظرف وجيز ومتزامن، نعجز فيه حتى عن التفريق بين وقت إبرام وتحرير السند وتوقيعه، ويتخذ صوراً وأشكالاً تُميِّز توقيعا عن توقيع آخر، وتُبقى حجية التوقيع الإلكتروني رهيناً بمدى الثقة والأمان التي يوفرهما التوقيع، واللتان تمنحان الثقة للمتعاملين به وتمدان القاضي بالأساس الذي تستمد منه قناعاته، كما سيتم التطرق إليه لاحقاً.

(30) إبراهيم الدسوقي أبو الليل، المرجع السابق، ص 36.

المطلب الثاني
استخدام التوقيع الإلكتروني وحجيته في الإثبات بالدفع الإلكتروني

لعل ما يهم في هذا المقام، هو تبيان كيفية الاستفادة من التوقيع الإلكتروني في الإثبات بوسائل الدفع الإلكتروني، ومدى حجيته في إثبات تلك المدفوعات. فمتى تكون للتوقيع الإلكتروني حجية في الإثبات في حالة قيام نزاع بين الأطراف المتعاقدة؟ هذا السؤال سنحاول معالجته، من خلال التطرق لاستخدام التوقيع الإلكتروني في الإثبات بالدفع الإلكتروني (الفرع الأول)، ليمكن الحديث بعد ذلك عن حجية التوقيع الإلكتروني في الإثبات بالدفع الإلكتروني (الفرع الثاني).

الفرع الأول
استخدام التوقيع الإلكتروني في الإثبات بالدفع الإلكتروني

تختلف كيفية استخدام التوقيع الإلكتروني في إثبات الدفع الإلكتروني بحسب النزاع القانوني المنبثق عن الإخلال بالعلاقات القانونية الناشئة عن أطراف العقد، فاستخدام التوقيع الإلكتروني في إثبات العلاقة الموجودة بين المستهلك ومؤسسة الإصدار يختلف عن ذلك القائم بين مؤسسة الإصدار والتاجر، وهذا ما سيتم التطرق إليه من خلال التالي:

أولا– في العلاقة بين مؤسسة الإصدار والمستهلك:

إذا ما شك العميل أو المستهلك بوجود خطأ ما يتعلق بعمليات السحب التي تتم من حساب النقد الإلكتروني الخاص به لدى المصدر، يجب عليه إبلاغ جهة الإصدار بذلك وبأسرع وقت ممكن. وفي هذه الحالة، تقوم هذه الأخيرة بالتأكد من صحة ما يزعم به العميل. فإذا ما تأكد صحة ادعاءاته، تقوم الجهة المصدرة بتصحيح الوضع عن طريق تصحيح هذه الأخطاء في الحال، أما إذا تطلب الأمر المزيد من التحقق والفحص للوصول إلى حقيقة الأمر، ففي هذه الحالة تقوم بزيادة رصيد العميل في حدود المبلغ محل النزاع[31]. فإذا جاءت النتيجة النهائية لهذا الفحص بعدم وجود خطأ من جانبها، ولم يقتنع بذلك العميل، ففي هذه الحالة يجب على مؤسسة الإصدار أن تثبت صحة نسبة عمليات السحب التي وقعت إلى العميل. وهنا تظهر أهمية التوقيع الإلكتروني

(31) Pay Cash Terms and Condition, Para. VII, Errors and Disputes, N.(1-2).

في صورة التوقيع باستخدام رقم التمييز أو الرقم السري«Code Pin»؛ ذلك أن كل عميل يختار كلمة أو عبارة خاصة به مكونة من عدد كبير من الحروف والأرقام أو كليهما معاً، ويعد ذلك هو الوضع المثالي لرقم التعريف الشخصي، ويحفظ ذلك كله في مكان آمن أو بطريقة مشفرة لمنع الغير من الاطلاع عليها أو استخدامها[32].

يضاف إلى ذلك، أن وسائل الدفع الإلكتروني لا يمكن تحميلها إلا على أدوات الدفع الخاصة التي تزود مؤسسة الإصدار عملائها بها لتمكينهم من التعامل بوحدات النقد التي تصدرها، لذلك يجب أن تتوفر أداة الدفع ورقم التعريف الشخصي معاً، ليتمكن حامل أداة الدفع من سحب النقود من الحساب المرتبط بهذه الأداة. ومن المفروض أن الحامل الشرعي للأداة، هو الوحيد الذي يعرف رقم التمييز الخاص بالأداة ويتحمل مسؤولية عدم الالتزام بالمحافظة عليه، وكذا إفشائه اتجاه مؤسسة الإصدار[33]. كما أن عملية السحب، لن تكتمل إلا بالتصديق عليها عن طريق الضغط على لوحة المفتاح المخصص لذلك على لوحة المفاتيح – والذي يعد صورة أخرى من صور التوقيع الإلكتروني[34]، بما يدل على موافقته على عملية السحب، وهذا كله إنما يدل على نسبة عمليات السحب للحائز الشرعي لأداة الدفع. ولا يفيد ادعاء هذا الأخير قيام شخص من الغير باستعمال وسائل الدخول الخاصة به، لأن هذا دليل على وجود خطأ من جانبه، والقول بغير هذا يفتح باب النصب والاحتيال في السحب من حساب النقد الإلكتروني لدى المصدر.

لكن قد يحدث أن يقر العميل باستخدام وسائل الدفع الخاصة به، لكن يدعي وجود خطأ في مفردات حسابه من النقد الإلكتروني مثلا، كما لو ادعى وجود زيادة في المبالغ المقيدة عن تلك التي تم سحبها بالفعل. ويدعم هذا الادعاء وجود اختلاف بين ما هو مدون في السجلات الإلكترونية التي تحتفظ بها مؤسسة الإصدار، ففي هذه الحالة تنعقد مسؤولية الأخيرة، بحجة أن الاختلاف يعد دليلاً على وجود خلل في نظام النقد الالكتروني ذاته[35].

(32) محمد أحمد محمد أنور جستنيه، مدى حجية التوقيع الالكتروني في عقود التجارة الالكترونية، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 2005، ص 83.

(33) شريف محمد غنام، محفظة النقود الإلكترونية، رؤية مستقبلية، دار الجامعة الجديدة، الإسكندرية، مصر، 2007، ص 60.

(34) ثروت عبد الحميد، التوقيع الالكتروني، ماهيته، مخاطره، دار الجامعة الجديدة، القاهرة 2007، ص53 وما بعدها؛ محمد سعيد أحمد اسماعيل، أساليب الحماية القانونية لمعاملات التجارة الالكترونية، دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت، لبنان، 2009، ص 184 وما بعدها؛ محمد أحمد محمد أنور جستنيه، المرجع السابق، ص80 وما بعدها.

(35) خالد عبد التواب مبارك، الدليل الإلكتروني أمام القاضي المدني، دار النهضة العربية، مصر، 2001، ص 349.

ثانيا- في العلاقة بين التاجر ومؤسسة الإصدار:

تظهر أهمية التوقيع الإلكتروني في هذا الفرض، في حالة وجود نزاع مثلاً بين التاجر ومؤسسة الإصدار، يتمحور حول مطالبة الأول الثانية استرداد النقود الإلكترونية التي في حيازته فادعت الأخيرة أن هذه النقود مزيفة ولا قيمة لها، هنا يقع عبء إثبات التزييف على مؤسسة الإصدار(36)، وذلك بإثبات أن وحدات النقد هذه قد سبق استعمالها، وأن التاجر قد قصر في التحقق من مدى صحة وأصالة هذه النقود. فإذا فشلت من إثبات زيف النقود وعدم تقصير التاجر، فعليها أن تنفذ التزامها والقاضي بتحويل هذه الوحدات الإلكترونية إلى نقود حقيقية. أما في حالة نجاحها في إثبات ادعاءها، فهنا ينتقل عبء الإثبات إلى التاجر، لكن يمكنه في هذه الحالة التخلص من هذه المسؤولية إذا ما نجح في إثبات أي من هذين الرأيين:

الأول: أنه قام بجميع الإجراءات اللازمة للتأكد من صحة وأصالة وحدات النقد الإلكتروني المستخدمة في عملية الدفع، وذلك بالاتصال بقاعدة البيانات المركزية الخاصة بمؤسسة الإصدار ولم تشر إلى وجود هذه النقود ضمن قائمة النقود المنفقة، وهذه الطريقة تتم بطريقة آلية وتسجل على الذاكرة الخاصة ببرنامج تلقي المدفوعات الخاص بالتاجر. فإذا استطاع إثبات ذلك، فإن هذا يدل على ضعف إجراءات الأمان التي يتخذها المصدر للكشف عن مدى صحة وشرعية النقود الإلكترونية(37)، وفي هذه الحالة تثبت مسؤولية الجهة المصدر اتجاه الحائز عن الإخلال بتنفيذ التزامه.

الثاني: إذا تمكن التاجر من إثبات نسبة هذه النقود إلى جهة الإصدار، ولن يتأت له ذلك إلا بالاعتماد على فكرة التوقيع الرقمي؛ حيث إن كل وحدة من وحدات النقد الإلكتروني تحمل توقيعاً خاصاً بمؤسسة الإصدار(38)، ومختلفاً عن باقي التوقيعات أو يحمل رقماً متسلسلا يختلف عن باقي الأرقام المتسلسلة لوحدات النقد المصدرة الأخرى(39)، وهذا كله حتى ولو لم يبذل العناية الكافية للاتصال بقاعدة البيانات الخاصة بالمصدر.

(36) المادة 323 من القانون المدني: «على الدائن إثبات الالتزام، وعلى المدين إثبات التخلص منه».
(37) أحمد السيد لبيب، الدفع بالنقود الإلكترونية الماهية والتنظيم القانوني دراسة تحليلية مقارنة، دار الجامعة الجديدة، الإسكندرية، مصر، 2009، ص 369.
(38) محمد أحمد محمود إسماعيل، مدى حجية التوقيع الإلكتروني في عقود التجارة الإلكترونية، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، 2005 ، ص162.
(39) محمد أحمد محمد أنور جستنيه، المرجع السابق، ص245.

كما يطلب التاجر من الجهة المصدرة تقديم مفاتيح التشفير الخاصة بها، بالإضافة إلى تقديم قائمة الأرقام المسلسلة للنقود الإلكترونية المصدرة، وذلك في سبيل إثبات صلاحية وشرعية هذه النقود(40).

وتجدر الإشارة إلى أن التوقيع الإلكتروني في بعض النظم يستعمل للتحقق من وحدات النقد الإلكتروني، كما هو معمول به في نظام Digicash إذ تقوم مؤسسة الإصدار، أثناء عملية الإصدار بتوقيع هذه الوحدات باستعمال مفتاح التشفير الخاص Private Key، فإذا تلقى التاجر هذه الوحدات من المستهلك، فإنه يقوم بالتحقق من الأرقام المسلسلة الخاصة بها، وكذا التحقق من صحة التوقيع الإلكتروني الذي تحمله، وذلك باستعمال مفتاح التشفير Public Key وثبت له صحة هذا التوقيع، فإن ذلك دليل على صحة وحدات النقد وبالتالي صحة عملية الدفع(41).

الفرع الثاني

حجية التوقيع الإلكتروني في الإثبات بالدفع الإلكتروني

تكتسي الحجية القانونية للتوقيع الإلكتروني أهمية بالغة في الإثبات الإلكتروني، وبالتالي في حماية حقوق المتعاملين عبر الوسائط الإلكترونية، لذلك كانت محل اهتمام المشرعين سواءً على الصعيد الدولي أو على الصعيد الوطني، إذ تتجه مختلف التشريعات الوطنية والدولية نحو الاعتراف بالتوقيع الإلكتروني باعتباره نظيراً للتوقيع الخطي، ومن ثم يحظى بنفس الحجية في الإثبات.

وسيتم البحث في هذا المقام، الجهود الدولية في تدعيم حجية الإثبات للتوقيع الإلكتروني وموقف بعض التشريعات الوطنية من حجية الإثبات للتوقيع الإلكتروني، حيث اختلفت التشريعات الوطنية المقارنة في مدى إعطائها الحجية للتوقيع الإلكتروني.

(40) وذلك تأسيساً على أنه يجوز طلب الخصم بتقديم ورقة موجودة تحت يده، كلما كانت هذه الأخيرة تثبت حقاً لطالبها، وتغلب هنا مصلحته على مصلحة الخصم في الاحتفاظ بها. سليمان مرقس، أصول الإثبات وإجراءاته في المواد المدنية في القانون المصري مقارناً بتقنينات سائر البلاد العربية، ج1، الأدلة المطلقة، عالم الكتب، القاهرة، 1987، ص 40.

(41) أحمد السيد لبيب إبراهيم، المرجع السابق، ص 370.

أولا- الجهود الدولية في تدعيم حجية الإثبات للتوقيع الإلكتروني:

نظراً لأهمية وحساسية التوقيع الإلكتروني في الإثبات، فإنه كان محل اهتمام المنظمات الدولية والتي بذلت جهوداً صبت نحو إقرار حجية للتوقيع الإلكتروني، ومن هذه المنظمات سيقتصر الحديث على منظمة الأمم المتحدة والاتحاد الأوروبي.

1- موقف المشرع الأوروبي من حجية التوقيع الإلكتروني:

دخل توجيه التجارة الإلكترونية الخاصة بالاتحاد الأوروبي (DirectiveEUE-Commerce) حيز التنفيذ في 17 يوليو 2000، وأصبح منذ نفاذه لازماً على الدول الأعضاء في الاتحاد الأوروبي (Européen Union) أن تطبقه بحلول 17 يناير من عام 2002. وقد كان الهدف من إصداره هو ضمان حرية حركة المعلومات والخدمات المعلوماتية، وتنشيط حركة ونمو التجارة الإلكترونية بين الدول الأعضاء[42]. كما صدر التوجيه الأوروبي الخاص بالتوقيع الإلكتروني، إذ أنه وفي عام1998 بدأت عدة دول أوروبية في إصدار تشريعات تتعلق بالتوقيع الإلكتروني المستخدم في التعاملات التجارية[43]، وقد خشي الاتحاد الأوروبي من وجود فروقات واختلافات بين تلك القوانين، لذلك سعى إلى إيجاد أساس موحد للوصول إلى توحيد تلك التشريعات، لذلك أصدر الاتحاد الأوروبي التوجيه الخاص بالتوقيع الإلكتروني للوصول إلى هذه الغاية .وأوجب الاتحاد الأوروبي على جميع الدول الأعضاء، تطبيق وتطويع قوانينها الداخلية بما يتوافق مع هذا التوجيه، بعد ثمانية عشر شهراً من صدور هذا التوجيه، ولقد نصت المادة 5/ 2 من التوجيه الأوروبي المتعلق بالتوقيع الإلكتروني على أنه :» يجب على الدول الأعضاء في الاتحاد الأوروبي مراعاة التأثير القانوني للتوقيع الإلكتروني وقبوله كحجة في الإثبات، لا يمكن أن يرفض لأحد الأسباب الآتية:

- لأن التوقيع قد قدم في شكل إلكتروني.
- لأنه لم يوضع على شهادة معتمدة.
- لأنه لم يوضع على شهادة معتمدة ومسلمة من أحد مقدمي خدمات التصديق على الشهادات المعتمدين.

(42) Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur («directive sur le commerce électronique») .Disponible sur:

http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32000L0031

(43) محمد سعيد أحمد إسماعيل، المرجع السابق، ص162.

– لأنه لم ينشأ بأمر بإنشاء هذا التوقيع»[44].

إن تحليل هذه الفقرة، يتطلب الإشارة إلى أمرين مهمين من الناحية العملية:

الأول: منحت هذه الفقرة التوقيع الخطي نفس الحجية القانونية الممنوحة للتوقيع الإلكتروني المقدم، أي الذي تم اعتماده والتصديق عليه من قبل الجهة المرخص لها بهذا العمل.

الثاني: لم تستخدم هذه الفقرة مصطلح التوقيع الإلكتروني المقدم، وبناء عليه يمكن تطبيق هذه المادة على التوقيع الإلكتروني البسيط قبل اعتماده من قبل مقدمي خدمات التصديق المعتمدين لدى الدولة. ومعنى ذلك، أنه يتعين قبول هذا التوقيع الإلكتروني البسيط كدليل إثبات، ولكن يجب أن نأخذ في الحسبان أنه عند حدوث ازدواجية في هذه الحالة بين توقيعين إلكترونيين، أحدهما بسيط والآخر مقدم، تكون الأولوية لهذا الأخير لكونه يتمتع بعناصر أمان يمكن أن تمنحه هذه الأولوية[45].

لقد أضفى هذا التوجيه على التوقيع الإلكتروني نفس الحجية في الإثبات الممنوحة للتوقيع العادي، كما تبنى مفهوماً واسعاً للتوقيع الإلكتروني يشمل جميع الصور التي يمكن أن يتخذها، والتي من شأنها تحديد صاحب التوقيع وتمييزه عند استخدام تقنيات الاتصال الحديثة.

2- قانون اليونسترال النموذجي للتوقيع الإلكتروني:

تعرض قانون اليونسترال النموذجي الخاص بالتجارة الإلكترونية لسنة[46]1996

(44) Art. 5: Effets juridiques des signatures électroniques:» b) soient recevables comme preuves en justice. … 2. Les États membres veillent à ce que l'efficacité juridique et la recevabilité comme preuve en justice ne soient pas refusées à une signature électronique au seul motif que:
la signature se présente sous forme électronique ou
qu'elle ne repose pas sur un certificat qualifié ou
qu'elle ne repose pas sur un certificat qualifié délivré par un prestataire accrédité de service de certification ou
qu>elle n>est pas créée par un dispositif sécurisé de création de signature».

(45) سعيد السيد قنديل، التوقيع الإلكتروني، دار الجامعة الجديدة، مصر، 2006 ، ص 55.

(46) اعتمد في 12 جويلية1996. يهدف القانون النموذجي بشأن التجارة الإلكترونية، إلى التمكين من مزاولة التجارة باستخدام وسائل إلكترونية وتيسير تلك الأنشطة التجارية، من خلال تزويد المشرعين الوطنيين بمجموعة قواعد مقبولة دوليا ترمي إلى تذليل العقبات القانونية وتعزيز القدرة على التنبّؤ بالتطورات القانونية في مجال التجارة الإلكترونية. والغرض من قانون التجارة تحديدا، هو التغلّب على العقبات الناجمة عن الأحكام القانونية التي قد لا تكون متنوّعة تعاقديا عن طريق معاملة المعلومات الورقية والإلكترونية معاملة متساوية. وهذه المساواة في المعاملة مقوّم أساسي للتمكّن من استخدام الخطابات اللاورقية، مما يعزّز من الكفاءة في التجارة الدولية.

إن هذا القانون النموذجي، هو أول نص تشريعي يعتمد المبادئ الأساسية لعدم التمييز والحياد =

للشروط الواجب توفرها في التوقيع الإلكتروني، والمتمثلة في استخدام إحدى الطرق لتعيين هوية الشخص الموقع والتعبير عن موافقته على التصرف محل التوقيع وأن تكون هذه الطريقة جديرة بالثقة. إلا أنه وبصدور قانون الأمم المتحدة النموذجي بشأن التوقيعات الإلكترونية بتاريخ 05/06/2001 [47]، جاءت المادة السادسة[48] منه لتنص على أنه: «حيثما يشترط القانون وجود توقيع من شخص، يعد ذلك الشرط مستوفياً بالنسبة إلى رسالة البيانات إذا استخدم توقيع إلكترونيا موثوقا به بالقدر المناسب للغرض الذي أنشئت وأبلغت من أجله رسالة البيانات، في ضوء كل الظروف بما في ذلك أي اتفاق ذي صلة...». وتضيف الفقرة الثالثة من نفس المادة: «...يعتبر التوقيع الإلكتروني موثوقاً به لغرض الوفاء بالاشتراط المشار إليه في الفقرة الأولى:

- إذا كانت بيانات إنشاء التوقيع مرتبطة، في السياق الذي تستخدم فيه، بالموقع دون أي شخص آخر.
- إذا كانت بيانات إنشاء التوقيع خاضعة، وقت التوقيع، لسيطرة الموقع دون أي شخص آخر.
- إذا كان أي تغيير في التوقيع الإلكتروني، يجري بعد حدوث التوقيع، قابلاً للاكتشاف.
- إذا كان الغرض من اشتراط التوقيع قانوناً، هو تأكيد سلامة المعلومات التي يتعلق بها التوقيع وكان أي تغيير يجري في تلك المعلومات بعد وقت التوقيع

= التكنولوجي والتكافؤ الوظيفي ،التي يراها الكثيرون أسس قانون التجارة الإلكترونية الحديثة. ويكفل مبدأ عدم التمييز، وألاّ يُنكر الأثر القانوني لأي وثيقة أو تُنفى صحتها أو قابليتها للإنفاذ لمجرّد كونها في شكل إلكتروني. أما مبدأ الحياد التكنولوجي فيلزم باعتماد أحكام محايدة بشأن التكنولوجيا المستخدمة. وفي ضوء التقدم التكنولوجي السريع، فإن القواعد المحايدة تهدف إلى استيعاب ما يطرأ من تطوّرات في المستقبل دون الاضطلاع بمزيد من الأعمال التشريعية. ويحدّد مبدأ التكافؤ الوظيفي معايير يمكن بموجبها اعتبار الخطابات الإلكترونية مكافئة للخطابات الورقية. ويبين المبدأ بوجه خاص المتطلّبات المحدّدة التي ينبغي أن تستوفيها الخطابات الإلكترونية لكي تحقّق ذات المقاصد والوظائف التي تسعى إلى بلوغها بعض المفاهيم المعمول بها في النظام الورقي التقليدي – من قبيل المستندات «المكتوبة» و«الأصلية» و«الموقّعة» و«المسجَّلة». منشور على الموقع:

http://www.uncitral.org/uncitral/ar/uncitral_texts/electronic_commerce/1996Model.html

(47) Loi type de la CNUDCI sur les signatures électroniques et Guide pour son incorporation 2001, Disponible sur
http://www.uncitral.org/pdf/french/texts/electcom/ml-elecsign-f.pdf

(48) Art. 6. Satisfaction de l'exigence de signature : «1. Lorsque la loi exige la signature d'une certaine personne, cette exigence est satisfaite dans le cas d'un message de données s'il est fait usage d'une signature électronique dont la fiabilité est suffisante au regard de l'objet pour lequel le message de données a été créé ou communiqué, compte tenu de toutes les circonstances, y compris toute convention en la matière»

قابلاً للاكتشاف...»[49].

ومؤدى هذا النص، أن المشرع قد أقام قرينة لمصلحة من يستند إلى التوقيع الإلكتروني مفادها أنه متى كنا بصدد حالة من الحالات المشار إليها، فإن هذا التوقيع يتمتع بالحجية وقابلاً للتعويل عليه في الإثبات، مع ملاحظة أن الحالات المذكورة ليست واردة على سبيل الحصر، ومن تم يكون لمن يتمسك بالتوقيع الإلكتروني في غير هذه الحالات، الحق في إثبات قابليته للتعويل عليه بكافة الطرق. وبالمقابل نجد أن النص قد منح ذوي الشأن، الحق في إثبات عدم قابلية التوقيع الإلكتروني للتعويل عليه حتى ولو استوفى المعايير المنصوص عليها فيه، باعتبار أن قرينة قابلية التوقيع الإلكتروني للتعويل عليه تعد قرينة بسيطة على صحة التوقيع الإلكتروني وعدم تحريفه بعد إنشائه، ومن تم يمكن نقضها بالدليل العكسي، فما ورد بالمادة 6/3 من هذا القانون لا يحول دون قدرة أي شخص على تقديم الدليل بكافة الطرق على قابلية التعويل على التوقيع الالكتروني أو عدم قابليته لذلك[50].

ثانيا- موقف بعض التشريعات الداخلية من حجية الإثبات بالتوقيع الإلكتروني:

بالإضافة إلى الجهود الدولية في تدعيم حجية الإثبات للتوقيع الإلكتروني، دأبت الدول سواء الغربية أو العربية على وضع قوانين خاصة تتعلق بالتوقيع الإلكتروني

(49) Art. 6.3:»…3. Une signature électronique est considérée fiable en ce qu'elle satisfait à l'exigence indiquée au paragraphe 1 si:

a) Les données afférentes à la création de signature sont, dans le contexte dans lequel elles sont utilisées, liées exclusivement au signataire;

b) Les données afférentes à la création de signature étaient, au moment de la signature, sous le contrôle exclusif du signataire;

c) Toute modification apportée à la signature électronique après le moment de la signature est décelable; et

d) Dans le cas où l'exigence légale de signature a pour but de garantir l'intégrité de l'information à laquelle elle se rapporte, toute modification apportée à cette information après le moment de la signature est décelable».

(50) Art. 6.4:»Le paragraphe 3 ne restreint pas la possibilité pour toute personne:

a) D'établir de toute autre manière, aux fins de satisfaire l'exigence visée au paragraphe 1, la fiabilité de la signature électronique; ni

b) D'apporter des preuves de la non-fiabilité de la signature électronique».

أو وضع تعديلات في قوانينها الداخلية بما يتلاءم وهذه التطورات، ومن بين هذه التشريعات نذكر:

أ- التشريعات الغربية:

وسيقتصر الحديث في هذا المقام، على التشريعين الفرنسي والأمريكي:

1- موقف المشرع الفرنسي من التوقيع الإلكتروني:

لقد طبق المشرع الفرنسي الأحكام والتوجيهات الواردة بالتوجيه الأوروبي رقم 99-93 بشأن التوقيع الإلكتروني، لا سيما المادة 5/2[51]، التي تنص على أن تلتزم الدول الأعضاء في الاتحاد الأوروبي بتطبيق أحكام هذا التوجيه، وضرورة منح التوقيع الإلكتروني الحجية القانونية التي يتمتع بها التوقيع الخطي. ويلاحظ أن هذه المادة، تتعلق فقط بالتوقيع الإلكتروني الموثق أو ما يعرف بالتوقيع الإلكتروني المتقدم التي تعتمد على شهادة التوثيق، واتخاذ الإجراءات التي توفر الأمن لبيانات التوقيع[52]. واستجابة للمادة 13 من هذا التوجيه، والتي تلزم الدول الأعضاء في الاتحاد الأوروبي بتوفيق أوضاعها التشريعية بما يتفق مع أحكام هذا التوجيه في موعد لا يتعدى 15 يوليو 2001، قام المشرع الفرنسي بإدخال مجموعة من التعديلات، أهمها صدور القانون الفرنسي رقم 2000-230 والذي منح الحجية للتوقيع الإلكتروني[53] وبتاريخ 30 مارس 2001 صدر المرسوم رقم 01/272 والذي يتضمن القواعد والأحكام بشأن حماية وأمن بيانات التوقيع الإلكتروني[54]، والذي عدل المادة 1416/4 من القانون

(51) Art. 5.2:» Les États membres veillent à ce que l'efficacité juridique et la recevabilité comme preuve en justice ne soient pas refusées à une signature électronique au seul motif que:
la signature se présente sous forme électronique, ou
- quelle ne repose pas sur un certificat qualifié, ou
- qu'elle ne repose pas sur un certificat qualifié délivré par un prestataire accrédité de service de certification, ou
- qu'elle n'est pas créée par un dispositif sécurisé de création de signature.

(52) سمير حامد عبد العزيز الجمال، التعاقد عبر تقنيات الاتصال الحديثة (دراسة مقارنة)، دار النهضة العربية، القاهرة، مصر، 2006، ص 210.

(53) Loi N° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique (JORF n°62 du 14 mars 2000). Disponible sur: http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000399095&dateTexte=&categorieLien.

(54) 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 (JORF n°0077 du 31 mars 2001), (Dernière modification : 9 juillet 2009) . Disponible sur:

المدني الفرنسي، والتي أصبحت تنص على ما يلي: «وإذا ما تم التوقيع في الشكل الإلكتروني، وجب استخدام وسيلة موثوق بها لتمييز هوية صاحبه واتجاه إرادته للالتزام بالتصرف القانوني المرتبط به، ويفترض أن الوسيلة المستخدمة موثوق بها إلى أن يثبت العكس»[55]. وبتاريخ 18 أبريل 2002، صدر أيضاً المرسوم رقم 02–535 الذي تضمن القواعد والأحكام الخاصة بحماية وأمن المنتجات وأنظمة المعلومات[56].

كما صدر بتاريخ 21 جوان 2004 القانون رقم 04/75 الخاص بالثقة في الاقتصاد الرقمي (LCEM) الذي جاء لتكميل النظام التشريعي المعتمد عن طريق قانون 13/03/2000 الذي ينص أن الكتابة لازمة لصحة العقد. كما أكد القانون 04–75 على الاعتراف بالمحرر الإلكتروني، ويظهر ذلك من خلال المادة 1108/1 من القانون المدني الفرنسي والتي تنص على أنه: «عندما يستلزم محرر كتابي لصحة عمل قانوني، يمكن أن سيتحدث ويحفظ بطريقة إلكترونية»[57]. فالمشرع الفرنسي لم يقم بتنظيم الإثبات بالوسائل الحديثة، ومنها التوقيع الإلكتروني بموجب نص خاص منفصل عن نصوص القانون المدني، وإنما تبنى مفاهيم عامة بهدف استيعاب ما يطرأ على وسائل الإثبات من تطورات. كما أنه منح التوقيع الإلكتروني، ذات الحجية الممنوحة للتوقيع الخطي التقليدي متى كان الوسيلة المستخدمة في إنشائه موثوقاً بها.

http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000005630796&dateTexte=20020418

(55) Art. 1616-4 du code civil et relatif à la signature électronique «… Lorsqu'elle 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 électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'Etat». Disponible sur:
http://www.marche-public.fr/Marches-publics/Textes/Codes/Code-civil/code-civil-article-1316.htm

(56) 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, Dernier modification le Décret n°2010-1630 du 23 décembre 2010. Disponible sur:
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000005632663

(57) Art. 1108-1(Créé par Loi n°2004-575 du 21 juin 2004 - art. 25 JORF 22 juin 2004):»Lorsqu'un écrit est exigé pour la validité d'un acte juridique, il peut être établi et conservé sous forme électronique dans les conditions prévues aux articles 1316-1 et 1316-4 et, lorsqu'un acte authentique est requis, au second alinéa de l'article 1317. Lorsqu'est exigée une mention écrite de la main même de celui qui s'oblige, ce dernier peut l'apposer sous forme électronique si les conditions de cette apposition sont de nature à garantir qu'elle ne peut être effectuée que par lui-même». Disponible sur:
http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006436118&cidTexte=LEGITEXT000006070721

وتماشياً مع نهج التوجيه الأوروبي، فقد فرق بين نوعين من التوقيع الإلكتروني: الأول هو التوقيع الإلكتروني الموثق أو الآمن[58]، وهو ما يتم عن طريق مقدم خدمات التوثيق ويُدوَّن في شهادة معتمدة من قبله، فهذا التوقيع تسري في شأنه القرينة الواردة في المادة 1316/4، حيث يفترض أن الوسيلة المستخدمة لتمييز هوية صاحبه واتجاه إرادته للالتزام بالتصرف القانوني المرتبط به وسيلة موثوق بها، ويفترض نسبة العملية القانونية إلى الشخص الوارد اسمه في الشهادة. فالثقة هي الأساس الذي يعتمد عليه نظام التوقيع الإلكتروني، لا سيما فيما يتعلق بجدارة السلطات القائمة على خدمات التوثيق[59]، مع ملاحظة أن هذه القرينة ليست قاطعة بل بسيطة يمكن أن تقبل العكس[60]. والتوقيع الثاني هو التوقيع الإلكتروني البسيط[61]، وهو الذي لا تتوافر فيه الشروط الخاصة بالتوقيع الموثق، وفي هذه الحالة لا يستفيد من يستند إليه من قرينة الموثوقية، وإنما عليه أن يثبت أن الوسيلة المستخدمة في التوقيع موثوق بها[62].

كما أن القضاء الفرنسي أقر واعترف بصلاحية التوقيع الإلكتروني وحجيته في الإثبات من خلال مجموعة من الأحكام، وكان هذا أول اجتهادي قضائي يعترف بالتوقيع الإلكتروني[63]، منها الحكم الصادر عن محكمة مونبلييه Montpellier في 09/04/1987[64] بخصوص الاعتراف بحجية التوقيع الإلكتروني الناشئ عن

(58) Art. 1 (Décret n°2001- 272 du 30 mars 2001): …2. Signature électronique sécurisée : une signature électronique qui satisfait, en outre, aux exigences suivantes :

- être propre au signataire ;
- être créée par des moyens que le signataire puisse garder sous son contrôle exclusif ;
- garantir avec l'acte auquel elle s'attache un lien tel que toute modification ultérieure de l'acte soit détectable .

(59) ثروت عبد الحميد، المرجع السابق، ص 178.

(60) محسن عبد الحميد البيه، قانون الإثبات في المواد المدنية والتجارية، مكتبة الجلاء الجديدة، المنصورة،1997، ص 178.

(61) Arti. 1 (Décret n°2001-272 du 30 mars 2001): Au sens du présent décret, on entend par :

1. Signature électronique : une donnée qui résulte de l'usage d'un procédé répondant aux conditions définies à la première phrase du second alinéa de l'article 1316-4 du code civil…».

(62) خالد عبد التواب، المرجع السابق، ص 178.

(63) طوني عيسى، حول الدفع الإلكتروني بالبطاقة الائتمانية في شبكة الانترنت، الجديد في أعمال المصارف من الوجهتين القانون والاقتصادية، أعمال المؤتمر العلمي السنوي لكلية الحقوق بجامعة بيروت العربية، ج1، الجديد في التقنيات المصرفية، منشورات الحلبي الحقوقية، ص 246.

(64) مذكور عند؛ كيلاني عبد الراضي محمود، النظام القانوني لبطاقات الوفاء والضمان، دار النهضة العربية، مصر، 1998، ص 157 وما بعدها.

استخدام البطاقة والرقم السري، حيث جاء في حيثيات هذا الحكم: «أن البنك يستطيع إثبات مديونية العميل من خلال تسجيل الآلات التي ما كانت لتتم باستخدام مزدوج لكل من البطاقة والرقم السري معاً، ما لم يدع الحامل وجود خلل في سير نظام المعلوماتية ولم يخطر الحامل عن فقد رقمه السري». وقد تم تأييد هذا الحكم بتاريخ 1989/11/08 من قبل محكمة النقض الفرنسية(65)، والذي أقر بصلاحية التوقيع الرقمي الذي يتم بواسطة شخص من خلال الرقم المستخدم في البطاقات الرقمية وهذا بالنسبة للاتفاقات المتعلقة بالإثبات.

ويتفق مسلك القضاء الفرنسي، مع ما هو مقرر بشأن الدفع بوسائل الدفع الإلكتروني الذي يتم باستخدام البطاقة والرقم السري معاً، وباعتباره صادراً من العميل نفسه، وعليه أن يتحمل جميع النتائج التي تترتب عن الاستعمال غير المشروع لحسابه أو لأداة الدفع الخاصة به من قبل شخص غير مأذون له بذلك، حتى وان لم يثبت خطأ من جانبه في حفظ وسائل الدخول الخاصة به، ما لم يدعِ وجود خلل في نظام النقد ذاته، حيث ينتقل عبء الإثبات إلى مؤسسة الإصدار، ويجبَ عليها التخلص من المسؤولية في هذه الحالة، وأن يثبت دقة الدفع من الناحية الفنية، من خلال توضيح الإجراءات التي تتخذها لمنع أو اكتشاف أوجه القصور التي يمكن أن تعتريه، بالإضافة إلى إثبات عملية الدفع قد تم تنفيذها وتسجيلها بطريقة صحيحة.

2- موقف المشرع الأمريكي من التوقيع الإلكتروني:

تعد الولايات المتحدة الأمريكية من الدول السباقة لوضع تشريعات تعترف بالتوقيع الإلكتروني، ومنحه الحجية القانونية في الإثبات شأنه شأن التوقيع اليدوي، وكان لولاية «يوتا» «UTAH» السبق في هذا المجال بإصدارها في الأول من مايو 1995 قانون التوقيع الرقمي(66)، يقر بصحة التوقيع إذا حصل: «... بالارتكاز إلى مفتاح عمومي وارد في شهادة مصادقة صادرة عن سلطة التصديق». بمعنى آخر، إذا استخدمت في المصادقة على صحة المستندات

(65) مذكور عند؛ كيلاني عبد الراضي، المرجع السابق، ص 158.

(66) In addition, the National Conference of Commissioners on Uniform State Laws («NCCUSL») is completing a project to develop a Uniform Electronic Transactions Act («UETA») in the U.S - See more at: Thomas J. Smedinghoff and Ruth Hill Bro of Baker & McKenzie LLP, Electronic Signature Legislation, Disponible à http://corporate.findlaw.com/business-operations/electronic-signature-legislation.html

المعلوماتية آلية ترقيم التوقيع، أي تشفيره بواسطة مفاتيح عمومية من قبل هيئة مختصة لهذه الغاية[67]، لتضفي بمقتضاه على التوقيع الإلكتروني الحجية في الإثبات، طالما تم عن طريق نظام المفتاح العام، وتم توثيقه بشهادة إلكترونية. بعد ذلك حذت عدة ولايات حذو ولاية يوتا منها: ولاية كاليفورنياCalifornie، فيرجينياVirginia، جورجياGeorgia وتكساسTexasبإصدار تشريعات أضفت بمقتضاها الحجية القانونية على التوقيع الإلكتروني طالما استوفى الشروط والمعايير التي حددتها هذه التشريعات[68]، بينما اكتفت ولايات أخرى في إضفائها الحجية القانونية على التوقيع الإلكتروني بأي توثيق إلكتروني يعززه، كولاية فلوريدالFlorida وماساشيسات Massachusetts. وقد بلغ عدد الولايات الأمريكية التي أصدرت تشريعات تعترف بالتوقيع الإلكتروني وتمنحه الحجية في الإثبات الخمسين (50) ولاية – وهي العدد الإجمالي للولايات المتحدة الأمريكية، بالإضافة إلى التشريع الفيدرالي الخاص بالتوقيع الإلكتروني ضمن نطاق التجارة الداخلية والعالمية الصادر في 30 جوان [69]2000، هذا القانون يعتمد مفهوماً مماثلاً للتوقيع الإلكتروني ويساويه بالتوقيع البياني بخط اليد إذا حصل على هذا الشكل[70].

(67) طوني عيسى، المرجع السابق، ص 248.

إن هذا القانون معرف باسم Utah Digital Signature Act الذي عدل العنوان رقم 46 في الفصل الثالث من قانون ولاية Utah. وقد ورد تعريف التوقيع الإلكتروني بالانجليزية كالآتي:

Where a rule of law requires a signature, or provides for certain consequences in the absence of a signature, that rule is satisfied by a digital signature if: 1. That digital signature is verified by reference to the public Key listed in a valid certificate issued y a licensed certification authority», (Utah Digital Signature Act, EDI Law Review, 1995, vol 2,n.3). Jonathan E. Stern, The Electronic Signatures in Global and National Commerce Act, Berkeley Technology Law Journal, Volume 16 | Issue 1 Article 21, P.7, Disponible sur:

http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1316&context=btlj

(68) إبراهيم الدسوقي أبو الليل، المرجع السابق، ص 1024.

Voir plus, E-signature Law, , Disponible sur: http://www.e-signature.com/e-signature-law/

(69) سمير حامد عبد العزيز الجمال، المرجع السابق، ص 211.

The Electronic Signatures in Global and National Commerce Act (E-Sign Act.), Disponible sur:

https://www.fdic.gov/regulations/compliance/manual/pdf/X-3.1.pdf

(70) الاسم الأساسي لهذا القانون بالانجليزية: Act Commerce Electronic Signatures in Global and National
راجع النص الكامل لهذا القانون، على الرابط التالي: yrarbil/moc.semityu.www

ب- التشريعات العربية:

رغم أن هناك عدة دول عربية كانت سباقة لوضع نصوص تتعلق بالتوقيع الإلكتروني، منها التشريع التونسي والإماراتي والأردني، إلا أنه سوف يقتصر الحديث في هذا المقام على التشريعين المصري والجزائري.

1-موقف المشرع المصري من التوقيع الإلكتروني:

يعد موقف المشرع المصري الأكثر وضوحاً في الاعتراف بحجية التوقيع الإلكتروني في الإثبات، إذ نصت المادة 14 من القانون رقم 15 لسنة 2004: «للتوقيع الإلكتروني في نطاق المعاملات المدنية والتجارية والإدارية ذات الحجية المقررة للتوقيعات في أحكام قانون الإثبات في المواد المدنية والتجارية إذا روعي في إنشائه وإتمامه الشروط المنصوص عليها في هذا القانون والضوابط الفنية والتقنية التي تحددها اللائحة التنفيذية لهذا القانون». كما نصت المادة 18 من نفس القانون على أنه:»يتمتع التوقيع الإلكتروني والكتابة الإلكترونية والمحررات الإلكترونية بالحجية في الإثبات إذا ما توافرت الشروط الآتية:

- ارتباط التوقيع الإلكتروني بالموقع وحده دون غيره .
- سيطرة الموقع وحده دون غيره على الوسيط الإلكتروني.
- إمكانية كشف أي تعديل أو تبديل في بيانات المحرر الإلكتروني أو التوقيع الإلكتروني .
- وتحدد اللائحة التنفيذية لهذا للقانون الضوابط الفنية والتقنية اللازمة لذلك».

ويتحقق ارتباط التوقيع الإلكتروني بشخص الموقع، إذا كان هذا التوقيع مرتبطاً بشهادة تصديق إلكتروني معتمدة ونافذة المفعول وصادرة عن جهة تصديق مرخص لها ومعتمدة قانوناً، وفي مصر هي هيئة تنمية صناعة تكنولوجيا المعلومات. أما إمكانية الكشف عن أي تعديل أو تبديل في بيانات التوقيع الإلكتروني فيتم من الناحية الفنية والتقنية باستخدام شفرة المفتاح العام والخاص، ومضاهاة شهادة التصديق الإلكتروني وبيانات إنشاء التوقيع الإلكتروني بأصل هذه الشهادة وتلك البيانات أو بأية وسيلة أخرى مشابهة[71].

(71) راجع المواد 2، 3، 4، 7، 9، 11 من اللائحة التنفيذية رقم 15 لسنة 2004، وكذلك القرار الوزاري رقم 109 لسنة 2005 بتاريخ 15/ 5/ 2005، بإصدار اللائحة التنفيذية لقانون التوقيع الإلكتروني وإنشاء هيئة تنمية صناعية تكنولوجيا للمعلومات . منشور على الموقع:

http://www.laweg.net/Default.aspx?action=LegsTakenForm&FIID=1488

ومفاد النصوص السابقة أن يكون للتوقيع الإلكتروني نفس حجية التوقيع الخطي في الإثبات، وقد نصت المادة 14 من قانون الإثبات: "يعد المحرر العرفي صادرا ممن وقّعه ما لم ينكر صراحة ما هو منسوب إليه من خط أو إمضاء أو ختم أو بصمة..."[72]. وهذا يعني أن من يحتج عليه بورقة عرفية باعتبارها صادرة ومُوقّعة منه، يجب عليه إذا لم يكن مُسلِّماً بذلك أن ينكر توقيعه إنكارا صريحاً. فإذا لم يذكر صاحب التوقيع توقيعه صراحة، أو اعترف به، كان للورقة العرفية حجة بصدورها ممن نسبت إليه كالورقة الرسمية تماماً. أما إذا أنكر صاحب التوقيع توقيعه صراحة، فإنه يتعين على القاضي في هذه الحالة أن يتحقق أولاً من صدور هذا التوقيع ممن يحتج به عليه، فإذا ثبت له ذلك، كان لهذا التوقيع حجية كما لو اعترف به صاحبه[73].

2- موقف التشريع الجزائري من التوقيع الإلكتروني:

لقد نصت المادة 327 من القانون المدني المعدلة بموجب القانون رقم 05/10 على اعتماد التوقيع الإلكتروني، وفقاً لشروط حددتها المادة 323 مكرر، والتي بموجبها يعتبر التوقيع الإلكتروني كالتوقيع التقليدي الورقي بشرط إمكانية التأكد من هوية الشخص المُوقِّع، وأن يكون معداً ومحفوظاً في ظروف تضمن سلامته. هذا ما أكده القانون 15/04، حينما فرق بين التوقيع الإلكتروني العادي والتوقيع الإلكتروني الموصوف، وهذا تماشياً مع نهج المشرع الفرنسي والتوجيه الأوروبي، ومنح هذا الأخير حجية كالتوقيع المكتوب[74]، كما أوجب أن تكون آلية إنشاء التوقيع الإلكتروني الموصوف مؤمنة، ولا يتأت ذلك إلا بتوافر الشروط التالية[75]:

«يجب أن تضمن بواسطة الوسائل التقنية والإجراءات المناسبة، على الأقل، ما يأتي:

- ألاّ يمكن عمليا مصادفة البيانات المستخدمة لإنشاء التوقيع الإلكتروني إلا مرّة واحدة، وأن يتم ضمان سريتها بكل الوسائل التقنية المتوفرة وقت الاعتماد،
- ألاّ يمكن إيجاد البيانات المستعملة لإنشاء التوقيع الإلكتروني عن طريق

(72) قانون رقم 25 لسنة 1968 بإصدار قانون الإثبات في المواد المدينة والتجارية معدلا بالقانون 23 لسنة 1992والقانون 18 لسنة 1999 (ج.ر العدد 22 الصادر في 30 / 5 / 1968. منشور على الموقع: http://ar.jurispedia.org/index.php

(73) عبد الرزاق أحمد السنهوري، الوسيط في شرح القانون المدني الجديد، نظرية الالتزام بوجه عام، الجزء الثالث، دار إحياء التراث العربي، بيروت، 1968، ص 192 وما بعدها. سليمان مرقس، المرجع السابق، ص 206 وما بعدها.

(74) المادة 08 من القانون 15/04 –السالف ذكره–.

(75) المادة 11 من نفس القانون.

الاستنتاج وأن يكون هذا التوقيع محميا من أي تزوير عن طريق الوسائل التقنية المتوفرة وقت الاعتماد،

- أن تكون البيانات المستعملة لإنشاء التوقيع الإلكتروني محمية بصفة موثوقة من طرف الموقع الشرعي من أي استعمال من قبل الآخرين.

يجب ألا تُعدّل البيانات محل التوقيع وألا تمنع أن تعرض هذه البيانات على الموّقع قبل عملية التوقيع».

وتضيف المادة 12 من نفس القانون، أنه يجب أن تكون آلية التحقق من التوقيع الإلكتروني الموصوف موثوقة، ولتحقيق ذلك يجب أن تتوفر فيها المتطلبات الآتية[76]:

- أن تتوافق البيانات المستعملة للتحقق من التوقيع الإلكتروني مع البيانات المعروضة عند التحقق من التوقيع الإلكتروني.
- أن يتم التحقق من التوقيع الإلكتروني بصفة مؤكدة وأن تكون نتيجة هذا التحقق معروضة عرضا صحيحا.
- أن يكون مضمون البيانات الموقعة، إذا اقتضى الأمر، محددا بصفة مؤكدة عند التحقق من التوقيع الإلكتروني.
- أن يتم التحقق بصفة مؤكدة من موثوقية وصلاحية شهادة التصديق الإلكتروني المطلوبة عند التحقق من التوقيع الإلكتروني.
- أن يتم عرض نتيجة التحقق وهوية الموقّع بطريقة واضحة وصحيحة.

كما يتم التأكد من مطابقة الآلية المؤمنة لإنشاء التوقيع الإلكتروني الموصوف، والآلية الموثوقة للتحقق من التوقيع الإلكتروني الموصوف، مع المتطلبات المنصوص عليها في المادتين11و13أعلاه، من طرف الهيئة الوطنية المكلفة باعتماد آليات إنشاء التوقيع الإلكتروني والتحقق منه[77].

وعلى عكس المشرع الفرنسي، خص المشرع الجزائري التوقيع الالكتروني والتصديق الالكترونيين بنص خاص منفصل عن نصوص القانون المدني، يتماشى والأهمية التي أصبحت تحضى به هذا النوع من وسائل الإثبات، والذي من شأنه أن يضع إطارا قانونيا قصد التكفل بالمتطلبات القانونية والتنظيمية والتقنيات التي ستسمح بإحداث جو من الثقة، المواتية لتعميم وتطوير المبادلات الإلكترونية، وترسيخ المبادئ العامة المتعلقة بنشاطي التوقيع والتصديق الإلكترونيين في الجزائر.

(76) المادة 13 من القانون 15/04 – السالف ذكره–.

77 – المادة 14 من نفس القانون.

ويكون المشرع الجزائري قد تبنى موقف مختلف التشريعات الحديثة، التي اعترفت بالتوقيع الإلكتروني والتي أشارت إلى طبيعة النظام المستخدم والى إجراءات التوثيق المعتمدة والتي بتوفرها يعتبر التوقيع الإلكتروني موثوقاً، ويمكن الاعتداد به للإثبات.

المبحث الثاني
دور التشفير وشهادات التوثيق الإلكتروني (التصديق الإلكتروني) في حماية الدفع الإلكتروني

يمكن أن يتعرض استعمال وسائل الدفع الإلكتروني لعدد من المخاطر ذات الطابع الأمني، وهذا يترك أثراً بالغاً في ثقة المتعاملين بهذه الوسائل. ومن شأن إغفال معالجة هذه المخاطر أن يشجع أكثر على تعريض هذه الوسائل للضرر، وهو ما يجعل مستقبل العمل بوسائل الدفع الإلكتروني مهدداً. ولا يقتصر الأمر على تطوير تقنيات جديدة لمواجهة هذه المخاطر، بل يلتزم كذلك ايجاد ضمانات كفيلة بإرساء الأمان القانوني للتعامل بوسائل الدفع الإلكتروني، وقد تكون هذه الضمانات من الجهة نفسها التي توفر هذا الأمان، لكن غالبا ما تكون من جهة ثالثة.

لذلك سيتم التطرق خلال هذا المبحث، لتشفير البيانات كوسيلة لتأمين الدفع الإلكتروني(المطلب الأول)، ليتسنى لنا البحث عن دور جهات التصديق الإلكتروني في حماية الدفع الإلكتروني، من خلال البحث عن الدور الذي تؤديه شهادات التوثيق الإلكتروني –التصديق الإلكتروني– في هذا المجال (المطلب الثاني).

المطلب الأول
تشفير البيانات كوسيلة لتأمين الدفع الإلكتروني

يؤدي التشفير[78] دوراً هاماً كإجراء من إجراءات تأمين المعاملات الإلكترونية بصفة عامة[79]، التي يمكن أن تطال الأجهزة والنظم الإلكترونية المستخدمة في مجال النقود والتجارة الإلكترونية، وهذا بفضل ما تحققه هذه التقنية من سرية وخصوصية

(78) هو العلم وممارسة إخفاء البيانات، أي بوسائل تحويل البيانات (مثل الكتابة) من شكلها الطبيعي المفهوم لأي شخص إلى شكل غير مفهوم، بحيث يتعذّر على من لا يملك معرفة سرية محددة معرفة فحواها. يحظى هذا العلم اليوم بمكانة مرموقة بين العلوم، إذ تنوعت تطبيقاته العملية لتشمل مجالات متعددة نذكر منها: المجالات الدبلوماسية والعسكرية، والأمنية، والتجارية، والاقتصادية، والإعلامية، والمصرفية والمعلوماتية. في شكلها المعاصر فإن التعمية علم من أفرع الرياضيات وعلوم الحوسبة. منشور على الموقع:

https://dvd4arab.maktoob.com/f5652475344/.html

(79) علاء التميمي، التنظيم القانوني للبنك الإلكتروني على شبكة الإنترنت، دار الجامعة الجديدة، الإسكندرية، مصر، 2012، ص 669.

المراسلات والبيانات والاتصالات المستخدمة في الصفقات[80]. يضاف إلى ذلك، الاستخدامات المختلفة للتشفير في نظام التجارة الإلكترونية، والتي تهدف جميعها إلى توفير الثقة في المعاملات المصرفية والتجارة الإلكترونية.

وبالإضافة إلى ذلك، فإن التشفير يستخدم في التحقق من سلامة الرسائل المتبادلة بين الأجهزة في نظم الدفع الإلكتروني وخاصة النقود الإلكترونية، أي يعمل على التأكد من عدم تعرض الرسائل لأي تعديل غير مشروع قبل وصولها إلى متلقيها، ويعمل أيضاً على حماية المعلومات البرمجية خلال انتقالها عبر الشبكة المفتوحة، وذلك من خلال مجموعة من الوسائل الفنية التي تمكن المُرسَل إليه فقط من الاطلاع على محتوى الرسالة المُرسَلة[81].

من خلال هذا التقديم، تتجلى لنا أهمية التشفير كآلية لتأمين المعاملات الإلكترونية وخاصة تلك الخاصة بالدفع الإلكتروني، وهذا لمعرفة أكثر بهذه التقنية، سوف يتم التطرق لتعريفه، أنواعه، وآلية استخدامه، وذلك على التفصيل التالي:

الفرع الأول
مفهوم التشفير

لقد شكَّل الكمبيوتر في بدايات ظهوره وسيلةً جديدة للاتصالات الآمنة، وفك تشفير رسائل العدو، واحتكرت الحكومات في فترة الستينيات حق التشفير وفك التشفير. لكن مع مرور الوقت ما لبثت هذه التقنية أن أصبحت متاحة للجميع. ويقوم نظام التشفير، على استخدام أدوات أو وسائل لتحويل البيانات من شكلها الذي كانت عليه الى شكل آخر (عبارة عن رموز وخوارزميات رياضية غير مفهومة على سبيل المثال)، وذلك لعدم اختراقها وعدم معرفة محتوياتها، وكذا الحيلولة دون استخدامها استخداماً غير مشروعاً من قبل شخص غير مخول له باستعمالها[82].

(80) طارق محمد حمزة، النقود الالكترونية كإحدى وسائل الدفع، تنظيمها القانوني والمسائل الناشئة عن استعمالها، الطبعة الأولى، منشورات زين الحقوقية، بيروت، لبنان، 2011، ص 430.

(81) عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظم القانونية المقارنة، دار الفكر الجامعي، مصر، ط1، 2005، ص 131.

(82)حسين الماحي، نظرات قانونية في التجارة الإلكترونية في التجارة الإلكترونية، مجلة البحوث القانونية والاقتصادية، كلية الحقوق، جامعة المنصورة، العدد الحادي والثلاثين، أبريل، 2002، ص 298. ويعد تقديم خدمات التشفير واحدا من أهم الأهداف المعنية في السنوات الأخيرة لدى الحكومات المختلفة، وهذا ما أوضحه تقرير لجنة (Jack) في نهاية 1988، والتي ذهبت إلى أن التشفير يشهد تطوراً كبيراً، وأن المتوقع أن تكون البنوك من أكثر المؤسسات التي يمكن أن تستفيد من ذلك من خلال تأمين المعاملات المصرفية الإلكترونية، =

لذلك سيتم التطرق إلى مفهوم التشفير من خلال الحديث على تعريف هذه التقنية، وكمرحلة ثانية الحديث على أنواع وطرق التشفير.

أولا- تعريف التشفير:

وهو ما يطلق عليها أيضاً لفظ «التعمية»[83] للتعبير عن الرسالة المشفرة، بحيث لو تم اعتراض الرسالة فلا ينكشف مضمونها، ويُعرَّف التشفير بأنه: «كل العمليات التي تؤدي بفضل البروتوكولات السرية إلى تحويل معلومات أو إشارات مفهومة (مقروءة)، أو القيام بالعكس وذلك باستخدام برامج مصممة لهذه الغاية»، كما يُعرَّف بأنه: «آلية يتم بمقتضاها ترجمة معلومة مفهومة إلى معلومة غير مفهومة عبر تطبيق بروتوكولات سرية قابلة للانعكاس، أي يمكن إرجاعها إلى حالتها الأصلية». كما يعرف بأنه: «تقنية تعتمد على الخوارزميات الرياضية الذكية التي تسمح لمن يمتلك مفتاحاً سرياً يُحوَّل رسالة مقروءة إلى رسالة غير مقروءة والعكس»[84]. أما من الناحية القانونية، فلقد عرَّفه القانون الفرنسي رقم 1170 الصادر بشأن تنظيم الاتصالات عن بعد في عام 1990 -السالف ذكره- بأنه: «مجموعة الأعمال التي تهدف إلى تحويل بيانات أو إشارات واضحة عبر اتفاقات سرية، إلى بيانات أو إشارات غامضة للغير، أو إجراء العملية العكسية، وذلك عبر وسائل مادية أو مخصصة لهذا الغرض».

وقد وضع قانون الاتصالات الإلكترونية البريطاني الصادر في العام 2000 تعريفاً ليس للتشفير ولكن «لخدمة دعم الشفرة»، حيث نصت المادة السادسة من القسم الأول[85]

بالنظر إلى التشفير على أنه من أنجح الوسائل للحفاظ على سرية وسلامة هذه المعاملات. إسماعيل عبد النبي شاهين، أمن المعلومات في الإنترنت بين الشريعة والقانون، ج3، مؤتمر القانون والكومبيوتر والإنترنت، كلية الشريعة، جامعة الإمارات العربية المتحدة، من 1 إلى 3 مايو 2000، ط3، 2004، ص 979. =

(83) علم التشفير أو التعمية Cryptography: هو الحقل المهتم بالتقنيات اللغوية والرياضية لتحقيق أمن المعلومات، خاصة في عملية الاتصال. تاريخياً، اهتم علم التعمية فقط بالتشفير أي وسائل تحويل المعلومات من شكلها الطبيعي المفهوم إلى شكل غير مفهوم ولقد اهتم الإنسان منذ آلاف السنين بهذا العلم لحجب المعلومات السرية عن أعداءه. منشور على الموقع: http://ar.wikiversity.org/wiki.

وقد شاع لدى مؤرخي العلوم في الغرب أن هذا العلم نتاج الحضارة الغربية الصرفة، غير أن العلماء المسلمون هم أول من كتب في طرائق التعمية الرئيسة التي لا يزال... بعض منها مستخدما حتى الآن وأسسوا منهجيات استخراج المعمى وسبقوا الغرب بنحو من سبعة قرون. منشور على الموقع:

http://www.afkaaar.com/html/article114.html

(84) مر خالد زريقات، المرجع السابق، ص 269 وما بعدها.

(85) Regulation of Investigatory Powers Act 2000, 2000 c. 23Part I Chapter I, (6):"For the purposes of this section references to the modification of a telecommunication system include references to the attachment of any apparatus to, or other modification of or interference with:

(a)any part of the system; or

منه على ما يلي: «في مفهوم هذا القسم فإن اصطلاح خدمات دعم الشفرة تعني أي خدمة تُقدَم لمُرسلي ومستقبلي الاتصالات الإلكترونية أو لهؤلاء الذين يخزنون البيانات الإلكترونية والمصممة لتسهيل استخدام تقنيات الشفرة للأغراض الآتية:

1. ضمان أن تكون هذه الاتصالات أو البيانات من الممكن الدخول إليها أو أن توضع في شكل مفهوم للتعرف عليها من قبل أشخاص بعينهم.
2. ضمان إمكانية التأكد من صحة وسلامة هذه الاتصالات أو البيانات».

مما سبق يمكن القول، بأن هذه التقنية تعتمد على نظام تشفير مصمم من قبل تقنيين مختصين في مجال الحاسوب، مستخدماً فيها برامج كومبيوترية معقدة بواسطة مفاتيح مختارة ضمن بروتوكولات مرخصة ومعتمدة[86].

ثانيا- طرق أو أنواع التشفير:

تختلف تقنية التشفير باختلاف الوسائل المستعملة في تنفيذها، لكنها كلها تتفق في أن الهدف من التشفير ضمان تأمين المعاملات المشفرة ومنها المعاملات الإلكترونية محل الدراسة، كما يسمح بضمان سلامة التوقيع الإلكتروني ونسبته للموقع، وبفضله كذلك تضمن سرية المعاملات وسرية الرسائل المتبادلة إلكترونياً، وهذا ما نجده في المعاملات المتعلقة بوسائل الدفع الإلكتروني. ففي هذا المجال، تبدو أهمية التعرض لأنواع التشفير في التعرف على الطريقة الفنية التي يعمل بها كل نظام في علاقة البنك بعميله سواء كان المستهلك أو التاجر، حيث يتم تحديد النظام المتبع في ضوء تصميم الشبكة الداخلية للبنك. ويمكن القول، أنه توجد ثلاث طرق رئيسية للتشفير أو بالأحرى طريقتين، أما الطريقة الثالثة فلا تعدو إلا أن تكون نتاج مزج بين الطريقتين الأخريين وهي:

الطريقة الأولى- التشفير بالمفتاح المتماثل (Symmetric Key Encyption):

وتسمى هذه الطريقة كذلك بمنظومة التشفير المتناسق أو التشفير السيمتري (Symétrique)[87]، ويقوم هذا النظام على استخدام مفتاح متماثل للتشفير وحله،

= (b)any wireless telegraphy apparatus used for making transmissions to or from apparatus comprised in the system". Disponible sur: http://www.legislation.gov.uk/ukpga/2000/23/part/I/chapter/I

(86) حمودي ناصر، المرجع السابق، ص 314. عمر خالد زريقات، المرجع السابق، ص 270.

(87) Chiffrement par clef symétrique: Avec le chiffrement par clef symétrique, le chiffrement peut être calculé avec la clef de déchiffrement et vice versa. Avec la plupart des algorithme symétrique, la

حيث يقوم المنشئ بعد كتابة الرسالة وتشفيرها وتزويد المرسل إليه بذات المفتاح (المتماثل) ليتبين له فيما بعد تلقي الرسالة المشفرة وحلها، واستعادة محتوى الرسالة في صورتها الأصلية[88]. الجدير بالذكر أنه إلى غاية 1975 كانت جميع أنظمة التشفير تعتمد على نظام واحد والذي نحن بصدد الحديث عنه، كما أن هذه الطريقة تعتمد على العديد من المعايير التي يتم التشفير من خلالها ومن أشهرها معيار (DES)[89].

ومع تطور وسائل فك الشفرة، ظهرت العديد من المثالب والعيوب في هذا النوع من أنواع التشفير، وأضحت الحاجة ملحة للجوء إلى أنواع أخرى من أنواع التشفير[90].

= même clef est utilisée pour le chiffrement et le déchiffrement. disponible sur: https://developer.mozilla.org/fr/docs/Introduction_%C3%A0_la_cryptographie_%C3%A0_clef_publique/Chiffrement_et_d%C3%A9chiffrement

(88) عايض راشد عايض المري، المرجع السابق، ص 97. حمودي ناصر، المرجع السابق، ص 315. لمزيد من التفصيل راجع: علاء التميمي، المرجع السابق، ص 673.

(89) هنالك عدة خوارزميات للقيام بهذا النوع من التشفير، أشهرها على الإطلاق هي خوارزمية Data (DES Encryption Standard)، التي لا تزال تستخدم على نطاق واسع لتحقيق الاتصال الآمن على الانترنت ضمن بروتوكول SSL ومجالات أخرى شبيهة، وهي أيضا الخوارزمية التي أعلنت كخوارزمية معتمدة لتشفير البيانات في الدوائر الحكومية في الولايات المتحدة الأمريكية منذ عام 1976.

لكن سرعان ما أظهر هذا المعيار ضعفاً خلال السنوات الأخيرة أمام أساليب كسر التشفير، وبدأت تنتشر في العديد من الأماكن بنسخ معدلة عنها مثل معيار Triple DES، إلا أن DES استبدلت كلياً كمعيار معتمد في الحكومة الأمريكية في نهاية عام 2001 بمعيار أفضل وأكثر تطوراً Advensed Encyption) AES Standard). أحمد الهاشمي، التشفير بالمفتاح المتناظر، مقالة على منشورة على الموقع الالكتروني:

http://www.boosla.com/showArticle.php?Sec=Security&id=35

أدى ضعف خوارزمية DES إلى استحداث خوارزمية جديدة مشتقة من نفس هيكلة هذه الخوارزمية، ولكنها تختلف عنها في عدد المفاتيح المستخدمة في التشفير حيث أنها تستخدم ثلاثة مفاتيح مختلفة، ولهذا سميت بخوارزمية التشفير المضاعفة TDES وهذا ساعد بدوره إلى زيادة قوة الخوارزمية وبالتالي زيادة أمنيتها وهذا هو المطلوب في عمل أي خوارزمية تشفير. كما أن خوارزمية TDES تستغرق وقتاً كبير لكسرها بسب احتوائها على ثلاثة مفاتيح مختلفة وهذا يزيدها صعوبة أكبر بالنسبة للمهاجم. ومن جهة أخرى، فان خوارزمية TDES تكون عدد دوراتها كبير حيث تكون 48 دورة وذلك عكس خوارزمية DES التي تكون عدد دوراتها 16 دورة فقط. راجع: ميمونة حميد الحداد، دراسة عامة للمقارنة بين خوارزميتي التشفير، العراق، جامعة الكوفة، كلية التربية للبنات، مقالة منشورة على الموقع: www.boosla.com

(90) عمر حسن المومني، التوقيع الإلكتروني وقانون التجارة الالكترونية، ط 1، دار وائل للنشر، الأردن، 2003، ص55.

الطريقة الثانية– التشفير بالمفتاح غير المتماثل (Asymmetric Key Encyption):

جاء التشفير اللامتماثل بديلاً عن التشفير المتماثل كحل لمشكلة التوزيع غير الآمن للمفاتيح، فعوضاً عن استخدام مفتاح واحد يستخدم التشفير اللامتماثل مفتاحين اثنين. فبعد ما كان التشفير وفكه يتم بمفتاح واحد، نظرا لان كلاً من مرسل المعاملة أو البيان الإلكتروني ومستلمه يملك نفس المفتاح، أصبح يتم بمفتاحين أحدهما للتشفير ويسمى المفتاح الخاص، والثاني لفك التشفير[91] ويسمى المفتاح العام، لذلك يطلق على هذا النوع من التشفير أيضا بالتشفير بالمفتاح العلني (Public-Key Encryption)، لأنك تستطيع أن تنشر أحد المفتاحين وهو يسمى المفتاح العلني (Public-Key)[92] وتحتفظ بالآخر سريا، ويسمى المفتاح الخاص (Private-Key)[93] أو المفتاح السري، وهما مفتاحان متحاكيان[94] بحيث يحمل كل مفتاح علامة رياضية معقدة. وكما يشير الاسم، فإن المفتاح الخاص يقصد به أن يضل سراً بحيث يكون المستخدم فقط وحده قادراً على الدخول إليه، أما المفتاح العام فليس المقصود جعله سراً، بل يمكن طباعته بحيث تستطيع جهات خارجية معرفته[95].

وتجدر الاشارة في الأخير، أنه من الناحية العملية فيما يخص نظم النقود الإلكترونية، فإنها تتطلب المحافظة على سرية المفاتيح التشفيرية، بهدف منع نسخ أو تعديل البيانات المخزنة أو المرسلة. ففي النقود الإلكترونية ذات البطاقة، تم تطوير عدد من التقنيات التي تخزن على الرقاقة والتي تساهم في نجاح عملية التشفير. أما النقود الالكترونية ذات البرمجيات، والتي تنتقل عبر الشبكة المفتوحة، فان تخزين مثل هذه التقنيات يمكن أن يثير المزيد من التحديات، ذلك أن احتمالات الاختراق تكون أكبر من تلك في حالة البطاقة، حيث لا يمكن ضمان درجة الأمان بالكامل في ظل الشبكة المفتوحة[96].

---

(91) السيد محمد السيد عمران، الالتزام بالإعلام الإلكتروني قبل التعاقد عبر شبكة الإنترنت، الدار الجامعية، القاهرة، 2006، ص 96،97. طاهر شوقي مؤمن، عقد البيع الإلكتروني «بحث في التجارة الإلكترونية»، دار النهضة العربية، مصر، 2007، ص75.

(92) وتشير كلمة المفتاح (Key) إلى قيمة رياضية عبارة عن مجموعة كبيرة من أرقام تستخدم كخوارزميات تشفير (Cryptographic algorithms)، بحيث يمكن من خلالها تشفير الرسالة الإلكترونية وحل شفرتها. علاء التميمي، المرجع السابق، ص 675.

(93) وأشهر خوارزميات هذا النوع من التشفير هي خوارزمية RSA نسبة إلى مخترعيها (Shamir.Rivest, A.R) عام 1977 الذين وضعوا هذه الخوارزمية، والتي تستخدم في مجالات التوثيق المختلفة. علاء التميمي، المرجع السابق، ص 675.

(94) عمر حسن المومني، المرجع السابق، ص 56.

(95) عايض راشد عايض المري، المرجع السابق، ص 98. عمر خالد زريقات، المرجع السابق، ص272.

(96) طارق محمد حمزة، المرجع السابق، ص432.

الطريقة الثالثة– المزج بين نظامي المفتاح المتماثل والمفتاح غير المتماثل:

تقوم هذه الطريقة على المزج بين النظامين لتحقيق درجة تأمين عالية في أقل وقت ممكن وذلك بإتباع الخطوات التالية:

- تشفير الرسالة الأصلية المرسلة بمفتاح متماثل أي بالطريقة السيميترية.
- تشفير المفتاح المتماثل بالمفتاح العام للمرسل اليه.
- يتم إرسال الرسالة المشفرة والمفتاح المتماثل للمشفر بأي وسلة اتصال عادية.
- يقوم المتلقي بتلقي الرسالة والمفتاح المتماثل.
- يحل المتلقي تشفير المفتاح المتماثل باستخدام المفتاح الخاص به.
- يحل مفتاح الرسالة الأصلية باستخدام المفتاح المتماثل حتى يحصل على الرسالة الأصلية[97].

الفرع الثاني
آلية استخدام التشفير

تتم عملية التشفير بصورة عملية في علاقة المرسل والمرسل إليه من خلال مرحلتين: المرحلة الأولى الاتفاق بين المرسل والمرسل إليه على أدوات التشفير مثلا البنك وأحد عملائه، قد يكون مستهلكاً أو تاجراً إذا ما تعلق الأمر بعلاقات الدفع الإلكتروني. أما الثانية: مرحلة نقل البيانات، وذلك على الشاكلة التالية:

المرحلة الأولى– الاتفاق بين المرسل والمرسل اليه على أدوات التشفير:

يتم في هذه المرحلة الاتفاق بين الطرفين على أدوات التشفير التي ستتم في عملية التشفير، ويتضمن الاتفاق تحديد مجموعة الخوارزميات (Algoriyhms)[98] التي تستخدم لحماية البيانات المتبادلة، والموافقة كذلك على مجموعة مفاتيح التشفير

(97) عبد الفتاح بيومي حجازي، التجارة الإلكترونية في القانون العربي لمكافحة جرائم الكومبيوتر والانترنت، دار الفكر الجامعي، 2006، ص 274.

(98) الخوارزمية (Algorithm) عبارة عن مجموعة من الخطوات الرياضية والمنطقية والمتسلسلة اللازمة لحل مشكلة ما. سميت الخوارزمية بهذا الاسم نسبة إلى العالم المسلم أبو جعفر محمد بن موسى الخوارزمي الذي ابتكرها في القرن التاسع الميلادي. كلمة خوارزم (algorism) في الأصل كانت مقتصرة على القوانين الرياضية التي تستخدم الأرقام العربية وطُورت في اللاتينية من الخوارزمي (al–Khwarizmi) لتصبح (algorithm) في القرن الثامن عشر الميلادي لتشمل جميع إجراءات حل المشكلات وتنفيذ المهمات. لذلك ظهرت خوارزمية التشفير، التي هي عبارة عن معدلات رياضية معقدة جداً تعمل على تشفير الرسالة من خلال تحويلها من شكلها الأصلي إلى ملخص، على أن يتم تحويلها مرة أخرى عند حل شفرة الرسالة، راجع محمد سعيد أحمد إسماعيل، المرجع السابق، ص 190.

(Key Cryptographic)، وأيضاً الوسيلة التي تمكن المرسل مثلاً البنك من التحقق من شخصية العميل والعكس.

المرحلة الثانية– مرحلة نقل البيانات:

بمجرد الانتهاء من المرحلة الأولى وإبرام الاتفاق بين البنك والعميل مثلا، يتم استخدام هذه الأدوات والبرامج المخصصة لذلك على حاسوب كل من المرسل ومتلقي المعلومة أو البيانات ونقلها بينهما، حيث تعمل هذه البرامج على تقسيم الرسالة المراد إرسالها إلى أجزاء، وتنقل في صورة سلسلة من السجلات المؤمنة، حيث يحمل كل سجل منها رقماً سرياً معيناً، وعندما تصل الرسالة يتم تجميع هذه الأجزاء من خلال أدوات لفك الشفرة. من هنا تظهر أهمية تشفير البيانات، في عملية الدفع الإلكتروني بين أطرافه الثلاث في العلاقات التعاقدية الثنائية بين أطرافه.

المطلب الثاني

دور شهادات التوثيق الإلكتروني

(التصديق الإلكتروني) في حماية الدفع الإلكتروني

لا يستلزم التطور الذي تعرفه التجارة الإلكترونية، تطوير تقنيات جديدة للكتابة الإلكترونية والتوقيع الإلكتروني وكذا الاعتراف القانوني بهما فقط، بل يلتزم كذلك إيجاد ضمانات كفيلة بإرساء الأمان القانوني ووضع الثقة فيهما، وقد تكون هذه الضمانات من الجهة نفسها لكن غالبا ما تكون من جهة ثالثة. ولدراسة دور شهادات التوثيق الإلكتروني (التصديق الإلكتروني) في حماية الدفع الإلكتروني، أولا يجب بحث الحصول على الترخيص بالاستعمال (الفرع الأول)، لكي يمكن الحديث عن شهادات التوثيق الإلكتروني (التصديق الإلكتروني) (الفرع الثاني).

الفرع الأول

الحصول على الترخيص بالاستعمال

وهو عملية الطلب إلى الجهة المصدرة لوسائل الدفع الإلكترونية خاصة في مجال النقود الإلكترونية، على أساس أن عمليات الدفع هذه تتم على شبكة الإنترنت من قبل

المستخدم، والسماح له بإجراء الصفقات بواسطة هذه النقود؛ وهذا الأمر مطلوب في النقود ذات البطاقة ونقود البرمجيات أيضاً.

ففي أنظمة النقود ذات البطاقة، فإن الترخيص يطلب عادة في مرحلة التخزين في الحساب المصرفي للمستخدم، وهي تتطلب استخدام رقم تعريف شخصي PIN. ويطلب الترخيص أيضاً بين التاجر والمشغلين لضمان عدم الدفع لذات الصفقة أكثر من مرة، وعادة ما يكون ذلك عبر نظام مركزي.

وكذلك الأمر بالنسبة للنقود ذات البرمجيات، اذ يفترض الحصول على مثل هذا الترخيص في أثناء إجراء الصفقات لتلافي إعادة استخدام النقود مرات متعددة، حيث تقوم السلطة المركزية المصدرة بالترخيص لإجراء الصفقات على أساس المعلومات والوحدات المصدرة مسبقاً[99].

إضافة إلى كل هذا فإن أنظمة النقود الإلكترونية، يمكن أن تؤمن مستويات إضافية من الأمن في مواجهة الأعمال غير المشروعة، فقد يتطلب إجراء الصفقات عدداً من الإثباتات على صحتها، مثال: تاريخ الصلاحية، عدد الصفقات المبرمة بواسطة وسيلة الدفع، الأرصدة الموجودة على البطاقة والحد الأعلى للرصيد المسموح به في الصفقات. كما يمكن أن تتضمن أيضا، بعض التدابير التي تمنع تكوين أرصدة غير مشروعة نتيجة إعاقة الصفقات. فالبروتوكولات الخاصة بالرسائل، لا تعتبر أن الصفقات قد تمت ما لم يتم التثبت من أن جميع الرسائل الخاصة بالصفقة قد وصلت إلى الجهة المرسلة إليها. فاعتراض أمر هذه الرسائل، قد يؤدي إلى تحويل الرصيد إلى غير الجهة المقصودة، ما يتولد عنه عدم إتمام الصفقة، وخلق رصيد غير شرعي لدى الجهة التي اتجهت إليها النقود بعد الدخول عليها بطريقة غير مشروعة.

الفرع الثاني
شهادات التوثيق الالكتروني (التصديق الالكتروني)

الثقة والأمان عنصران ضروريان لتطوير التجارة الإلكترونية، التي تعتمد على شبكة الاتصال المفتوحة. ولا توجد ضمانات بوجود الشركة صاحبة الموقع التي يزودها العميل بالمعلومات عن بطاقته الائتمانية، مما يقتضي وجود خدمة محايدة

(99) باسم علوان العقابي، علاء عزيز الجبوري، نعيم كاظم جبر، النقود الالكترونية ودورها في الوفاء بالالتزامات التعاقدية، موقع جامعة أهل البيت، منشور على الموقع:

http://www.ahlulbaitonline.com/karbala/New/html/research/research.php?ID=79

تتضمن هذه الموثوقية، والتي تُعرَف بشهادات التوثيق أو شهادات التعريف الرقمية. ويمكن استخدام هذه التقنية في تحديد هوية مستخدمي الشبكة، سواء أكانوا من الداخل أم من الخارج وأهليتهم القانونية للتعاقد، والتحقيق في مضمون التعامل وسلامته، كذلك تقوم بإصدار المفاتيح الإلكترونية سواء المفتاح الخاص بالتشفير أو العام المتعلق بفك التشفير، كما تقوم بإصدار شهادات التوثيق(100).

وتقوم كذلك بالتأكد من جدية الإرادة في التعاقد بين الأطراف وبعدها عن الغش والنصب، بالإضافة إلى تحديد مضمون الإرادة تحديداً دقيقاً، وكذلك مدى صحتها ونسبتها إلى من صدرت منه والتيقن من طبيعة التعاقد(101). لذا كان من الضروري التطرق لهذا الموضوع، من خلال تحديد تعريف جهة التصديق وبيان الالتزامات التي تقع على عاتقها، وكذلك الحديث عن شهادات التصديق الصادرة عنها.

أولا- تعريف جهة التوثيق الإلكتروني:

تعدد تسميات جهة التوثيق الإلكتروني، بين سلطات التصديق «أو الغير مصدق»، أو «الغير الموثوق» أو «الغير موثق»، وهي جهات تعمل على ضمان الدخول القانوني لمنظومة التشفير لأجل تأمين سرية المعاملات(102). جهة التوثيق هذه أو مقدم خدمات التصديق Prestataire de Service de Certification ويرمز له باختصار (PSC)، هو هيئة عامة أو خاصة تعمل تحت إشراف السلطة التنفيذية، وتتكون غالبا من ثلاثة مستويات مختلفة من السلطة:

تأتي في المرتبة العليا «السلطة الرئيسية»، وهي تختص بالتصديق على تكنولوجيا وممارسات جميع الأطراف المرخص لهم بإصدار أزواج مفاتيح التشفير، أوهي جهة خاصة بعملية «سلطة التصديق» شهادات تتعلق باستخدام تلك المفاتيح، وتليها في المرتبة التصديق على أن المفتاح العام لأحد المستخدمين يناظر بالفعل المفتاح الخاص لذلك المستخدم، ومهمتها تلقي الطلبات من الأشخاص الراغبين في الحصول على خدمة التصديق الإلكتروني، ثم «سلطة تسجيل محلية» وهي الأدنى في المستوى تأتي على أزواج مفاتيح التشفير -العام والخاص- والتأكد من هوية وشخصية هؤلاء المستخدمين ومنح شهادات تصديق تفيد صحة توقيع العملاء. ويتم تدخل الموثق الإلكتروني بناء

(100)طارق كاظم عجيل ، ثورة المعلومات وانعكاساتها على القانون المدني «دراسات وبحوث « الطبعة الأولىن منشورات الحلبي الحقوقية، بيروت- لبنان، 2011 ، ص 122، 123.

(101) إبراهيم الدسوقي أبو الليل، المرجع السابق، ص 187.

(102) حمودي ناصر، المرجع السابق، ص 305.

على طلب شخصين أو أكثر بهدف إنشاء وحفظ وإثبات الرسائل الإلكترونية[103].

وقد عرف قانون اليونيسترال النموذجي للتوقيع الإلكتروني مقدم خدمات التصديق بأنه: «شخصاً يصدر الشهادات ويجوز أن يقدم خدمات أخرى ذات صلة بالتوقيعات الإلكترونية». لذلك يقوم مقدمو خدمات التصديق بدور هام وفعال في ضمان التوقيعات والاعتراف بها قانونا[104]. ووفقا للقرار الأوروبي الصادر في 13 ديسمبر 1999 والمتعلق بالتجارة الإلكترونية وتحديداً نص المادة الثانية، التي تعرضت لتعريف مقدم خدمات الشهادات بأنه: «كل شخص طبيعي أو معنوي يصدر شهادات توثيق التوقيع الإلكتروني، أو يتولى أية خدمات أو مهمات متعلقة بها أو بالتواقيع الإلكترونية»[105].

أما قانون التوقيع الإلكتروني المصري 15 لسنة 2004، فقد جاء خاليا من تعريف لجهة التوثيق الإلكتروني، وإن كان حظر مزاولة نشاط إصدار شهادات التصديق الإلكتروني، إلا بعد الحصول على ترخيص بذلك من الهيئة المختصة، وهي هيئة تنمية صناعة تكنولوجيا المعلومات[106]. أما بالنسبة للمشرع الجزائري، فقد عرَّف مؤدي خدمات التصديق الإلكتروني بأنه: «كل شخص طبيعي أو معنوي يقوم بمنح شهادات تصديق إلكتروني موصوفة، وقد يقدم خدمات أخرى في مجال التصديق الإلكتروني»[107].

وتعتمد جهات التوثيق في عملها على سجلات خاصة تنظم بموجبها قوائم بالتوقيعات الفاعلة، وقوائم أخرى بالتوقيعات الملغاة أو المبطلة، بالإضافة إلى قوائم بالتوقيعات الموقوفة أو ما تم تعليق العمل بها[108].

---

(103) عادل أبو هشيمة محمود حوته، عقود خدمات المعلومات الإلكترونية في القانون الدولي الخاص، دار النهضة العربية، مصر، 2004، ص 196.

(104) المادة 2/ هـ من قانون اليونسترال النموذجي بشأن التوقيع الإلكتروني مع دليل الاستشراع 2001.

(105) Art. 2:» DIRECTIVE 1999/93/CE DU PARLEMENT EUROPÉEN ET DU CONSEIL» Définitions…»11)

prestataire de service de certification», toute entité ou personne physique ou morale qui délivre des certificats ou fournit d>autres services liés aux signatures électroniques».

(106) نصت المادة 2 من قانون التوقيع الإلكتروني المصري على أنه:» تنشأ هيئة عامة تسمى هيئة تنمية صناعة تكنولوجيا المعلومات تكون لها الشخصية الاعتبارية العامة وتتبع الوزير المختص، ويكون مقرها الرئيسي محافظة الجيزة، ولها إنشاء فروع في جميع أنحاء جمهورية مصر العربي».

(107) المادة 02/ 12 من القانون 15/ 04 – السالف ذكره–.

(108) إبراهيم الدسوقي أبو الليل، توثيق التعاملات الإلكترونية، المرجع السابق، ص 187.

تتم التبادلات على شبكة الإنترنت من خلال شبكة مفتوحة لا تحتوي على أي وجود مادي، لذا فلا يمكن التعرف على هوية الأشخاص الذين نتواصل معهم، فالعالم الافتراضي يعرضنا لعدد من المخاطر مثل سرقة الهوية، واعتراض الآخرين على رسائل الغير واستنكار عملية البيع أو الدفع أو التبادل، وعليه فإن وضع أجهزة أمنية مثل التصديق الإلكتروني بات إحدى الضروريات الملحة. كما أن التصديق الإلكتروني هو عملية تضمن أربعة (04) جوانب أمنية لتبادل المعلومات على شبكة الإنترنت وهي: السرية والتوثيق والنزاهة وعدم الاستنكار، كون هذه الجوانب تسمح في إرساء مناخ ثقة عن طريق إقامة بنية ذات مفتاح عمومي «PKI»[109].

والذي يساعد على تحديد أصحاب المفاتيح[110]عن طريق إصدار شهادات إلكترونية، وهي عبارة عن ملف رقمي يوضح الصلة بين بيانات مراجعة التوقيع والموقع، وهي بذلك تلعب دور بطاقة الهوية.

(109) تعريف PKI: هي اختصار Public Key Infrastructure (هيكل المفتاح العمومي) وتعني اصطلاحا مقاييس البنية التحتية للتعاملات التجارية الآمنة وهي عبارة عن مجموعة من البرامج وتقنيات التشفير والخدمات التي تمكن المؤسسات والشركات الكبرى من ضمان أمن اتصالاتها وتعاملاها التجارية على الإنترنت مع الشركات الأخرى أو مع الأفراد. ولقد ظهرت الحاجة لهذه البنية نظرا للمخاطر التي تواجهها الاستخدامات التجارية في الإنترنت والتي من أهمها انتحال الشخصيات وتغيير المعلومات المتناقلة عبر الإنترنت أو التجسس عليها. محمد عبيد العمري، النسخة الأولى، المقالات العلمية، PKI، مركز التمييز لأمن المعلومات، ص 2، منشور على الموقع: https://www.google.dz/url?sa

(110) البنية التحتية للمفتاح العموميPKI هي عبارة عن منظومة أمنية متكاملة لتوفير بيئة مناسبة للتعامل الآمن عبر شبكات الحاسب الآلي وتعتبر نظاما لإدارة مفاتيح التشفير بواسطة الشهادة الرقمية، وتتلخص أهداف البنية التحتية للمفتاح العمومي PKI كالتالي:

التحقق من الهوية Authentication: هي تمكين المستخدمين من معرفة هوية بعضهم البعض و التحقق منها بشكل قاطع.

سرية البيانات Confidentiality: هي التمكن من تبادل المعلومات بحيث لا يمكن للآخرين معرفة طبيعة تلك البيانات.

سلامة البيانات Integrity: هي التمكن من كشف أي محاولة لتغيير أو تعديل محتوى المعلومة بعد الإرسال.

التوقيع الإلكتروني Electronic Signature : التوقيع على وثيقة مع مقدرة المستلم التحقق من صحة التوقيع، و بذلك يتم التحقق من الهويات عبر الوثائق الإلكترونية و الشهادات الرقمية Digital Certificats. أماني بنت عوض بن سليم العنزي، هيكل المفتاح العمومي PKI، 9 أوت 2014، منشور على الموقع:

http://www.geek4arab.com/home

كما تعد سلطة التصديق، العنصر الرئيسي للبنية ذات المفتاح العمومي والتي دورها الأساسي هو إصدار الشهادات الإلكترونية. وبالإضافة إلى ذلك، تعدّ سلطة التصديق، مسؤولة عن وضع وضمان وجود صلة رسمية بين الشخص والمفتاح العمومي كجزء من بنية ذات مفتاح عمومي، ويتمثل دورها في التحقق من دقة المعلومات الواردة في الشهادة الإلكترونية التي تصدرها، والتأكد من صحة الوثيقة مقابل شخص آخر، كما يمكن لسلطات التصديق التفاعل ما بينها وفقا لأنماط أو نماذج تنظيمية مختلف[111].

إن التعامل عبر الإنترنت يتطلب أن يتأكد كل طرف متعامل عبر هذه الشبكة من هوية الطرف المتعامل الآخر، ومن الممكن أن يتم ذلك من قبل طرف ثالث معتمد وموثوق به من قبل الجميع، وكما هو الحال في بعض الولايات الأمريكية، فإن هذا الطرف والذي يسمى بـ»سلطة التصديق» (Certificate Authority) هو بمثابة كاتب العدل (Notary) في العالم المادي (Physical World)، يقوم بتأكيد هوية الأطراف المتعاملة عبر الإنترنت بالإضافة إلى المصادقة على تواقيعهم الرقمية (On Line digital signatures).

ثانياً- إلزامية إنشاء جهة مختصة بالتوثيق الإلكتروني:

ألزم التوجيه الأوربي رقم 93 لسنة 1999، الدول الأعضاء في الاتحاد الأوروبي بالترخيص لإنشاء جهات خاصة تتولى مهام اعتماد التوقيعات الإلكترونية، وذلك عن طريق إصدارها لشهادات تثبت استيفاء التوقيع الإلكتروني للشروط اللازمة لكي يعتد به في الإثبات، وارتباطه بالمستند المذيل به مع تأمينه ضد أي تعديل أو تغيير في مضمونه[112].

أما قانون التوقيع الإلكتروني المصري رقم 15 لسنة 2004 تحديداً في نص المادة19 فقرة –ب–، أنشا هيئة تنمية صناعة تكنولوجيا والمعلومات التي تتولى وضع القواعد الفنية والإدارية والمالية، والضمانات الخاصة بإصدار التراخيص

(111) منشور على الموقع الرسمي لسلطة ضبط البريد والمواصلات السلكية واللاسلكية arpt:

http://www.arpt.dz/ar/gd/ce

(112) إبراهيم الدسوقي أبوالليل، توثيق التعاملات الإلكترونية، المرجع السابق، ص 1.

Art. 3, DIRECTIVE 199993//CE DU PARLEMENT EUROPÉEN ET DU CONSEIL: « Accès au marché…3.3. Chaque État membre veille à instaurer un système adéquat permettant de contrôler les prestataires de service de certification établis sur son territoire et délivrant des certificats qualifiés au public. …».

اللازمة لمزاولة أنشطة خدمات التوقيع الإلكتروني، وغيرها من الأنشطة في مجال المعاملات الإلكترونية، وتكنولوجيا المعلومات»، حيث يتم تحديد مدة الترخيص من قبل مجلس إدارة الهيئة بحيث لا تزيد على تسعة وتسعين عاماً، كما أوكل لها القانون تقديم المشورة الفنية بشأن المنازعات التي تنشأ بين الأطراف المعنية بالأنشطة التوقيع الإلكتروني والمعاملات الإلكترونية وتكنولوجيا المعلومات[113].

وبخصوص المشرع الجزائري، فقد منح صلاحية إصدار الترخيص للسلطة الاقتصادية للتصديق الإلكتروني، والتي تعينها السلطة المكلّفة بضبط البريد والمواصلات السلكية واللاسلكية[114]. وتكلف السلطة بمتابعة ومراقبة مؤديي خدمات التصديق الإلكتروني، الذين يقدمون خدمات التوقيع والتصديق الإلكتروني لصالح الجمهور[115].

تقوم السلطة الاقتصادية للتصديق الالكتروني بعدة مهام لعل أهمها[116]:

1. إعداد سياستها للتصديق الإلكتروني وعرضها على السلطة الوطنية للتصديق الإلكتروني[117] للموافقة عليها والسهر على تطبيقها.
2. منح التراخيص لمؤديي خدمات التصديق الإلكتروني بعد موافقة السلطة.

إعداد دفتر الشروط الذي يحدد شروط وكيفية تأدية خدمات التصديق الإلكتروني وعرضه على السلطة للموافقة عليه،

كما إن هذه الجهات المحايدة الخاصة بالتوثيق الإلكتروني، تخضع لإشراف الدولة التي تقوم بتحديد القواعد والإجراءات التي تنظم عملها، وتقوم هذه الجهات بإصدار شهادات التوثيق الإلكتروني وفق الترخيص الصادر لها من الجهات المسؤولة في الدولة[118]. إن وجود هذه الجهات يحقق أهداف التجارة الإلكترونية، وخاصة من

(113) المادة 04 فقرة 5 من قانون التوقيع الإلكتروني المصري.

(114) المادة 29 من القانون 15/04 – السالف ذكره–.

(115) المادة 30 من نفس القانون.

(116) المادة 30/1، 2،12 من نفس القانون.

(117) سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي، تكلف السلطة بترقية استعمال التوقيع، والتصديق الإلكترونيين وتطويرهما وضمان موثوقية استعمالهما، المادتين 16 و18 من القانون 15/04 السالف ذكره.

(118) المادة الثانية من التوجيه الأوروبي. للمزيد انظر؛ أسامة أحمد بدر، حماية المستهلك في التعاقد الإلكتروني، دراسة مقارنة، دار الكتب القانونية، مصر، ص 165. السيد محمد السيد عمران، الالتزام =

حيث تدعيم الثقة بين المتعاقدين بما يحقق الثقة والأمان بالتعاقد عبر شبكة الإنترنت، وكذا إمكانية الصفقات التجارية التي تتم عن بعد.

ثالثا- مهام جهات التصديق الإلكتروني:

تعدّ سلطة التصديق مسؤولة عن وضع وضمان وجود صلة رسمية بين الشخص والمفتاح العمومي كجزء من بنية ذات مفتاح عمومي، كما يمكن تلخيص المهام التي يقوم بها مزود خدمات التصديق الإلكتروني في النقاط التالية:

1- التحقق من هوية الشخص الموقع:

إن أهم التزام يقع على عاتق جهات التصديق، هو تحديد هوية المتعاملين في التعاملات الإلكترونية[119] وتحديد أهليتهم في التعاقد والتعامل.

2- إثبات مضمون التبادل الإلكتروني:

تتولى جهة التوثيق التحقق من مضمون التبادل الإلكتروني بين الأطراف وسلامته وجديته وبعده من الغش والخداع، فضلا عن إثبات مضمونه[120]، وتجنب حدوث أي غش تجاه المتعاملين بالإنترنت، نجد أن جهات التوثيق تقوم بتعقب المواقع التجارية للتحري عن وجودها الفعلي ومصداقيتها، فإذا اتضح لها أن تلك المواقع غير حقيقية أو غير جدية فإنها تقوم بتحذير المتعاملين[121]، ويجوز اللجوء إلى هذه الجهات قبل إبرام العقد للتحقق من أمر الشركة التي سيتم التعاقد معها.

3- تعقب المواقع التجارية الإلكترونية:

وذلك عن طريق التحري عنها وعن جديتها ومصداقيتها، وإذا تبين لها عدم أمن أحد هذه المواقع فإنها تقوم بتوجيه رسالة تحذيرية إلى المتعاملين معها توضح فيها عدم مصداقية هذه المواقع.

= بالإعلام الالكتروني قبل التعاقد عبر شبكة الإنترنت الدار الجامعي، القاهرة، 2006، ص102.

نص المادة 16من القانون 15/04 السالف ذكره: « تنشأ لدى الوزير الأول سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي، تسمى السلطة الوطنية للتصديق الإلكتروني...».

(119) سعيد السيد قنديل، المرجع السابق، ص90.

(120) إبراهيم الدسوقي أبو الليل، المرجع السابق، ص 1869.

(121) إيمان مأمون أحمد سليمان، الجوانب القانونية لعقد التجارة الإلكترونية، رسالة دكتوراه، كلية الحقوق، جامعة المنصورة، 2005/2006، ص 313.

4- إصدار المفاتيح الإلكترونية:

تتولى هذه الجهات إصدار المفاتيح الإلكترونية، سواء المفتاح الخاص الذي من خلاله يتم تشفير المعاملة الإلكترونية، أو المفتاح العام الذي يتم بواسطته فك هذا التشفير، وبالتالي تضمن هذه الجهات أن المفتاح العام هو المناظر حيث تتحقق من تطابقه وصلاحيته. كما تقوم هذه الجهة بإصدار التوقيع الرقمي، حيث يقوم طالب التوثيق بتقديم البيانات اللازمة إلى جهة التوثيق، ثم يتم إصدار المفتاح الخاص بصاحب طلب توثيق التوقيع الذي استخدمه في التوقيع، ولا يمكن استخدامه، أي المفتاح الخاص، إلا من جهاز حاسب آلي واحد فقط، وذلك حتى يتم التأكد من أن التوقيع الرقمي صادر من صاحبه، لذا يتعين على الموقع بالمفتاح الخاص أن يحتفظ به سريا ولا يطلع عليه أحد، أما المفتاح العام فتحتفظ به عادة جهة التوثيق، حيث تقوم بإرساله بالبريد الإلكتروني إلى كل من يرغب في التعامل مع صاحب التوقيع الإلكتروني، وبذلك يمكن التحقق من صحة التوقيع، ويجب على جهة التوثيق أن تنقل التوقيع الإلكتروني بمفتاحه الخاص بطريقة آمنة موثوق بها دون احتفاظ بصورة من التوقيع بمفتاحه الخاص[122].

كما يجب على جهات التوثيق إمساك سجلات خاصة بالتواقيع الإلكترونية، توضح فيها من الذي قام بهذه التوقيعات وما تم إلغاؤه منها، وكذلك ما تم إيقافه وتعليق العمل به.

إن الغرض من شهادة التوثيق الإلكترونية، هو تأكيد أن التوقيع الإلكتروني أو الرسالة الإلكترونية بصفة عامة صادرة ممن نسبت إليه، وأن توقيعه صحيح، كما تؤكد الشهادة أن البيانات الموقع عليها بيانات صحيحة صادرة عن الموقع، ولم يتم التلاعب فيها، فلم يطرأ عليها أي تبديل سواء بالحذف أو بالإضافة أو التغيير، فهذه البيانات تصبح موثوقة ولا يمكن إنكارها.

رابعا- أنواع شهادات التوثيق الإلكتروني:

في الواقع إن هناك عدة مستويات لشهادة التصديق التي تصدرها سلطات التصديق تبعاً لنوع الوثائق الثبوتية المعتمدة للتأكد من الشخصية، فوفقاً لشركة (Belsing) وهي إحدى شركات سلطات التصديق العالمية، هناك ثلاث مستويات من شهادة التصديق، فمن المستوى الأول (الأدنى)، الذي يتطلب إصداره من المشترك أن يقدم عنواناً إلكترونياً صالحاً للاستعمال، ليتم إصدار شهادة مجانية تستعمل

(122) سعيد السيد قنديل، المرجع السابق، ص81.

في معاملات ذات قيم مالية منخفضة، الى المستوى الثالث (الأعلى)، الذي يتطلب من المشترك الحضور أمام سلطة تسجيل محلية وبحوزته وثائقه الثبوتية، قبل إصدار شهادة توثيق له يمكن استعمالها في معاملات مالية ضخمة.

كما أن شهادات التوثيق قد تختلف أيضاً من حيث وظيفة كل منها، فهناك شهادات تعرف فقط بشخصية المشترك دون تقديم بيانات أخرى، وشهادات تصدر لكي تستعمل في تعامل واحد فقط، وشهادات أخرى تستعمل من قبل أشخاص مخولين للتوقيع على شركة أو هيئة معينة. وإلى جانب شهادة توثيق التوقيع الرقمي، هناك شهادات أخرى تتنوع بحسب الهدف منها، ومن أمثلة ذلك[123].

شهادة الإذن Authorizing Certificate التي تتولى تقديم بيانات عن صاحب التوقيع كالمؤهلات، ومحل الإقامة.

شهادة البيان Attesting Certificat والتي تثبت صحة واقعة معينة، ووقت وقوعها[124].

شهادة Digital Time Stamp التي توثق تاريخ ووقت إصدار التوقيع الرقمي، حيث يقوم صاحب الرسالة بعد التوقيع عليها بإرسالها إلى جهة التوثيق التي تقوم بتسجيل التاريخ عليها وتوقيعها من جهتها، ثم تعيدها إلى مرسلها.

وغالباً ما تصدر الشهادة لفترة محدودة، وبمجرد انتهاء مدتها فإنها تصبح غير قابلة للاستعمال، حيث يتم غالباً رفضها تلقائياً من قبل برمجيات المستقبل، ولهذا فإن سلطات التصديق غالباً ما تقوم بإعداد ونشر قائمة بالشهادات الصالحة للاستعمال، وأخرى للشهادات التي تنتهي فترة استعمالها أو تصبح غير صالحة للاستعمال للأسباب أخرى، كما يمكن أن يتم إبطال مفعول الشهادة أو إلغاؤها في بعض الحالات، كما هو الحال عندما يفقد صاحب الشهادة السيطرة على مفتاحه الخاص أو يتم كشفه، حيث يقع على عاتقه في مثل هذه الحالة إبلاغ سلطة التصديق، أو الجهة المزودة بالتوقيع الرقمي، وذلك حتى يتم إلغاءه ونشر وإعلان ذلك إلكترونياً من خلال سلطة التصديق، تحت طائلة تحمل الطرف المقصر المسؤولية تجاه أي متعامل حسن النية يستند إلى شهادة التصديق التي لم يتم إلغاءها[125].

(123) عايض راشد عايض المري، المرجع السابق، ص 244

(124) ابراهيم الدسوقي أبو الليل، المرجع السابق، ص186.

(125) عمر حسن المومني، التوقيع الإلكتروني وقانون التجارة الإلكترونية، ط1، دار وائل للنشر، الأردن، 2003، ص66.

هذا بالنسبة لشهادات التصديق التي تصدر داخل التراب الوطني، كما يمكن أن تكون هناك شهادات تصديق أجنبية، ولقد عالجت المادة 12 من القانون النموذجي للتوقيع الإلكتروني الفرنسي مسألة الشهادات والتوقيعات الأجنبية.

ولم يشد المشرع الجزائري عما ذهب إليه المشرع الفرنسي، حين تطرق لحالة شهادات التصديق التي يسلمها مؤدي خدمات تصديق إلكتروني مقيم في بلد أجنبي، ومنح لها نفس القيمة القانونية لتلك المسلمة بموجب أحكام القانون رقم 15--04 السالف ذكره-، بشرط أن يتصرف المؤدي الأجنبي في إطار اتفاقية للاعتراف المتبادل أبرمتها السلطة الوطنية للتصديق الإلكتروني معه[126].

مما سبق يمكن القول أن التوقيع الإلكتروني وشهادات التصديق الأجنبية، يُعوَّل عليها شرط توافر عنصر الثقة والاطمئنان فيها، وتلك وسيلة أيضا للاعتراف بالتوقيعات والشهادات المقابلة اعتمادا على مبدأ المعاملة بالمثل.

(126) المادة 63 من القانون رقم 15/ 04.

الخاتمة:

لقد حاول المشرع الجزائري من خلال قانون 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين، إلى وضع أرضية قانونية من شأنها حماية المتعاملين في مجال التكنولوجيا الرقمية بصفة عامة، والدفع الإلكتروني بشكل خاص، لذلك وبعد صدور هذا القانون من الضروري على الجهات المعنية «الإسراع» في تكييف ومطابقة الأنظمة الخاصة بالتعاملات الإلكترونية مع أحكام القانون السالف ذكره، وسن تشريع «لحماية البيانات والخصوصية على الإنترنت وردع المخالفات المتعلقة بهما». كما يجب وضع استراتيجية وطنية شاملة لتعميم استخدام التعاملات الإلكترونية في جميع المجالات، سيما منها التجارة والطب والتعليم وغيرها من التطبيقات، والقيام بحملات تحسيسية حول فوائد التعاملات الإلكترونية، مثل الدفع الإلكتروني إلى جانب التوعية في مجال أساليب الاختراق والقرصنة والغش وسرقة المعلومات الشخصية.

كما يجب وضع سياسات تعليمية وتكوينية قصد تلبية حاجيات سوق العمل من قوى عاملة متخصصة ومؤهلة في مجال التصديق الإلكتروني وتحديث أساليب التدريس والارتقاء بها بهدف «عصرنة» كل القطاعات وكذا دعم الدولة لأنشطة البحث العلمي في مجال تكنولوجيات الإعلام والاتصال مع الحرص على التأهيل والتدريب المتواصل للمورد البشري في مجال التعاملات الإلكترونية.

قائمة المراجع:

أولا- باللغة العربية:

1- الكتب والمؤلفات:

1. أحمد السيد لبيب، الدفع بالنقود الالكترونية الماهية والتنظيم القانوني دراسة تحليلية مقارنة، دار الجامعة الجديدة، الإسكندرية، مصر، 2009.
2. السيد محمد السيد عمران، الالتزام بالإعلام الالكتروني قبل التعاقد عبر شبكة الانترنت، الدار الجامعية، القاهرة، 2006.
3. أيمن علي حسين الحوثي، التوقيع الالكتروني بين النظرية التطبيق، دار المطبوعات الجامعية، 2011، ص 103 وما بعدها.
4. ثروت عبد الحميد، التوقيع الالكتروني، ماهيته، مخاطره، دار الجامعة الجديدة، القاهرة 2007.
5. حسين الماحي، نظرات قانونية في التجارة الالكترونية في التجارة الالكترونية، مجلة البحوث القانونية والاقتصادية، كلية الحقوق، جامعة المنصورة، العدد الحادي والثلاثين، أبريل، 2002.
6. خالد عبد التواب مبارك، الدليل الإلكتروني أمام القاضي المدني، دار النهضة العربية، مصر، 2001.
7. شريف محمد غنام، محفظة النقود الإلكترونية، رؤية مستقبلية، دار الجامعة الجديدة، الإسكندرية، مصر، 2007.
8. سعيد السيد قنديل، التوقيع الإلكتروني، دار الجامعة الجديدة، مصر، 2006.
9. سليمان مرقس، أصول الإثبات وإجراءاته في المواد المدنية في القانون المصري مقارناً بتقنينات سائر البلاد العربية، ج1، الأدلة المطلقة، عالم الكتب، القاهرة، 1987.
10. سميحة القليوبي، الأوراق التجارية، دار النهضة العربية، القاهرة، مصر، 1992.
11. طارق كاظم عجيل، ثورة المعلومات وانعكاساتها على القانون المدني "دراسات وبحوث" الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت- لبنان، 2011.
12. طارق محمد حمزة، النقود الإلكترونية كإحدى وسائل الدفع، تنظيمها القانوني والمسائل الناشئة عن استعمالها، الطبعة الأولى، منشورات زين الحقوقية، بيروت، لبنان، 2011.
13. طاهر شوقي مؤمن، عقد البيع الإلكتروني "بحث في التجارة الالكترونية"، دار النهضة العربية، مصر، 2007.
14. عادل أبو هشيمة محمود حوته، عقود خدمات المعلومات الالكترونية في القانون الدولي

الخاص، دار النهضة العربية، مصر، 2004.
15. عبد الفتاح بيومي حجازي، التجارة الالكترونية في القانون العربي لمكافحة جرائم الكومبيوتر والانترنت، دار الفكر الجامعي، 2006.
16. عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظم القانونية المقارنة، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2005.
17. علاء التميمي، التنظيم القانوني للبنك الالكتروني على شبكة الإنترنيت، دار الجامعة الجديدة، الإسكندرية، مصر، 2012.
18. عمر حسن المومني، التوقيع الالكتروني وقانون التجارة الالكترونية، ط1، دار وائل للنشر، الأردن، 2003.
19. عمر خالد زريقات، عقد البيع عبر الانترنت، دار الحامد للنشر والتوزيع، عمان، الأردن، 2007.
20. كيلاني عبد الراضي محمود، النظام القانوني لبطاقات الوفاء والضمان، دار النهضة العربية، مصر، 1998.
21. محمد المرسي زهرة، الحماية المدنية للتجارة الإلكترونية (العقد الإلكتروني، الإثبات الإلكتروني، المستهلك الإلكتروني)، دار النهضة العربية، القاهرة، 2008.
22. محمد حسين منصور، الإثبات التقليدي والالكتروني، دار الفكر الجامعي، الإسكندرية، مصر، 2006.
23. محمد سعيد أحمد إسماعيل، أساليب الحماية القانونية لمعاملات التجارة الالكترونية، دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت، لبنان، 2009.
24. محسن عبد الحميد البيه، قانون الإثبات في المواد المدنية والتجارية، مكتبة الجلاء الجديدة، المنصورة،1997.

2- مذكرات ورسائل جامعية:

1. إيمان مأمون أحمد سليمان، الجوانب القانونية لعقد التجارة الإلكترونية، رسالة دكتوراه، كلية الحقوق، جامعة المنصورة، 2005/2006.
2. حمودي ناصر، النظام القانوني لعقد البيع الدولي الإلكتروني المبرم عبر الإنترنت، رسالة دكتوراه في القانون الخاص، كلية الحقوق، جامعة مولود معمري تيزي وزو، 2009.
3. عايض راشد عايض المري، مدى حجية الوسائل التكنولوجية الحديثة في اثبات العقود التجارية، رسالة دكتوراه، جامعة القاهرة، مصر، 1998.

4. عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، القاهرة، مصر، 2004.
5. محمد أحمد محمود إسماعيل، مدى حجية التوقيع الإلكتروني في عقود التجارة الإلكترونية، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، 2005.
6. محمد أحمد محمد أنور جستنيه، مدى حجية التوقيع الالكتروني في عقود التجارة الإلكترونية، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 2005.

3- بحوث ومقالات قانونية:

1. إبراهيم الدسوقي أبو الليل، توثيق التعاملات الإلكترونية ومسؤولية جهة التوثيق تجاه الغير المضرور، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، الجزء الخامس، دبي، جامعة الإمارات العربية المتحدة، المنعقد ما بين 9–11 ربيع الأول 1424هـ الموافق 10–12 مايو 2003م.
2. أحمد الهاشمي، التشفير بالمفتاح المتناظر، مقالة منشورة على الموقع الالكتروني:
3. http://www.boosla.com/showArticle.php?Sec=Security&id=35
4. طوني عيسى، حول الدفع الإلكتروني بالبطاقة الائتمانية في شبكة الانترنت، الجديد في أعمال المصارف من الوجهتين القانون والاقتصادية، أعمال المؤتمر العلمي السنوي لكلية الحقوق بجامعة بيروت العربية، ج1، الجديد في التقنيات المصرفية، منشورات الحلبي الحقوقية.
5. فياض ملفي القضاه، مسؤولية البنك عن استخدام الكومبيوتر كوسيلة وفاء، مؤتمر القانون والكومبيوتر والإنترنت، الذي نظمته كلية الشريعة الإسلامية والقانون في جامعة الإمارات العربية المتحدة، الجزء الأول، الطبعة الثالثة، دبي الفترة الممتدة من 1–3 مايو 2000، 2004.
6. محمد المرسي زهرة، الدليل الكتابي وحجية مخرجات الكومبيوتر في المواد المدنية والتجارية، بحث مقدم إلى مؤتمر القانون والكومبيوتر والإنترنت، جامعة الإمارات العربية المتحدة، الجزء الثالث، المنعقد من 1–3 مايو 2000.

4- المراجع النصية:

أ- القوانين الجزائرية:

1. القانون المدني الجزائري.
2. القانون 15–03 المؤرخ في 11 ربيع الثاني 1436 الموافق لأول فبراير 2015 يتعلق بعصرنة

العدالة، ج.ر.عدد 06.

3. القانون 15/04 المؤرخ في 11 ربيع الثاني 1436 الموافق لأول فبراير سنة 2015، المتضمن قانون التوقيع والتصديق الالكترونيين، ج.ر.عدد 06.
4. المرسم التنفيذي رقم 07/ 162 المؤرخ في 13 جمادى الأولى عام 1428 الموافق لـ 30 ماي سنة 2007، المعدل والمتمم للمرسوم التنفيذي 01/123 والمتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية (ج.ر. عدد 37).

ب- القوانين العربية المقارنة:

- قانون رقم 25 لسنة 1968 بإصدار قانون الإثبات في المواد المدينة والتجارية المصريمعدلا بالقانون 23 لسنة1992والقانون 18 لسنة 1999 (ج.ر العدد 22 الصادر في 30 / 5 / 1968. منشور على الموقع:

http://ar.jurispedia.org/index.php

- اللائحة التنفيذية رقم 15 لسنة 2004، وكذلك القرار الوزاري المصري رقم 109 لسنة 2005 بتاريخ 15/5/ 2005، بإصدار اللائحة التنفيذية لقانون التوقيع الالكتروني وإنشاء هيئة تنمية صناعية تكنولوجيا للمعلومات . منشور على الموقع

http://www.laweg.net/Default.aspx?action=LegsTakenForm&FIID=1488

- قانون اليونسترال النموذجي بشأن التجارة الالكترونية لسنة 1996 منشور على الموقع:
http://www.uncitral.org/uncitral/ar/uncitral_texts/electronic_commerce/1996Model.html

- قانون اليونسترال النموذجي بشأن التوقيع الالكتروني لسنة 2001 منشور على الموقع:
https://www.uncitral.org/pdf/arabic/texts/electcom/ml-elecsig-a.pdf

Listes des Matières En Langue Etrangère:

1- Ouvrage:

MARTIN(S), TESSALONIKOS(A) et BENSOUSSAN(A), La signature électronique,premières réflexions après la publication de la directive du 13 décembre 1999 et la loi du 13mars 2000, Gaz. pal., recueil juillet-aout 2000.

II- Les Lois

- Loi type de la CNUDCI sur les signatures électroniques et Guide pour son incorporation 2001, Disponible sur
http://www.uncitral.org/pdf/french/texts/electcom/ml-elecsign-f.pdf
- code civil et relatif à la signature électronique, Disponible sur:
http://www.marche-public.fr/Marches-publics/Textes/Codes/Code-civil/code-civil-article-1316.htm
- Loi N° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique (JORF n°62 du 14 mars 2000). Disponible sur:
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000399095&dateTexte=&categorieLien
- Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur («directive sur le commerce électronique») .Disponible sur:
http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32000L0031
- 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 (JORF n°0077 du 31 mars 2001), (Dernière modification : 9 juillet 2009) .Disponible sur:
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000005630796&dateTexte=20020418
- 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, Dernier modification le Décret n°2010-1630 du 23 décembre 2010.Disponible sur:
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000005632663
- In addition, the National Conference of Commissioners on Uniform State Laws ("NCCUSL") is completing a project to develop a Uniform Electronic Transactions Act ("UETA") in the U.S - See more at: Thomas J. Smedinghoff and Ruth Hill Bro of Baker & McKenzie LLP, Electronic Signature Legislation, Disponible à
http://corporate.findlaw.com/business-operations/electronic-signature-

legislation.html

- E-signature Law, Disponible sur: http://www.e-signature.com/e-signature-law/
- Electronic Signatures in Global and National Commerce Act, Disponible sur: www.uytimes.com/library
- DIRECTIVE 1999/93/CE DU PARLEMENT EUROPÉEN ET DU CONSEIL

المحتوى:

الملخصات العربية للأبحاث الإنجليزية

المنظمات الدولية..وسيادة القانون والتنمية

د. أرديت ميميتي[1]

أ.د. ديفيد مورغان[2]

الملخص:

تشدد المنظمات الدولية بما فيها الأمم المتحدة والبنك الدولي والاتحاد الأوروبي على أهمية سيادة القانون كشرط مسبق للتنمية الاقتصادية والسياسية والاجتماعية. وعلى هذا الأساس، تنفق هذه المنظمات قدرًا كبيرًا من المال وتتخلص من الكثير من النفوذ. ومع ذلك، فإن سيادة القانون مفهوم متنازع عليه بشكل كبير، ومن الصعب تحديد العلاقة بين سيادة القانون والتنمية.

وإزاء هذه الخلفية، تقدم هذه الورقة أولا مناقشة للتعاريف المختلفة لمفهوم سيادة القانون من منظور المنظمات الدولية وممارسي سيادة القانون (الجزء 2). ومع ذلك، فقد اخترنا هنا التركيز بشكل رئيسي، على سبيل المثال لا الحصر، على الاتحاد الأوروبي، الذي يتم من خلال ممارساته استخلاص كل دراسة من دراسات الحالة (الجزء 3 و 4). بينما يقدم الجزء الخامس تعليقات ختامية حول ما إذا كان استخدام مصطلح "سيادة القانون" مفيدًا حقًا (أو غير مفيد) في هذا المجال.

المصطلحات المفتاحية:

المنظمات الدولية، سيادة القانون، التنمية، الأمم المتحدة، الاتحاد الأوروبي، البنك الدولي، بولندا، كوسوفو

---

(1) أستاذ مساعد – كلية القانون الكويتية العالمية

(2) أستاذ بكلية القانون الكويتية العالمية– وأستاذ فخري بكلية كورك الجامعية – **ايرلندا**

مجلة فصلية أكاديمية
محكّمة تعنى بنشر البحوث
والدراسات القانونية والشرعية

مجلة الحقوق

تصدر عن مجلس النشر العلمي - جامعة الكويت

صدر العدد الأول في
يناير ١٩٧٧

الاشتراكات

	في الكويت	في الدول العربية	في الدول الأجنبية
الأفراد	٣ دنانير	٤ دنانير	١٥ دولاراً
المؤسسات	١٥ ديناراً	١٥ ديناراً	٦٠ دولاراً

المراسلات

توجه جميع المراسلات إلى رئيس التحرير على العنوان الآتي:
مجلة الحقوق - جامعة الكويت ص.ب: ٦٤٩٨٥ الشويخ - ب 70460 الكويت
تلفون: ٢٤٨٣٥٧٨٩ - ٢٤٨٤٧٨١٤ فاكس: ٢٤٨٣١١٤٣
E.mail: jol@ku.edu.kw

عنوان المجلة في شبكة الإنترنت http://www.pubcouncil.kuniv.edu.kw/jol

ISSN 1029 - 6069