مجلة جامعة الأزهر – غزة، سلسلة العلوم الإنسانية 2014، المجلد 16، العدد 1 ص 319–350

الحمايـة الجنائيـة للتوقيــع الإلكترونــي في التشريعين الإماراتي والبحريني "دراسة مقارنة"

محمد أمين الخرشة
mohammadamin76@yahoo.com
كلية القانون
جامعة العين للعلوم والتكنولوجيا – الامارات

نايف عبدالجليل الحمايدة
كلية القانون
جامعة العين للعلوم والتكنولوجيا – الامارات

تاريخ الاستلام 2013/10/8 تاريخ القبول 2014/4/7

المخلص:

يتناول هذا البحث موضوع الحماية الجنائية للتوقيع الإلكتروني في التشريعين الإماراتي والبحريني، حيث حرص المشرع الإماراتي على تقرير حماية جنائية للتوقيع الإلكتروني في قانون المعاملات والتجارة الإلكترونية رقم 1 لسنة 2006م، وخطا أيضاً خطوة إيجابية في هذا الاتجاه فأصدر القانون الاتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات، أما المشرع البحريني فقد اهتم بموضوع التوقيع الإلكتروني، وأصدر القانون رقم (28) لسنة 2002م بشأن المعاملات الإلكترونية .

وفي سبيل التعرف على الحماية الجنائية للتوقيع الإلكتروني في التشريعين الإماراتي والبحريني، فقد آثرنا ان نبحث عن حقيقة التوقيع الإلكتروني في المبحث الأول ، لندخل من ذلك إلى رحاب المبحث الثاني لبيان صور الحماية الجنائية للتوقيع الإلكتروني في التشريعين الإماراتي والبحريني ، وقد أنهينا البحث بخاتمة اشتملت على أهم النتائج والتوصيات .

Abstract:

The criminal protection of electronic signature in the Emiratis and Bahraini legislation

This article deals with the criminal protection of electronic signature in the Emiratis and Bahraini legislation.

The Emiratis legislature provides criminal protection for electronic signature in the law of electronic transactions and commerce N 1 of 2006. Another positive step was taken with the promulgation of the federal law N 5 of 2012 concerning the prevention of information technology crimes. The Bahraini legislature also provides for the protection of electronic signature in the law N 28, 2002 concerning electronic transactions.

This article is divided in to two sections. The first one deals with concept of electronic signature; while the second is devoted to the various aspect of

criminal protection of electronic signature in both the Emiratis and Bahraini legislation. The conclusion presents the aim result and recommendations.

المقدمة:

يطالعنا تطور تكنولوجيا المعلومات والاتصال الحديث في كل يوم بأوضاع جديدة، أصبحت معه الوسائل الإلكترونية العصب المحرك للتجارة الإلكترونية، فمعظم المعاملات المالية والتجارة أصبحت تتم إلكترونيا، وبالتالي لم تعد الوسيلة التقليدية في إثبات التصرفات القانونية " التوقيع التقليدي " ملائمة للتعاقدات الحديثة التي تتم في الشكل الإلكتروني، لذا ظهر التوقيع الإلكتروني ليكون بديلا عن التوقيع التقليدي، ليتوافق وطبيعة التعاقدات القانونية والعقود التي تتم باستخدام الوسائل والأجهزة الإلكترونية الحديثة .

ويحتاج هذا التطور السريع في مجال التجارة الإلكترونية الى تنظيم، وقد تنبهت الدول المتقدمة مبكراً إلى غياب القوانين التي تنظم التجارة الإلكترونية، إلا أنها اختلفت في موضع النص على حمايتها جنائيا، فمنها من أصدر قانونا مستقلا عاقب بمقتضاه على الجرائم التي تمس بقدسية التعاقد الإلكتروني(التشريع الأمريكي)، وهناك تشريعات أخرى ذهبت إلى إدخال تعديلات على النصوص التشريعية القائمة على نحو يؤدي بها إلى استيعاب الصور المستحدثة من الجرائم الالكترونية ومن بينها التشريع الفرنسي، وإلى جانب الجهود الدولية في هذا المجال هناك جهود المنظمات غير الحكومية والتي تناولت موضوع التعاقد الإلكتروني، ومن ذلك على سبيل المثال ما يتعلق بالتجارة الالكترونية، مثل: القانون النموذجي للتجارة الإلكترونية لسنة 1996، والمبادرة الأوروبية التي قامت بها اللجنة الأوروبية للاتصالات في أبريل سنة1997 م[1].

ولا يتم حماية التوقيع الإلكتروني الا بقواعد قانونية جديدة تواجه هذا التطور السريع، لذا نجد أن المشرعين الإماراتي والبحريني قد أظهر كل منها استجابة لهذا التطور، وتمكنا من إضفاء الحماية الجنائية للتوقيع الإلكتروني، فقد حرص المشرع الإماراتي على تقرير حماية جنائية للتوقيع الإلكتروني في قانون المعاملات والتجارة الإلكترونية رقم 1 لسنة2006 م، وأفرد الفصل التاسع منه للعقوبات على الجرائم الماسة بالتوقيع الإلكتروني.

وخطا أيضاً خطوة إيجابية في هذا الاتجاه فأصدر القانون الاتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات[2]، وتضمن القانون العديد من المواد التي من شأنها توفير الحماية

[1] – د. اشرف توفيق شمس الدين، الحماية الجنائية للمستند الإلكتروني، مؤتمر الأعمال المصرفية والإلكترونية بين الشريعة والقانون، جامعة الامارات، 10 – 12 مايو 2003م، المجلد الثاني، ص487.

[2] – الذي ألغي بموجبه القانون الاتحادي رقم (2) لسنة 2006 بشأن مكافحة جرائم تقنية المعلومات.

القانونية لخصوصية ما يتم نشره وتداوله على الشبكة المعلوماتية من معلومات وبيانات وأرقام تتعلق بالبطاقات الائتمانية وأرقام وبيانات الحسابات المصرفية أو أية وسيلة من وسائل الدفع الإلكتروني، وكذلك كل استخدام لأي من وسائل تقنية المعلومات في تزوير أو تقليد أو نسخ للبطاقات الائتمانية . كما اهتم المشرع البحريني بموضوع التوقيع الإلكتروني، اصدر القانون رقم (28) لسنة2002 م بشأن المعاملات الإلكترونية، وأورد نصاً خاصاً بالعقوبات على الأفعال الإجرامية التي تنال من التوقيع الإلكتروني، ويعد إصدار القانونين خطوة مهمة أدركها كل من المشرعين البحريني والإماراتي في الوقت المناسب، ليواكب التطور التكنولوجي في مجال تقنية المعلومات ووسائل الاتصال.

وبما أن المشرعين الإماراتي والبحريني قد أظهر كل منهما استجابة لهذا التطور، فإننا سنبين معالم الحماية الجنائية للتوقيع الإلكتروني وحدود ونطاق هذه الحماية واستظهار الأفعال الإجرامية التي تنال منه، وبيان خطة المشرعين الاماراتي والبحريني في كفالة الحماية الجنائية له.

وبيان مدى كفاية هذه الخطة في تجريم الأفعال التي تنال من التوقيع الإلكتروني.

منهج البحث:

اتبعنا في هذا البحث المنهج الوصفي التحليلي المقارن للنصوص القانونية في التشريعين الإماراتي والبحريني، مع التعرض لبعض التشريعات الغربية والعربية .

خطة البحث :

وفي سبيل التعرف على الحماية الجنائية للتوقيع الإلكتروني في التشريعين الإماراتي والبحريني، فإن بناء هذا البحث قام على تقسيمه إلى مبحثين على النحو الآتي:-

المبحث الأول:- حقيقة التوقيع الإلكتروني.

المطلب الأول: تعريف التوقيع الإلكتروني وتمييزه عن التوقيع الكتابي.

المطلب الثاني: شروط صحة التوقيع الإلكتروني وصوره.

المبحث الثاني:- صور الحماية الجنائية للتوقيع الإلكتروني .

المطلب الأول:- صور الحماية الجنائية للتوقيع الإلكتروني في التشريع الإماراتي .

المطلب الثاني:- صور الحماية الجنائية للتوقيع الإلكتروني في التشريع البحريني.

المبحث الأول

حقيقة التوقيع الإلكتروني

بظهور فكرة التوقيع الإلكتروني في مجال المبادلات والمعاملات التجارية الإلكترونية كبديل عن العناصر المادية في الإثبات، أثر ذلك على البناء القانوني الذي وجد نفسه ملزماً بضرورة التصدي لمثل هذا النوع من التقنيات الرقمية، لذا نجد أن معظم التشريعات قد لجأت لتحديد مدلول

التوقيع الإلكتروني وشروط صحته ، باعتباره الوسيلة الضرورية التي لا غنى عنها في مجال المعاملات الإلكترونية . فإذا كان التوقيع الإلكتروني يتميز بطبيعته غير المادية وغياب الطابع الشكلي المحسوس وقت إجراء العقد، فإن ذلك يطرح مشكلة مدى انسجام هذا الوسط الجديد مع التوقيع الكتابي الذي يعتمد على الورق؟ و هل هناك اعتراف قانوني بالتوقيع الالكتروني ؟ وهل له شروط معينة ؟

وعليه وفي سبيل التعرف على حقيقة التوقيع الإلكتروني لابد من الوقوف على تعريف التوقيع الإلكتروني وتمييزه عن التوقيع الكتابي، بالإضافة إلى بيان شروط صحة التوقيع الإلكتروني وصوره، وهو ما سنعالجه في هذا المبحث، ونقسمه الى مطلبين:

المطلب الأول: تعريف التوقيع الإلكتروني وتمييزه عن التوقيع الكتابي.

المطلب الثاني: شروط صحة التوقيع الإلكتروني وصوره

المطلب الأول

تعريف التوقيع الإلكتروني وتمييزه عن التوقيع الكتابي

سوف نتناول تعريف التوقيع الإلكتروني ، ثم نبين أوجه الاتفاق والاختلاف بينه وبين التوقيع الكتابي في الفرعيين الآتيين .

الفرع الأول

تعريف التوقيع الإلكتروني

وقد عرف المشرع الإماراتي التوقيع الإلكتروني في المادة الأولى من القانون الاتحادي رقم (1) لسنة 2006م في شأن المعاملات والتجارة الإلكترونية تعريفا مزدوجا بحيث عرفه تعريفا عاما بقوله إنه: "توقيع مكون من حروف أو أرقام أو رموز أو صوت أو نظام معالجة ذي شكل إلكتروني وملحق أو مرتبط منطقياً برسالة إلكترونية بنية توثيق أو اعتماد تلك الرسالة ".

و من جهة أخرى أضاف تعريفا نوعيا ثانيا خاصا بالتوقيع الإلكتروني المحمي، بحيث يعامل التوقيع على أنه توقيع الكتروني محمي إذا كان من الممكن التحقق من خلال تطبيق إجراءات توثيق محكمة منصوص عليها في هذا القانون أو معقولة تجاريا و متفق عليها بين الأطراف من أن التوقيع الإلكتروني كان في الوقت الذي تم فيه ينفرد به الشخص الذي استخدمه، ومن الممكن أن يثبت هوية ذلك الشخص، ويكون تحت سيطرته التامة سواء بالنسبة لإنشائه أو وسيلة استعماله وقت التوقيع،

كما أنه يرتبط بالرسالة الإلكترونية، بحيث إذا تم تغيير السجل الالكتروني فإن التوقيع الإلكتروني يصبح غير محمي[1].

وعرف المشرع البحريني التوقيع الإلكتروني في المادة الأولى من القانون رقم (28) لسنة 2002م بشأن المعاملات الإلكترونية بقوله إنه (معلومات في شكل إلكتروني تكون موجودة في سجل إلكتروني أو مثبته أو مقترنة به منطقياً، ويمكن للموقع استعمالها لإثبات هويته)، كذلك عرفته المادة الأولى من القانون المصري رقم 15 لسنة 2004 بشان تنظيم التوقيع الإلكتروني بأنه "كل حروف أو أرقام أو رموز أو أي علامات أخرى تثبت على دعامة إلكترونية أو رقمية أو ضوئية أو أية وسيلة أخرى مشابهة وتعطي دلالة قابلة للإدراك"[2].

ولقد جاء تعريف معظم التشريعات العربية للتوقيع الإلكتروني منسجماً مع تعريف قانون الأمم المتحدة النموذجي (الأونسيترال) بشأن التوقيعات الإلكترونية لعام 2001، حيث عرفت المادة الثانية منه التوقيع الإلكتروني بأنه "بيانات في شكل إلكتروني مدرجة في رسالة بيانات أو مضافة إليها أو مرتبطة بها منطقياً، يجوز أن تستخدم لتعيين هوية الموقع بالنسبة إلى رسالة البيانات، ولبيان موافقة الموّقع على المعلومات الواردة في رسالة البيانات"

ومن خلال هذا التعريف نجد أن لجنة الأمم المتحدة للتجارة الإلكترونية (الأونسترال) وضعت القواعد الموحدة بشأن التوقيعات الإلكترونية وهي:

---

[1]- المادة 17 من القانون رقم 1 لسنة 2006م في شأن المعاملات والتجارة الإلكتروتي الإماراتي.

[2]- ويتماثل هذا التعريف مع تعريف المشرع العماني الذي عرف التوقيع الإلكتوني بموجب المادة الأولى من قانون المعاملات الإلكترونية رقم 69 لسنة 2008م بأنه"التوقيع على رسالة او معاملة إلكترونية في شكل حروف او أرقام أو إشارات أو غيرها ويكون له طابع متفرد يسمح بتحديد شخص الموقع وتمييزه عن غيره.
وكذلك جاء تعريف المشرع القطري مطابقاً لهذا التعريف، انظر المادة رقم1 من قانون المعاملات والتجارة القطري رقم 16 لسنة 2010م، وفي نفس المعنى جاء تعريف المشرع السوداني للتوقيع الالكتروني في المادة 1 من قانون المعاملات الإلكترونية السوداني لسنة2007 . كما عرف المشرع الأردني التوقيع الإلكتروني في المادة الثانية من قانون المعاملات الإلكترونية رقم 58 لسنة 2001 بأنه: "البيانات التي تتخذ هيئة حروف أو أرقام أو رموز أو إشارات أو غيرها وتكون مدرجة بشكل إلكتروني أو رقمي أو ضوئي أو أي وسيلة أخرى مماثلة في رسالة معلومات أو مضافة عليها أو مرتبطة بها ولها طابع يسمح بتحديد هوية الشخص الذي وقعها ويميزه عن غيره من أجل توقيعه وبغرض الموافقة على مضمونة".
وعرفه المشرع السوري قي المادة الأولى من القانون الخاص بالتوقيع الإلكتروني الصادر عام 2009 بأنه: "جملة بيانات تدرج بوسيلة إلكترونية على وثيقة إلكترونية وترتبط بها، وتتخذ شكل حروف أو أرقام أو رموز أو إشارات أو أي شكل آخر مشابه، ويكون لها طابع متفرد يسمح بتحديد شخص الموقع ويميزه عن غيره وينسب إليه وثيقة إلكترونية بعينها".

1. عدم تحديد الوسيلة التي يتم بها استخدام التوقيع الإلكتروني، فاتحاً المجال لإيراد أي وسيلة تراها الدول ملائمة من ترميز أو تشفير أو أي وسيلة أخرى تكون مناسبة.
2. إن اللجنة ركزت على أن أي وسيلة للتوقيع يجب أن تحقق وظائف التوقيع من تحديد لهوية الشخص الموقع والتعبير عن إرادته بالموافقة على مضمون رسالة البيانات، ومن المؤكد أن كل توقيع أيا كانت الطريقة المستخدمة في إنشائه يجب أن يحقق تلك الوظائف.

أما في التشريعات الغربية فإننا نجد بأن مجلس البرلمان الأوروبي عرف التوقيع الالكتروني بأنه " بيان ذات طابع الكتروني يكون مضافاً أو مرتبطاً إلكترونياً ببيانات إلكترونية أخرى، وذلك بهدف أن يكون وسيلة للإثبات"[1].

[1] – La Directive 1999/ 93 CE du Parlement européen et du conseil du 13 décembre 1999 surune cadre communautaire pour la signature électronique (JO L 13 du 19. 1.2000., p. 12) définit la signature électronique comme " une donnée sous forme électronique qui est jointe ou liée électronique à d'autre données électroniques et qui sert de méthode d'authentification".....

قدم التوجيه الأروبي تعريفاً مزدوجاً للتوقيع الإلكتروني ، فمن جهة عرفه بشكل عام في المادة الثانية بأنه " بيانات إلكترونية مرتبطة ببيانات أخرى يهدف الى التصديق " ومن جهة اخرى فقد أضاف تعريفاً نوعياً خاصاً لما يسمى التوقيع الإلكتروني المحمي أو المركب : التوجيه الاتحادي الصادر فى 13 ديسمبر 1999 (19/1/200 J.O.C.E 13/12) ، والذى عنى بوضع نظام قانونى اتحادى للتوقيع الالكترونى . ويتكون هذا التوجيه من خمسة عشر مادة وأربع ملاحق.

Art.02-01 : « une don née sous forme électronique jointe ou liée logiquement à d'autres données électroniques et servant de méthode d'authentification »..

« Les Etats membres veillent à ce que les signatures électroniques avancées [...] répondent aux exigences légales d'une

signature à l'égard de données électronique de la même manière qu'une signature manuscrite répond à ces exigences à

l'égard de données manuscrites ou imprimées sur papier », Directive n° 1999/93/CE du Parlement et du Conseil du 13

Décembre 1999 sur un cadre communautaire pour les signatures électroniques (JOCE 19 Janv. 2000, n° L13, p.12

73 Art.02-02:«On entend par signature électronique avancée, une signature électronique qui satisfait aux exigences

suivantes : a) être liée uniquement au signataire ;

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 ».

وكذلك عرف المشرع الفرنسي التوقيع الإلكتروني في القانون المدني، بموجب نص المادة 1316- 4 من القانون المدني التوقيع الإلكتروني بأنه يشتمل على مختصرات لمعاملة موثقة إلكترونيا للتحقق من شخصية من تصدر عنه هذه الإجراءات، وقبوله بمضمون التصرف الذي يصدر التوقيع بمناسبته[1].

وعرف القانون الاتحادي الأمريكي التوقيع الإلكتروني بأنه " صوت أو رمز أو إجراء يقع في شكل إلكتروني متحد بعقد أو سجل آخر يتم تنفيذها أو إصدارها من شخص بقصد التوقيع على السجل"[2].

وفي نفس الاتجاه ذهب المشرع الإنجليزي إذ نص الفصل الأول من لائحة التوقيع الإلكتروني الصادرة في 8 مارس 2002 على ان "التوقيع الإلكتروني يعني بيانات في شكل إلكتروني ملحقة أو متحدة منطقياً بغيرها من البيانات الإلكترونية والتي تصلح كوسيلة للتوثيق"[3]. هذا فيما يتعلق بالتعريف التشريعي للتوقيع الإلكتروني .

أما على الصعيد الفقهي، فقد كان هناك العديد من المحاولات لتعريف التوقيع الإلكتروني، بعضها ركز على طريقة إنشاء التوقيع ، أما الأخرى فركزت على الوظائف التي يقوم بها التوقيع الإلكتروني فذهب جانب من الفقه في تعرفه للتوقيع الالكتروني بأنه: عبارة عن ضغط رسالة –

---

[1] –En droit française et selon l'article 1316-4 du Code Civile la législature dispose que ". Lorsqu'elle (la signature) est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signature assurée et l'intégrité de l'acte garantie, dans des conditions fixées en conseil d'Etat". En savoir plus voir L n° 2000-230, du 13 mars 2000, JO 13 et 14 mars 2000, p. 3968; Directive 1999/ 93/ CE, n° L 13 du 19 janvier 2000, p. 12 et s; J.C.P éd. E. 2000, p. 198; D. 2000, lège. P. 95

د . عبدالإله محمد النوايسة، مدى توفير حماية جزائية للتوقيع الإلكتروني ومعطياته في القانون الاردني دراسة مقارنة، المجلة الأردنية في القانون والعلوم السياسية، المجلد(2) العدد(2)، 2010م ، ص 120 .

[2] – " all electronic sound ، sybol ، or process" that is" attached to or logically associated with" a contract or other record, and that is "executed or adopted by a person with the intent to sign the record. E- sign law S 106 (5).

[3] – د. اشرف توفيق شمس الدين، الحماية الجنائية للمستند الإلكتروني، مؤتمر الأعمال المصرفية والإلكترونية بين الشريعة والقانون، جامعة الامارات، 10 – 12 مايو 2003م، المجلد الثاني، ص506

بتشفير هذه الرسالة المضغوطة – برمز سري خاص بموقع الرسالة[1]. في حين عرفه رأي آخر بأنه (حرف أو أرقام أو رموز أو إشارات لها طابع منفرد، تسمح بتحديد شخص صاحب التوقيع وتمييزه عن غيره، ويتم اعتماده من جهة مختصة)[2]. وذهب رأي آخر ـ نؤيده ـ وعرفه بأنه: عبارة عن بيانات إلكترونية أياً كان الشكل الذي تكون عليه، ويكون لها دلالة في تحديد مستخدميها ويكون لها نفس الأثر المترتب على التوقيع التقليدي وتميز صاحب التوقيع عن غيره [3] .

ونخلص إلى أن التعريفات لم تشر بشكل حصري لصور التوقيع الإلكتروني، ، بل أجازت أن يتخذ أي شكل سواء كان في هيئة صور أو حرف أو رقم أو رمز أو إشارة أو حتى صوت، شريطة أن يكون له طابع منفرد يسمح بتمييز شخص صاحب التوقيع وتحديد هويته وإظهار رغبته في إقرار العمل القانوني أو الرضا بمضمونه، كما أن التعريفات لم تربط التوقيع بشكل مادى محدد بل أشارت إلى كونه مرتبطاً بسجل ارتباطاً منطقياً. تاركةً المجال مفتوحاً كي يتسع هذا التعريف لما يستجد من تطورات تكنولوجية قد تفرز اشكالاً وصوراً جديدة من التواقيع الإلكترونية .

الفرع الثاني

التمييز بين التوقيع الإلكتروني والتوقيع الكتابي

يتفق التوقيع الإلكتروني والتوقيع الكتابي باعتبارهما من أهم الآليات الخاصة التي يعتد بها في إثبات التصرفات القانونية، و أن فحوى كل منهما الحقيقة التي يريد المشرع حمايتها، إلا أنهما يختلفان من عدة نواح:

1. تحدد أغلب التشريعات صور التوقيع الكتابي، حيث يكون غالباً في الإمضاء أو بصمة الختم أو بصمة الأصابع ، أما بالنسبة للتوقيع الإلكتروني، فإن التشريعات التي صدرت لم تضع

---

[1] – Alain BENSSONSAN, L'informatique et droit . mémento- guide, Tomme II. Hermès. 1994. p. 34

[2] – منير محمد الجنبيهي وممدوح محمد الجنبيهي، التوقيع الإلكتروني وحجيته في الإثبات، دار الفكر العربي، القاهرة ، 2004م، ص 8

[3] – د . عبدالإله محمد النوايسة، مدى توفير حماية جزائية للتوقيع الإلكتروني ومعطياته في القانون الاردني دراسة مقارنة، المرجع السابق، ص 122.

وحول تعريف التوقيع الإلكتروني انظر: د. ثروت عبد الحميد، التوقيع الإلكتروني ، ماهيته، مخاطره، كيفية مواجهتها،حجيته في الإثبات، مكتبة الجلاء المنصورة، 2001م. و د. د .ممدوح محمد خيري المسلمي، مشكلات البيع الإلكتروني عن طريق الانترنت ، دار النهضة العربية، القاهرة، 2000م،ص164. د. سعيد السيد قنديل : التوقيع الإلكتروني، "الجامعة الجديدة للنشر ، الإسكندرية 2004، ص49. ، د. نجوي أبو هيبه : التوقيع الإلكتروني ، تعريفه ، مدي حجيته في الإثبات ، دار النهضة العربية ، 2002 .

صورة معينة للتوقيع الإلكتروني، بل أجازت أن يتخذ أي شكل سواء كان في هيئة صور أو حرف أو رقم أو رمز أو إشارة أو حتى صوت، شريطة أن يكون له طابع منفرد يسمح بتميز شخص صاحب التوقيع وتحديد هويته وإظهار رغبته في إقرار العمل القانوني أو الرضا بمضمونه[1].

2. الوسيط المستخدم في التوقيع الكتابي يكون في الغالب دعامة ورقية تذيل بالتوقيع الكتابي . أما بالنسبة للتوقيع الإلكتروني، فإن الوسيط يكون وسيطاً إلكترونياً من خلال أجهزة الحاسب الآلي وعبر شبكة الإنترنت[2].
3. يتميز التوقيع الإلكتروني عن التوقيع الكتابي بأنه يمكن من خلاله استنباط مضمون المحرر الإلكتروني وتأمينه من التعديل بالإضافة أو الحذف، وذلك بالربط بينه وبين التوقيع الإلكتروني، بحيث يقتضي أي تعديل لاحق توقيع جديد، كما يتميز التوقيع الإلكتروني بأنه يمنح للمستند صفة المحرر الأصلي، وبالتالي يجعل منه دليلاً معداً مسبقًا للإثبات قبل أن يثور النزاع بين الأطراف.
4. يمكن التوقيع الكتابي بالعديد من الوسائل، مثل: الإمضاء أو الختم أو بصمة الأصابع، ويمكن أن يستبدل أي من هذه الوسائل محل الأخرى على عكس التوقيع الإلكتروني الذي لا يتم إلا بوسيلة واحدة محددة سلفًا ووفق إجراءات تقنية آمنة بحيث تسمح بالتعرف على شخصية الموقع وتضمن سلامة المحرر من العبث أو التحريف[3].
5. من حيث الأطراف في التوقيع الكتابي طرفين فقط الموجب و القابل، أما في التوقيع الإلكتروني ثلاثة أطراف الموجب و القابل و مزود خدمة المصادقة الإلكترونية[4].

---

[1]- انظر المادتين 17،1 من القانون الاتحادي رقم(1) لسنة 2006م في شأن المعاملات والتجارة الإلكترونية الاماراتي .

[2]- عرف المشرع الإمارتي الوسيط الإلكتروني المؤتمت بأنه برنامج او نظام إلكتروني لوسيلة تقنية المعلومات التي تعمل تلقائياً بشكل مستقل، كلياً أو جزئياً دون إشراف من أي شخص طبيعي في الوقت الذي يتم فيه العمل أو الاستجابة له. انظر المادة 1 من القانون الاتحادي رقم(1) لسنة 2006م في شأن المعاملات والتجارة الإلكترونية .

[3]- د .ثروت عبد الحميد، التوقيع الإلكتروني – مكتبة الجلاء الجديدة بالمنصورة مصر .٢٠٠٢/ ٢٠٠٣ الطبعة الثانية ،ص51–52. د .فاروق محمد أحمد الأباصيري، عقد الاشتراك في قواعد المعلومات عبر شبكة الإنترنت دراسة تطبيقية لعقود التجارة الإلكترونية الدولية – دار الجامعة الجديدة للنشر مصر ،٢٠٠٢ الطبعة الأولى، ص79.

[4]- عرف المشرع الإمارتي مزود خدمة المصادقة الإلكترونية بأنه (أي شخص أو جهة معتمدة او معترف بها تقوم بإصدار شهادات تصديق إلكترونية أو أية خدمات أو مهمات بها وبالتوقيعات الإلكترونية). انظر المادة 1 من القانون الاتحادي رقم(1) لسنة 2006م في شأن المعاملات والتجارة الإلكترونية .

6. يتميز التوقيع الإلكتروني بطبيعته غير المادية وغياب الطابع الشكلي المحسوس وقت اجراء العقد، فهو يحدد هوية و شخصية الموقع المتعاقد عن بعد، ويحقق قدر من الأمن و الثقة في صحته، أما التوقيع الكتابي فإنه يحدد هوية و شخصية الموقع ويعد دليلاً على الحضور المادي.
7. التحقق من صحة التوقيع الكتابي يتم بواسطة متخصصين و بعد اللجوء للقضاء، ويمكن الاقتطاع منه، وسهل التزوير، أما التحقق من صحة التوقيع الإلكتروني يتم تلقائيًا أثناء عملية التوقيع ذاتها وعند مستقبل الرسالة الموقعة الكترونياً.
8. إن تزوير التوقيع الكتابي يترك أثراً في كثير من الأحوال يدل عليه، بخلاف التزوير المنصب على التوقيع الإلكتروني الذي يتألف من شفرة تحدد هوية الموقع، وهذه الشفرة يمكن التدخل فيها أو محوها، لذا فإنه يصعب اكتشافه والوقوف على مرتكب التزوير[1].

المطلب الثاني

شروط صحة التوقيع الإلكتروني وصوره

هناك شروط يجب أن يتضمنها التوقيع الإلكتروني، فضلاَ عن أن التوقيع الإلكتروني لا يأخذ صورة واحدة، فكما تختلف صور التوقيع التقليدي بين التوقيع بالإمضاء، والختم ، والتوقيع ببصمة الإصبع، فإن التوقيع الإلكتروني له أيضا صور مختلفة ومتعددة. لذا سنبين شروط وصور التوقيع الإلكتروني في الفرعين الآتيين:

---

[1]– د. اشرف توفيق شمس الدين، الحماية الجنائية للمستند الإلكتروني، المرجع السابق ، ص537.

التشفير هو تغيير في شكل البيانات عن طريق تحويلها إلى رموز أو إشارات لحماية هذه البيانات من اطلاع الغير عليها أو تعديلها أو تغييرها. د. هدى حامد قشقوش، الحماية الجنائية للتوقيع الإلكتروني، مؤتمر الأعمال المصرفية والإلكترونية بين الشريعة والقانون، جامعة الامارات، 10 – 12 مايو 2003م، المجلد الثاني، ص590.

انظر فى المقصود بالتشفير، وضوابطه، وعلته، وطرقه،

Golic، Jovan Dj. 2001. How to Construct Cryptographic primitives from stream Ciphers. Comuters and security. Vo1 20، no.i .pp. 79—88. Amesterdam.

د. لورانس محمد عبيدات ، اثبات المحرر الالكترونى، دار الثقافة للنشر والتوزيع ، 2005م ، ص 136 وما بعدها . ود. محمد فواز المطالقة، الوجيز في عقود التجارة الإلكترونية، دار الثقافة للنشر والتوزيع، عمان، 2006م، ص165 وما بعدها. كما عرفه المشرع التونسى فى مادة 5/2 من قانون المبادلات والتجارة الالكترونية التونسى بأنه " استعمال رموز وإشارات غير متداولة تصبح بمقتضاها المعلومات المرغوب تحريرها أو إرسالها غير قابلة للفهم من قبل الغير أو إستعمال رموز وإشارات لا يمكن وصول المعلومة بدونها".

الفرع الأول

شروط صحة التوقيع الإلكتروني

وردت هذه الشروط بصورة مفصلة في قانون الأمم المتحدة النموذجي1 (الأونستيرال) لسنة 2001 ، ونصت على الشروط ذاتها الفقرة الثانية من المادة الثانية، والفقرة الأولى من المادة الخامسة من التوجه الأوروبي الخاص بالتوقيع الإلكتروني2، كما وردت هذه الشروط في قانون المعاملات والتجارة الإلكترونية الإماراتي3 وقانون المعاملات الإلكترونية البحريني[1]. وهذه الشروط هي:

---

[1] - نصت المادة السادسة من قانون الأمم المتحدة النموذجي ، في فقرتها الثالثة على أنه:

يعتبر التوقيع الإلكتروني قابلاً للتعويل عليه لغرض الوفاء بالاشتراط المشار إليه في الفقرة 1 إذا :

(أ) كانت بيانات إنشاء التوقيع مرتبطة، في السياق الذي يستخدم فيه، بالموقع دون أي شخص آخر .

(ب) كانت بيانات إنشاء التوقيع خاضعة، وقت التوقيع، لسيطرة الموقع دون أي شخص آخر .

(ج) كان أي تغيير في التوقيع الإلكترونيُ يجري بعد حدوث التوقيع قابلاً للأكتشاف .

(د) كان الغرض من إشتراط التوقيع قانوناً هو تأكيد سلامة المعلومات التى يتعلق بها التوقيع وكان أي تغيير يجري في تلك المعلومات بعد وقت التوقيع قابلاً للإكتشاف .

[2]- Article 2 – Definitions: For the purpose of this Directive: 2- "advanced electronic signature" means an electronic signature which meets the following requirements:
(a) It is uniquely linked to the signatory (b) it is capable of identifying the signatory. (c) It is created using means that signatory can maintain under his sole control, & (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

[3] – نصت المادة (17) من القانون رقم 1 لسنة 2006م في شأن المعاملات والتجارة الإلكترونية الاماراتي، بأنه "(1) يعامل التوقيع على أنه توقيع الإلكتروني محمي إذا كان من الممكن التحقق من خلال تطبيق إجراءات توثيق محكمة، منصوص عليها في هذا القانون أو معقولة تجارياً ومتفق عليها بين الطرفين من أن التوقيع الإلكتروني كان في الوقت الذي تم فيه:

أ- ينفرد به الشخص الذي استخدمه. ب- ومن الممكن أن يثبت هوية ذلك الشخص . ج- وأن يكون تحت سيطرته التامة سواء بالنسبة لإنشائه أو وسيلة استعماله وقت التوقيع. د- ويرتبط بالرسالة الإلكترونية ذات الصلة به بطريقة توفر تأكيداًيعتمد عليه حول سلامة التوقيع، بحيث اذا تم تغيير السجل الإلكتروني فإن التوقيع الإلكتروني يصبح غير محمي .

(2) يعد الاعتماد على التوقيع الإلكتروني المحمي معقولاً ما لم يثبت العكس".

اولاَ: أن يكون استخدام الأداة التي يتم فيها إنشاء التوقيع الإلكتروني مقصوراً على الموقع وحده فقط دون غيره، ويجب أن تكون هذه الوسيلة آمنة لتحديد هوية الموقع وتضمن صلته بالتصرف الذي وقع عليه.

ثانياً: أن تخضع الأداة المستخدمة في إنشاء التوقيع الإلكتروني – وقت التوقيع– لسيطرة صاحب التوقيع دون أي شخص آخر. ولكي يكون للتوقيع الإلكتروني قيمة قانونية يجب أن تكون الأدوات والوسائل المستخدمة في وضع التوقيع تحت السيطرة المباشرة لصاحب التوقيع وحده لأنها هي التي تميزه عن غيره من الأشخاص، كما يجب أن تكون هناك صلة بين هذا التوقيع والتصرف القانوني الذي وضع التوقيع الإلكتروني بسببه، ودون ذلك فلا يترتب على التوقيع الإلكتروني أثر قانوني ولا يكون حجة في الإثبات، لأنه في هذه الحالة لا يعبر عن هوية صاحب التوقيع[2].

ثالثاَ: إمكانية كشف ومعرفة أي تغيير قد يحصل للتوقيع الإلكتروني بعد وضع هذا التوقيع .ويعني هذا الشرط وجوب المحافظة على صحة التوقيع الإلكتروني، بحيث يكون بالصورة نفسها التي صدر فيها من صاحبه، و إذا جرى عليه أي تغيير أو حذف أو إضافة، بعد وضعه على التصرف القانوني يمكن كشفه بوضوح.

رابعاَ: إمكانية كشف ومعرفة أي تغيير قد يحصل في المعلومات المرتبطة بالتوقيع بعد وضعه على هذه المعلومات أي أن التوقيع الإلكتروني لا ينشأ مجرداً، وإنما يكون متصلاً بتصرف قانوني معين،

---

[1] - نصت المادة (3/6، 4/6) من قانون المعاملات الإلكترونية البحريني رقم 28 لسنة 2002 بأنه " .....(3) إذا عرض بصدد أية إجراءات قانونية توقيع إلكتروني مقرون بشهادة معتمدة، قامت القرينة على صحة ما يأتي ما لم يثبت العكس أو يتفق الأطراف على خلاف ذلك:

(أ) أن التوقيع الإلكتروني على السجل الإلكتروني هو توقيع الشخص المسمى في الشهادة المعتمدة.

(ب) أن التوقيع الإلكتروني على السجل الإلكتروني قد وضع من قبل الشخص المسمى في الشهادة المعتمدة بغرض توقيع هذا السجل الإلكتروني .

(ج) ان السجل الإلكتروني لم يطرأ عليه تغيير منذ وضع التوقيع الإلكتروني عليه.

(4) إذا لم يتم وضع التوقيع الإلكتروني باستعمال شهادة معتمدة، فإن قرينة الصحة المقررة بموجب أحكام البند السابق لا تلحق أياً من التوقيع أو السجل الإلكتروني ".

[2] – عرف المشرع الإماراتي أداة التوقيع في المادة الأولى من القانون سالف الذكر بأنها: "جهاز أو معلومات إلكترونية معدة بشكل مستقل او بالاشتراك مع أجهزة ومعلومات إلكترونية أخرى لوضع توقيع إلكتروني لشخص معين، وتشمل هذه العمليات أية أنظمة أو أجهزة تنتج أو تلتقط معلومات معينة مثل رموز أو مناهج حسابية أو حروف أو أرقام أو مفاتيح خصوصية أو أرقام تعريف الشخصية أو خواص شخصية".

وهذا التصرف عادة يفرغ في شكل إلكتروني، وعليه يشترط المحافظة على الدعامة التي توضع عليها بيانات التصرف القانوني، ولكي تنتج هذه البيانات الإلكترونية أثرها في الإثبات، لابد أن تحفظ بحيث يمكن الحصول عليها عند الحاجة، و إذا جرى تغيير عليها سواءً بالحذف أو الإضافة، فمن الممكن كشفه بسهولة[1].

وللتحقق من صحة التوقيع لابد من وجود جهة موثوق بها لربط شخص أو كيان بعينه بالتوقيع، ويتم ذلك باستخدام طرف ثالث محايد يطلق عليه مزود خدمات التصديق، هو أي شخص أو جهة معتمدة أو معترف بها تقوم بإصدار شهادات تصديق إلكترونية أو أي خدمات أو مهمات متعلقة بها وبالتوقيعات الإلكترونية[2].

الفرع الثاني

صور التوقيع الإلكتروني

إن أغلب التشريعات لم تحدد نوعاً معيناً من التواقيع، ولم تحدد على سبيل الحصر ماهية هذه التواقيع ، بل تركت المجال مفتوحاً كي يتسع لما يستجد من تطورات تكنولوجية قد تفرز أشكالاً

---

[1] – د .عادل علي المقدادي، إبرام العقد الإلكتروني وفقاً لقانون المعاملات الإلكترونية العماني(دراسة مقارنة)، مجلة الحقوق،جامعة البحرين،18 ،2012م، ص 233. حسن عبد الباسط، إثبات التصرفات القانونية التي يتم إبرامها عن طريق الإنترنت، دار النهضة العربية، القاهرة، 2000م، ص28 . د.سعيد السيد قنديل، التوقيع الإلكتروني، الدار الجامعية للنشر، الإسكندرية، 2004 م، ص52 .

ومن جانبه فقد بين قانون التوقيع الإلكتروني في مصر هذه الشروط بوضوح في المادة 18 منه على النحو التالي : يتمتع التوقيع الإلكتروني والكتابة الإلكترونية والمحررات الإلكترونية بالحجية في الإثبات إذا ما توافرت فيها الشروط الآتية :

(أ) ارتباط التوقيع الإلكتروني بالموقع وحده دون غيره (ب) سيطرة الموقع وحده دون غيره على الوسيط الإلكتروني (ج) إمكانية كشف أي تعديل أو تبديل في بيانات المحرر الإلكتروني أو التوقيع الإلكتروني.

كما نصت على هذه الشروط المادة 22 من قانون المعاملات الإلكترونية العُماني بالقول" يعتبر التوقيع محمياً وجديراً بأن يعتمد عليه إذا تحقق الآتي: (أ)كانت أداة إنشاء التوقيع في سياق استخدامها مقصورة على الموقع دون غيره .(ب) كانت أداة إنشاء التوقيع في وقت التوقيع تحت سيطرة الموقع دون غيره .(ج) كان ممكنا كشف أي تغيير للتوقيع الإلكتروني يحدث بعد وقت التوقيع .(د) كان ممكناً كشف أي تغيير في المعلومات المرتبطة بالتوقيع يحدث بعد وقت التوقيع. ومع ذلك يجوز لكل ذي شأن يثبت بأية طريقة أن التوقيع الإلكتروني جدير بأن يعتمد عليه أو أنه ليس كذلك".

[2] – المادة الأولى من قانون المعاملات والتجارة الإلكترونية الاماراتي .

وصوراً جديدة من التواقيع الإلكترونية، فكما تختلف أشكال التوقيع التقليدي بين التوقيع بالإمضاء، والختم ، وتوقيع ببصمة الإصبع. فإن التوقيع الإلكتروني له أيضا أشكال مختلفة ومتعددة وهي1:

أولاً: التوقيع الرقمي أو الكودي.

و يسمى أيضا التوقيع بواسطة المفتاح، وسمي" رقيما "لأنه يحتوي على رقم سري لا يعرفه سوى صاحبه و يشيع استخدامه في التعاملات المالية و البنكية وبواسطة بطاقة الائتمان، ويتم إعداد التوقيع الرقمي من خلال تحويل المحرر والتوقيع المرفق به، من نمط الكتابة العادية إلى معادلة رياضية وأرقام عن طريق استخدام العمليات الحسابية، بحيث يتم إعادة المحرر قبل تصديره للمرسل إليه في شكل يختلف عن البيانات والمعلومات الأصلية الواردة به، مع ربط هذا المحرر بمفتاح معين، على نحو لا يمكن لأحد أن يعيدها إلى الصيغة المقررة إلا الشخص الذي لديه المعادلة الخاصة بذلك والتي يطلق عليها المفتاح2.

وأوضح الأمثلة عليه بطاقات الائتمان التي تحتوي على رقم سري لا يعرفه سوى العميل الذي يدخل البطاقة في جهاز الصرف الآلي حيث يطلب منه في حالة الاستعلام عن حسابه أو سحب مبالغ نقدية في الحدود المتفق عليها بين العميل والبنك بموجب عقد إصدار البطاقة مثلا إدخال الرقم السري، وهي تعمل بنظامين هما: of– line أو on line .3.

ودقة هذا النظام تكمن بأن الرقم السري لا يعلم إلا من قبل العميل، لأن استخراجه يعتمد على مجموع الطلبات التي قدمت للبنك في وقت معين، ومن ثم يتم طباعة الرقم على بطاقات معينة ويقوم العميل بكشط مكان معين في بطاقة أخرى لمعرفة رقمه السري، وبالتالي فإن الموظف نفسه لا يعلم الرقم، ويلاحظ أنه في حالة الفقدان يتم إصدار بطاقة جديدة تحمل جميع المعلومات التي كانت مقيدة

---

[1] – حول صور التوقيع الإلكتروني انظر. د. سيد السعيد قنديل ، المرجع السابق، ص68 . د. عبدالإله محمد النوايسة، مدى توفير حماية جزائية للتوقيع الإلكتروني ومعطياته في القانون الاردني دراسة مقارنة، المرجع السابق، ص 122 وما بعدها. . د .فاروق محمد أحمد الأباصيري، عقد الاشتراك في قواعد المعلومات عبر شبكة الإنترنت دراسة تطبيقية لعقود التجارة الإلكترونية الدولية، المرجع السابق، ص118. د. هدى حامد قشقوش، الحماية الجنائية للتوقيع الإلكتروني، المرجع السابق،ص591.

[2] – د . عبد الله مسفر الحيان و د .حسن عبد الله عباس، التوقيع الإلكتروني دراسة نقدية لمشروع وزارة التجارة والصناعة الكويتية، مجلة العلوم الاقتصادية والإدارية، المجلد التاسع عشر ، العدد الأول ، يونيه 2003 ، ص 20

[3] – د. هدى حامد قشقوش، الحماية الجنائية للتوقيع الإلكتروني، المرجع السابق،ص591.

على البطاقة المفقودة باستثناء الرقم السري، ويلاحظ أنه في بعض البنوك يطلب من العميل اختيار رقم رباعي ليكون رقمه السري.1

ثانياً: التوقيع بالقلم الالكتروني

طريقة هذا التوقيع تتمثل في استخدام قلم إلكتروني ضوئي وحساس يمكنه الكتابة على شاشة جهاز الحاسب الآلي بحيث يوجد برنامج خاص لالتقاط التوقيع و التحقق من صحته بالاستناد إلى حركة هذا القلم على الشاشة والأشكال التي يتخذها من انحناءات أو التواءات أو نقاط و درجة الضغط بالقلم، و غير ذلك من سمات التوقيع و للتحقق من صحة التوقيع يقوم البرنامج عن طريق مقارنة التوقيع الموجود مع التوقيع المخزن ، وتعتمد هذه المقارنة على الخصائص البيولوجية للموقع ، ويتم تحديد صحة التوقيع بدقة متناهية تبعا لنوع المعاملة .

ويقوم هذا البرنامج بوظيفتين أساسيتين لهذا النوع من التوقيعات، الأولى: هي التقاط التوقيع وكتابته في مكان مخصص على شاشة الحاسب الآلي بوساطة قلم الكتروني حساس، بعد قيامه بإدخال الرقم السري الخاص به عن طريق بطاقة تحتوي على البيانات الخاصة به، والثانية: مقارنة التوقيع الحالي مع التوقيع الأصلي المخزن على الموقع الإلكتروني، أو الحاسب الآلي؛ للتحقق من المطابقة بينهما، وبيان مدى صحة هذا التوقيع2.

ثالثاً: التوقيع بالخواص الذاتية (البيومتري)

هذا النوع من التوقيعات الإلكترونية يعتمد بشكل أساسي على الخصائص الذاتية للإنسان كالبصمة بكافة أنواعها، سواء أكانت بواسطة بصمة الإصبع أو شبكية العين أو بصمة الصوت، إلى غير ذلك من الخواص الذاتية، ويتم تخزين هذه البصمة عن طريق إدخال المعلومات بطريقة بيومترية لذاكرة الحاسب الآلي، وعند فك التشفير يتم التحقق من مدى مطابقتها للعميل المستخدم للتوقيع.

ويبرمج الجهاز على أساس أن لا أوامر بفتح القفل المغلق إلا بعد أن يطابق هذه البصمة مع ما تم تخزينه فيه من قبل، فإذا تم التطابق تم فتح القفل وإتمام العملية المراد القيام بها[3].

---

[1] – عبد الفتاح حجازي، المرجع السابق، ص23 وما بعدها. د. خالد ممدوح إبراهيم، إبرام العقد الإلكتروني، دراسة مقارنة، دار الفكر الجامعي، مصر،2006م ، ص200.

[2] – د. خالد ممدوح إبراهيم، إبرام العقد الإلكتروني، دراسة مقارنة، المرجع السابق، ص200. د. هدى حامد قشقوش، الحماية الجنائية للتوقيع الإلكتروني، المرجع السابق،ص593.

[3] – د. عبدالإله محمد النوايسة، مدى توفير حماية جزائية للتوقيع الإلكتروني ومعطياته في القانون الاردني دراسة مقارنة،

المبحث الثاني

صور الحماية الجنائية للتوقيع الإلكتروني

يطالعنا تطور تكنولوجيا المعلومات والاتصال الحديث في كل يوم أوضاع جديدة تحتاج الى تنظيم، ولا يتم ذلك إلا بقواعد قانونية جديدة تواجه هذا التطور السريع، لذا نجد أن المشرع الإماراتي والبحريني قد اظهر كل منها استجابة لهذا التطور، وتمكنا من إضفاء الحماية الجنائية للتوقيع الإلكتروني، ولكن كيف عالج كل من المشرعين هذ الحماية؟ سنبين ذلك في مطلبين، المطلب الأول نخصصه لبيان صور الحماية الجنائية للتوقيع الإلكتروني في التشريع الإماراتي، ونفرد المطلب الثاني لبيان صور الحماية الجنائية للتوقيع الإلكتروني في التشريع البحريني.

المطلب الأول

صور الحماية الجنائية للتوقيع الإلكتروني في التشريع الإماراتي

لتوفير حماية فعالة للتوقيع الإلكتروني حرص المشرع الإماراتي على تقرير حماية جنائية للتوقيع الإلكتروني في قانون المعاملات والتجارة الإلكترونية رقم 1 لسنة 2006م، وافرد الفصل التاسع منه للعقوبات على الجرائم الماسة بالتوقيع الإلكتروني.

وخطا أيضاً خطوة إيجابية في هذا الاتجاه بأن أصدر القانون الاتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات[1]، وتضمن القانون العديد من المواد التي من شأنها توفير الحماية القانونية لخصوصية ما يتم نشره وتداوله على الشبكة المعلوماتية من معلومات وبيانات وأرقام تتعلق بالبطاقات الائتمانية وأرقام وبيانات الحسابات المصرفية، أو أي وسيلة من وسائل الدفع الإلكتروني، وكذلك كل استخدام لأي من وسائل تقنية المعلومات في تزوير أو تقليد أو نسخ للبطاقات الائتمانية، وعليه سنتناول صور الحماية الجنائية للتوقيع الإلكتروني والمقررة في كل من القانونين سالفي الذكر على النحو الآتي .

اولاً: جريمة تزوير التوقيع الإلكتروني.

جاء النص على هذه الجريمة في المادة (6) من القانون الاتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات بقولها "يعاقب بالسجن المؤقت والغرامة التي لا تقل عن مائة

المرجع السابق، ص 122. د .عبد الله مسفر الحيان و د .حسن عبد الله عباس، التوقيع الإلكتروني دراسة نقدية لمشروع وزارة التجارة والصناعة الكويتية، ص 20.

[1]– الذي ألغي بموجبه القانون الاتحادي رقم (2) لسنة 2006 بشأن مكافحة جرائم تقنية المعلومات.

وخمسون الف درهم ولا تتجاوز سبعمائة وخمسون ألف درهم كل من زور مستندا من مستندات الحكومة الاتحادية أو المحلية أو الهيئات أو المؤسسات العامة الاتحادية والمحلية.

وتكون العقوبة الحبس والغرامة التي لا تقل مائة ألف درهم ولا تتجاوز ثلاثمائة ألف درهم، أو احدى هاتين العقوبتين إذا وقع التزوير في مستندات جهة غير تلك المنصوص عليها في الفقرة الأولى من هذه المادة .

ويعاقب بذات العقوبة المقررة لجريمة التزوير، بحسب الأحوال، من استعمل المستند الإلكتروني المزور مع علمه بتزويره".

كما جرم قانون العقوبات الفرنسي لسنة 1992م التزوير الإلكتروني حيث عدل نص المادة 1/441 منه الخاصة بالتزوير وتم تعريف التزوير في هذه المادة على أنه:" كل تغيير للحقيقة بسوء نية من شأنه الإضرار بالآخرين أياً كانت الوسيلة المتبعة في مستند مكتوب، أو في دعامة من دعائم التعبير عن الفكر التي لها شأن في إثبات حق، أو واقعة لها نتائج قانونية" [1]

وقد اضفى المشرع الفرنسي من خلال هذا التعريف الحماية على المعلومات المبرمجة في مجال التزوير ومنها بطبيعة الحال التوقيع الإلكتروني.

وباعتبار البطاقات الائتمانية من صور التوقيع[2]، فقد حرص المشرع الإماراتي علي تجريم تزوير أو تقليد أو نسخ بطاقة ائتمانية أو أي وسيلة من وسائل الدفع الإلكتروني، وذلك باستخدام إحدى

---

[1] Selon l'article 441-1 de NCPF " Constitue un faux toute altération frauduleuse de la vérité de nature à causer un préjudice et accomplir par quelque moyen que ce soit' dans un écrit ou tout autre support d'expression de la pensée qui a pour objet ou qui peut avoir pour effet d'établir la preuve d'un droit ou d'un fait ayant des conséquences juridiques.

Le faux et l'usage de faux sont puni de trois ans d'emprisonnement et de 300 000 Franc d'amende"

كما جاء النص على هذه الجريمة في المادة 23/(أ) من القانون المصري بشأن التوقيع الإلكتروني لسنة 2004 ، حيث نصت على أن إتلاف أو تعييب توقيعاً أو محرراً إلكترونياً أو تزوير شئ من ذلك بطريق الإصطناع أو التعديل أو التحوير أو بأي طريق آخر يعاقب الفاعل بالحبس وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز مائة ألف جنيه أو بإحدي هاتين العقوبتين . كما جرم المشرع العماني تزور التوقيع الإلكتروني بموجب نص المادة 14/52 من قانون المعاملات الإلكترونية رقم 69/ 2008م بقوله " مع عدم الإخلال بأية عقوبة أشد ينص عليها قانون الجزاء العماني أو أي قانون آخر ،يعاقب بالسجن لمدة لا تتجاوز سنتين و بغرامة لا تتجاوز ـ /5000 ريال (خمسة آلاف ريال عماني) أو بإحدى هاتين العقوبتين كل من:- ..... زور سجلاً إلكترونيا أو توقيعا إلكترونيا أو استعمل أيا من ذلك مع علمه بتزويره".

[2]- راجع ما سبق ص18

وسائل تقنية المعلومات، أو برنامج معلوماتي، وذلك بموجب المادة(13) من قانون جرائم تقنية المعلومات والتي تنص بأنه " يعاقب بالحبس والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تتجاوز مليوني درهم أو بإحدى هاتين العقوبتين كل من زور أو قلد أو نسخ بطاقة ائتمانية أو بطاقة مدنية أو أي وسيلة أخرى من وسائل الدفع الإلكتروني، وذلك باستخدام إحدى وسائل تقنية المعلومات، أو برنامج معلوماتي".

و يدور الركن المادي لهذه الجريمة حول فعل التزوير أو التقليد الإلكتروني – المعلوماتى ، ويقصد بالتزوير المعلوماتى " أي تغيير للحقيقة يرد على مخرجات الحاسب الآلي سواء تمثلت في مخرجات ورقية مكتوبة كتلك التي تتم عن طريق الطابعة أو كانت مرسومة عن طريق الراسم، ويتم في مخرجات غير ورقية شرط أن تكون محفوظة على دعامة – كبرنامج منسوخ على أسطوانة – وشرط أن يكون المحرر المعلوماتى ذا أثر في إثبات حق أو أثر قانوني معين[1].

ويرد التزوير المعلوماتى على وثائق معلوماتية وهي تلك الوثائق التي يتم الحصول عليها بوسائل إلكترونية ، أي تكون ناشئة عن جهاز إلكتروني .

ولابد من الإشارة هنا إلى أن المشرع الإماراتي لم يقصر الجريمة على مجرد التزوير، بل جرم فعل استعمال المستند الإلكتروني، وعاقبه بذات العقوبة المقررة لجريمة التزوير، كما جرم التعامل ببطاقات الائتمان المزورة أو غيرها من وسائل الدفع مع علمه بعدم مشروعيتها[2].

وتعد هذه الجريمة من الجرائم العمدية ، وصورة الركن المعنوي فيها القصد الجنائي العام بعنصريه العلم والإرادة ، حيث يجب أن يعلم الجاني بأنه يقوم بتزوير أو استعمال توقيع إلكتروني لشخص آخر ، و تتجه إرادته الحرة إلى القيام بهذا النشاط ويقبل النتيجة المترتبة عليها.

ثانياً: الدخول غير المشروع على قاعدة بيانات تتعلق بالتوقيع الإلكتروني.

جاء النص على هذه الجريمة في المادة (2) من القانون الاتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات بقولها: " يعاقب بالحبس والغرامة التي لا تقل عن مائة ألف درهم ولا تزيد على ثلاثمائة ألف درهم أو بإحدى هاتين العقوبتين كل من دخل موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات، أو وسيلة تقنية معلومات، بدون تصريح أو بتجاوز حدود التصريح أو البقاء فيه بصورة غير مشروعة".

---

[1]– د. عبد الفتاح بيومي حجازي: الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت ، دار الكتب القانونية ، القاهرة 2002م ص 170.

[2]– المادة (3/13) من قانون جرائم تقنية المعلومات الاماراتي .

وقد شدد المشرع الإماراتي العقاب في حالة ما إذا ترتب على الدخول في النظام أو البقاء فيه، إلغاء أو تدمير أو إفشاء أو إتلاف أو تعديل البيانات التي يحويها النظام، ويجب لتوافر هذا الظرف أن تتوافر علاقة السببية بين فعل الدخول غير المشروع أو البقاء في النظام، وبين محو أو تعديل البيانات أو تعطيل النظام عن القيام بعمله. أما إن كان هذا المحو أو التعديل يرجع إلى أسباب أخرى هي التي أدت إليه، كالقوة القاهرة والحادث الفجائي، فإن صلة السببية تعد منتفيه ولا يسأل الجاني في هذه الحالة عن الظرف المشدد[1].

ويلاحظ على هذا النص تأثره بنص المادة 1/323 من قانون العقوبات الفرنسي والتي تجرم الدخول أو البقاء غير المصرح بهما، كما جرم المشرع العماني الدخول بطريق الغش إلى نظام معلومات أو قاعدة بيانات بغرض العبث بالتوقيعات الإلكترونية[2].

و يدور الركن المادي لهذه الجريمة حول فعل الدخول غير المشروع على نظام معلومات أو قاعدة بيانات تتعلق بالتوقيع الإلكتروني ذاته، ويقصد بقاعدة البيانات المخزنة عن موضوع ما داخل الحاسب الآلي، أو على قرص منفصل، ومن ذلك البيانات المتعلقة باسم صاحب التوقيع ومهنته وكافة بياناته الشخصية وكافة المعلومات المتعلقة بذلك التوقيع الذي يفترض سريتها[3]، ويلاحظ أن المشرع الإماراتي لم يشترط تحقق نتيجة معينة ، على إثر الدخول إلى قاعدة بيانات أو نظم المعلومات من قبل الجاني، وكل ما اشترطه المشرع في وقوع الجريمة أن يكون الدخول قد تم بدون تصريح أو بتجاوز حدود التصريح أو البقاء فيه بصورة غير مشروعة.

---

[1]- وشدد العقوبة بوجب نص المادة (3) من نفس القانون وجعلها الحبس مدة لا تقل عن سنة واحدة والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تتجاوز مليون درهم أو بإحدى هاتين العقوبتين اذا كان قد ارتكبها بمناسبة أو بسبب تأدية عمله. فضلا عن أنه جعل الجريمة جناية عقوبتها السجن الموقت والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تتجاوز مليون وخمسمائة ألف درهم أو بإحدى هاتين العقوبتين اذا كان الدخول بقصد الحصول على بيانات حكومية، أو معلومات بمنشأة مالية، أو تجارية، أو اقتصادية. بموجب نص المادة (4) من ذات القانون

[2]- نص المادة 3/52 من قانون المعاملات الإلكترونية رقم 69/ 2008م بقوله :" مع عدم الإخلال بأية عقوبة أشد ينص عليها قانون الجزاء العماني أو أي قانون آخر ،يعاقب بالسجن لمدة لا تتجاوز سنتين و بغرامة لا تتجاوز ـ /5000 ريال (خمسة آلاف ريال عماني) أو بإحدى هاتين العقوبتين كل من:-.....(3) دخل بطريق الغش إلى نظام معلومات أو قاعدة بيانات بغرض العبث بالتوقيعات الإلكترونية"

[3]- د. عبد الفتاح بيومي حجازي : التجارة الإلكترونية وحمايتها الجنائية ، دار الفكر الجامعي ، الإسكندرية ص 306.

وتصنف هذه الجريمة من جرائم الخطر، حيث يتم تجريم السلوك دون توقف ذلك على نتيجة معينة ، فهذه الجريمة ليست من جرائم الضرر التي يرتبط العقاب عليها بحصول ضرر بالمجني عليه.

وتعد هذه الصورة من الجرائم العمدية ، وصورة الركن المعنوي فيها هو القصد الجنائي العام بعنصرية العلم والإرادة، حيث يجب أن يعلم الجاني بأنه يقوم بالدخول على أداة إنشاء توقيع لشخص آخر دون تصريح أو بتجاوز حدود التصريح أو البقاء فيه بصورة غير مشروعة ، و تتجه إرادته الحرة إلى القيام بهذا النشاط، وبالتالي فإن الدخول قد يكون مشروعا إذا كان عن طريق الصدفة أو الخطأ أو السهو ويشترط على الشخص في هذه الحالة أن يقطع اتصاله وينسحب فوراً فإن بقي سرى عليه نص العقاب[1].

ولابد من الإشارة هنا إلى أن المشرع الإماراتي قد عاقب على هذه الجريمة بالحبس والغرامة، وتصاعد بقيمة العقوبة ــ ونؤيده في ذلك ــ نظراً للخسائر المادية الناتجة عن الدخول غير المشروع،كما عاقب على الشروع في الجنح بنصف العقوبة المقررة للجريمة التامة[2].

ثالثاً: جريمة اغتصاب التوقيع الإلكتروني.

نصت على هذه الجريمة المادة (12) من قانون تقنية المعلومات الاماراتي رقم (5) لسنة 2012م بقولها "يعاقب بالحبس والغرامة أو بإحدى هاتين العقوبتين كل من توصل بغير حق، عن طريق استخدم الشبكة المعلوماتية أو نظام معلومات إلكتروني أو إحدى وسائل تقنية المعلومات، إلى أرقام أو بيانات بطاقة ائتمانية أو إلكترونية أو ارقام أو بيانات حسابات مصرفية أو اي وسيلة أخرى من وسائل الدفع الإلكتروني..... ويعاقب بذات العقوبة المنصوص عليها في الفقرة السابقة كل من نشر أو أعاد نشر أرقام أو بيانات بطاقة ائتمانية أو إلكترونية أو ارقام أو بيانات حسابات مصرفية تعود للغير أو أي وسيلة أخرى من وسائل الدفع الإلكتروني "[3].

و يدور الركن المادي لهذه الجريمة حول فعل الوصول بغير حق أو نشر أو أعاد نشر أرقام أو بيانات بطاقة ائتمانية أو إلكترونية أو ارقام أو بيانات حسابات مصرفية تعود للغير أو أي وسيلة أخرى من وسائل الدفع الإلكتروني، كما يأخذ الركن المعنوي فيها صورة القصد الجنائي العام بعنصرية العلم والإرادة، حيث يجب أن يعلم الجاني بأنه يقوم الوصول بغير حق أو نشر أو أعاد

[1]– اشرف توفيق شمس الدين، الحماية الجنائية للمستند الإلكتروني، المرجع السابق ، ص528.

[2]– المادة رقم (40) من قانون جرائم تقنية المعلومات الاماراتي .

[3]– تقابل نص المادة (23/هـ) من القانون المصري بشأن التوقيع الإلكتروني لسنة 2004م.

نشر أرقام أو بيانات بطاقة ائتمانية أو إلكترونية أو ارقام أو بيانات حسابات مصرفية تعود للغير أو أي وسيلة أخرى من وسائل الدفع الإلكتروني ، وتتجه إرادته الحرة إلى القيام بهذا النشاط وتحقق النتيجة، كما عاقب على الشروع في الجنح بنصف العقوبة المقررة للجريمة التامة[1].

رابعاً: جريمة إنشاء أو نشر شهادة مصادقة لغرض احتيالي.

نصت على هذه الجريمة المادة (26) من قانون المعاملات والتجارة الإلكترونية الإماراتي بقولها" يعاقب بالحبس مدة لا تقل عن سنة، والغرامة التي لا تقل عن خمسين ألف درهم ولا تزيد على مائتين وخمسين ألف درهم أو بإحدى هاتين العقوبتين كل من أنشأ أو نشر أو وفر أو قدم أية شهادة مصادقة إلكترونية تتضمن أو تشير إلى بيانات غير صحيحة مع علمه بذلك".

المشرع هنا يجرم إنشاء أو نشر شهادة مصادقة الإلكترونية التي عرفها بموجب نص المادة(1) من القانون ذاته بأنها" الشهادة التي يصدرها مزود خدمات التصديق يفيد فيها تأكيد هوية الشخص أو الجهة الحائزة على أداة توقيع معينة.

ويلاحظ أن الإنشاء هنا نوع من الاصطناع الذي يعد إحدى طرق التزوير المنصوص عليها قانوناً[2]، ويمثل بالإضافة الى النشر عنصر النشاط الجرمي في الركن المادي للجريمة. وتعد هذه الصورة من الجرائم العمدية، وصورة الركن المعنوي فيها هو القصد الجنائي العام بعنصرية العلم والإرادة.

خامساً: جريمة الطلب المزيف أو غير المصرح به.

ورد تجريم الطلب المبني على بيانات غير صحيحة باستصدار أو إلغاء أو إيقاف شهادة مصادقة إلكترونية، في نص المادة (27) من قانون المعاملات والتجارة الإلكترونية الإماراتي بقولها " يعاقب بالحبس مدة لا تزيد عن ستة أشهر والغرامة التي لا تزيد على مائة ألف درهم أو إحدى هاتين العقوبتين كل من قدم متعمداً بيانات غير صحيحة إلى مزود خدمات التصديق بغرض استصدار أو إلغاء أو إيقاف شهادة مصادقة إلكترونية".[3]

---

[1]– المادة رقم (40) من قانون جرائم تقنية المعلومات الاماراتي .

[2]– د. هدى حامد قشقوش، المرجع السابق ، ص 589.

[3]– وقد عرف المشرع الإماراتي مزود خدمات التصديق بأنه " اي شخص أو جهة معتمدة أو معترف بها تقوم بإصدار شهادات تصديق إلكترونية أو اية خدمات أو مهمات متعلقة بها وبالتوقيعات الإلكترونية والمنظمة بموجب أحكام هذا القانون " المادة رقم (1) من ذات القانون والمتعلقة بالتعاريف . وعرفه التوجيه الأوروبي بأنه " كل شخص قانونى، طبيعي أو اعتباري، يقوم بتقديم شهادات الكترونية للجمهور أو يقدم له خدمات مرتبطة بالتوقيع الالكترونى " انظر المادة الثانية من التوجيه الأوروبي الاتحادي الصادر في 13 ديسمبر 1999 (J.O.C.E 13/12 19/1/200) ، والذى

سادساً: جريمة إعداد أو تصميم أو حيازة برنامج لإعداد توقيع إلكتروني.

حرص المشرع الإماراتي بموجب نص المادة (14) من قانون تقنية المعلومات رقم (5) لسنة 2012م تجريم ذلك بقوله " يعاقب بالحبس والغرامة التي لا تقل عن مائتي ألف درهم ولا تزيد على خمسمائة ألف درهم أو إحدى هاتين العقوبتين كل من اعد أو صمم أو أنتج أو اشترى أو استورد أو عرض للبيع أو اتاح أي برنامج معلوماتي أو أي وسيلة تقنية معلومات، أو روج بأي طريقة روابط لمواقع إلكترونية أو برنامج معلوماتي، أو أي وسيلة تقنية معلومات مصممة لأغراض ارتكاب أو تسهيل أو التحريض على ارتكاب الجرائم المنصوص عليها في هذا المرسوم بقانون" ، كما أشار إلى ذلك في المادة (13) من القانون ذاته والمتعلقة بتزوير بطاقات الائتمان[1]، كما عاقب على الشروع في الجنح بنصف العقوبة المقررة للجريمة التامة[2].

سابعاً: جريمة إفشاء سرية بيانات التوقيع الإلكتروني أو أداة إنشائه.

حرص المشرع الإماراتي على سرية بيانات التوقيع وأداة إنشائية وأفرد لذلك نص المادة (28) من قانون المعاملات والتجارة الإلكترونية بقوله " يعاقب بالحبس مدة لا تقل عن ستة أشهر والغرامة التي لا تقل عن عشرين ألفاً ولا تزيد على مائتي ألف درهم أو بإحدى هاتين العقوبتين كل شخص تمكن بموجب أية سلطات ممنوحة له في هذا القانون من الاطلاع على معلومات في سجلات أو مستندات أو مراسلات إلكترونية، وأفشى أياً من هذه المعلومات"[3]. ويستثنى من ذلك حالات التصريح بالمعلومات التي تتم لأغراض تنفيذ هذا القانون، أو لأي إجراءات قضائية، وتنص كذلك على هذه الجريمة المادة(22) من قانون تقنية المعلومات الاماراتي[4].

عنى بوضع نظام قانونى اتحادى للتوقيع الالكترونى . وعرفه قانون الانسترال النموذجى بشأن التوقيعات الالكترونية بأنه " شخصا يصدر شهادات ويجوز أن يقدم خدمات أخرى ذات صلة بالتوقيعات الالكترونية " ، المادة الثانية فقرة هـ من قانون الانسترال النموذجى الصادر بتاريخ 2001/1/10م.

[1]- نصت المادة (13) من القانون بأنه "يعاقب بالحبس والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تتجاوز مليوني درهم أو بإحدى هاتين العقوبتين كل..... صنع أو صمم أي وسيلة من وسائل تقنية المعلومات، أو برنامج معلوماتي، بقصد تسهيل أي من الأفعال المنصوص عليها في الفقرة الأولى من المادة"

[2]- المادة رقم (40) من قانون جرائم تقنية المعلومات الاماراتي .

[3]- تقابل المادة (21 ، 23) من القانون المصري بشأن التوقيع الإلكتروني لسنة 2004م. و المادة (10/52) من قانون المعاملات الإلكترونية رقم(2008/69) العماني.

[4]- نصت المادة (22) من القانون بأنه" يعاقب بالحبس مدة لا تقل عن ستة أشهر والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تتجاوز مليون درهم أو بإحدى هاتين العقوبتين كل من استخدم، بدون تصريح، أي شبكة معلوماتية، أو موقعاً إلكترونياً، أو وسيلة تقنية معلومات لكشف معلومات سرية حصل عليها بمناسبة عمله أو بسببه".

ونلخص إلى تأييد المشرع الإماراتي في حرصه على احاطة التوقيع الإلكتروني بالحماية الكاملة بأن جرم كل اعتداء على التوقيع الإلكتروني حتى لو لم يكن منصوصاً عليه في قانون المعاملات والتجارة الإلكترونية، ولكنه منصوص عليه في تشريع آخر نافذ، فيجب العقاب عليه وفقاً لهذا النص على أن يتم الفعل باستخدام وسيلة إلكترونية[1]، ولا يخل تطبيق العقوبات المنصوص عليها في هذا القانون بأي عقوبة أشد ينص عليها في أي قانون آخر[2]، وكذلك نص المشرع الإماراتي على المسؤولية الجنائية للشخص الاعتباري[3].

المطلب الثاني

صور الحماية الجنائية للتوقيع الإلكتروني في التشريع البحريني

اهتم المشرع البحريني بموضوع التوقيع الإلكتروني، وخطا خطوة إيجابية في هذا الاتجاه بأن أصدر القانون رقم (28) لسنة 2002م بشأن المعاملات الإلكترونية، وأورد نصاً خاصاً بالعقوبات على الأفعال الإجرامية التي تنال من التوقيع الإلكتروني، ويعد إصدار هذا القانون خطوة مهمة أدركها المشرع البحريني في الوقت المناسب ليواكب التطور التكنولوجي في مجال تقنية المعلومات ووسائل الاتصال، الأمر الذي فرض بدوره انتشار المعاملات ذات الطابع الإلكتروني التي باتت السمة المميزة والبارزة في المعاملات داخل مملكة البحرين.

وقد اشار المشرع البحريني الى صور الاعتداء على التوقيع الإلكتروني بموجب نص المادة (1/24) من القانون بقوله " **1** – مع عدم الإخلال بأية عقوبة أشد ينص عليها أي قانون

---

[1]– نصت المادة (29) من قانون المعاملات والتجارة الإلكترونية الاماراتي بأنه: " يعاقب بالحبس لمدة لا تزيد على ستة أشهر وبالغرامة التي لا تزيد على مائة ألف درهم أو بإحدى هاتين العقوبتين كل من ارتكب فعلاً يشكل جريمة بموجب التشريعات النافذة، باستخدام وسيلة إلكترونية"

[2]– المادة (33) من قانون المعاملات والتجارة الإلكترونية الإماراتي. تقابل المادة(1/24) من قانون المعاملات الإلكترونية البحريني.

[3]– نصت المادة (30) من قانون المعاملات والتجارة الإلكترونية الإماراتي بأنه: " (1) يعاقب بالحبس أو الغرامة التي لا تقل عن عشرة ألف درهم ولا تتجاوز مائة ألف درهم رؤساء وأعضاء مجالس الإدارات ومدراء الشخص الاعتباري إذا تسببوا بموافقتهم أو تسترهم أو أي تصرف آخر منهم بوقوع مخالفة لأي حكم من أحكام هذا القانون. (2) يعاقب موظف الشخص الاعتباري بالحبس أو الغرامة التي لا تقل عن عشرة ألف درهم ولا تزيد على مائة ألف درهم إذا ارتكب مخالفة لأحكام هذا القانون أو اللوائح الصادرة تنفيذاً له وتثبت أن هذه المخالفة قد جاءت نتيجة لتصرفه أو إهماله أو موافقته أو تستره. (3) وفي حالة الحكم بالإدانة في أي من البندين(1و2) من هذه المادة يحكم على الشخص الاعتباري الذي يتبع له المحكوم عليهم بغرامة تعادل الغرامة المحكوم بها على أي منهم".
وفي نفس الاتجاه ذهب المشرع البحريني، المادة (25) من قانون المعاملات الإلكترونية البحريني.

آخر ، يعاقب بالسجن مدة لا تزيد على عشر سنوات ، وبغرامة لا تجاوز مائة ألف دينار أو بإحدى هاتين العقوبتين كل من ارتكب عمداً فعلاً من الأفعال الآتية : (أ) نسخ أو حيازة أو إعادة تكوين أداة إنشاء توقيع إلكتروني لشخص آخر أو الدخول على أداة إنشاء هذا التوقيع دون تفويض بذلك من هذا الشخص ، وبسوء نية . (ب) تحريف أو تغيير أو استعمال أو إفشاء أداة إنشاء توقيع إلكتروني لشخص آخر دون تفويض منه بذلك ، أو بما يجاوز حدود هذا التفويض . (ج) إنشاء أو نشر أو تحريف أو استعمال شهادة ، أو توقيع إلكتروني لغرض احتيالي أو لأي غرض غير مشروع . (د) انتحال هوية شخص آخر ، أو الادعاء زوراً بأنه مفوض من قبله في طلب الحصول على شهادة أو قبولها ، أو طلب تعليق العمل بها أو إلغائها . (هـ) نشر شهادة أو وضعها في متناول أي شخص ، يحتمل أن يعتمد عليها أو على توقيع إلكتروني وارد بها من خلال الاستناد لأية بيانات مدرجة بهذه الشهادة مثل الرموز أو كلمات السر أو الغوريثمات أو مفاتيح التشفير العامة أو أية بيانات تستعمل لأغراض التحقق من صحة التوقيع الإلكتروني ، إذا كان من ارتكب ذلك الفعل على علم بأي من الآتي :-

- عدم إصدار الشهادة من قبل مزود خدمة الشهادات المدون في تلك الشهادة .
- عدم قبول الشهادة من قبل صاحبها المدون بها .
- إلغاء الشهادة أو وقف العمل بها ، بشرط ألا يكون نشر الشهادة أو وضعها في متناول الجمهور قد تم بغرض تمكين الغير من التحقق من صحة توقيع إلكتروني تم إنشاؤه قبل إلغاء الشهادة أو وقف العمل بها أو لغرض الإخطار بالإلغاء أو الوقف ." وسنتناول توضيح هذه الصور بالتفصيل الآتي:

أولا: جريمة نسخ أو حيازة أو إعادة أداة إنشاء توقيع إلكتروني[1]

نصت على هذه الجريمة الفقرة(1/أ) من المادة 24 من القانون سالف الذكر بأنه " مع عدم الإخلال بأية عقوبة أشد ينص عليها أي قانون آخر ، يعاقب بالسجن مدة لا تزيد على عشر سنوات ، وبغرامة لا تتجاوز مائة ألف دينار أو بإحدى هاتين العقوبتين كل من ارتكب عمداً فعلاً من الأفعال الآتية : (أ) نسخ أو حيازة أو إعادة تكوين أداة إنشاء توقيع إلكتروني لشخص آخر أو الدخول على أداة إنشاء هذا التوقيع دون تفويض بذلك من هذا الشخص ، وبسوء نية ".

يتكون الركن المادي لهذه الجريمة من ثلاث صور هي:

[1]- عرف المشرع البحريني أداة إنشاء التوقيع بأنها: أداة تستخدم لإنشاء توقيع إلكتروني ، مثل برمجية مجهزة أو جهاز إلكتروني. المادة (1) من قانون المعاملات الإلكترونية البحريني .

1. نسخ أداة إنشاء توقيع إلكتروني لشخص آخر.
2. حيازة أداة إنشاء توقيع إلكتروني لشخص آخر.
3. إعادة تكوين أداة إنشاء توقيع إلكتروني لشخص آخر.

وتعد من الجرائم العمدية ، وصورة الركن المعنوي فيها القصد الجنائي العام بعنصريه العلم والإرادة ، حيث يجب أن يعلم الجاني بأنه يقوم بنسخ أو حيازة أو إعادة تكوين أداة إنشاء توقيع إلكتروني لشخص آخر ، و تتجه إرادته الحرة إلى القيام بهذا النشاط ويقبل النتيجة المترتبة عليها.

ثانياً: جريمة الدخول بسوء نية على قاعدة بيانات تتعلق بالتوقيع الإلكتروني.

نصت على هذه الجريمة الفقرة(1/أ) من المادة 24 من القانون سالف الذكر. ولقيام هذه الجريمة لا بد وأن يقع الركن المادي المتمثل في الدخول غير المشروع على نظام معلومات أو قاعدة بيانات تتعلق بالتوقيع الالكتروني ذاته، ويقصد بقاعدة البيانات المخزنة عن موضوع ما داخل الحاسب الآلي، أو على قرص منفصل، ومن ذلك البيانات المتعلقة باسم صاحب التوقيع ومهنته وكافة بياناته الشخصية وكافة المعلومات المتعلقة بذلك التوقيع والذي يفترض سريتها[1]، ويلاحظ أن المشرع البحريني لم يشترط تحقق نتيجة معينة على إثر الدخول إلى قاعدة بيانات أو نظم المعلومات من قبل الجاني، وكل ما اشترطه المشرع في وقوع الجريمة أن يكون الدخول قد تم بسوء نية.

وتصنف هذه الجريمة من جرائم الخطر، حيث يتم تجريم السلوك دون توقف ذلك على نتيجة معينة ، فهذه الجريمة ليست من جرائم الضرر التي يرتبط العقاب عليها بحصول ضرر بالمجني عليه.

وتعد هذه الصورة من الجرائم العمدية ، وصورة الركن المعنوي فيها هو القصد الجنائي العام بعنصرية العلم والإرادة، حيث يجب أن يعلم الجاني بأنه يقوم بالدخول على أداة إنشاء توقيع لشخص آخر دون تفويض منه ، و تتجه إرادته الحره إلى القيام بهذا النشاط، وبالتالي فإن الدخول قد يكون مشروعا إذا كان عن طريق الصدفة أو الخطأ أو السهو ويشترط على الشخص في هذه الحالة أن يقطع إتصاله وينسحب فوراً، فإن بقي سرى عليه نص العقاب[2].

ثالثاً: جريمة تحريف أو تغيير أو استعمال أداة إنشاء توقيع إلكتروني.

نصت على هذه الجريمة الفقرة(1/ب) من المادة 24 من القانون سالف الذكر بأنه " مع عدم الإخلال بأية عقوبة أشد ينص عليها أي قانون آخر ، يعاقب بالسجن مدة لا تزيد على عشر سنوات

[1]- د. عبد الفتاح بيومي حجازي : التجارة الإلكترونية وحمايتها الجنائية ، دار الفكر الجامعي ، الإسكندرية ص 306.

[2]- اشرف توفيق شمس الدين، الحماية الجنائية للمستند الإلكتروني، المرجع السابق ، ص528.

، وبغرامة لا تتجاوز مائة ألف دينار أو بإحدى هاتين العقوبتين كل من ارتكب عمداً فعلاً من الأفعال الآتية :..... (ب) تحريف أو تغيير أو استعمال أو إفشاء أداة إنشاء توقيع إلكتروني لشخص آخر دون تفويض منه بذلك ، أو بما يتجاوز حدود هذا التفويض ".

يتكون الركن المادي لهذه الجريمة من اربع صور هي: تحريف أو تغيير أو استعمال أو إفشاء أداة إنشاء توقيع إلكتروني. ونشير هنا إلى أن الجريمة تقع على أداة إنشاء توقيع إلكتروني التي عرفها المشرع بأنها: أداة تستخدم لإنشاء توقيع إلكتروني ، مثل برمجية مجهزة أو جهاز إلكتروني. ويشترط أن يتم التحريف أو التغيير دون تفويض من صاحب أداة إنشاء توقيع إلكتروني، أو بما يجاوز حدود هذا التفويض .

كما يأخذ الركن المعنوي فيها صورة القصد الجنائي العام بعنصرية العلم والإرادة، حيث يجب أن يعلم الجاني بأنه يقوم بتحريف أو تغيير أو استعمال أو إفشاء أداة إنشاء توقيع إلكتروني لشخص آخر دون تفويض منه بذلك، أو أنه تجاوز حدود التفويض إن كان ممنوحاً له، وتتجه إرادته الحره إلى القيام بهذا النشاط وتحقق النتيجة.

رابعاً: جريمة إنشاء أو نشر أو تحريف أو استعمال شهادة أو توقيع إلكتروني لغرض إحتيالي.

نصت على هذه الجريمة الفقرة(1/ج) من المادة 24 من القانون سالف الذكر بأنه " مع عدم الإخلال بأية عقوبة أشد ينص عليها أي قانون آخر ، يعاقب بالسجن مدة لا تزيد على عشر سنوات، وبغرامة لا تجاوز مائة ألف دينار أو بإحدى هاتين العقوبتين كل من ارتكب عمداً فعلاً من الأفعال الآتية :..... (ج) إنشاء أو نشر أو تحريف أو استعمال شهادة ، أو توقيع إلكتروني لغرض احتيالي أو لأي غرض غير مشروع "[1].

تختلف هذه الجريمة عن الجريمة السابقة من حيث المحل، فالجريمة تقع على شهادة مصادقة الإلكترونية التي عرفها المشرع بموجب نص المادة(1) من القانون ذاته بأنها" سجل إلكتروني يتسم بأنه : يربط بيانات تحقق من توقيع بشخص معين، ويثبت هوية ذلك الشخص، ويكون صادراً من قبل مزود خدمة شهادات معتمد، ومستوفٍ للمعايير المتفق عليها بين الأطراف المعنية أو المنصوص عليها في القرارات التي تصدر استناداً لأحكام هذا القانون "[2].

---

[1]– تقابل نص المادة (8/52) من قانون المعاملات الإلكترونية رقم(2008/69) العماني.

[2]– وقد تكلم المرسوم الفرنسى الصادر في 30 مارس 2001 على نوعين من الشهادات : الأولى : الشهادة الالكترونية البسيطة وهى عبارة عن مستند يظهر في شكل الكتروني ويشهد بوجود علاقة بين بيانات التحقق من التوقيع الالكتروني وشخصية الموقع، والثانية الشهادة الالكترونية المعتمدة وهى تلك التي ينبغي أن تستوفى مجموعة من الضوابط والمعايير

يتكون الركن المادي لهذه الجرمة من اربع صور هي: إنشاء أو نشر أو تحريف أو استعمال شهادة أو توقيع الإلكتروني، وهذ الجريمة تتماثل مع جريمة التزوير التي ورد النص عليها في أغلب التشريعات[1]. ويلاحظ أن الإنشاء هنا نوع من الاصطناع الذي يعتبر إحدى طرق التزوير المنصوص عليها قانوناً[2]. وتعد هذه الصورة من الجرائم العمدية، وصورة الركن المعنوي فيها هو القصد الجنائي العام بعنصرية العلم والإرادة.

خامساً: جريمة الطلب غير المصرح به.

نصت على هذه الجريمة الفقرة(1/د) من المادة 24 من القانون سالف الذكر بأنه " مع عدم الإخلال بأية عقوبة أشد ينص عليها أي قانون آخر ، يعاقب بالسجن مدة لا تزيد على عشر سنوات، وبغرامة لا تجاوز مائة ألف دينار أو بإحدى هاتين العقوبتين كل من ارتكب عمداً فعلاً من الأفعال الآتية :.....(د) انتحال هوية شخص آخر ، أو الادعاء زوراً بأنه مفوض من قبله في طلب الحصول على شهادة أو قبولها ، أو طلب تعليق العمل بها أو إلغائها".

يلاحظ أن صورة الركن المادي للجريمة هي انتحال هوية شخص، أو الادعاء زوراً تتفق مع اتخاذ اسم كاذب أو صفة غير صحيحة والتي تعد إحدى طرق الاحتيال المنصوص عليها في المادة (391) من قانون العقوبات البحريني، وتعد هذه الصورة من الجرائم العمدية، وصورة الركن المعنوي فيها هو القصد الجنائي العام بعنصرية العلم والإرادة.

سادساً: جريمة سرية بيانات التوقيع الإلكتروني أو أداة إنشائه.

نصت على هذه الجريمة الفقرة(1/هـ) من المادة 24 من القانون سالف الذكر بأنه " مع عدم الإخلال بأية عقوبة أشد ينص عليها أي قانون آخر ، يعاقب بالسجن مدة لا تزيد على عشر سنوات ، وبغرامة لا تجاوز مائة ألف دينار أو بإحدى هاتين العقوبتين كل من ارتكب عمداً فعلاً من الأفعال

التي ورد النص عليها بالمرسوم. ووفقا لما ورد النص عليه فى المادة السادسة من هذا المرسوم فانه يجب أن تسلم الشهادة المعتمدة من مقدم خدمة توثيق مؤهل لتسليم هذا النوع من الشهادات. انظر حول ذلك، د. مصطفى أبو مندور موسى، خدمات التوثيق الالكترونى " تدعيم للثقة وتأمين للتعامل عبر الإنترنت "
دراسة مقارنة، ندوة الجوانب القانونية للتعاملات الإلكترونية، مسقط 2008/11/23م، ص32 .

[1]– نصت المادة 23 من قانون التجارة الإلكترونية المصري بأنه: "مع عدم الإخلال بأية عقوبة أشد وردت في قانون آخر، يعاقب بالحبس مع الشغل كل من زور أو قلد محرراً أو توقيعاً إلكترونيا أو شهادة اعتماد توقيع إلكتروني. ويعاقب بذات العقوبة المقررة كل من استعمل محرراً إلكترونياً مزور أو شهادة مزورة باعتماد توقيع إلكتروني مع علمه بذلك"

[2]– د. هدى حامد قشقوش، المرجع السابق ، ص 589. انظر المادة (270) من قانون العقوبات البحريني.

الآتية :..... (هـ) نشر شهادة أو وضعها في متناول أي شخص ، يحتمل أن يعتمد عليها أو على توقيع إلكتروني وارد بها من خلال الاستناد لأية بيانات مدرجة بهذه الشهادة مثل الرموز أو كلمات السر أو الغوريثمات أو مفاتيح التشفير العامة أو أية بيانات تستعمل لأغراض التحقق من صحة التوقيع الإلكتروني ، إذا كان من ارتكب ذلك الفعل على علم بأي من الآتي :-

- عدم إصدار الشهادة من قبل مزود خدمة الشهادات المدون في تلك الشهادة .
- عدم قبول الشهادة من قبل صاحبها المدون بها .
- إلغاء الشهادة أو وقف العمل بها ، بشرط ألا يكون نشر الشهادة أو وضعها في متناول الجمهور قد تم بغرض تمكين الغير من التحقق من صحة توقيع إلكتروني تم إنشاؤه قبل إلغاء الشهادة أو وقف العمل بها أو لغرض الإخطار بالإلغاء أو الوقف ."

ونلخص الى تأييد المشرع البحريني في حرصه على إحاطة التوقيع الإلكتروني بالحماية الكاملة بأن جرم كل اعتداء على التوقيع الإلكتروني، وتشديد العقوبة الى حد السجن الذي لا يزيد على عشر سنوات، فضلاً عن أنه أشار إلى أن تطبيق العقوبات المنصوص عليها في هذا القانون لا يخل بأي عقوبة أشد ينص عليها في أي قانون آخر، وكذلك حرصه على المسؤولية الجنائية للشخص الاعتباري وموظفيه التي جاء النص عليها بالمادة (25) من القانون بأنه " يسأل الشخص الاعتباري جنائيا ويعاقب بالغرامة التي لا تتجاوز مائتي ألف دينار ، إذا ارتكبت أي من الجرائم المنصوص عليها في هذا القانون باسمه أو لحسابه أو باستعمال إحدى وسائله ، وكان ذلك نتيجة تصرف أو إهمال جسيم أو موافقة أو تستر من أي عضو مجلس إدارة أو مدير أو أي مسئول آخر – في ذلك الشخص الاعتباري – أو ممن يتصرف بهذه الصفة . ويعد مرتكبا للجريمة كل من أسند إليه من هؤلاء الأشخاص الطبيعيين ارتكاب أي من الأفعال المذكورة، ويعاقب بالعقوبة المقررة لها طبقا لأحكام هذا القانون "

ولا بد من الاشارة هنا إلى أن كلمة عمداً التي وردت بالنص السابق تثبت أهمية تأكد القاضي من توافر القصد الجنائي لدى الجاني عند اقتراف الجرم وهو ما يعد تضييقا على القاضي في هذا الأمر.

الخاتمة :

تناولنا في هذا البحث موضوع الحماية الجنائية للتوقيع الإلكتروني في التشريعين الاماراتي والبحريني، فبينا حقيقة التوقيع الإلكتروني من خلال بيان تعريفه وتمييزه عن التوقيع الكتابي، وشروط صحة التوقيع الإلكتروني ، ثم بحثنا صور الحماية الجنائية للتوقيع الإلكتروني في التشريعين الإماراتي والبحريني .

النتائج :

أولاً: عرف المشرع الإماراتي التوقيع الإلكتروني في المادة الأولى من القانون الاتحادي رقم (1) لسنة 2006م في شأن المعاملات والتجارة الإلكترونية تعريفا مزدوجا بحيث عرفه تعريفا عاما، من جهة أخرى أضاف تعريفا نوعيا ثانيا خاصا بالتوقيع الإلكتروني المحمي. كما عرف المشرع البحريني التوقيع الإلكتروني في المادة الأولى من القانون رقم (28) لسنة 2002م بشأن المعاملات الإلكترونية.

ثانياً: جاء تعريف معظم التشريعات العربية للتوقيع الإلكتروني منسجماً مع تعريف قانون الأمم المتحدة النموذجي (الأونسيترال) بشأن التوقيعات الإلكترونية لعام 2001 .

ثالثاً: إن التعريفات لم تشر بشكل حصري لصور التوقيع الإلكتروني، بل أجازت أن يتخذ أي شكل سواء كان في هيئة صور أو حرف أو رقم أو رمز أو إشارة أو حتى صوت، شريطة أن يكون له طابع منفرد يسمح بتميز شخص صاحب التوقيع وتحديد هويته وإظهار رغبته في إقرار العمل القانوني أو الرضا بمضمونه، كما أن التعريفات لم تربط التوقيع بشكل مادي محدد، بل أشارت إلى كونه مرتبطاً بسجل ارتباطاً منطقياً، تاركتاً المجال مفتوحاً كي يتسع هذا التعريف لما يستجد من تطورات تكنولوجية قد تفرز أشكالاً وصوراً جديدة من التواقيع الإلكترونية .

رابعاً: إن التوقيع الإلكتروني وإن اختلفت صوره عن صور التوقيع الكتابي، إلا أنه يؤدي نفس الوظائف التي يؤديها من حيث دلالته على هوية صاحبه وشخصيته وانصراف إرادته إلى الإلتزام بما وقع.

خامساً: حرص المشرع الإماراتي على تقرير حماية جنائية للتوقيع الإلكتروني في قانون المعاملات والتجارة الإلكترونية رقم 1 لسنة 2006م، وأفرد الفصل التاسع منه للعقوبات على الجرائم الماسة بالتوقيع الإلكتروني، وأصدر القانون الاتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات، وتضمن القانون العديد من المواد التي من شأنها توفير الحماية القانونية لخصوصية ما يتم نشره وتداوله على الشبكة المعلوماتية من معلومات وبيانات وأرقام تتعلق بالبطاقات الائتمانية وأرقام وبيانات الحسابات المصرفية أو أي وسيلة من وسائل الدفع الإلكتروني، وكذلك كل استخدام لأي من وسائل تقنية المعلومات في تزوير أو تقليد أو نسخ للبطاقات الائتمانية .

سادساً: أشار المشرع البحريني إلى صور الاعتداء على التوقيع الإلكتروني بموجب نص المادة (1/24) من القانون رقم (28) لسنة 2002م بشأن المعاملات الإلكترونية . وإحاطة التوقيع الإلكتروني بالحماية الكاملة بأن جرم كل اعتداء على التوقيع الإلكتروني حتى لو لم يكن منصوص عليه في قانون المعاملات والتجارة الإلكترونية، ولكنه منصوصاً عليه في تشريع آخر نافذ فيجب

العقاب عليه على أن يتم الفعل باستخدام وسيلة إلكترونية، ولا يخل تطبيق العقوبات المنصوص عليها في هذا القانون بأي عقوبة أشد ينص عليها في أي قانون آخر، وكذلك نص على المسؤولية الجنائية للشخص الاعتباري.

وأخيراً، فإن مجرد اتجاه المشرّعين الإماراتي والبحريني إلى إصدار التشريعات التي تنظيم المعاملات الإلكترونية يمثل خطوة هامة لذا نوجز **أهم الاقتراحات** فيما يلي:

أولاً: تدريب المتخصصين في هذا المجال من مأموري الضبط القضائي والنيابة العامة والقضاء على وسائل وأدوات تقنية المعلومات الإلكترونية لكشف الطرق الاحتيالية والتزوير في التوقيعات الخاصة بالمحررات الإلكترونية .

ثانياً: دعم التعاون الدولي في مجال مكافحة جرائم تقنية المعلومات. حيث أنها أصبحت جرائم عابرة الحدود بفعل التطور التقني والتكنولوجي، مما يقضي تبادل المساعدة القضائية بين الدول، وتوقيع اتفاقيات تسليم المجرمين.

ثالثاً : ندعو المشرع البحريني الى ضرورة تنظيم جرائم تقنية المعلومات بقانون جزائي خاص، يتناول جميع جرائم تقنية المعلومات. مسترشداً في ذلك بالموقف الذي تبناه المشرع الاماراتي [1].

رابعاً: حول موقف المشرع الفلسطيني، نجد ان المشرع لم يفرد قانون جزائي خاص يتناول جرائم تقنية المعلومات والتي تشمل الحماية الجنائية للتوقيع الإلكتروني، لذا نهيب بالمشرع الفلسطيني ان يعمل على اصدار قانون جزائي خاص يتناول جميع جرائم تقنية المعلومات. مسترشداً بالقانون الاماراتي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات.

المراجع العربية:

اشرف توفيق شمس الدين، الحماية الجنائية للمستند الإلكتروني، مؤتمر الأعمال المصرفية والإلكترونية بين الشريعة والقانون، جامعة الامارات، 10 – 12 مايو 2003م، المجلد الثاني.

ثروت عبد الحميد، التوقيع الإلكتروني ، ماهيته، مخاطرة، كيفية مواجهتها، حجيته في الإثبات، مكتبة الجلاء المنصورة، 2001م.

حسن عبد الباسط، إثبات التصرفات القانونية التي يتم إبرامها عن طريق الإنترنت، دار النهضة العربية، القاهرة، 2000م .

خالد ممدوح إبراهيم، إبرام العقد الإلكتروني، دراسة مقارنة، دار الفكر الجامعي، مصر،2006م.

[1]- القانون الاتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات.

سعيد السيد قنديل : التوقيع الإلكتروني، "الجامعة الجديدة للنشر ، الإسكندرية 2004 .

عادل علي المقدادي، إبرام العقد الإلكتروني وفقاً لقانون المعاملات الإلكترونية العماني(دراسة مقارنة)، مجلة الحقوق، جامعة البحرين ،2012م.

عبد الفتاح بيومي حجازي: الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت ، دار الكتب القانونية ، القاهرة 2002م .

عبد الله مسفر الحيان و د .حسن عبد الله عباس، التوقيع الإلكتروني دراسة نقدية لمشروع وزارة التجارة والصناعة الكويتية، مجلة العلوم الاقتصادية والإدارية، المجلد التاسع عشر ، العدد الأول ، يونيه 2003 .

عبدالإله محمد النوايسة، مدى توفير حماية جزائية للتوقيع الإلكتروني ومعطياته في القانون الاردني دراسة مقارنة، المجلة الأردنية في القانون والعلوم السياسية، المجلد(2) العدد(2)، 2010م.

فاروق محمد أحمد الأباصيري، عقد الاشتراك في قواعد المعلومات عبر شبكة الإنترنت دراسة تطبيقية لعقود التجارة الإلكترونية الدولية – دار الجامعة الجديدة للنشر مصر ،٢٠٠٢ الطبعة الأولى.

لورانس محمد عبيدات ، اثبات المحرر الإلكتروني، دار الثقافة للنشر والتوزيع ، 2005م

محمد فواز المطالقة، الوجيز في عقود التجارة الإلكترونية، دار الثقافة للنشر والتوزيع، عمان، 2006م.

مصطفى أبو مندور موسى، خدمات التوثيق الإلكتروني " تدعيم للثقة وتأمين للتعامل عبر الإنترنت " دراسة مقارنة، ندوة الجوانب القانونية للتعاملات الإلكترونية، مسقط 2008/11/23م.

ممدوح محمد خيري المسلمي، مشكلات البيع الإلكتروني عن طريق الانترنت ، دار النهضة العربية، القاهرة، 2000م.

منير محمد الجنبيهي وممدوح محمد الجنبيهي، التوقيع الإلكتروني وحجيته في الإثبات، دار الفكر العربي، القاهرة ، 2004م.

نجوي أبو هيبه : التوقيع الإلكتروني ، تعريفه ، مدي حجيته في الإثبات ، دار النهضة العربية ، 2002 .

هدى حامد قشقوش، الحماية الجنائية للتوقيع الإلكتروني، مؤتمر الأعمال المصرفية والإلكترونية بين الشريعة والقانون، جامعة الامارات، 10 – 12 مايو 2003م، المجلد الثاني .

المراجع الأجنبية:

Alain BENSSONSAN, L'informatique et droit . mémento- guide, Tomme II. Hermès. 1994.

Golic, Jovan Dj. 2001. How to Construct Cryptographic primitives from stream Ciphers. Commuters and security. Vo1 20, Amsterdam.