جامعة مولود معمري - تيزي وزو

كليّـــة الحقوق والعلوم السياسية

مدرسة الدكتوراه للقانون الأساسي والعلوم السياسية

أمن التوقيع الإلكتروني

مذكرة لنيل شهادة الماجستير في القانون

فرع "القانون الدولي للأعمال"

إعـــداد الطـــالبة: **إشـــراف الأستاذ:**

لالوش راضية **د/ إقلولي محمد**

لجنة المناقشة:

د. جعفور محمد السعيد، أستاذ ، **كلية الحقوق، جامعة مولود معمري، تيزي وزو،..... رئيسا**

د. إقلولي محمد، أستاذ ، كلية الحقوق، جامعة مولود معمري، تيزي وزو،..... مشرفا ومقررا.

د. يسعد حورية، أستاذة محاضرة أ، كلية الحقوق، جامعة مولود معمري، تيزي وزو،..... ممتحنة.

تاريخ المناقشة 2012/ 09/23

بسم الله الرحمن الرحيم

﴿...وما توفيقي إلاّ بالله عليه توكلت وإليه أنيب﴾

(سورة هود الآية .88.)

إهــداء

إلــى

النور الذي أستضيء به طريقي في هذه الدنيا أمي الغالية أتمنى لها الشفاء العاجل والعودة بإذن الله.

وأبي العزيز الذي أشقى نفسه علينا، أطال الله في عمره.

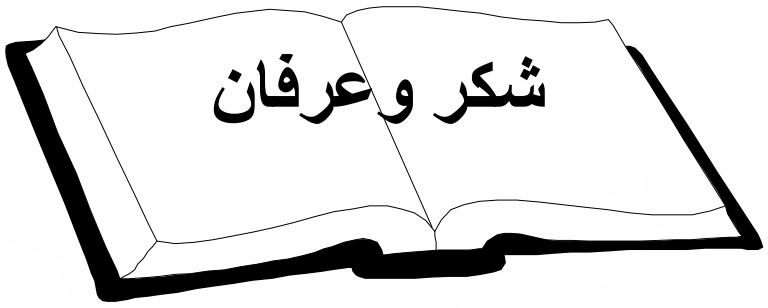
أختي العزيزة وأخوايا العزيزان

وأبناء أختي أليسيا وماسينيسا

كل من خصني بدعاء مخلص من القلب، و كل من شجعني في إنجاز هذه المذكرة

و إلى كل طالب علم

? راضية



شكر وعرفان

إلى

الأستاذ المشرف الدكتور محمد إقلولي، عرفانا وشكرا على توجيهاته القيمة وتثمينا على عطائه من معلومات، وعلى طول صبره، فرغم انشغالاته، والتزاماته الكثيرة ، قبل الإشراف على هذا العمل، ومراجعته من جديد، مع تقديمه لملاحظات قيمة أنارت لي طريق البحث والتقصي،

فله كل عبارات الشكر والتقدير، عرفانا مني بالجميل.

? راضية

قائمة أهم المختصرات

أولا: باللغة العربية:

ص ص	: من الصفحة إلى الصفحة.
ج ر	: الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية
ق م ج	: القانون المدني الجزائري.
ق ت ج	: القانون التجاري الجزائري.
ق ع ج	: قانون العقوبات الجزائري.
د ت	: دون تاريخ

ثانيا: باللغة الفرنسية:

Art	: **Art**icle
CD	: **D**isque **C**ompact
CNUDCI	: **C**ommission des **N**ations **U**nies sur le Droit **C**ommercial **I**nternational
EDI	: **E**change de données informatisée
EMV	: **E**uropay **M**asterCard and **V**isa card.
http	: **P**rocole de transfert de fichier
IP	: **P**rotocole **I**nternet
ISO	: **I**nternational **O**rganization for **S**tandardization.
NTCI	: **N**ouvelles **T**echnologies de la **C**ommunication et de **l**'Information..
OCDE	: **O**rganization de **C**ooperation et de **D**éveloppement **E**conomique
Op cit	: référence precitee
PIN	: **P**ersonal **I**dentification **N**umber.
RIM	: **R**éseau **M**onétique **I**nterbancaire.
SET	**: S**ecure **E**lectronic **T**ransaction
SSL	: **S**ecure **S**ockets **L**ayer (protocole)
TPE	: **T**erminal de **P**aiement **E**lectronique.

مقدمـة

أدّى التطور المتسارع والهائل الذي شهدته البشرية في الآونة الأخيرة إلى ظهور ثورة تكنولوجية هائلة فرضت على الجميع واجب الاستفادة منها. بداية من ظهور التلكس والفاكس، وانتهاء بشبكة الإنترنت[1]، التي أصبحت الآن وسيلة عالمية تتجاوز الحدود الوطنية، حيث بات العالم قرية صغيرة، أو كما يطلق عليه البعض قرية الكترونية[2].

ألقى هذا التقدم بظلاله على النشاط التجاري الدولي على نحو أدى إلى خلق أنشطة تجارية عالمية، تتم وتنفذ دون الحضور المادي لأطرافها. هكذا أصبحت الوسائل الإلكترونية للاتصال ذات أثر فعّال ودور هام في إبرام العقود، وانتقال السلع والخدمات ورؤوس الأموال. فضلا عن النظم والأفكار بين الدول[3]. والحقيقة هي أنه مع اختراع جهاز الحاسوب أو الحاسب الإلكتروني وانتشاره، واستعماله في مختلف نواحي الحياة ودمجه وتزاوجه بشبكة الاتصال الدولية(الإنترنيت)، تحققت ثورة حقيقية أطلق عليها تسمية ثورة المعلومات، حيث بدأ الحديث معها عن مجتمع المعلوماتية، وما رافقه من مصطلحات جديدة، ومنها: الأرشيف الإلكتروني، معلوماتية الإدارة، المعالجة عن بعد الحكومة الإلكترونية، المحكمة الإلكترونية، التحكيم الإلكتروني، الإثبات الإلكتروني

[1]-فكلمة انترنت ذات شقين: الأول (inter) ومشتقة من مصطلح (Interconnections) ويعني البينية، الاتصال أو الدخول، والثاني (net) ومشتقة من مصطلح (net work)، وتعني الشبكة.فهي شبكة اتصال عالمية تربط عدد لا متناه من الحاسبات الالكترونية "الكمبيوتر"إما عن طريق الهاتف أو عن طريق الأقمار الصناعية في جميع أنحاء العالم وعلى مدار الساعة. وقد نشأت هذه الشبكة في الولايات المتحدة الأمريكية في الستينات على أسس وجذور عسكرية فتبنت الأولى وزارة الدفاع والثانية الجامعات الأمريكية. وفي العام 1969 قامت أول شبكة باسم (arpante) كشبكة تجريبية أولي في العالم، وفي عام 1985 أعلن رسميا عن قيام شبكة الإنترنت وذلك باتصال خمس شبكات هي Arpante،Usenet،CSN،Nsfne، وهكذا أنظمت شبكات أخرى عديدة. باستمرار تسارع نمو هذا الوليد العملاق قررت أمريكا وقف دعمها الحكومي والمالي لمشروع الانترنت فاتحة الباب أمام الاستثمار في هذه الشبكة، للمزيد من التفاصيل أنظر: **زريقات عمر خالد**، عقد البيع عبر الإنترنت، دار الحامد للنشر والتوزيع، عمان، 2007، ص ص36 .83

[2]-**ROGER Larry-Miller andGQYLOURD A-Gentz**, Law for electronic commerce, THOMSON LEARMING, New-York, 2000, p 7.

[3]- **محمد إبراهيم موسى**، انعكاسات العولمة على عقود التجارة الدولية، دار الجامعة الجديد للنشر، الإسكندرية، 2007 ص 6.

والشكلية الإلكترونية...الخ[1].وقد نتج في الواقع العملي عن هذا النوع الجديد من التجارة طرق ووسائل حديثة في التعاملات الإلكترونية، أهمها إبرام العقود على دعامات غير ورقية مما تسبب في ظهور بعض المشكلات العملية والقانونية، حيث أنّ فكرة التوقيع بمفهومه التقليدي أصبحت عقبة من المستحيل تكيفها مع هذه العقود الجديدة، ولمواكبة هذه التطورات تمّ البحث عن بديل للتوقيع التقليدي يكون قادرا على التناسب وهذه التصرفات الإلكترونية والذي نتج عنه التوقيع الإلكتروني،بالفعل فقد تم التوصل إلى وسيلة بديلة ذات طبيعة إلكترونية لها أشكال مختلفة، يمكن أن تحقق الوظائف التي يقدمها التوقيع التقليدي والمتعلقة بتحديد هوية الشخص الموقع والتعبير عن إرادته في الالتزام بمضمون ما تمّ التوقيع عليه.

يعتبر العقد الإلكتروني الأداة الأساسية لممارسة التجارة الإلكترونية، بحيث يرتبط بها ارتباطا وثيقا، فهو يمثل ترجمة قانونية لتلاقي الإرادة بين البائع (مقدم الخدمة) من جهة، والمشتري (مستهلك الخدمة) من جهة أخرى[2]، أي أنّه اتفاق يتم إبرامه بين طرفين وينفذ كليا أو جزئيا من خلال تقنية الاتصال عن بعد بدون حضور مادي متزامن لأطرافه[3].

بدأت التجارة الإلكترونية تغزو كل العالم حتى أصبح من لا يمارسها يعتبر متخلفا عن ركب الحضارة[4]، مما أدّى إلى زيادة أعداد الممارسين لهذه التجارة مزاياها الكثيرة وما تحققه من فوائد[5] قد لا تتحقق عن طريق التجارة التقليدية، وإذا كان للتجارة

---

[1]- **ناصيف إلياس**، العقود الدولية: العقد الإلكتروني في القانون المقارن، منشورات الحلبي الحقوقية، لبنان، 2009، ص 5.

[2]- **سمير حامد عبد العزيز الجمال**، التعاقد عبر تقنيات الاتصال الحديثة، دراسة مقارنة دار النهضة العربية، 2006 ص 56.

[3]-**خالد مصطفى فهمي**، النظام القانوني للتوقيع الإلكتروني في ضوء التشريعات العربية والاتفاقيات الدولية، دار الجامعة الجديدة 2007، ص 240.

[4]- **سمير حامد عبد العزيز الجمال**، المرجع السابق، ص 56، و **خالد مصطفى فهمي**، المرجع السابق، ص 240.

5- تعمل التجارة الإلكترونية على توفير الكثير من النفقات بالمقارنة مع التجارة التقليدية، ولعل أهم أوجه هذا التوفير في النقاط التالية: قلة تكاليف النقل في التجارة الإلكترونية خاصة مع إمكانية الوصول إلى أسواق لم تكن متاحة من قبل حيث يمكن إنشاء محل تجاري على شبكة الإنترنت مجانا أو برسوم قليلة، كما يمكن وبرسوم قليلة أيضا اختيار وتسجيل الاسم التجاري للمنشأة على الإنترنت تعمل على توفير كثير من الوقت، مما يؤدي إلى سرعة إنجاز الصفقات التجارية،

الإلكترونية مزايا فإنها لا يخلو من العيوب والتي قد تؤدي إلى الانتقاص من أهميتها، وبالتالي تحد من انتشارها وازدهارها، ويمكن تلخيص هذه العيوب أو السلبيات فيما يلي:

- عدم توافر الأمان فيها وهذا نتيجة للعديد من العوائق الفنية والتقنية، وهو الأمر الذي مهد الطريق أمام مخترقي نظم المعلوماتية في غياب الحماية الكافية للتطفل على البيانات الشخصية للأفراد، وخاصة تزوير ومعالجة التوقيعات الرقمية مما يمكن أي شخص من انتحال صفة لا يتمتع بها، أو استخدام هذه المعلومات بطرق غير مشروعة[1].
- يجب على المتعامل عبر شبكة الإنترنت إبراز هويته الشخصية، وتقديم المعلومات الثبوتية الموثقة التي تبدد شك الطرف الآخر، ولا يتمّ هذا إلاّ من خلال توافر الوسائل التي يمكن من خلالها تحقيق أمن التجارة الإلكترونية.

تتمثل هذه الوسائل في تشفير البيانات أو وجود طرف ثالث يقوم بالتحقق من هوية الشخص ويصدر شهادة توثيق توقيعه الإلكتروني[2].

تشغل مشكلة الأمن والخصوصية على شبكة الإنترنت حيزا كبيرا من اهتمام فقهاء القانون، كما تثير قلق الكثير من الأفراد مما يسبب نوع من انعدام الثقة بهذه الشبكة لذلك تم اللجوء إلى تكنولوجيا التوقيع الالكتروني حتى يتم رفع مستوى الأمن والخصوصية للمتعاملين عبر الشبكة، ويتم ذلك بقدرة هذه التكنولوجيا على الحفاظ على سرية المعلومات أو الرسالة، وعدم قدرة أي شخص آخر على الاطلاع أو تعديل أو تحريف مضمونها. إلاّ أنّ الحياة العملية ورغم الثقة الممنوحة للتوقيع الالكتروني، سواء للموقع، أو الموقع له وحتى الغير، أفرزت العديد من المشاكل، لذا يعتبر مخالفا للقانون كل فعل يقصد به

وعلى تسهيل تكوين شركات تكاملية مبنية على مشاركة أفضل في المعلومات وعلى علاقة عمل إستراتيجية، مما يحقق قفزات نحو تكامل أنظمة الترويج والشراء والدفع الإلكتروني على شبكة الإنترنت تتيح التجارة الإلكترونية للعملاء التسوق وإجراء المعاملات مع توفير عنصر الاختيار عن أفضل عرض وأقل ثمن وذلك بالتسوق في أماكن عديدة وإجراء مقارنة سريعة عبر شبكة الإنترنت. تعمل على اتساع نطاق التجارة العالمية وفي أي مكان في العالم.

[1]- **محمد أحمد محمد نور جستينية**، مدى حجية التوقيع الإلكتروني في عقود التجارة الإلكترونية، رسالة دكتوراه جامعة القاهرة، 2007، ص 25.

[2]- **جميل حلمي**، محاذير الشراء الإلكتروني، بحث منشور على الموقع الإلكتروني:
www.islamonlaine.net/arabic/elonomics/2003/12/articale02.shtml.

تزوير، تقليد أو كلّ أوجه الاعتداء عليه، سواءا بموافقة صاحبه أو بدونها. ونظرا لخصوصية التوقيع اللامادي والقيمة القانونية التي يتمتع بها في مجال التجارة الالكترونية في بيئة الانترنت،ولأهميته وحداثته كدليل إثبات إلكتروني، وأنّه موضوع ثقة وأمان في عالم افترضي يصعب حمايته من أيّ إعتداء، وللوصول إلى مدى فعالية وملائمة النصوص القانونية المتعلقة بالتوقيع الالكتروني في القوانين المقارنة والضمانات التي يوفرها التوقيع الالكتروني للمتعاملين في بيئة الانترنت لذلك لابد من البحث: **عن مدى فعالية الآليات والنصوص القانونية في حماية و تأمين التوقيع الإلكتروني؟**

تستوجب الإجابة على الإشكالية المطروحة التعرض لأحكام التوقيع الإلكتروني محل الحماية القانونية وحجيته في الإثبات في مختلف التشريعات المقارنة **(الفصل الأول)** ولكونه وسيلة لحماية التجارة الإلكترونية يتطلب الأمر إبراز آليات حماية التوقيع الإلكتروني ومدى فعالية النصوص القانونية المتعلقة به نظرا لعجز الأحكام والقوانين التقليدية أمام هذا المولود الجديد **(الفصل الثاني)**، معتمدين في هذه الدراسة على المنهج المقارن والتحليلي.

الفصل الأول

التوقيـــع الالكتروني محل الحمـــاية القـــانونية

الفـــصـــل الأول

التوقيع الالكتروني محل الحماية القانونية

التوقيع الإلكتروني مثله مثل التوقيع التقليدي، يقوم بتحديد هوية صاحبه وتأكيد رضاء هذا الأخير الالتزام بمضمون المستند الموقع. غير أنّ الطبيعة الإلكترونية للتوقيع الإلكتروني والوسيلة التي يوضع بها طرحت عدّة مشاكل، كمشكلة الثقة والأمان في هذا النوع من التوقيع، وكذا مشكلة تأمينه من أي اعتداء.

نظراً للمشكلات القانونية التي يطرحها التوقيع الإلكتروني والذي أصبح أمراً واقعا تتزايد أهميته يوما بعد يوم، خاصة في ظل انتشار وازدهار التجارة الإلكترونية، تضافرت الجهود الدولية لتنظيم هذا النوع من التوقيع بإصدار تشريعات وتوجيهات دولية، تضفي له نوعا من الأمان والثقة وتضع القواعد التي تكفل الاعتراف له بحجية كاملة في الإثبات.

لبيان ماهية التوقيع الإلكتروني نتطرق لمختلف التعريفات التي قدمت له في التشريعات الوطنية والتوجيهات الدولية **(المبحث الأول)**. ثم نتطرق لبيان صور ونطاق تطبيقه وحجيته في الإثبات بإظهار الشروط التي يجب توفرها ليؤدى دوره في الإثبات **(المبحث الثاني)**.

المـــبحث الأول

مـــاهية التوقيع الالكتروني

تتمثل أهم المشاكل التي تعرقل نمو التجارة الإلكترونية في عدم التعرف عن هوية أطراف التعاقد وأهليتهم، وهو الشرط الوحيد الذي يضفي الصحة على الورقة حتى يعتد بها في الإثبات، فقد تمّ إلغاء القواعد والأحكام التقليدية المألوفة في التوقيع اليدوي وتحويله إلى توقيع إلكتروني مثلما حولت المحرر الورقي إلى محرر إلكتروني، لذلك نتطرق إلى المقصود بالتوقيع الإلكتروني **(المطلب الأول)**، ثم إلى وظائف التوقيع الإلكتروني ومدى تحققها وأهم خصائصه **(المطلب الثاني)**.

المـــطلب الأول

مفـــهوم التـــوقيع الإلـــكتروني

اجتهدت أغلب التشريعات المقارنة والمنظمات الدولية والإقليمية في وضع تشريعات تنظيمية للتوقيع الإلكتروني وللمسائل المرتبطة به مبينة طبيعته القانونية، من خلال تنظيمه والاعتراف له بالحجية الكاملة في الإثبات، حيث يعتبر حجر الزاوية في الإثبات، ويعدّ الشرط الوحيد في المحررات العرفية، إلاّ أنّه لم يعط له تعريفا جامعا مانعا[1].

لبيان الطبيعة القانونية للتوقيع الإلكتروني نتطرق لتعريف التوقيع الإلكتروني وفقا للتشريعات والتوجيهات الدولية **(فرع أول)**، ثم إلى تعريفه وفقاً للتشريعات الوطنية **(فرع ثاني)**، وأخيرا تعريف الفقه والقضاء له **(فرع ثالث)**.

الفـــرع الأول

تعريف التوقيع الإلكتروني وفقاً للتشريعات والتوجيهات الدولية

تختلف التعاريف التي أطلقت على التوقيع الإلكتروني، باختلاف النظرة إليها فالبعض يعرفه بناء على الرسائل التي يتمّ بها، أو بحسب الوظيفة أو بناء على التطبيقات العملية للتوقيع[2].

تصدّت أكثر من منظمة لتعريف التوقيع الإلكتروني من خلال قوانين التجارة الإلكترونية أو من خلال قوانين وضعت خصيصا للتوقيع الإلكتروني، غير أننا سنتناول الحديث هنا عن منظمتين دوليتين فقط هما: لجنة الأمم المتحدة لقانون للتجارة الدولية

---

[1] - **حابت أمال**، استغلال خدمات الانترنت، مذكرة لنيل شهادة الماجستير في القانون، فرع قانون الأعمال، جامعة مولود معمري، تيزي وزو، 2004، ص 80.

[2] -**محمد فواز المطالقة**، الوجيز في عقود التجارة الالكترونية، دراسة مقارنة، دار الثقافة للنشر والتوزيع، عمان 2008، ص 172.

المعروفة بـــاليونسيترال، والإتحاد الأوربي كمثال لمنظمة إقليمية، إذ أنّ باقي المنظمات التي حاولت تعريف التوقيع الإلكتروني تأثرت بتعريف اليونسيترال[1].

أولا: قانون اليونسيترال النموذجي بشأن التجارة الإلكترونية *1996*م:

لقد منح قانون اليونسيترال النموذجي بشأن التجارة الإلكترونية[2]، راسائل البيانات الإلكترونية حجية في الإثبات، كما اعترف بالتوقيع الإلكتروني وسوى بينه وبين التوقيع التقليدي[3]، غير أنه عند الإطلاع على مواد قانون الأمم المتحدة النموذجي بشأن التجارة الإلكترونية، نجد أنه لم يعرف التوقيع الإلكتروني، واكتفى في مادته السابعة بالإشارة للشروط الواجب توافرها في التوقيع، حيث نصّت الفقرة الأولى منها على أنّه "**عندما يشترط القانون وجود توقيع من شخص يستوفى ذلك الشرط بالنسبة إلى رسالة البيانات[4] إذا استخدمت طريقة لتعيين هوية ذلك الشخص والتدليل على موافقة ذلك الشخص على المعلومات**

---

[1]- **اليونيسترال**: هي لجنة قانون التجارة الدولية التابعة للأمم المتحدة، وتضم في عضويتها غالبية دول العالم الممثلة لمختلف النظم القانونية الرئيسية، وغرضها الأساسي هو تحقيق الانسجام والتوائم بين القواعد القانونية الناظمة للتجارة الإلكترونية، وتحقيق وحدة القواعد المتبعة وطنيا في التعامل مع مسائل التجارة الإلكترونية، وقد حققت اليونسيترال العديد من الانجازات في الميدان، أبرزها عدد من الاتفاقيات الدولية أشهرها اتفاقية فينا لعقود البيع الدولية لسنة 1980 والاتفاقيات الخاصة بالتحكيم التجاري الدولي وغيرها.

[2]-اعتمدت الأمم المتحدة هذا القانون النموذجي في دورتها التاسعة والعشرين، وأصدرته في 16 ديسمبر 1996، وقد طالبت اللجنة أن تولى جميع الدول اعتباراً لهذا القانون عندما تقوم بين قوانينها المتعلقة باستخدام بدائل للأشكال الورقية للاتصال وتحرير المعلومات. هادفة من ذلك العمل على توحيد القوانين الواجبة التطبيق على البدائل للأشكال الورقية للاتصال وتحرير المعلومات – أنظر الدليل التشريعي لقانون الأونسيترال النموذجي بأن التجارة الإلكترونية: منشور باللغتين الإنجليزية والعربية على الموقع: http://www.uncitral.org

[3]- **إيمان مأمون أحمد سليمان**، "الجوانب القانونية لعقد التجارة الإلكترونية"، رسالة دكتوراه، جامعة المنصورة 2006 ص249.

[4]- **رسالة البيانات**: يقصد بها المعلومات التي يتم إنتاجها أو إرسالها أو استلامها أو تخزينها بوسائل إلكترونية أو بصرية أو وسائل تقنية أخرى بما في ذلك تبادل البيانات الإلكترونية أو البريد الإلكتروني أو البرق أو التلكس أو النسخ البرقي.

الواردة في رسالة البيانات، كانت تلك الطريقة جديرة بالتعويل عليها بالقدر المناسب للغرض الذي أنشئت أو بلغت من أجله رسالة البيانات،في ضوء كل الظروف بما في ذلك أي اتفاق متصل بالأمر"[1].

تركّز هذه المادة على ضرورة قيام التوقيع الإلكتروني بالوظائف التقليدية للتوقيع العادي وهي تحديد هوية الشخص والتعبير عن رضائه عند الارتباط بالعمل القانوني على نحو ما ورد بالفقرة (أ)، كما تركز أيضاً على أنه يتعين أن تكون طريقة التوقيع الإلكتروني الواردة بالفقرة (ب) – طريقة موثوقة بها[2]، لذلك نجد أن قانون الأمم المتحدة النموذجي للتجارة الإلكترونية وضع القواعد الأساسية التي يقوم عليها التوقيع الإلكتروني من خلال الاعتراف به ومساواته بالتوقيع التقليدي

ثانيا: التوجيه الأوروبي بشأن التوقيعات الإلكترونية لعام *1999*م:

لم تكن المجموعة الأوروبية بمنأى عن الاهتمام الدولي بتطوير القواعد القانونية لتتلاءم مع عصر المعلوماتية،بل بالعكس تماما، فقد أولت اهتماما خاصا للتنسيق بين التشريعات الداخلية الخاصة بالدول الأعضاء، كما أدركت أن تحقيق هذا التنسيق في تشريعات هذه الدول من شأنه أن يساهم في إشاعة الثقة والأمان داخل السوق الأوروبية التي تعتمد بالدرجة الأولى على الثقة التي يوليها الأفراد للأمان المتوافر في عمليات التبادل الإلكتروني[3]، والتي ازدادت تطبيقاتها المرتبطة بالتوقيع الإلكتروني يوما بعد يوم خاصة في ظل انتشار وازدهار التجارة الإلكترونية.

فبتاريخ 13 ديسمبر 1999م صدر التوجيه الأوربي رقم 1999/93 بشأن التوقيع الإلكتروني[4]، ويتكون هذا التوجيه من (28) حيثية و(15) مادة وأربعة ملاحق، حيث جاء

---

[1]- نقلا عن **خالد ممدوح إبراهيم**، إبرام العقد الإلكتروني، دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، 2008، ص242.

[2]- راجع المادة 7 من قانون اليونسيترال النموذجي بأن التجارة الإلكترونية الصادر في 1996.

[3]- **ثروت عبد الحميد**، ماهيته، مخاطره، وكيفية مواجهتها، مدى حجيته في الإثبات، دار الجامعة الجديدة، القاهرة 2007، ص157.

[4]-للإطلاع على نصوص قانون التوجيه الأوربي، أنظر الموقع: http://www.ec.europa.eu.
http://www.fs.dk/uk/acts/eu/pdf/esign-fr.pdf.

في مادته الأولى أن الهدف منه هو تسهيل استخدام التوقيعات الإلكترونية والمساهمة بالاعتراف القانوني بها كدليل إثبات، وهو ما ينشئ إطارا قانونيا للتوقيعات الإلكترونية وبذلك يكون هذا التوجيه قد أضفى على التوقيع الإلكتروني نفس الحجية القانونية في الإثبات الممنوحة للتوقيع التقليدي.

وقد نصّت المادة (1/2) من هذا التوجيه، على أن التوقيع الإلكتروني هو عبارة عن "**بيان أو معلومة معالجة إلكترونيا، ترتبط منطقيا بمعلومات أو بيانات إلكترونية أخرى - كرسالة أو محرر - والتي تصلح كوسيلة لتمييز الشخص وتحديد هويته**[1].

كما ميز في مادته (2/2) بين التوقيع الإلكتروني المتقدم LA Signature électronique Avancée، والتوقيع الإلكتروني البسيط LA signature électronique simple فالتوقيع الإلكتروني المتقدم هو الذي يكون معتمدا من أحد مقدمي خدمات التصديق الإلكتروني ويمنح شهادة تفيد صحة هذا التوقيع الإلكتروني بعد التحقق من نسبة التوقيع إلى صاحبه[2].

ووفقا لنص المادة (2/2)، نجد أنها اشترطت في التوقيع المتقدم توافر المتطلبات التالية:

1. أن يكون قادرا على تحديد شخصية الموقع، ومميزا له عن غيره من الأشخاص.
2. أن ينشأ باستخدام وسائل وإجراءات تقنية تقع تحت سيطرة الموقع.
3. أن يرتبط بالمعلومات التي يتضمنها المحرر الإلكتروني بطريقة تسمح بكشف أية محاولة لتعديل هذه البيانات.

---

[1]- وجاء نصها في النسخة الفرنسية كما يلي:
« signature électronique ،une données sous forme électronique, qui est jointe ou liée logiquement a d'autres données électronique et qui sert méthode d'authentification ».

[2]- **VALERIE Sédalian**: preuve et signature électronique, paris, P4, sur Le site: http://www.juriscom.net/chr2/fr20000509.htm

متى توافرت هذه الشروط يكون للتوقيع الإلكتروني المتقدم الحجية القانونية الكاملة في الإثبات، أمّا التوقيع الإلكتروني البسيط فيتمتع بالحجية القانونية في حالة عدم إنكاره، وفي حالة إنكاره يقع على عاتق من يتمسك به إقامة الدليل، بأنه قد تم بطريقة تقنية موثوق بها، وفي حالة ما إذا وجد ازدواجية بين توقيعين إلكترونيين أحدهما متقدم والآخر بسيط، فإنّ الأولوية تكون للتوقيع المتقدم، لأنّه يتمتع بعناصر أمان وثقة لا تتوفر في التوقيع البسيط[1] هذا وقد أكدّت المادة (5) من التوجيه مبدأ عدم التمييز بين التوقيعات الإلكترونية والتوقيعات اليدوية.

يتضح مما سبق أن التوجيه الأوروبي رقم 1999/93 قد وضع تعريفا وصفيا للتوقيع الإلكتروني، أي أنّه تبني مفهوما موسعا للتوقيع الإلكتروني، حيث جاء عاما وشاملاً لجميع صور التوقيع، والتي من شأنها أن تحدد صاحب التوقيع، وتميزه عند استخدام تقنيات الاتصال الحديثة.

ثالثا: قانون الأونسيترال النموذجي الخاص بالتوقيعات الإلكترونية لعام *2001*م.

قامت لجنة الأمم المتّحدة للقانون التجاري الدولي في دورتها الرابعة والثلاثين بوضع القانون الذي تعرض لتنظيم التوقيع الإلكتروني الموثوق به، والجهة التي تقوم بتحديده، والواجبات التي يتحملها الموقع، وما يبذله من عناية حيال توقيعه والسلوك الذي يتعين أن يتبعه الطرف الذي يعول على هذا التوقيع، كما نظم أوضاع مقدم خدمات التصديق أو التوثيق الإلكتروني وشهادات التصديق التي يصدرها.

فقد نص في المادة الأولى على نطاق تطبيق قواعد هذا القانون[2] فنص على أنّ تلك القواعد تطبق حيثما تستخدم توقيعات إلكترونية في سياق أنشطة تجارية، فهذا لا يحد من

---

[1]-**سعيد سيد قنديل**، "التوقيع الإلكتروني" ماهيته، صوره، حجيته في الإثبات بين التداول والاقتباس، دار الجامعة الجديدة، الإسكندرية، 2006، ص55.

[2]- بموجب نص المادة الأولى من هذا القانون فإن نطاق تطبيقه يقتصر فقط على استخدام التوقيعات الإلكترونية في مجال أنشطة تجارية. والنشاط التجاري وفقا لدليل هذا التشريع يشمل جميع الوسائل الناشئة عن كل العلاقات ذات

إمكانية قيام أيّ دولة من توسيع نطاق تطبيق هذا القانون عندما تضع قانون خاص بها مستلهمة إياه من هذا القانون النموذجي[1].

عرفت المادة الثانية من قانون الأمم المتحدة النموذجي بشأن التوقيعات الإلكترونية إلى تعريف التوقيع الإلكتروني بأنه "**بيانات في شكل إلكتروني مدرجة برسالة أو مضافة إليها أو مرتبطة بها منطقيا، بحيث يمكن أن تستخدم لبيان هوية الموقع بالنسبة إلى هذه الرسالة، ولبيان موافقته على المعلومات الواردة في الرسالة**"[2].

نلاحظ من النص السابق أن قانون اليونسيترال بشأن التوقيعات الإلكترونية لم يقيد مفهوم التوقيع الإلكتروني، بل أن هذا النص يمكن أن يستوعب أي تكنولوجيا تظهر في المستقبل تفي بإنشاء توقيع إلكتروني، وهذا ما نصت عليه المادة الثالثة من ذات القانون حيث نصت على أنّه: "**لا تطبق أي من أحكام هذا القانون، باستثناء المادة الخامسة بما يشكل استبعادا أو تقيدا أو حرمانا من مفعول قانوني لأي طريقة لإنشاء توقيع إلكتروني تفي بالاشتراطات المشار إليها في الفقرة الأولى من المادة السادسة أو تفي على أي نحو آخر بمقتضيات القانون المنطبق**"[3].

يتمثل الهدف من إصدار هذا القانون النموذجي في جعل التوقيع الإلكتروني أداة أكثر فاعلية لدى الدول فيما يتعلق بمسائل التوقيعات الإلكترونية لتقديمه معلومات تفسيرية للحكومات وللمشرعين، ممّا يؤدي بتلك الجهات إلى استخدام القانون النموذجي ومنح

=الطابع التجاري سواء كانت علاقات تعاقدية أو غير تعاقدية، ومنها على سبيل المثال لا الحصر: توريد أو تبادل السلع والخدمات الوكالة التجارية، الأعمال المصرفية، الخدمات الاستثمارية، نقل الأشخاص والبضائع أيا كانت وسيلة النقل برا أو بحرا أو جوا.

[1]- **منير محمد الجنبيهي، ممدوح محمد الجنبيهي**، التوقيع الإلكتروني وحجيته في الإثبات، دار الفكر الجامعي الجديد الإسكندرية، 2005، ص 29.

[2]- قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية لسنة 2001 مع دليل تشريعه على الموقع: http://www.unicitral.org/pdf/Arabic/texts/selectcom/mt-elecsig-a-pdf

التوقيع الإلكتروني الحجية القانونية الكاملة التي يمكن أن تساير مستجدات التجارة الإلكترونية.

الفرع الثاني

تعريف التوقيع الإلكتروني وفقا للتشريعات الوطنية

نظرا لتطور الآلية التي يتم بها التوقيع وظهور التوقيع الإلكتروني كونه واقعة مستجدة تحتاج للبحث والإقناع، شرعت العديد من الدول في تحديد مفهومه،سعيا منها إلى إزالة ما يواجه هذا المفهوم الجديد من مشكلات قانونية في مجال الإثبات، وذلك بعد ما فرض هذا النوع من التوقيع نفسه في ظل انتشار وازدهار التجارة الإلكترونية[1].

تحت هذا العنوان نتطرق إلى بعض التشريعات الوطنية التي لم تتوان – أسوة بالتشريعات والتوجيهات الدولية – عن وضع تعريف للتوقيع الإلكتروني ضمن قانون مستقل خاص به،أو خاص بالتجارة الإلكترونية أو من خلال تحديث – إضافة أو تعديل– نصوصها القانونية.

أولا:تعريف التوقيع الإلكتروني من قبل التشريعات الأجنبية.

برزت التجارة الإلكترونية لأول مرة في الـــولايات المتحدة الأمريكية، ثم انتقلت إلى الدول الغربية (إنجلترا، فرنسا، سويسرا...الخ)، وبالتالي كان أول استعمال لتقنية التوقيع الإلكتروني في هذه الدول أيضا، لذلك سنتطرق لتعريفه بعض تشريعات هذه الدول على النحو التالي:

***1*: في القانون الأمريكي:**

حظي التوقيع الإلكتروني بنصيب وافر من التنظيم التشريعي سواء على مستوى الإتحاد الفدرالي أو على مستوى الولايات، حيث ورد تعريفان للتوقيع الإلكتروني، الأول

[1]-**ARNAUD Fausse**, La signature électronique transaction et confiance sur internet, Edition Dunod, Paris, 2001, p 87.

في القانون الفدرالي للتوقيع الإلكتروني، والثاني في قانون المعاملات الإلكترونية الموحد. بادرت الولايات المكونة للولايات المتحدة الأمريكية في إصدار تشريعات تنظم الاعتراف بالتوقيع الإلكتروني في الإثبات مثل كاليفورنيا، ميسوري إلينوي، غير أن الأمر كان أيضاً محلاً لعناية المشرع الفدرالي، وهذا من خلال تنظيم مسألة التوقيع الإلكتروني على المستوى الاتحادي، سعيا منه في تحقيق الانسجام وإزاحة الاختلاف في تشريعات الولايات المختلفة، وبالفعل فبتاريخ 30 جويلية 2000 صدر القانون الفدرالي الأمريكي بشأن التوقيعات الإلكترونية[1]في مجال التجارة على المستوى الداخلي والخارجي، وقد نص في الجزء (5/106) على أن مصطلح توقيع إلكتروني يعني "**أصوات أو إشارات أو رموز، أو أي إجراء آخر، يتصل منطقيا بنظام معالجة المعلومات إلكترونيا، ويقترن بتعاقد أو مستند أو محرر،ويستخدمه الشخص قاصدا التوقيع على المحرر (المستند)**" **أمّا المستند (المحرر) الإلكتروني فقد عرفه هذا القانون كما يلي "كل مستند ينشأ أو يرسل أو يستقبل، أو يخزن بوسائل إلكترونية"**[2].

نصّ هذا القانون على أنّه لا يمكن تجريد التوقيع من آثاره القانونية أو حجيته لمجرد أنّه جاء في شكل إلكتروني، وأنّه إذا تطلب القانون وجود توقيع، فإن وجود توقيع إلكتروني يجعل هذا المطلب محققا.

لم يشترط القانون الفدرالي الأمريكي توفر خصائص معينة في التوقيع لكي تكون له حجية قانونية، أي أنّه يعترف بالتوقيع الإلكتروني والمحررات الإلكترونية – كما بيّنا سابقا – ولا يشترط لذلك الحصول على شهادة توثيق أو تصديق، تثبت أو توافق على هذا التوقيع من جهة معينة أو مختصة.

[1]-للإطلاع على القانون الفدرالي الأمريكي أنظر الموقع الإلكتروني:
http://www.frwebgate.access.gpo.gov.cgibin/getdoc.cgi?dbname106-cong-public-laws.
http://www.gigalawcom/articles/2000-all/aston-2000-06-all.htm.

وما يلاحظ على هذا القانون ما يلي:

- أنّ التعريف أشار إلى بعض صور التوقيع الإلكتروني على سبيل المثال لا الحصر، فقد ذكر الأصوات والرموز ثم فتح المجال أمام أيّة وسيلة أخرى تقع في شكل إلكتروني لتكون قادرة على تحقيق متطلبات التوقيع الإلكتروني، ومن ثم الاعتراف بها كوسيلة صالحة للتوقيع[1].

- لم يشترط أن يكون التوقيع مرتبطا بشكل مادي بالسجل الذي يقع عليه، بل اكتفى بارتباطه بالسجل ارتباطـــا منطقيا كونه واردا بشكل إلكتروني بخلاف حالة الإمضاء الخطي الذي يلحق بالكتابة.

نصّ على عملية (تنفيذ أو إصدار) التوقيع من قبل الشخص وفي ذلك تجاوز لعملية التوقيع بخط اليد التي كانت تتطلبها التشريعات، فاكتفى بالنص على عملية التنفيذ أو الإصدار بأي طريقة كانت.

يتمّ تنفيذ أو إصدار التوقيع الإلكتروني بقصد التوقيع على السجل دون أن ينصّ على العقد من التوقيع، أي دون أن يفصح صراحة عن وظيفة التوقيع، وقد يكون ذلك لأنّ كلمة (التوقيع) على السجل تشمل تحديد هوية الموقع وتعبر عن إرادته.

أمّا تعريف قانون المعاملات الإلكترونية الموحد فيلاحظ عليه أنّه:

لم يحدّد صورا للتوقيع الإلكتروني بل اكتفى بأن يكون التوقيع في شكل إلكتروني فقط أيّا كان هذا الشكل، على عكس القانون الفدرالي الذي ضرب أمثلة لصور التوقيع

[1]-**عبد الفتاح بيومي حجازي**، التوقيع الإلكتروني في النظم القانونية المقارنة، دار الفكر العربي، الإسكندرية، 2005 ص، ص 135،139.

واعتقد أنّ هذا المنحى أفضل، كونه يفتح المجال أمام للاعتراف بجميع صور التوقيع الإلكترونية التي تتمتع بالثقة الكافية وتحقيق وظائف التوقيع[1].

اشترط القانون أن يكون التوقيع مرتبطا بسجل إلكتروني فقط، فلا يمكن استخدام التوقيع الإلكتروني، حيث يكون مرتبطا بسجل عادي، والسجل الإلكتروني حسب تعريف القوانين الأمريكية هو: "**أي عقد أو أي سجل آخر جرى إنشاؤه أو إرساله أو استقباله أو تخزينه بالوسائل الإلكترونية**" وعليه فعلى التوقيع الإلكتروني أن يكون مرتبطا بسجل من هذا القبيل[2].

2: القانون الفرنسي:

طبق المشرع الفرنسي التعليمات والأحكام الواردة بالتوجيه الأوربي رقم 1999/93 بشأن التوقيع الإلكتروني، لاسيما المادة (2/5) التي تنص على أن تلتزم الدول الأعضاء في الإتحاد الأوربي بتطبيق أحكام هذا التوجيه فيما يتعلق بالتوقيعات الإلكترونية المتقدمة وتطبيقا لذلك أجرى المشرع الفرنسي تعديلا على القانون المدني–القسم الذي يحتوي على قواعد الإثبات– لتكييفه مع تكنولوجيا المعلومات والتوقيع الإلكتروني، وذلك من خلال القانون رقم 230/2000 الصادر بتاريخ 13 مارس 2000م[3]، حيث جاءت المادة (1316-4) وأشارت إلى تعريف التوقيع الإلكتروني بأنّه "**التوقيع الضروري لاكتمال التصرف القانوني، والذي يحدد هوية من يحتج به عليه، ويعبر عن رضا الأطراف بالالتزامات الناشئة عن هذا التصرف، وعندما يتم التوقيع بمعرفة موظف عام يكون التصرف رسميا، وعندما**

---

[1]-**PIETTE-COUDOL Thierry**, échange électronique, certification et sécurité, édition LITEC, Paris 2000, pp 28, et **THIEFFRY Patrick**, commerce électronique, droit international et Européen, LITEC, Paris, 2002, p 183

[2]- **وائل أنور بندق**، موسوعة القانون الالكتروني وتكنولوجيا الاتصالات، دار المطبوعات الجامعية، الإسكندرية 2007، ص 301.

[3]- قانون رقم 230-2000 المؤرخ في 13مارس 2000، المتعلق بتطويع قانون الإثبات لتكنولوجيا المعلومات والتوقيع الإلكتروني المنشور بالجريدة الرسمية رقم 62 في 14 مارس 2000م، للإطلاع على هذا القانون أنظر الموقع الإلكتروني: www.journal.officiel.gouv.fr

يكون التوقيع الإلكتروني ينبغي استخدام وسيلة آمنة لتحديد الشخص بحيث تضمن صلته بالتصرف الذي وقع عليه ويفترض أمان هذه الوسيلة – ما لم يوجد دليل مخالف – بمجرد وضع التوقيع الإلكتروني الذي يتحدد بموجبه شخص الموقع، ويضمن سلامة التصرف. وذلك بالشروط التي يتم تحديدها بمرسوم يصدر من مجلس الدولة"[1].

ترك المشرّع الفرنسي لمجلس الدولة -وهذا حسب المادة (1316_4) السابقة الذكر- إصدار القرارات التي تبين الشروط القانونية والضوابط الفنية والتقنية اللازمة لتمتع التوقيع الإلكترونية بالحجية في الإثبات. أصدر مجلس الدولة الفرنسي القرار رقم 2001/272[2]، تطبيقا لأحكام المادة (1316_4) من القانون المدني والخاص بالتوقيع الإلكتروني، الذي فرق بين التوقيع الإلكتروني العادي أو البسيط وبين التوقيع الإلكتروني المعزز أو المتقدم[3].

حسب ما تضمنته الفقرة الثانية من المادة الأولى من هذا المرسوم، يشترط في التوقيع الإلكتروني ليتم وصفه بالتوقيع الآمن أن يستوفى المقتضيات التالية:

1. أن يكون خاصا بصاحب التوقيع.
2. أن ينشأ بوسائل يمكن لصاحب التوقيع أن يضعها تحت رقابته.
3. أن يرتبط هذا التوقيع بالعقد الملازم له، بحيث كل تعديل لاحق للعقد يمكن فصله.

---

[1]- ART. 1316 – 4.c.civ: «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.».

[2]- المرسوم رقم 272-2001م، الصادر في 30 مارس 2001، المنشور في الجريدة الرسمية الفرنسة صفحة 5070 الصادرة في 2001/03/31، والذي جاء تطبيقا للمادة (4/1316) من القانون المدني، للإطلاع على هذا المرسوم أنظر الموقع الإلكتروني: www.journal.officiel.gouv.fr

[3]- **Rojinsky (c)**, signature Electronique : « Le décret et le devront Etre complètes » P.2. sur le site : http://www.jurcon.het/pro/2/ce2001/04/9.htm

يتضح من النصوص السابقة أن المشرع الفرنسي قد وضع مفهوما موسعا للتوقيع ولم يفرق بين التوقيع التقليدي والتوقيع الإلكتروني، حيث يكون لكل منهما نفس الحجية القانونية في الإثبات طالما كان هذا التوقيع يميز صاحبه، وتم إنشائه بإجراءات آمنة تضمن سرية بيانات هذا الموقع.

3: القانون الانجليزي:

نصت المادة 1/7 من قانون الاتصالات الإنجليزي لعام 2000، على أنّه في مسائل الإثبات القانوني يعتبر التوقيع المرتبط بأية وسيلة اتصالات إلكترونية، وأنه شهادة تفيد توقيع صاحبها أنهما مقبولان كدليل إثبات في أية منازعة تتعلق بالتوقيع أو البيانات[1].

4: القانون السويسري:

عرفت المادة الثانية من القانون الفيديرالي السويسري لعام 2004 التوقيع الالكتروني على أنّه :"**المعطيات الالكترونية مجتمعة أو مرتبطة منطقيا بمعطيات الكترونية أخرى تستخدم في التحقق من مصداقيته**"، وهو حسب القانون السويسري التوقيع الذي يفي بالمتطلبات الآتية:

1- أن يرتبط فقط بصاحبه.

2- أن يسمح بالتعرف على الموقع.

3- أن يكون قد أنشئ بوسائل يحفظها الموقع تحت رقابته المنفردة.

4- أن يرتبط بالمعطيات التي يتعلق بها بحيث يمكن اكتشاف أي تغيير لاحق عليها[2].

[1]-**أيمن سعد سليم**، التوقيع الإلكتروني، دراسة مقارنة، دار النهضة العربية، القاهرة، 2004، ص 62.

[2]-**وائل أنور بندق**، المرجع السابق ، ص106.

ثانيا: تعريف التوقيع الإلكتروني في التشريعات العربية.

اقتداءا منه بالدول الغربية وبالقوانين الدولية، قامت الدول العربية إمّا بإصدار تقنيات خاصة بتنظيم التوقيع الإلكتروني، وأخرى عدلت من قوانينها الخاصة بالإثبات من أجل مواكبة التقدم التكنولوجي، ونذكر منها ما يلي:

***1*: القانون التونسي:**

تعدّ تونس من الدول العربية الأولى التي سنت قانونا متعلقا بالتجارة الإلكترونية فقد أصدر المشرع التونسي قانون المبادلات والتجارة الإلكترونية رقم 2000/83[1]، عالج من خلاله مسائل مختلفة متعلقة بالتجارة الإلكترونية والتوقيع الإلكتروني في سبعة أبواب وثلاثة وخمسين فصلاً (مادة)، منها الأحكام العامة، والوثيقة الإلكترونية والإمضاء الإلكتروني ، الوكالة الوطنية للمصادقة الإلكترونية ، خدمات المصادقة الإلكترونية والمعاملات التجارية الإلكترونية، حماية المعطيات الشخصية، والمخالفات والعقوبات الملاحظ على القانون التونسي رقم 2000/83 بشأن المبادلات والتجارة الإلكترونية أنّه لم يتضمن تعريفا للتوقيع الإلكتروني، واكتفى بتعريف العناصر المؤدية له[2]، حيث تناول الفصل الثاني منه تعريف منظومة إحداث الإمضاء بأنها "**مجموعة وحيدة من عناصر التشفير الشخصية أو مجموعة من المعدات المهيأة خصيصا لإحداث إمضاء إلكتروني**".

---

[1]-قانون المبادلات والتجارة الإلكترونية رقم 83-2000 الصادر في 9-9-2000 المنشور في الرائد الرسمي للجمهورية التونسية في العدد 24من الصفحة رقم2084إلى غاية الصفحة 2089– أنظر الموقع:
http://www.infocom.th/fileadmin/documentation/juridiques/jortAR/jort_6411 8 2000 pdf

[2]- قبل صدور القانون رقم 2000/57 المؤرخ في 31 جوان 2000م المتعلق بتنقيح مجلة الالتزامات والعقود، لم يتضمن الفصل 453 منها تعريفا للإمضاء وإنما اقتصر على اشتراط أن يكون الإمضاء بيد العاقد نفسه. وبموجب التنقيح المذكور أضيفت فقرة ثانية للفصل 453 المشار إليه لتعريف الإمضاء ولتجعل منه يشمل كلا من الإمضاء اليدوي والإمضاء الإلكتروني حيث نص على ما يلي "يتمثل الإمضاء في وضع اسم أو علامة خاصة بخط يد العاقد =نفسه مدمجة بالكتب المرسوم بها، أو إذا كان التوقيع إلكترونيا في استعمال منوال تعريف موثوق به يضمن صلة الإمضاء المذكور بالوثيقة الإلكترونية المرتبط به".

ورد في ذات الفصل تعريف منظومة التدقيق في الإمضاء بأنّها "**مجموعة من عناصر التشفير العمومية أو مجموعة من المعدات التي تمكن من التدفيق في الإمضاء الإلكتروني**"، وقد نص الفصل الخامس من الباب الثاني أيضا على أنّه "**يمكن لكل من يرغب في إمضاء وثيقة إلكترونية إحداث إمضائه الإلكتروني بواسطة منظومة موثوق بها يتم ضبط مواصفاتها التقنية بقرار من الوزير**".

2: القانون الأردني:

جاء في المادة (41) من قانون المعاملات الإلكتروني رقم 2001/85م[1]، تنظيم عدة مسائل في المعاملات الإلكترونية منها السجل ،العقد والرسالة والتوقيع الإلكتروني غيرها من الأمور، وقد خص المشرّع الأردني المادة الثانية منه لتعريف التوقيع الإلكتروني، والتي عرّفته بأنّه عبارة عن "**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.**

كما أنّه ووفقا للمادة (7/أ) من ذات القانون، منح المشرع الأردني الحجية القانونية الكاملة للتوقيع الإلكتروني شأنه في ذلك شأن نظيره التقليدي، أي أنّه ساوى بين التوقيعين الإلكتروني والتقليدي وأعطى لهما نفس الحجية القانونية في الإثبات.

3: قانون إمارة دبي:

أصدر المشرع الإماراتي القانون رقم 2002/2م بشأن المعاملات والتجارة الإلكترونية والذي نشر في الجريدة الرسمية عدد 277 في 16 فبراير 2000م، وقد جاء هذا القانون في خمسة فصول وتسعة وثلاثون مادة، عالج من خلالها المشرع الإماراتي

[1]-أنظر قانون المعاملات الإلكترونية الأردني رقم 85 /2001، نشر في الجريدة الرسمية للملكة الأردنية في العدد 4524 بتاريخ 11 ديسمبر 2001م على الموقع: http://www.lob.gov.jo/ui/laws/index.jsp

متطلبات المعاملات الإلكترونية من تسجيلات وتوقيعات إلكترونية وأحكام متصلة بالشهادات أو خدمة التصديق على التوقيع الإلكتروني، وقد جاء تعريف التوقيع الإلكتروني في المادة الثانية من هذا القانون أنّه هناك مستويين للتوقيع الإلكتروني[1].

يتمثل الأول في التوقيع الإلكتروني البسيط ويعرف بأنّه: "**توقيع مكون من حروف وأرقام أو رموز أو صوت أو نظام معالجة ذي شكل إلكتروني أو مرتبط منطقيا برسالة إلكترونية وممهور بنية توثيق واعتماد تلك الرسالة**".

في حين يتمثل الثاني في التوقيع الإلكتروني المحمي، ويكون التوقيع الإلكتروني محميا إذا استوفى الشروط المنصوص عليها في المادة (20) من هذا القانون، هذه الشروط تتمثل في:

1- أنّه ينفرد به الشخص الذي استخدمه وكذا إمكانية إثبات هوية ذلك الشخص[2].

2- أن يكون تحت سيطرته التامة سواء بالنسبة لإنشائه أو وسيلة استعماله وقت التوقيع.

3- أن يرتبط بالرسالة الإلكترونية ذات الصلة به أو بطريقة توفر تأكيدا يعول عليه حول سلامة التوقيع، حيث إذا تم تغيير السجل الإلكتروني فإن التوقيع الإلكتروني يصبح غير محمي.

4: القانون المصري:

جاء قانون الإثبات المصري رقم 1968/25م خال من أي نص بشأن تعريف التوقيع، واكتفى في المادة (14) منه بتحديد بعض الصور المختلفة له وهي: الإمضاء الختم أو بصمة الإصبع، غير أنّه مع ظهور التجارة الإلكترونية والمعاملات الإلكترونية تغيرت النظرة لمفهوم التوقيع التقليدي[3]، وذلك بظهور صورة حديثة له وهي التوقيع

---

[1]-**عبد الفتاح بيومي حجازي**، المرجع السابق، ص، 135، 139.

[2]- **عبد الفتاح بيومي حجازي**، مقدمة في التجارة الإلكترونية العربية، الكتاب الأول، شرح قانون المبادلات والتجارة الالكترونية التونسي، دار الفكر العربي، الإسكندرية، 2003، ص210.

[3]- **محمد أمين الرومى**، النظام القانوني للتوقيع الإلكتروني، دار الكتب القانونية، مصر،2008، ص 10 وما بعدها.

الإلكتروني، ونظرا لابتكار هذه الصورة الجديدة من التوقيع ودخولها مجال التطبيق كان من الضروري تدخل المشرع لتنظيمها قانونا، حسنا فعل المشرع المصري بإصداره قانونا مستقلا ينظم التوقيع الإلكتروني، ويعترف بحجيته في الإثبات وهو القانون رقم 2004/15 بشأن تنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات الصادر في22 أبريل 2004م طبقا لما ورد في هذا القانون[1]، عرف المشرع المصري التوقيع الإلكتروني في المادة (1/جـــ) بأنّه "**ما يوضع على محرر إلكتروني ويتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها، ويكون له طابع متفرد يسمح بتحديد شخص الموقع ويميزه عن غيره**".

ووفقا للفقرة (هـــ) من نفس المادة فإن الموقع هو "**الشخص الحائز على بيانات إنشاء التوقيع ويوقع على نفسه أو من ينيبه أو يمثله قانونا**". تبنت اللائحة التنفيذية الخاص بالقانون رقم 15/ 2004م بتنظيم التوقيع الإلكتروني ذات التعريف[2]كما أن مشروع قانون التجارة الإلكترونية المصري والذي لم يصدر بعد، عرف التوقيع الإلكتروني بأنه "**حروف أو أرقام**

[1]- قانون رقم2004/15م بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات منشور بالجريدة الرسمية العدد 17 في 2 أبريل 2004م، وقد صدر هذا القانون بعد أن أصدر معالي الأستاذ الدكتور طارق وزير الاتصالات والمعلومات القرار رقم 209 بتاريخ 18 ديسمبر سنة 2000م بتشكيل لجنه تختص بإعداد مقترحات لمشروع قانون تنظيم التوقيع الإلكتروني، وقد ضمت تلك اللجنة ممثلين عن وزارة العدل، المالية، الداخلية، الخارجية الاقتصاد والتجارة الخارجية، وزارة الدولة لتنمية الإدارة، مجلس الدفاع الوطني، البنك المركزي المصري، مركز المعلومات ودعم اتخاذ القرار بمجلس الوزراء، بالإضافة إلى خبراء قانونيين وفنيين متخصصين في مجال المعاملات الإلكترونية، كما ضمت اللجنة مستشارو مجلس الدولة ومجلس الوزراء. أنظر: **قدري عبد الفتاح الشهاوي** قانون التوقيع الإلكتروني ولائحته التنفيذية، والتجارة الإلكترونية في التشريع المصري والعربي والأجنبي، دار النهضة العربية للنشر، القاهرة، 2005، هامش ص 29.

[2]- قرار رقم 109- 2005 المؤرخ في 2005/5/15م، خاص بإصدار اللائحة التنفيذية لقانون التوقيع الإلكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات رقم 15 لسنة 2004م، صدر ونشر بالوقائع المصرية العدد 115 تابع بتاريخ 2005/5/25م.

أو رموز أو إشارات لها طابع منفرد تسمح بتحديد شخص صاحب التوقيع وتميزه عن غيره "،وقد جاء ذلك التعريف ضمن الفصل الأول المتعلق بالتعريفات من مشروع القانون المذكور[1].

أضفى قانون التوقيع الإلكتروني المصري رقم 2004/15 على كل من التوقيع الإلكتروني والكتابة الإلكترونية والمحررات الإلكترونية في نطاق المعاملات المدنية والتجارية والإدارية ذات الحجية المقررة للكتابة والمحررات الرسمية والعرفية والتوقيعات في أحكام قانون الإثبات في المواد المدنية والتجارية، إذا ما توافرت فيها الشروط المنصوص عليها في هذا القانون والضوابط الفنية والتقنية التي تحددها اللائحة التنفيذية لهذا القانون طبقا للمواد (14و15و18) من هذا القانون[2].

رغم المكانة التي أفردها المشرع المصري لموضوع التوقيع الإلكتروني، إلاّ أنّ هناك بعض الآراء الفقهية ترى أنه كان من المستحسن لو وضعت نصوص هذا القانون ضمن نصوص قانون الإثبات، أي بمعنى تعديل بعض النصوص الواردة بقانون الإثبات حيث تستوعب المعاملات الإلكترونية، وتأتي مع المعاملات العادية على درجة المساواة في الإثبات أمام المحاكم وكافة الجهات المعنية كي لا يتشتت القاضي في البحث عن قيمة التوقيع مرة في قانون الإثبات، ومرة أخرى في القانون الخاص بالتوقيع الإلكتروني.

5: القانون الجزائـــــري:

أجرى المشرع الجزائري، تعديلا في مواد الإثبات من القانون المدني، بما يتلاءم مع تقنيات الاتصال الحديثة والتوقيع الإلكتروني بالقانون رقم 10/05 المؤرخ في 20 جويلية 2005م[3]، لكنّه لم يضع تعريفا للتوقيع الإلكتروني على الرغم من أنه لم ينكر

---

[1]- **هدى حامد قشقوش**، الحماية الجنائية للتجارة الإلكترونية عبر الإنترنت، دار النهضة العربية، القاهرة، ص 94.

[2]- **ممدوح محمد على مبروك**، مدى حجية التوقيع الإلكتروني في الإثبات، دراسة مقارنة بالفقه الإسلامي، دار النهضة العربية، القاهرة، 2005، ص133.

[3]- قانون رقم 10/05 المؤرخ في 20 جويلية 2005م، معدل ومتمم للأمر رقم 58-75 المؤرخ في26 سبتمبر والمتضمن القانون المدني،والمنشور في الجريدة الرسمية عدد 44 الصادر في 2005/7/21م.

التعامل به، فبالرجوع إلى نص المادة (327)[1] من القانون المدني نجد أن المشرع قد اعتد به شريطة أن تتوافر فيه الشروط المنصوص عليها في المادة 323 مكرر 1 من ق م ج التي تنص على أنّه "**يعتبر الإثبات بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة على الورق بشرط إمكانية التأكد من هوية الشخص الذي أصدرها وأن تكون معدة ومحفوظة في ظروف تضمن سلامتهاوهذه الشروط هي إمكانية التأكد من هوية الشخص الموقع وأن تكون منظومة إنشاء التوقيع الإلكتروني محفوظة في ظروف تضمن سلامته**"، هذا وقد جاء نص المادة (2/323) كما يلي: "**يعتد بالتوقيع الإلكتروني وفقا للشروط المذكورة في المادة 323 مكرر 1** ". أمّا عن تعريف التوقيع، فإن القانون الجزائري ميّز بين التوقيع المؤمن وذلك بموجب المادة 3 من المرسوم التنفيذي 162/07[2] التي جاء فيها أن: "**التوقيع الإلكتروني هو أسلوب عمل يستجيب للشروط المحددة في المادتين 323 مكررو 323 مكرر1،حيث أنه أعتبر التوقيع الإلكتروني المؤمن هو توقيع إلكتروني يفي بالمتطلبات الآتية:**

- **يكون خاصا بالموقع.**
- **يتم بوسائل يمكن أن يحتفظ بها الموقع تحت مراقبته الحضرية.**
- **يضمن مع الفعل المرتبط به صلة ببحث يكون كل تعديل لاحق للفعل قابلا للكشف عنه".**

كما اعترف المشرع الجزائري صراحة بالتوقيع الإلكتروني استكمالا باعترافه بحجية الكتابة في الشكل الإلكتروني في المادة (323 مكرر 1)، وذلك تماشيا مع إفرازات التطور التكنولوجي، الذي أدخل وسائل حديثة في إبرام العقود والتوقيع عليها إلكترونيا إلا أنّه يؤخذ على المشرع الجزائري عدم إصدار نص قانون أو مرسوم يبين كيفية تنظيم هذا التوقيع الإلكتروني ويحدد إطاره العام ويوضح مفاهيمه القانونية على غرار التشريعات المقارنة. لذلك على الجزائر أن تضع حيز التنفيذ هذه النصوص في أقرب وقت ممكن

[1]- الفقرة الثانية من المادة (327) أضيفت بالقانون رقم 05-10 بالمؤرخ في 20 جويلية 2005، المنشور بالجريدة الرسمية عدد44 /2005.

[2]-مرسوم تنفيذي 07- 162 يعدل ويتمم المرسوم 01-123، المتعلق بنظام للاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية.

وذلك قصد إعطاء الدفع للمبادلات الإلكترونية والتجارة الإلكترونية بأكملها التطوير التجارة الخارجية لأي بلد.

يتضح مما تقدم أن مشرعي مختلف الدول على النحو السالف بيانه، قد اتجهوا إلى مساواة التوقيع الإلكتروني بالتوقيع التقليدي، ومنحه ذات الحجية في الإثبات، إذا توافرت فيه الشروط القانونية والضوابط الفنية التي تضمن صحة وسلامة التوقيع الإلكتروني وتوفر الثقة في نسبته للموقع، كما يلاحظ على هذه التشريعات أن أياً منها لم يركز على طريقة معينة أو شكلاً معيناً للتوقيع الإلكتروني، وهذا حتى يتسع المجال في انتشار أشكال حديثة يظهرها التقدم التكنولوجي.

وبعدما تعدّدت الجهود الدولية والإقليمية التي سارعت لمحاولة حصر المستجدات الحديثة في مجال التوقيع عبر الوسائط التكنولوجية الحديثة، اتجهت الاتجاهات الفقهية والقضائية لذلك، وهو الأمر الذي سنحاول بيانه فيما سيأتي:

الـــفرع الثالـــث

التـــعريف الـــفقهي والـــقضائي للـــتوقيع الإلـــكتروني

ظهر التوقيع الإلكتروني كنتيجة للتزاوج الذي حصل بين التكنولوجيا الحديثة ووسائل الاتصالات متخذا أشكال عديدة ومختلفة تعتمد في مجملها على رموز وأرقام وبيانات تعتمد بدورها على المعادلات الرياضية واللورغاريتمية[1]، ومدعومة بتكنولوجيا حماية من نوع خاص لم تكن معروفة، وقبل أنيتم تجسيد هذا النوع من التوقيعات قانونا اختلف الفقه في تعريفه وإيجاد معنى له، بينما نجد القضاء قد تصدى للمسالة من قبل بفضل محكمة النقض الفرنسية.

[1] - اللوغاريتم هو مسار حسابي بالوصول إلى نتيجة نهائية محددة، حيث يرى البعض:
«Un ensemble de chiffre qui résulte d'un calcul algorithmique déclenché ou initie par la frappe d'un code confidentiel », voir : **JEAN_BAPTISTE Michelle, «** créer et exploiter un commerce électronique », Edition LITEC, Paris, 1998, p 12.

أولاً: التعريف الفقهي للتوقيع الإلكتروني.

تعدّدت التعريفات الفقهية للتوقيع الإلكتروني، ورغم تعددها وتعدد مصطلحاتها المترادفة، إلاّ أنّها تدور حول محور واحد ألا وهو عدم الخروج عن تحديد وظيفتي التوقيع، وهما تحديد هوية الموقع والتعبير عن رضاه بالالتزام بمضمون المحرر، كما تطرقت بعض التعريفات إلى الجانب التقني للتوقيع الإلكتروني، وهو ارتباطه بالمحرر بشكل غير قابل للانفصال، هذا من جانب، ومن جانب آخر كشف أي تعديل لاحق يمس بيانات المحرر الإلكتروني.

فقد عرّف جانب من الفقه الفرنسي التوقيع الإلكتروني بأنّه "**عبارة عن حروف أو أرقام أو رموز أو إشارات لها طابع منفرد تسمح بتحديد شخص صاحب التوقيع وتميزه عن غيره، وهو الوسيلة الضرورية للمعاملات الإلكترونية في إبرامها وتنفيذها والمحافظة على سرية المعلومات والرسائل**[1].

عرف البعض الآخر التوقيع الإلكتروني بأنّه "**مجموعة من الإجراءات والوسائل التي يتبع استخدامها عن طريق الرموز أو الأرقام لإخراج رسالة إلكترونية تتضمن علامة مميزة لصاحب الرسالة المنقولة إلكترونيا، يجرى تشفيرها باستخدام زوج من المفاتيح، واحد معلن والآخر خاص بصاحب الرسالة**[2]،من هذا التعريف يتضح لنا أن هذا الجانب من الفقه ارتكز على أحد أشكال التوقيع الإلكتروني ألا وهو التوقيع الرقمي الذي يقوم على التشفير اللاتماثلي، أي التشفير القائم على زوج من المفاتيح (العام والخاص).

كما عرفه البعض بأنّه "**مجموعة من الإجراءات التقنية التي تسمح بتحديد شخصية من تصدر عنه هذه الإجراءات، وقبوله بمضمون التصرف الذي يصدر التوقيع بمناسبته**".

---

[1]- **محمد حسين منصور**: المسؤولية الإلكترونية، دار الجامعة الجديدة للنشر والتوزيع، الإسكندرية، 2003، ص179.

[2]- **أحمد شرف الدين**: التوقيع الإلكتروني وقواعد الإثبات، ومقتضيات الأمان في التجارة الإلكترونية، ورقة عمل مقدسة لمؤتمر التجارة الإلكترونية المنعقد في جامعة الدول العربية مصر في تشرين الثاني، 2000، ص3.

ثانيًا: التعريف القضائي لتوقيع الإلكتروني.

سلكت محكمة النقض الفرنسية في تعريفها للتوقيع الالكتروني مسلك تعريفه على ضوء التوقيع التقليدي، فبعدما عرفت هذا الأخير بأنه: "**شهادة بخط اليد تكشف عن رضا الموقع بهذا التصرف وتمكن من التحقق من إسناد التوقيع لصاحب الوثيقة**"، قرّرت بشأن التوقيع الالكتروني أن: "**هذه الطريقة الحديثة (التوقيع الإلكتروني) تقدم نفس الضمانات التي يوفرها التوقيع اليدوي الذي يمكن أن يكون مقلدا، بينما الرمز السري لا يمكن أن يكون إلا لصاحب الكارت فقط**"[1].

كما كرّس القضاء بعد ذلك في أحكامه على الاعتداد بهذا النوع الجديد من التوقيعات وبين بأنّه يشكّل توقيعا صحيحا يعتد به قانونا، وعرّفه بأنّه: "**كل رمز خطي مميز وخاص يسمح بتحديد وتشخيص صاحبه بدون لبس ولا غموض وانصراف إرادته الصريحة للالتزام بمحتوى ما تمّ التوقيع عليه**".

لقد أقر هذا الاتجاه القضاء الفرنسي،وذلك من خلال حكم لمحكمة النقض الفرنسية صدر في 1989/11/18، بخصوص قبول التوقيع الرقمي في حالات الوفاء بالبطاقة البنكية، تطبيقا لحكم محكمة النقض الفرنسية في حكمها السابق المشهور بقضية "**كريدي كاس**" أين أسست حكمها على أن قواعد الإثبات المنصوص عليها في المادتين 1134 و1341 من التقنين المدني الفرنسي اللتان تجيزان للأفراد مخالفة أحكامها باعتبارهما قاعدتين مكملتين غير آمرتين، كما قررت ذات المحكمة في تقريرها السنوي لعام 1989 أن: "**التوقيع الذي يتم بتلك الإجراءات الحديثة (التوقيع المعلوماتي)، يقدم الأمان والضمان والثقة التي يقدمها التوقيع الخطي بل يفوقه بكثير، حيث أن الرقم السري للبطاقة البنكية لا يعرفه إلا صاحبها**"، وهو الاتجاه الذي جاء من قبل محكمة استئناف مونبلييه في حكم لها بتاريخ

[1]- **حمودي ناصر**، النظام القانوني لعقد البيع الدولي الإلكتروني المبرم عبر الإنترنيت، رسالة لنيل شهادة دكتوراه دولة في العلوم، التخصص: القانون، كلية الحقوق، جامعة مولود معمري تيزي وزو، 2009، ص 286-287. نقصد بالكارت البطاقة .

1987/04/05، حيث اعترفت بالتوقيع الالكتروني وجاء في حيثيات الحكم: أنه طالما أن صاحب البطاقة هو الذي قام باستخدامها، وهو الذي قام أيضا بإدخال الرقم السري،فإنّه يكون قد عبر عن رضاه وقبوله سحب هذا المبلغ المسجل[1]، وبناءا عليه فإن شركة Credicas قد قدمت دليل كاف على ديونها بواسطة تسجيل الآلة لتلك العملية والتي كان يتعذر قبولها لو لم يكن استخدام البطاقة متزامنا مع إدخال الرقم السري[2].

غير أنّه واستجابة لمتطلبات الدقة والفعالية والأمن في النظم المعلوماتية وقصد إضفاء مصداقية عليها، ذهبت محكمة النقض الفرنسية في حكم حديث لها نسبيا بتاريخ 1996/11/26 بشأن صحة المبادلات المالية، حين قضت أنّه بناءا على نص المادة 130 من التقنين التجاري الفرنسي، فإنّ التوقيع الصادر من الشخص الذي يدعي صحته وصلاحيته، لا يتمّ بمجرد ذكر الرقم السري في النص المرسل بواسطة التلكس، إذ أنّ هذا الرقم لا يعدوا أن يكون المفتاح السري[3].

يتّضح من مجمل هذه الأحكام بأنّ التوقيع الإلكتروني وسيلة حديثة لتحديد هوية صاحب التوقيع ووفائه بالتصرف القانوني الموقع عليه، وبالتالي يقوم بذات وظائف التوقيع التقليدي المعهود، كلّ ما هنالك أنّه ينشأ عبر وسيط إلكتروني استجابة لنوعية المعاملات التي تعتبر بدورها إلكترونية، وجب توقيعها إلكترونيا كونه لا مكان فيها للإجراءات اليدوية وأيا كانت الألفاظ أو العبارات المستعملة في تعريفه فإنها تتحد في المضمون، وهو تحديد هوية الشخص الموقع وتمييزه عن غيره، حيث أن العبرة هي المساواة الوظيفية بين هذين النوعين من التوقيعات[4].

---

[1]- **حمودي ناصر**، المرجع السابق، ص 287.

[2]- **لملوم كريم**، الإثبات في معاملات التجارة الإلكترونية بين التشريعات الوطنية والدولية، مذكرة لنيل شهادة الماجستير، جامعة مولود معمري، تيزي وزو،2011، ص141.

[3]- أنظر وقائع هذه القضية لدى: **محمد السعيد رشدي**، المرجع السابق، ص53.

[4]- **حمودي ناصر**،المرجع نفسه، ص 287.

المـــطلب الـــثاني

وظائـــف وخـــصائص التوقيع الإلكتروني

تتّفق جميع التشريعات التي اعترفت بالتوقيع الإلكتروني وأضفت عليه الحجية القانونية في الإثبات، على ضرورة توافر شروط معيّنة تعزّز من هذا التوقيع وتوفر فيه الثقة، حيث يمكن رد هذه الشروط إلى الدور أو الوظيفة التي يؤديها التوقيع، وهي تحديد هوية الموقع الذي يسند إليه الدليل أو المستند والتعبير عن إرادة الموقع في الالتزام بما وقع عليه[1].

ولكن قد يبدو لنا أن التوقيع الإلكتروني يعجز عن أداء الوظائف أو القيام بالأدوار المنوطة للتوقيع التقليدي في تحديد هوية الموقع، والإفصاح أو التعبير عن إرادته بالعمل القانوني ورضائه بمضمون الالتزام الموقع عليه، ولعل ما يدفع إلى هذا الاعتقاد هي الطريقة التي يتم بها صياغة المحرر على دعامة غير مادية – إلكترونية – والطريقة التي يوضع بها التوقيع عبر وسيط إلكتروني، وهي وسائل لا تسمح بالتعرف على هوية صاحب التوقيع بطريقة محسوسة، كما في حالة التوقيع التقليدي.

وعليه نتطرق إلى وظائف التوقيع الإلكتروني **(الفرع الأول)**، ثم نتطرق لدراسة خصائصه **(الفرع الثاني)**.

[1]-**حسن عبد الباسط جميعي**، إثبات التصرفات القانونية التي يتم إبرامها عن طريق الإنترنت، دار النهضة العربية القاهرة، 2000، ص20.

الـــفرع الأول

وظائف التوقيع الإلكتروني

اعتبارا للأهمية الكبرى التي يكتسيها التوقيع الإلكتروني نحاول إبراز أهمّ الوظائف التي يؤدّيها التوقيع الإلكتروني:

أولاً: مدى تحديد التوقيع الإلكتروني لهوية الشخص الموقع.

يستلزم لصحة التوقيع الإلكتروني بداية ارتباطه بشخص موقعه، ولا يكون هذا إلاّ إذا كان له طابع منفرد يسمح بتحديد هوية الموقع ويميّزه عن غيره من الأشخاص، أي يسمح بالتعرف على هويته بطريقة محسوسة، كما في حالة التوقيع في شكله الكتابي[1]. وهذا يتعلّق بنوع التكنولوجيا المستخدمة في تأمين التوقيع الإلكتروني، والذي لا يتحقّق إلاّ من خلال وسائل وإجراءات موثوق بها، تتمثل في استخدام نظام التشفير المزدوج أو وجود طرف ثالث يتولى التأكد من هوية صاحب التوقيع يسمى بجهة التصديق[2].

اشترطت المادة (4/1316) من القانون المدني الفرنسي لحجية التوقيع: "**أن يتم استخدام وسيلة آمنة لتحديد هوية الموقع وضمان صلته بالتصرف الذي وقع عليه**".

أفصحت المادة (1/ج) من قانون التوقيع الإلكتروني المصري عن حقيقة التوقيع الإلكتروني بأنه "**يكون له طابع منفرد يسمح بتحديد شخص الموقع ويميزه عن غيره**".

يقوم التوقيع الإلكتروني بذلك في شكل حروف أو أرقام أو رموز أو إشارات أو غيرها. تدل على شخصية الموقع وتحدد هويته وتميزه عن غيره من الأشخاص[3].

توجد مسألة أخرى تتصل بتحديد هوية الموقع وتميّزه عن غيره، وهي الخاصة بتحديد أهلية الشخص للتوقيع على المحرّر والتأكّد من سلطاته لإبرام التصرف القانوني

---

[1]- **خالد مصطفى فهمي**، المرجع السابق، ص 95.

[2]- راجع المادة 7 من قانون الأونسيترال النموذجي للأمم المتحدة بشأن التوقيعات الإلكترونية، 2001م.

[3]- **ممدوح محمد على مبروك**، المرجع السابق، ص140.

خاصة إذا كان الشخص الذي يتولى التوقيع ليس طرفا في العمل القانوني المراد إبرامه كما لو كان وكيلاً أو وصيا أو وليا على قاصر أو ممثلاً عن الشخص المعنوي[1]، إذ يجب عليه في هذه الحالات أن يحدد هويته بأن يوقع باسمه شخصيا، ثم يوضح مصدر سلطته في التوقيع كما لو كان توكيلا أو حكما قضائيا أو قرارا صادرا من شخص معنوي يمثله بموجب تفويض[2].

تتمثل الوظيفة الأولى للتوقيع في تحديد هوية الشخص الموقع، وهذا يحققه التوقيع الإلكتروني، لكن بطريقة إلكترونية، حيث أن الدقة في تحديد هوية الشخص الموقع في هذا المجال، معلقة على حداثة التقنية المستخدمة وقدرتها على توفير الأمان والسرية، فكلما كانت آلية تشغيل منظومة التوقيع الإلكتروني محلا للثقة والأمان، كان لها القدرة على تحديد هوية الشخص الموقع والتعرف عليه بطريقة تكاد أن تكون محسومة كما هو في التوقيع التقليدي.

التوقيع سواء الإلكتروني أو الكتابي يؤدي هذه الوظيفة، يكمن الاختلاف في كيفية وضع التوقيع على المحرر،ففي حين ينشأ التوقيع الكتابي على محررات ورقية ذات طبيعة مادية تترجم الشكل الذي تم به التصرف القانوني، وذلك بالحضور المادي لأطراف التصرف ومقابلتهم وجها لوجه في مجلس واحد، كان من الضروري أن يأتي التوقيع أيضا ماديا على ذات المحررات الورقية، حيث يتم إبرام العقود إلكترونيا عبر وسائل الاتصال الحديثة وتبادل المعلومات والخدمات عبر وسيط غير مادي بين أشخاص فإنّهم لا يرتبطون بعلاقة مباشرة، بل تتمّ دون رؤية الأشخاص لبعضهم البعض، ظهر التوقيع الإلكتروني الذي يوضع على المحرر عبر الأجهزة الإلكترونية.

---

[1]- راجع المادة (2/1) قانون تنظيم التوقيع الإلكتروني المصري رقم 15 لسنة 2004، وكذلك المادة (12) من قانون تنظيم التوقيع الإلكتروني.

[2]- **سمير حامد عبد العزيز الجمال**، المرجع السابق، ص230.

ذهب الكثير من الفقهاء إلى ضرورة منح التوقيع الإلكتروني حجية في الإثبات لأنه يمكن من خلاله التأكد من هوية صاحب التوقيع وهي من أهم وظائف التوقيع عامة[1].

ثانيًا: التعبير عن إرادة الموقع.

تتمثل الوظيفة الثانية التي يقوم بها التوقيع في إظهار إرادة الموقع بالتعبير عنها والالتزام بمحتويات التصرف القانوني والإقرار به، والسؤال المطروح هل يستوي في ذلك بأن يكون التوقيع الإلكتروني الذي يتم على دعامات إلكترونية؟ بمعنى آخر هل يحقق التوقيع الإلكتروني وظيفة التعبير عن إرادة الموقع في الالتزام بمضمون المحرر الذي وقع عليه؟

يرى بعض فقهاء القانون الفرنسي أن التوقيع الإلكتروني في حقيقته هو إجراء آلي يتضمن الطبيعة الإرادية للتوقيع التقليدي، وأنّه يفصح عن إرادة الموقع[2].

يستفاد رضى الموقع وقبوله بالالتزام الوارد بالمحرر بمجرد وضع توقيعه بالشكل الإلكتروني على البيانات التي يحتويها المحرر الإلكتروني، فحين يأخذ التوقيع الإلكتروني شكل أرقام سرية أو رموز محددة وتحفظ في حوزة صاحبها ومن ثم لا يعلمها غيره، فإذا استخدمت هذه الأرقام أي وقع بها صاحبها فإن مجرد توقيعه هذا يدل على موافقته على البيانات والمعلومات التي وقع عليها وأنّه يرغب في الالتزام بها[3].

وهذا ما يجري فعلا عند استخدام البطاقة الممغنطة المقترنة بالرقم السري -بطاقة الائتمان- وهي إحدى صور التوقيع الإلكتروني[4]، ففي هذه العملية نجد أن العميل صاحب البطاقة يعبر عن إرادته الصريحة بمجرد توقيعه الإلكتروني المترجم في شكل أرقام أو

---

[1]- **فيصل سعيد الغريب**، التوقيع الإلكتروني وحجيته في الإثبات، منشورات المنظمة العربية للتنمية الإدارية، مصر 2005، ص223.

[2]-**ممدوح محمد علي مبروك**، المرجع السابق، ص141.

[3]- **نجوى أبو هيبة**، التوقيع الإلكتروني ومدى حجيته في الإثبات، دار النهضة العربية، القاهرة، 2004، ص111.

[4]- أنظر في ذلك **ثروت عبد الحميد**، المرجع السابق، ص56.

رموز أو شفرة معينة استعملها، حيث تعامل مع جهاز الصراف الآلي، ثم أعطى أمرا للجهاز بسحب المبلغ الذي يريده شخصيا، كل هذا يعد رضاء منه وقبولا بمضمون المحرر الإلكتروني.

نجد أيضا أنّ هذا الشرط – التعبير عن إرادة الموقع - الذي يجب على التوقيع الإلكتروني أن يحققه قد ورد بالمادة (7/1) من قانون اليونسيترال بشأن التجارة الإلكترونية لعام 1996 والتي تنص على أنّه: "...**والتدليل على موافقة ذلك الشخص على المعلومات الواردة في رسالة البيانات**"، وأيضا ورد بنص المادة (2/أ) من قانون اليونسيترال بشان التوقيعات الإلكترونية لعام 2001م والتي تنص على أن "...**ولبيان موافقة الموقع على المعلومات الواردة في رسالة البيانات**".

يختلف الأمر بالتعبير عن الإرادة في الالتزام بمحتويات التصرف القانوني على ما هو في تحديد هوية الشخص الموقع، فدقة التعبير عن الإرادة معلق على حداثة التقنية المستخدمة، وقدرتها على توفير الأمان والسرية، فكلّما كانت آلية تشغيل منظومة التوقيع محلا للثقة والأمان، كان لها القدرة على التعبير عن إرادة الموقع في الالتزام بمحتويات التصرف القانوني.

ثالثًا: التوقيع يدل على حضور صاحب التوقيع.

يستلزم لصحته التوقيع ضرورة وجود شخص الموقع بنفسه أو من ينوب عنه قانونا لوضع التوقيع على المحرر الكتابي، فإذا وجد التوقيع على الورقة وثبتت صحته ونسبته إلى موقعه كان ذلك دليلا على حضور الموقع شخصيا[1].

[1]- **محمد عبد الرحيم الشريفات**، التراضي في تكوين العقد عبر الانترنت، دار الثقافة للنشر والتوزيع، الأردن، 2009 ص، ص 208، 209. وكذا: **عيسى غسان عبد الله الربضي**، القواعد الخاصة بالتوقيع الإلكتروني، رسالة دكتوراه كلية الحقوق، جامعة عين شمس، 2006 ، ص43. وكذلك **حمودي ناصر**، المرجع السابق، ص302.

أمّا بالنسبة للتوقيع الإلكتروني فلا يتصور الحضور المادي للأشخاص فهو في الأساس وسيلة حديثة تستعمل في مجال التعاقد عن بعد، غير أن البعض من الفقهاء يرون أنّ قيام الشخص بإدخال البطاقة المصرفية في الصرف الآلي مصحوبة بالرقم السري، ثم إجابته عن قيمة المبلغ المطلوب سحبه، كان دليلا على حضور الشخص ذاته، أي وجود صاحب التوقيع الإلكتروني بشخصه وقت إدخال الرقم السري، فإدخال العميل الرقم السري يعد دليلا على أنه توقيعا صدر منه شخصيا، وأنّه كان متواجد فعلا حين صدر منه التوقيع في صورة أرقام سرية لا يعرفها إلاّ هو، لكن هذا لا يعني الوجود المادي أو الجسدي للأطراف في مجلس واحد وقت إبرام التصرف القانوني وإلاّ ما كان ضروريا اللجوء للتوقيع الإلكتروني، ومنه يمكننا القول أنّ للتوقيع الإلكتروني (الإجرائي أو السري) نفس وظائف التوقيع الخطي وهذا ما أدى بالفقه إلى اعتبار الرقم السري أو الرموز أو الشفرة السرية كالتوقيع دليلا على الحقيقة[1].

نخلص مما سبق إلى أن التوقيع الإلكتروني أمكن أن يؤدي نفس الوظائف التي يتطلبها القانون من التوقيع وهو ذات الدور الذي يقوم به التوقيع الكتابي، لذا ذهب الفقه إلى اعتبار الرقم السري أو تلك الشفرة السرية كالتوقيع دليلا على الحقيقة[2]، بل ذهب إلى أكثر من ذلك، حيث يرى أن التوقيع الإلكتروني يفوق التوقيع الكتابي.

[1]- **عايض راشد المري**: مدى حجية الوسائل التكنولوجية الحديثة في إثبات العقود التجارية، رسالة دكتوراه، جامعة القاهرة، 1998، ص117.

[2]- **محمد مرسي زهرة**،مدى حجية التوقيع الإلكتروني في الإثبات، مؤتمر الكمبيوتر والقانون –كلية الحقوق- جامعة عين شمس، 1994 ص90.

الفـــرع الثاني

خصـــائص التـــوقيع الإلـــكتروني

يتميز التوقيع الإلكتروني بأنه لا يتم عبر وسيط مادي، بحيث تذيل به الكتابة، كما هو الحال بالنسبة للتوقيع الكتابي، وإنما يتم كليا أو جزئيا عبر وسيط إلكتروني من خلال أجهزة الكمبيوتر، أو عبر الانترنيت، بحيث يكون بإمكان أطراف العقد الاتصال ببعضهم البعض والإطلاع على وثائق العقد، والتفاوض بشأن شروطه وإفراغ هذا العقد في محررات إلكترونية، وأخيرا التوقيع عليها إلكتروني[1].

لزوم تدخل طرف ثالث Tiers de confiance الذي يقوم بدور الوسيط بين أطراف العقد، حيث استلزمت ضرورة الأمن القانوني وجوب استخدام تقنية آمنة في التوقيع الإلكتروني تسمح بالتعرف على شخصية الموقع[2]، وسوف نتعرض إلى أهم خصائص التوقيع الإلكتروني في النقاط التالية:

أولاً: يوفر الخصوصية.

حماية البيانات ضد الاستخدام غير المشروع، أو بمعنى أخر تحديد صلاحيات الوصول للبيانات وعدم السماح للأشخاص بتنفيذ إجراء معين على البيانات لا يمتلكون الصلاحيات الكافية لتنفيذه، وتتمّ هذه العملية بتفعيل صلاحية الوصول أثناء حفظ بيانات التوقيع الإلكتروني الموجود على بطاقة ذكية ولا يغادرها أبدا ومحمى برقم سرى، بتشفير

---

[1]- **يونس عرب**، منازعات التجارة الإلكترونية، الإختصاص والقانون الواجب التطبيق وطرق التقاضي، ورقة عمل مقدمة إلى مؤتمر التجارة الإلكترونية الذي أقامته منظمة الأمم المتحدة، الفترة ما بين 8 و10 تشرين الثالث 2000 بيروت، ص ص 17-18، منشور على الموقع: http://www.aeab-low.com

[2]- **محمد بودالي**، التوقيع الإلكتروني، مجلة الإدارة، العدد الثاني، 2003، ص 57.

البيانات أثناء إرسالها وهي إحدى مزايا التوقيع الإلكتروني التي تهدف إلى التأكد من أن الشخص المقصود هو الوحيد الذي اطلع على المستند المرسل[1].

نعني بالخصوصية أن البيانات متوفرة فقط للأشخاص المسموح لهم الإطلاع عليها بعبارة أخرى عدم إطلاع الآخرين غير المخول لهم الإطلاع على مضمون المستند الموقع إلكترونيا سوى الشخص المرسل له.

ثانيا: يوفر التعرف على المستخدم:*(Authentification)*

تتمّ عملية التحقق من هوية الأشخاص أو التعرف على مصادر البيانات عن طريق كلمات السر والبطاقات الذكية، أو عن طريق شهادة التصديق الإلكتروني المصدرة من جهة تصديق الكتروني، وكلّما زادت الحاجة لدقة تحديد الهوية يتمّ اللّجوء إلى جمع عدّة وسائل وزيادة تعقيد وسيلة التحقق من هوية المستخدم.

ثالثا:يوفر وحدة البيانات: (*integrité*)

هي عملية حماية البيانات ضدّ التغير أو التعويض عنها ببيانات أخرى، وتتم هذه العملية باستخدام تقنية تشفير البيانات ومقارنة بصمة الرسالة المرسلة ببصمة الرسالة المستقبلة -عدم تغيير البيانات أثناء نقلها-، وأن مستقبل الرسالة يمكنه معرفة ذلك عند تلقي الرسالة، حيث إن حصل أي تغير أو تعديل على المستند أثناء إرساله اعتبر تزويرا[2].

رابعًا: يوفر عدم القدرة على الإنكار: *(Non –Répidiation)*

عدم قدرة الشخص الموقع إلكترونيا أو الشخص الذي قام بإرسال رسالة إلكترونية لوجود طرف ثالث يمكنه إثبات قيام طرف معين بفعل إلكتروني معين، وكذا عدم قدرة

---

[1]- **قارة مولود**، الإطار القانوني للتوقيع والتوثيق الإلكترونيين في قانون المعاملات والتجارة الالكترونية، مقال منشور عبر الموقع: www.minshawi.com

[2]- **صلاح عبد الحكيم المصري**، متطلبات استخدم التوقيع الإلكتروني في إدارة مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية في قطاع غزة، رسالة لنيل شهادة الماجستير في إدارة الأعمال، كلية التجارة، الجامعة الإسلامية غزة، 2007، ص ص24، 25.

مستلم رسالة معينة على إنكاره استلامه لرسالة ما، حيث أن المفتاح العام يثبت استلام الرسالة من قبل المستقبل وذلك بإرسال رد (وصل تسليم) إلى المرسل،فعدم الإنكار تعنى حماية المستند أو العقد الإلكتروني من الإنكار من أحد الطرفين (المرسل أو المستقبل)[1].

خامسًا: تاريخ توقيع الرسالة.

لا يستطيع مرسل الرسالة تغيير تاريخ توقيع وإرسال الرسالة وكذلك مستقبل الرسالة، حيث أن ذلك له أهمية كبيرة في مجال التجارة الإلكترونية والعقود القانونية يعني تاريخ توقيع الرسالة عدم قدرة مرسل الرسالة أو مستقبلها من إجراء أي تعديل على تاريخ إرسال أو استلام المستند فهو ملزم للطرفين خاصة في حال إبرام العقود التجارية عبر الانترنت.

سادساً: يوفر السرعة ودقة إنجاز المعاملات.

يزيد التوقيع الإلكتروني من سرعة ودقة المعاملات الإلكترونية ويقلل من تأخر إرسال واستلام العقود والمستندات التجارية وغيره من العقود حول العالم.

المبحث الثاني

صور التوقيع الإلكتروني وحجيته في الإثبات

ظهرت العديد من الصور التي يتخذها التوقيع الإلكتروني، وهي تختلف تبعا لاختلاف الطريقة التي يتم بها، كما تتباين فيما بينها من حيث درجة الثقة والأمان ومستوى ما تقدمه من ضمان، بحسب الوسيلة التقنية المستخدمة، والإجراءات المتبعة في إصداره وتأمينه. فهناك تقنية تعتمد على منظومة الأرقام أو الحروف أو الإشارات، وما

[1]- **منانى فراح**، العقد الإلكتروني وسيلة إثبات حديثة في القانون المدني الجزائري، دار الهدى للطباعة والنشر والتوزيع، الجزائر، 2009، ص ص196ــ197. وكذا لنفس المؤلف، أدلة الإثبات الحديثة في القانون، دار الهدى للطباعة والنشر، الجزائر، 2008، ص ص 87، 145.

يعتمد على الخواص الفيزيائية والطبيعية والسلوكية للأشخاص، كبصمة الإصبع، أو بصمة اليد أو نبرة الصوت أو قرنية العين وغير ذلك من الخواص.

ولعلّ أهم صور التوقيع الإلكتروني وأكثرها انتشاراً هي التوقيع بواسطة الرقم السري المقترن بالبطاقة الممغنطة، وكذلك التوقيع بالقلم الإلكتروني والتوقيع البيومتري والتوقيع الرقمي، وسوف نتناول كل نوع ونطاق التطبيق **(مطلب أول)** ثم دراسة حجية التوقيع الإلكتروني في الإثبات من خلال استيفائه للشروط اللازمة للاعتداد به كتوقيع كامل، سيما وأن معظم التشريعات الحديثة منحته الحجية القانونية في الإثبات **(مطلب ثاني)**.

المطلب الأول

صور التوقيع الإلكتروني ومجالات تطبيقه

لا يعني الحديث عن التوقيع الإلكتروني حديث عن توقيع يأخذ صورة واحدة، فكما أنّ التوقيع التقليدي قد يظهر على عدة أشكال فإنّ للتوقيع الإلكتروني أيضا عدّة أشكال وصور تشترك في استخدامها تقنيات حديثة تستطيع أن تحول بعض الصفات المميزة للشخص والأرقام والحروف إلى بيانات ينفرد هو باستعمالها من أجل توقيع مستندات وعقود إلكترونية.

يتخذ التوقيع الإلكتروني عدة صور فقد يأتي في صورة رقم سري أو مجموعة أحرف وهو ما يعرف بالتوقيع الكودي أو السري، حيث غالبا ما يرتبط هذا النوع من التوقيع بالبطاقات الذكية أو البطاقات الممغنطة، كما أنّه قد يتم عن طريق قيام الموقع بكتابة توقيعه الشخصي باستخدام قلم إلكتروني ضوئي خاص.

الفرع الأول

صور التوقيع الإلكتروني

إنّ حصر كلّ أنواع التوقيع في هذه النقطة،أمر يتجاوز قدراتنا بالنظر للعدد الهائل الذي أسفرت عنه التطورات التكنولوجية والمختلفة من جهة، ومن جهة أخرى باعتبار المسالة تقنية أكثر منها قانونية، لذا سنركز دراستنا على أهم الأشكال المتداولة وأكثرها استعمالا وشيوعا على الساحة الدولية، وهو ما سنتطرق إليه فيما يأتي.

أولا: التوقيع بواسطة الرقم السري المقترن بالبطاقة الممغنطة.

تعتبر هذه الصورة الأكثر انتشارا في التعاملات الإلكترونية خاصة المعاملات البنكية حيث درجت البنوك على إصدار بطاقات ذكية-بطاقات بلاستيكية-[1] مصحوبة برقم سري يتمثل في أرقام أو حروف أو رموز تمنحها لعملائها لاستخدامها في سحب وإيداع النقود أو لسداد ثمن السلع والخدمات[2]، وتتمّ عملية سحب النقود أو إيداعها أو عملية الدفع الإلكتروني من خلال جهاز آلي تؤمنه البنوك للعملاء كجهاز الصراف الآلي (A.T.M)[3] أو جهاز الدفع الإلكتروني الموجود في المحلات التجارية، أي المحلات التي تقبل الدفع بهذه البطاقة بموجب اتفاق مع الجهة المصدرة لها.

استخدام البطاقة في السحب أو الإيداع من الصراف الآلي عن طريق قيام العميل صاحب البطاقة بعمليتين متعاصرتين:

---

[1]- القليوبي **سميحة**، الأوراق التجارية (الكمبيالة، السند لأمر، الشيك، الشيك السياحي، الشيك المسطر، الشيك المعتمد وسائل الدفع الحديثة)، الطبعة الخامسة، دار النهضة العربية، القاهرة، 2006، ص547 وما بعدها.

[2]- **حسين عبد الباسط جميعي**، المرجع السابق، ص35

[3]- أجهزة الصراف الآلي يرمز لها (A.T.M) اختصار لـــ:Automatic Teller Machine، وقد وجدت ماكينات الصرف الآلية في أماكن مختلفة خارج البنوك في المحلات الكبرى والفنادق وشركات الطيران وأصبح للعميل حرية التعامل مع رصيده بالسحب أو الإيداع باستعمال بطاقته من خلال جهاز الصراف الآلي (A.T.M) دون الرجوع للبنك وطوال اليوم دون التقييد بأوقات العمل الرسمية أو غيره. أنظر: **نجوى أبو هيبة**، المرجع السابق، ص90.

إدخال البطاقة التي تحتوي على البيانات الخاصة بالعميل بالوضع الصحيح على فتحة خاصة في جهاز الصراف الآلي (A.T.M).

إدخال الرقم السري[1] المخصص له (الذي يعدّ بمثابة التوقيع)، وذلك بكتابته بواسطة لوحة المفاتيح الموجودة على الجهاز الآلي، فإذا كان الرقم صحيحا فإنّ بيانات الجهاز توجه العميل إلى تحديد المبلغ المراد سحبه أو إيداعه، وذلك بالضغط على مفاتيح خاصة بذلك فيتم صرف المبلغ المطلوب، وتعاد البطاقة للعميل من نفس فتحة البداية.

في حالة استخدام البطاقة لوفاء ثمن المشتريات أو الخدمات فإن التاجر يتولى تمرير البطاقة عبر جهاز خاص يتصل بدوره بنظم المعلومات الخاصة بالبنك، وهذا لقراءة البطاقة فيعلم التاجر جميع البيانات الخاصة بالعميل وحدود التعامل معه قبل إبرام عقد البيع أو تقديم الخدمة له، فتتحدد بذلك حقوق التاجر ومسؤوليته طبقا لقراءة هذه البيانات[2].

فإذا ما قام العميل بإدخال الرقم السري (PIN) الخاص به في الجهاز يتم سداد المستحقات عن طريق التحويل من حساب العميل لدى البنك إلى حساب التاجر لدى نفس البنك أو لدى بنك آخر[3].

يوجد نظامان تعمل عليهما أجهزة الصرف الآلية (A.T.M): الأول يعرف بنظام الدفع غير المباشر (off-line). وفي حالة استخدام ذلك النظام، يقوم جهاز التاجر بتسجيل العملية التي أنجزها العميل على شريط مغناطيسي، ولا يتغير موقفه المالي ويبقى

---

[1]- يطلق على الرقم السري الخاص بالبطاقة باللغة الفرنسية بـــ Numéros d'identification personnel، ويرمز له بالمختصر Nip، وفي الإنجليزية personal identification number، ويرمز له بالمختصر P.I.N أنظر: **سعيد السيد قنديل**، المرجع السابق، ص67.

[2]- **إبراهيم سطم بن خلف العنزي**، التوقيع الإلكتروني وحمايته الجنائية، أطروحة دكتورة الفلسفة في العلوم الأمنية جامعة نايف العربية للعلوم الأمنية، الرياض، 2009، ص ص 51، 64.

[3]- **ثروت عبد الحميد**، المرجع السابق، ص57 .

كما هو حتى يتم نقل هذه الشرائح المغناطيسية إلى الجهة مصدرة البطاقة –البنك- حسب المدة الزمنية المتفق عليها –يوميا أو أسبوعيا-، ليقوم موظف البنك في النهاية بتوثيق هذه العملية عن طريق تسجيلها في الحاسب المركزي التابع للجهة مصدرة البطاقة[1].

بعرف النظام الثاني بنظام الدفع المباشر (on-line)، وهو يقوم فورا وبمجرد انتهاء العميل من العملية بتحديد موقفه المالي[2].

يتميز هذا الشكل من التوقيع الإلكتروني –بالإضافة إلى سهولته وبساطته- بقدر كبير من الأمان والثقة، كما أنّه يتميز بقدرته على تحديد هوية شخص الموقع، فإتباع العميل الإجراءات التي ذكرناها سابقا، يؤكد أن من قام بالعملية المصرفية هو الشخص صاحب الرقم السري[3].

في حالة فقدان البطاقة، أو سرقتها، أو نسيان الرقم السري، يتمّ تجميد كلّ التعاملات التي تتم بواسطتها بمجرد إخبار البنك بذلك، أضف إلى هذا أن عملية السحب يتم إثباتها على ثلاثة أنواع من المخرجات على شريط ورقي موجود خلف جهاز السحب وعلى أسطوانة ممغنطة، كما يتسلم العمل بدوره إيصالا يثبت قيامه بالعملية ويحدد- بالإضافة إلى بيانات أخرى- المبلغ الذي تم سحبه[4].

يعتبر البعض أنّ هذا النوع من التوقيع - التوقيع بالرقم السري- لا يعادل التوقيع الخطي لأن استخدامه لا يقتضي الوجود المادي للشخص الذي ينسب إليه[5]، غير أنّ

---

[1]- **سميحة القليوبي**، المرجع السابق، ص 552.

[2]- أنظر:

GRPZIANO (Sueganske) And Baharoglu (Selma Fatma), Automated Teller Machines: Boon Or Bame? Commercial Law Journal, Vol, 91, N1, 1969, P456

المشار إليه لدى **عيسى غسان عبد الله الربضي**، المرجع السابق، ص60.

[3]- **محمد سعيد أحمد إسماعيل**، أساليب الحماية القانونية لمعاملات التجارة الإلكترونية، منشورات الحلبي الحقوقية الطبعة الأول، 2009، ص 270

[4]- **ثروت عبد الحميد**، المرجع السابق، ص58 .

[5]- **سعيد السيد قنديل**، المرجع السابق، ص 68.

الفقهاء أجمعوا على صلاحيته[1]، لقدرته على تحديد هوية صاحبه وتمتعه بالثقة والأمان وقد فـــند جميع الفقهاء المأخذ السابق وذلك وفقا للآراء التالية:

1: إن الرقم السري مساوي للتوقيع التقليدي من حيث أداء الوظائف، فإتباع العميل للإجراءات المحددة لسحب النقود أو إيداعها أو لدفع ثمن السلع أو الخدمات يشكل إقرارا منه بما يريد من بيانات بالشريط (الورقي أو الممغنط) الناتج عن الجهاز الآلي.

2: إن الحصول على البطاقة الممغنطة –بأي طريقة كانت- لا يعني الوصول للرقم السري، لانفصالهما عن بعضهما، إضافة إلى أن استعمال الرقم السري بطريقة غير مشروعة من قبل الغير مساوي لتزوير التوقيع التقليدي.

3: كل الأجهزة الخاصة بالسحب النقدي أو الدفع مبرمجة على رفض البطاقة بعد المحاولة الثالثة لإدخال الرقم السري، مما يعني تضيق فرصة استعمالها بالطرق غير الشرعية[2].

اعترف القضاء الفرنسي مبكراً بالتوقيع الإلكتروني المتمثل في التوقيع بواسطة الرقم السري المقترن بالبطاقة الممغنطة، كونه محاط بالضمانات نفسها الموجودة في التوقيع التقليدي، واستند في إضفاء الحجية القانونية لهذا التوقيع الإلكتروني على الاتفاقات التي تبرم بين ذوي الشأن والتي تنص على ذلك صراحة.

وهذا ما قامت به محكمة النقض الفرنسية عند اعترافها للتوقيع الإلكتروني الذي يصاحب عملية السحب بحجيته الكاملة في الإثبات، فقد اكتفت بالأدلة التي قدمها البنك من واقع التسجيلات التي يقوم بها جهاز الحاسب الآلي الملحق بجهاز الصرف، وألغت قرار محكمة الموضوع التي استبعدت هذا الدليل لتعارضه مع مبدأ عدم جواز اصطناع

[1]- **عبد الفتاح بيومي حجازي**، النظام القانوني لحماية التجارة الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2002 ص 90.

[2]- **سعيد السيد قنديل**، المرجع السابق، ص69.

الشخص دليلا لنفسه، على اعتبار أن اتفاق الإثبات الموجود بين البنك والعميل يبيح الاستناد إلى التسجيلات الموجودة لدى البنك في إثبات ما يقوم به العميل من معاملات[1].

أيّد الفقه في معظمه حكم محكمة النقض معتبرا أن التوقيع باستخدام الرقم السري لا يصدر عن جهاز الصراف الآلي وإنما من خلاله، فقيام العميل بإدخال البطاقة الممغنطة بفتحة الجهاز الآلي ثم كتابة الرقم السري، يعني أن العميل قد وقع على العملية، بواسطة الجهاز الآلي، فالجهاز يقوم بذات مهمة القلم في التوقيع، بمعنى أنه وسيلة لأداء التوقيع.

ثانيًا: التوقيع بالقلم الإلكتروني *(Pen-Op)*.

من الأشكال الأخرى للتوقيع الإلكتروني التي يمكن استخدامها في توثيق التصرفات القانونية التي يتم إبرامها على الوسائط الإلكترونية، التوقيع باستخدام قلم خاص، يعرف بالقلم الإلكتروني ، وهو عبارة عن قلم إلكتروني حساس يمكنه الكتابة على شاشة الحاسوب عن طريق برنامج معلوماتي يتيح التقاط التوقيع، والتحقق من صحته حيث يتلقى البرنامج المثبت على قاعدة بيانات الحاسوب، بيانات المستخدم عن طريق بطاقة تحقيق هوية إلكترونية خاصة تحتوي على بيانات كاملة عن هذا الشخص[2].

ثم يظهر بعد ذلك بعض التعليمات على شاشة الحاسوب ليتبعها المستخدم حتى تظهر رسالة على الشاشة تطلب من المستخدم كتابة توقيعه باستخدام القلم الإلكتروني داخل مربع يعرض على الشاشة، وعندما يقوم المستخدم بتحريك القلم على الشاشة وكتابة توقيعه، يلتقط البرنامج حركة اليد ويظهر التوقيع مكتوبا على الشاشة بسماته الخاصة من حيث: حجم وشكل الحروف، والمنحنيات والدوائر، والخطوط والنقاط وغيرها من الصفات[3]،إضافة إلى تحديد السرعة النسبية التي يجري بها وضع التوقيع، ثم يظهر

---

[1]- مشار إليه لدى: **إبراهيم الدسوقي أبو الليل**، المرجع السابق، ص158، **سعيد سيد قنديل**، المرجع السابق، ص69. **ثروت عبد الحميد**، المرجع السابق، ص 58.

[2]- **عايض راشد عايض المري**، المرجع السابق، ص 112. **ممدوح محمد علي مبروك**، المرجع السابق، ص14.

[3]- **أبو الليل إبراهيم الدسوقي**، المرجع السابق، ص 161.

للمستخدم ثلاثة مفاتيح الأول للموافقة على شكل هذا التوقيع، والثاني لإعادة المحاولة والثالث لإلغاء التوقيع، وعندما يضغط المستخدم على أيقونة قبول التوقيع يقوم الحاسوب بتجميع جميع البيانات الخاصة بالمستخدم (الموقع) ويدمجها مع شكل التوقيع الموافق عليه ثم يقوم بتشفير جميع هذه البيانات[1] والاحتفاظ بها على نحو يتيح استرجاعها واستخدامها عند الضرورة[2].

وعند حاجة الشخص لتوثيق التصرف القانوني الذي عزم على القيام به يرجع إلى البرنامج الذي تم حفظ التوقيع به، ولكي تتم عملية التوثيق يطلب الحاسب الآلي من الشخص كتابة توقيعه على الشاشة داخل مربع معين، ثم يقوم البرنامج بإجراء مقارنة بين خصائص التوقيع الموجود على الشاشة وتلك الخصائص المحفوظة على قاعدة البيانات فإذا تمت المطابقة بين خصائص التوقيع يصدر الحاسب الآلي تقريرا بالنتيجة التي تمّ التوصل إليها[3].

هناك عقبات ومشاكل تواجه هذا النوع من التوقيع الإلكتروني تحدّ من انتشاره ومن أهم هذه المشاكل أنّه لابدّ لإتمام التوقيع الإلكتروني من وجود حاسب آلي ذي مواصفات خاصة، كاحتوائه على وحدة القلم الإلكتروني والشاشة الحساسة، وهذا لتمكنه من أداء مهمته في التقاط التوقيع من شاشته، والتحقق من مطابقته للتوقيع المحفوظ بذاكرته[4]، إضافة إلى المشكلة السابقة هناك مشكلة أخرى لم تجد طريقا للحل حتى الآن هي مشكلة إثبات العلاقة بين التوقيع والمحرر، حيث لا توجد هناك تقنية تتيح التأكّد من إثبات هذه الرابطة، إذ بإمكان المرسل إليه الاحتفاظ بنسخة من صورة التوقيع التي وصلته

---

[1]- **سمير حامد عبد العزيز الجمال**، المرجع السابق، ص226.

[2]- تتمثل مهمة التشفير هنا في الحفاظ على أمن وسرية التوقيع وحمايته من محاولات المتطفلين والعابثين، لمزيد من التفاصيل أنظر: **عايض راشد عايض المري**، المرجع السابق، ص 112 وما بعدها، وكذا: **نجوى أبو هيبة**، المرجع السابق، ص 71.

[3]- **عيسى غسان عبد الله الربضي**، المرجع السابق، ص 68.

[4]- **أبو الليل إبراهيم الدسوقي**، المرجع السابق 161.

على أحد المحررات، ثم يعيد وضعها على وثيقة محرر عبر وسيط إلكتروني، ويدعي أن واضعها هو صاحب التوقيع الفعلي، وهو ما يخل بشروط الاعتراف بالحجية للتوقيع في الشكل الإلكتروني لانعدام الثقة والأمان في هذه الطريقة.

ثالثًا: التوقيع البيومتري *(LA Signature biométrique)*

تعتبر التكنولوجيا التي تستخدم في توثيق التعاقدات التي تتمّ عبر الوسائط الإلكترونية متغيرة نحو التطور، وبشكل مستمر، ومن التطورات التكنولوجية المبتكرة حديثا في هذا المجال تقنية التوقيع البيومتري[1]، حيث يتم هذا التوقيع بواسطة استخدام الخواص الطبيعية والسلوكية والجسدية للشخص، وذلك لتمييزه وتحديد هويته[2]، نظرا لارتباط هذه الخواص الذاتية به، وهو ما يسمح باستخدامها في إقرار التصرفات القانونية التي تبرم عبر وسيط إلكتروني.

تعتمد هذه الصورة من صور التوقيع الإلكتروني على حقيقة علمية، هي أن لكل شخص صفات ذاتية خاصة به تختلف من شخص إلى أخر تتميز بالثبات النسبي، الذي يجعل لها قدر كبير من الحجية في التوثيق والإثبات.

تتعدّد الصفات الجسدية أو البيومترية التي يعتمد عليها التوقيع البيومتري أهمّها: البصمة الشخصية، بصمة شبكية العين، بصمة الصوت، خواص اليد البشرية، وغير ذلك من طرق أخرى.

تبدأ طريقة تشغيل التوقيع البيومتري بأن يسند لجهة معينة مهمة أخذ صورة دقيقة لصفة ذاتية للشخص الذي يريد استخدام الإمضاء البيومتري وذلك عن طريق تقنية

---

[1]- يسمى هذا بعلم البيومترولوجي (biometriolog) الذي يهتم بدراسة الخواص المميزة لكل إنسان، وهناك من يرى إنها طريقة توفر الثقة والأمن للمعاملات الإلكترونية التي تعتمد هذا النوع من التوقيع، أنظر في ذلك: **حسن عبد الباسط جميعي**، المرجع السابق، ص ص40-41. و**ثروات عبد الحميد**، المرجع السابق، ص ص60-61، **وكذا: سعيد السيد قنديل**، المرجع السابق، ص ص 70-71.

[2]- **إبراهيم الدسوقي أبو الليل**، المرجع السابق، ص 159.

مخصصة لهذه المهمة، وبعد ذلك يتمّ حفظ هذه الصور بطريقة مشفرة في ذاكرة الحاسب الآلي، وعندما يدخل الشخص في تعاقدات عبر وسائط إلكترونية، ويراد التحقق من شخصيته فليس على الجهة المختصة إلاّ التأكيد من مطابقة سماته بالسمات المسجلة والمحفوظة عنه من قبل، وذلك عن طريق استخدام البرنامج الخاص الذي يقوم بإجراء مقارنه بين السمات الذاتية للمتعاقد والتي يلتقطها جهاز الحاسب الآلي وبين السمات المميزة لنفس الشخص والمخزنة من قبل بقاعدة بيانات الجهة المختصة، ليخلص البرنامج إلى تحديد ما إذا كانت سمات الشخص المتعاقد مطابقة لسماته المسجلة من قبل فيكون التوقيع صحيحا، أو غير مطابق فيكون التوقيع غير صحيح[1]، أي أنّه لا يسمح للمتعاقد بالتعامل إلاّ في حالة المطابقة الكاملة[2].

ممّا لا شك فيه أن ارتباط هذه الخصائص والسمات الذاتية بالإنسان يسمح بتميزه عن غيره بشكل موثوق به، ولذلك يمكن استخدام هذه الطريقة في التوقيع على التصرفات القانونية المبرمة عبر الوسائط الإلكترونية[3].

يؤخذ على هذا التوقيع أنه بالرغم من الدقة والأمان والثقة المتوافرة فيه، إلاّ أنّه ليس بعيد عن التزوير، فيمكن أن تخضع الذبذبات الحاملة للصوت أو صورة بصمة الإصبع للنسخ وإعادة الاستعمال بالإضافة إلى إمكانية إدخال تعديلات عليها، كذلك الشأن لبصمة العين، فيمكن تزويرها بتقليدها عن طريق بعض أنواع العدسات اللاصقة المصنوعة من رقائق السليكون والتي تحمل نفس اللون والشكل والخصائص المخزنة على

[1]- **محمد محمد أبو زيد**، المرجع السابق، ص 39.

[2]- **سعيد السيد قنديل**، المرجع السابق، ص 70.

[3]- **حسين عبد الباسط جميعي**، المرجع السابق، ص 41.

الحاسب الآلي[1]، خصوصا إذا أخذنا في الاعتبار سرعة التطور التقني المذهل في عالم الإلكترونيات[2].

يضاف إلي ما سبق أيضا أنّ الخواص أو السمات الجسدية لجسم الإنسان متغيرة مع تقدم السن أو المرض وعوامل أخرى، فقد تمنع الإصابة أو المرض الموقع من إمكانية إجراء مقارنة ومطابقة خواصه وسماته الذاتية التي يلتقطها جهاز الحاسب الآلي، ومن المآخذ الأخرى التي تؤخذ على هذا التوقيع، التكلفة العالية للتقنية التي يتطلبها صنع نظام آمن في شبكات المعلومات باستخدام السمات البيومترية، ممّا أدّى إلي الحدّ من انتشار هذا النوع من التوقيع، وجعله قاصرا على بعض الاستخدامات المحدودة[3].

وفي المقابل يرى جانب من الفقه، أن الخواص الطبيعية المميزة لكل إنسان تستطيع أن تميزه عن غيره، وبالتالي فإن التوقيع البيومتري يعتبر وسيلة موثوق بها لتمييز الشخصي وتحديد هويته، نظرا لارتباط الخصائص الذاتية به، وهو ما يمكن معه استخدام هذه الوسيلة في إقرار المعاملات الإلكترونية[4]، ورغم قابلية هذه الوسائل للتزوير أو التقليد فإن ذلك لا يجب أن ينال منها، لأن التزوير فيها مهما بلغ لن يصل إلي ما وصل إليه التقليد والتزوير في مجال الكتابة التقليدية والتوقيع التقليدي، فكلّ ما هو مطلوب في

---

[1]- من أنه "بالرغم من إدعاء الشركات المصنعة للأجهزة البيومترية أن نسبة الأمان الذي توفره للشبكات تصل إلى 10% إلاّ أنّه تمّ اكتشاف حالات احتيال باستخدام البصمة الشخصية المقلدة (البصمة البلاستيكية والمطاطية)، وعدم استطاعة بعض أجهزة التحقق البصرية المصنوعة من رقائق السليكون من كشفها وتميزها"، أنظر ما أشار إليه:**ثروت عبد الحميد**، المرجع السابق، ص 61 هامش 135.

[2]- **سعيد السيد قنديل**، المرجع السابق، ص 71.

[3]- يقتصر استخدام التقنية حاليا على بعض البنوك العالمية وعلى أجهزة الأمن والمخابرات كوسيلة التحقق من الشخصية وتحديد الاستخدام المرخص لها. أنظر: **نجوى أبو هيبة**، المرجع السابق، ص 69.

[4]- **ثروت عبد الحميد**، المرجع السابق، ص 61.

التوقيع أن يعلم نسبته لصاحبه، كما أن كل وسيلة تقوم بوظيفتي التوقيع، من تعيين صاحبه وتبيان انصراف إرادته نهائيا إلى الالتزام بمضمون ما وقع عليه، تعدّ بمثابة توقيع[1].

ومع هذا نوافق الرأي الفقهي القائل بأن استخدام هذا النوع من التوقيع الإلكتروني - التوقيع البيومتري- يعتمد في المقام الأول على مدى قدرته على توفير الثقة والأمان القانونيين، وعلى مدى قدرة التقنية المستخدمة على منع الغير من التلاعب به أو نسخه أو تزويره.

ويمكن أن يتحقق ذلك عن طريق تأمينه من خلال التصديق عليه من جهات معتمدة، مرخص لها بممارسة هذا العمل، وتخضع لرقابة الدولة، بحيث تكفل التحقق على نحو دقيق من شخصية الموقع والحفاظ على سرية هذا التوقيع، وحمايته، وتوفير وسائل الأمان له مما يضفي عليه مزيدا من الثقة لدى المتعاملين في إبرام التصرفات القانونية عبر الوسائط الإلكترونية، خاصة تلك المعاملات التجارية التي تتم عبر شبكة الاتصال الحديثة الإنترنت[2].

رابعًا: التوقيع بواسطة الماسح الضوئي.

يتم هذا النوع من التوقيع بواسطة استخدام جهاز يطلق عليه (إسكانر)، حيث يقوم الشخص عن طريق هذا الجهاز بنقل التوقيع المحرر بخط اليد إلى المستند المراد إرساله ويتم تذييله بالتوقيع ومن ثم إرساله إلى الطرف الآخر عن طريق الوسيط الإلكتروني.

غير أنّ هذه الطريقة لم تلق رواجاً في الاستعمال بسبب ضعف الثقة في قدرتها على تفادي قيام أيّ شخص بتصوير هذا التوقيع ووضعه على أيّ مستند غريب عن

---

[1]- **نجوى أبو هيبة**، المرجع السابق، ص 70.

[2]- أنظر **سمير حامد عبد العزيز الجمال**، التعاقدات عبر تقنيات الاتصال الحديثة، المرجع السابق، ص 225. **حسن عبد الباسط جميعي**، المرجع السابق، ص 41. **وعبد الفتاح بيومي حجازي**، المرجع السابق، ص 198، و**سعيد السيد قنديل**، المرجع السابق، ص 71.

الموقع نفسه، وبالتالي لا يمكن بواسطتها التحقق على وجه اليقين بوجود صلة قطعية بين التوقيع وصاحبه وما يفيد الالتزام بما هو موقع عليه.

خامسًا: التوقيـــع الرقمـــي.

يعرف التوقيع الرقمي بأنه[1] "**بيان أو معلومة يتصل بمنظومة بيانات أخرى أو صياغة منظومة في صورة شيفرة (كود)، والذي يسمح للمرسل إليه إثبات مصدرها والإستيثاق من سلامة مضمونها، وتأمينها ضد أي تعديل أو تحريف**". وهو صورة أخرى للتوقيع الإلكتروني تستخدم في إبرام التصرفات القانونية عبر الوسائط الإلكترونية[2]، حيث يعتبر الأوسع نطاقا والأكثر استخداما نظرا لطابع الأمان والثقة الذي يوفرهما، لذا حاز على اعتراف وثقة العديد من الدول بشكل عام والشركات والبنوك بشكل خاص، ويعتمد هذا التوقيع على نظام التشفير (CRYPTOLOGIE)[3]، لذا يسمى بالتوقيع الرقمي القائم على التشفير.

لا يمكن فهم التوقيع الرقمي دون التطرق إلى التشفير، إذ أن التوقيع بالمفاتيح العمومية والخصوصية يرتكز على وسائل التشفير كآلية تقنية لحماية التوقيع الإلكتروني[4].

ترتكز طريقة تشغيل منظومة التوقيع الرقمي على فكرة اللوغاريتمات والمعاملات الرياضة المعقدة من الناحية الفنّية، وذلك بتحويل المحرر المكتوب والتوقيع الوارد عليه من نمط الكتابة العادية إلى معادلة رياضية، باستخدام مفاتيح ورموز سرية وطرق حسابية معقدة "لوغاريتمات"، ومؤدى ذلك تحويل المستند الإلكتروني من صورته المقروءة

---

[1]- **وفقا للمواصفات القياسية رقم (ISO 7498–2)** الصادرة عن المنظمة الدولية للمواصفات والمقاييس عام 1988 أنظر الموقع الإلكتروني: www.iso.org

[2]-يطلق على التوقيع الرقمي بالعربية ويسمى أيضا ب "التوقيع الكودي" بالفرنسية: signature numerique وبالانجليزية: Signature Digital

[3]-جاء في المادة الأولى بند (9) من اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري رقم 2004/15م بتنظيم التوقيع الإلكتروني بأن التشفير هو "منظومة تقنية حسابية تستخدم مفاتيح خاصة لمعالجة وتحويل البيانات والمعلومات المقروءة إلكترونيا بحيث تمنع استخلاص هذه البيانات والمعلومات إلا عن طريق استخدام مفتاح أو مفاتيح فك الشفرة".

[4]- سوف نتطرق إلى دراسة التشفير بنوع من التفصيل في الفصل الثاني.

والمفهومة إلى صورة رسالة رقمية غير مقروءة وغير مفهومة، ولا يكون بإمكان أيّ شخص إعادة هذه المعادلة اللوغاريتمية إلى صورتها المقروءة إلا الشخص الذي لديه المعادلة الخاصة بذلك والتي تتمثل في المفتاح، فالشخص المالك لمفتاح التشفير هو الذي يمكنه فقط فك هذا التشفير[1].

ويرى البعض أن تشفير البيانات يعني "**تغيير في شكل البيانات عن طريق تحويلها إلى رموز أو إشارات لحماية هذه البيانات من إطلاع الغير عليها أو من تعديلها أو تغييرها**"[2].

وعرفه البعض الآخر بأنّه "**عملية الحفاظ على سرية المعلومات الثابت منها والمتحرك باستخدام برامج لها القدرة على تحويل وترجمة تلك المعلومات إلى رموز بحيث إذا ما تم الوصول إليها من قبل أشخاص غير مخول لهم بذلك لا يستطيعون فهم أي شيء لأنّ ما يظهر لهم هو خليط من الرموز والأرقام والحروف غير المفهومة**"[3].

هذا و ينقسم التشفير إلى نوعين:

التشفير بالمفتاح المتماثل والتشفير بالمفتاح غير المتماثل-المزدوج- وسوف نتناول هذين النوعين من التشفير على النحو التالي:

1: التشفير بالمفتاح المتماثل.

يسمّى أيضا بالنظام السيمتري[4]، ويتمثل هذا النوع من التشفير باستخدام كل من المرسل والمستقبل نفس المفتاح السري للتشفير، فطريقة تشغيل هذا النظام تعتمد على مفتاح واحد يستخدمه المرسل في عملية تشفير بيانات الرسالة – المحرر الإلكتروني- كما يستخدمه المرسل إليه في عملية فك هذا التشفير، حيث يحرر المرسل الرسالة ثم يقوم بتشفيرها بالمفتاح المتماثل، وذلك بتحويل الرسالة من صورتها المقروءة والمفهومة إلى

[1]- **حسن عبد الباسط جميعي**، المرجع السابق، ص 42. و**ثروت عبد الحميد**، المرجع السابق، ص 62.

[2]- **محمد حسين منصور**، المرجع السابق، ص 180.

[3]- **هدى حامد قشقوش**، المرجع السابق، ص 59.

[4]- أنظر: **نجوى أبو هيبة**، المرجع السابق، ص 72.

صور رسالة رقمية غير مقروءة تتخذ أشكال ورموز وعلامات غير مفهومة، ثم يقوم بإرسال الرسالة وكذلك المفتاح المتماثل الذي شفر به بيانات المحرر الإلكتروني إلى المرسل إليه، ليتمكن هذا الأخير من فك شفرة هذه الرسالة وإعادتها إلى حالتها الأصلية.

تتميّز هذه الطريقة بالبساطة ومن ثمة بالسرعة والسهولة في إجراء التشفير، حيث لا تحتاج إلى حاسب آلي ذو تقنية متطورة أو وقت طويل في فك التشفير، ما يعاب عليهاهو عملية تبادل المفتاح المتماثل بين المرسل والمرسل إليه، فعملية التبادل تشكل خطورة على بيانات المحرر الإلكتروني المرسلة، بالتالي عدم توفر الأمان والثقة في هذا النوع من التشفير وهو ما أدى إلى تراجع استخدامه[1].

هذا ما أوجب اللجوء إلى وسيلة اتصال آمنه يتم من خلالها إبلاغ المرسل إليه مفتاح فك التشفير، لذلك فإن التعامل بالنظام السيمتري-التشفير بالمفتاح المتماثل- مقصور على الأشخاص التي تربطهم علاقة تعارف مسبقة، وأيضا هذا النظام فعال في الشبكات المختلفة[2]، كشبكة الانترانت (INTERANET) وشبكة الإكسترانت[3](EXTRANET).

---

[1]-**SEDAUIAN Valérie**: Preuve et signature Electronique. OP. cit, p.4-5

[2]-Trudel (p) . "LA Signature Electronique" P.1 disponible sur le site: http://www.ayora.qc.ca/tes/trudel.htm

[3]- شبكة الانترانت INTERANET: هي عبارة عن سلسلة من شبكات المعلومات يمتلكها مشروع أو مؤسسة واحدة وهذه الشبكات قد تكون شبكات داخلية محدودة النطاق تتصل بعضها البعض داخل نفس المكان أو تكون شبكات واسعة النطاق تتصل ببعضها البعض في أماكن مختلفة ومتعددة.

=شبكة الإكسترانت EXTRANET: هي شبكة خاصة مملوكة لمنشأة معينة تلتزم بذات البروتوكولات التي تستخدمها شبكة الانترنت في إجراء عملية الاتصال وتبادل البيانات والمعلومات بين المنشأة وموزعيها أو مورديها أو شركائها أو حتى عملائها بصورة آمنة، إذ أن هذه البيانات تتعلق في غالب الأمر بصفقات وعقود ومعاملات تجارية وعروض وكذلك بيانات سرية تخص العملاء وغير ذلك وقد أمعن من خلال استخدام شبكة الإكسترانت إتمام العديد من صفقات التجارة الإلكترونية، أنظر: **قدري عبد الفتاح الشهاوي**، المرجع السابق، ص ص 380-381.

2: التشفير بالمفتاح غير المتماثل.

يعتبر نظام التشفير بالمفتاح غير المتماثل أو كما يسمى أيضا بالنظام الأسيمتري[1]"Asymetriquo" الصورة الحديثة المعمول بها لإجراء التوقيع الرقمي، فهو نظام يعتمد على خلق وإنشاء مفتاحين لكل متعامل أحدهما يسمى بالمفتاح الخاص (Clé Privé)[2]، يكون سريا لدى صاحبه لاستخدامه في التشفير والتوقيع الإلكتروني على المحررات الإلكترونية المرسلة[3]، والمفتاح الآخر يسمى المفتاح العام "Clé Publique"[4]، وهذا المفتاح يكون معروفا للمرسل إليه بحيث يمكن استخدامه لفك التشفير، وللتحقق من شخصية الموقع على المحرر الإلكتروني والتأكد من صحة وسلامة المحرر الإلكتروني[5] وبالتالي فالمفتاح العام يتميز عن المفتاح الخاص كونه معروفا ومتاح إلكترونيا لطرفين أو أكثر، غير أن هذا التمييز الذي يخص المفتاح العام لا يفصله عن المفتاح الخاص لأنهما مترابطان في عملهما، ويكمل كل منهما الآخر، وهذا لوجود رابطة مباشرة بينهما، فإذا أستعمل المفتاح الخاص لتشفير الرسالة، فلا يمكن فك التشفير إلا بالمفتاح العام والعكس صحيح[6]، كما أنه لو عرف أحد المفتاحين فلا يمكن معرفة المفتاح الآخر حسابيا[7].

---

[1]- **SEDALIAN Valérie**, preuve et signature électronique, paris, sur Le site: http://www.juriscom.net/chr2/fr20000509.htm

[2]- يسمى بالانجليزية Private Key ويظل هذا المفتاح سريا لدى صاحبه ويتكون المفتاح الخاص من مجموعة من الأرقام الحسابية يتشكل منها التوقيع الإلكتروني ويخزن عادة المفتاح الخاص في بطاقة ذكية، يتم الوصول إليه عن طريق الرقم الشخصي، أنظر **إبراهيم الدسوقي أبو الليل**، المرجع السابق، ص162 .

[3]- أنظر المادة الأولى البند (11) من اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري.

[4]- يسمى المفتاح العام بالإنجليزية public Key ويتميز هذا المفتاح بعدم سريته وإنما يبلغ إلى المرسل إليه ليتمكن من فك شفرة الرسالة.

[5]- أنظر المادة الأولى البند (12) من اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري.

[6]- **وسيم شفيق الحجار**، الإثبات الإلكتروني، المنشورات الحقوقية، صادر بيروت، 2002، ص190.

[7]- **إيمان مأمون أحمد سليمان**, الجوانب القانونية لعقد التجارة الإلكترونية, رسالة دكتوراه, جامعة المنصورة، 2005-2006، ص 167.

فمن يرغب في التعامل إلكترونيا كالتاجر أو البائع مثلا عندما يعرض سلعته من خلال الانترنت في شكل رسالة بيانات، فإنه يتيح لأي شخص مهتم القيام بقراءة رسالة البيانات عبر الانترنت دون أن يتمكن من إجراء أي تعديل عليها لأنه لا يملك المفتاح الخاص بها، وهو المفتاح الخاص بصاحب الرسالة –البائع-، فإذا وافق المشتري عليها فإنه يقوم بالتوقيع عليها إلكترونيا باستخدام مفتاحه الخاص، وتمريرها من خلال برنامج خاص بالتشفير في الحاسب الآلي ليتم تشفيرها، ثم يعيد رسالة البيانات إلى مصدرها مرفقا بها توقيعه في ملف لا يمكن للتاجر إجراء أي تعديل به لأنّه لا يملك المفتاح الخاص بصاحب التوقيع[1].

حتّى يتمكن البائع من قراءة الرسالة المرسلة إليه يجب عليه أولا فك شفرتها ولا يتم ذلك إلاّ عن طريق المفتاح العام لمرسل الرسالة [2]، والذي يقوم بإرساله إلى مستلم الرسالة، وعن طريق هذا المفتاح العام وباستخدام برنامج التشفير الخاص بالحاسب الآلي يتمكن المرسل إليه -البائع- من فك شفرة الرسالة وتحويلها من صورتها الرقمية إلى صورتها الأصلية المقروءة.

ولا شك أن التوقيع الرقمي على هذا النحو يحقق أعلى درجات الثقة والأمان لدى المتعاقدين به، حيث أنه يضمن تحديد هوية موقعه ويعبر عن إرادته بالارتباط بالتصرف القانوني وقبول مضمونه بصورة واضحة لا لبس فيها، كما أنّه يحافظ على التصرف القانوني بصورته الأولى ويحول دون التعديل أو العبث والتحريف بمحتوياته، فتتوفر فيه

[1]- **ثروت عبد الحميد**، المرجع السابق، ص 63، و: **حسين عبد الباسط جميعي**، المرجع السابق، ص 42.

[2]- في حالة استعمال مفتاح آخر غير المفتاح العام المرسل مع الرسالة لفك شفرة الرسالة، فلن تقرأ الرسالة، وللمرسل أن يقوم بإرسال مفتاحه العام للمرسل إليه عن طريق وسط محايد يتمثل في جهاز أو سلطات التوثيق الإلكتروني. كما يمكن للمرسل أن يرسل مفتاحه العام للمرسل إليه مباشرة دون وساطة جهة التوثيق، **إبراهيم دسوقي أبو الليل**، المرجع السابق، ص163 هامش رقم173.

بذلك الشروط والضمانات التي يتطلبها المشرع في المحررات لكي تصلح لأن تكون دليلا كاملا في الإثبات[1].

لضمان الأمان في عملية التشفير الخاصة بالتوقيع الرقمي، وجدت الحاجة إلى طرف ثالث، يكون محل ثقة طرفي العقد والذي يتمثل في هيئة متخصصة يكون لها سلطة توثيق التوقيع الإلكتروني، يتم تسجيل التوقيع الرقمي لديها بناء على طلب العملاء، كما تمنح هذه الجهات شهادات إلكترونية موثقة تفيد بموجبها صحة توقيع العملاء[2].

اقترح البعض في سبيل تحقيق أقصى درجة من الأمان، أن يمتلك الشخص زوج من المفاتيح الخاصة بدلا من واحد، فإنه في حالة وجود زوج من المفاتيح الخاصة، يقوم الشخص من خلال المفتاح الأول بالتوقيع على الرسالة، ومن خلال المفتاح الثاني يتمّ تشفيرها، فهذا يحقق أقصى درجات الأمان. أمّا إذا كان الشخص لديه مفتاح خاص واحد يجري كلتا العمليتين به– التوقيع والتشفير- فإنّه يسهّل توصل شخص ما إلى ذلك المفتاح الخاص، فيتمكن بذلك من تغيير التوقيع وتعديل الرسالة[3].

[1]- **ثروت عبد الحميد**، المرجع السابق، ص 63، **سمير حامد عبد العزيز الجمال**، المرجع السابق، ص 222.

[2]- **ممدوح علي مبروك**، المرجع السابق، ص 19.

[3]- **ثروت عبد الحميد**، المرجع السابق، ص 65.

الفرع الثاني

مجالات تطبيق التوقيع الإلكتروني

أفرز انتقال مجال التجارة من المجال الواقعي إلى الافتراضي أنماطا جديدة وسلوكيات متعددة غير تقليدية، ومن هذه الإفرازات التي تتعلق ببحثنا نجد الدفع الإلكتروني[1]. حيث أتاحت وسائل الاتصال الحديثة بالتعاون مع مجال المعلوماتية للأشخاص في حالة رغبتهم في إبرام تصرفاتهم الكترونيا، الفرصة لتحديد نوعية السلعة أو الخدمة وشرائها ودفع ثمنها وحتى تسليمها فورا فيما إذا كانت ذات طبيعة غير مادية كما لو كانت من البرامج أو الصور أو الخدمات كالاستشارات الطبية أو القانونية فبواسطة شبكة الإنترنت أصبح بإمكان التاجر عرض وبيع منتجاته، وبإمكان الأشخاص اقتناء حاجاتهم دون أن يتطلب ذلك التقابل المادي للأطراف، وهذه هي ميزة التجارة الإلكترونية، وكما هو معروف، فإنّ إبرام العقد ينتج عنه التزامات على كلا الطرفين فمقابل التزام البائع (التاجر) بتأمين السلعة أو الخدمة المطلوبة للمشتري، فإن هذا الأخير ملزم بدفع الثمن،وبما أن العقد قدتم بوسائط الكترونية،فإن دفع ثمن السلعة غالبا ما يكون

[1]- صدرت العديد من التعاريف للدفع الإلكتروني مسايرةً لأوضاع ومتطلبات التجارة الإلكترونية فنجد القانون النموذجي للتحويلات الدولية للأموال model law oninternational crédit transferts الصادر في عام 1992 عن لجنة الأمم المتحدةuni citral يعرف هذا القانون التحويل المصرفي بأنه: "مجموعة العمليات التي تبدأ بأمر الدفع الصادر عن الآمر بهدف وضع قيمة الحوالة تحت تصرف المستفيد" ويشمل التعريف أي أمر الدفع صادر عن بنك الآمر أو أي بنك وسيط تهدف إلى تنفيذ أمر الدفع الصادر عن الآمر كما عرف الأستاذ " أيمن قديح " الدفع الإلكتروني على أنه: "**عملية تحويل الأموال في الأساس ثمن لسلعة أو خدمة بطريقة رقمية باستخدام أجهزة الكمبيوتر وإرسال البيانات عبر خط تليفوني أو شبكة ما أو أي طريقة لإرسال البيانات**" كما عرف المجلس الاقتصادي الفرنسي الدفع الإلكتروني أنه" **مجموعة التقنيات الإعلامية، المغناطيسية أو الإلكترونية...الخ. تسمح تحويل الأموال دون دعامة ورقية، والتي ينتج عنها علاقة ثلاثية من بين البنك البائع والمستهلك**" أنظر:

TOERING Jean Pierre et BRIAN Français, Des moyens de payements, Edition que sais-je ? , Paris 1999, p3.

بالنقود الرقمية (أو الافتراضية)[1]. أصبح من الممكن دفع ما يترتب على المشتري من ثمن السلع أو الخدمات عن طريق بطاقات الدفع الإلكتروني، فقد استحدثت وسائط الاتصال الحديثة بطاقات دفع تتماشى مع التجارة الإلكترونية، إذ بواسطتها يستطيع المشترى[2] تحويل أو إيداع ثمن السلعة أو الخدمة لرصيد البائع.

تمتاز شبكة "الإنترنت" بالفورية التي وفرت وسيلة دفع فورية تتلاءم مع طبيعة الاتصال السريع مثل: النقود الرقمية، الشيكات الإلكترونية، ووسائل الدفع المصرفية مثل الهاتف المصرفي "بنوك الإنترنت"، حيث يبرز دور التوقيع الإلكتروني، إذ لابد من توفر شكل معين من التوقيع لإتمام عملية الدفع[3].

وعليه لبيان تطبيقات التوقيع الإلكتروني عبر وسائل الاتصال الحديثة ومعرفة إن كان للدفع الإلكتروني سمات مميزة قريبة من سمات الدفع المادي، نتطرق إلى تطبيقات التوقيع الإلكتروني في بطاقات الدفع الإلكتروني **(أولا)**، وتطبيقاته في أنظمة الدفع الإلكترونية الحديثة **(ثانيا)**.

---

[1]- ثار جدل فقهي حول طبيعة النقود الإلكترونية فهل هي أموال تؤدي نفس الوظائف التي تؤديها الأموال وهل تعتبر نوع جديد من الأموال يصاف إلى الأموال النقدية والمكتوبة أم أنها تنتمي إلى وحدات من هذه الأنواع، فالإجابة على هذه التساؤلات ستحدد النظام القانوني الذي ينطبق على النقود الإلكترونية، فإذا كانت تنتمي إلى نوع معين من هذين النوعين انطبق النظام القانوني لهذين النوعين، أما إذا كانت هذه النقود تمثل نوعا جديدا من الأموال، فيجب أن يحكمها نظام قانوني يتماشى وطبيعتها الخاصة أنظر في ذلك، **شريف محمد غنام**، محفظة النقود الإلكترونية، رؤية مستقبلية بحث مقدم في مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، دبي 10 و12 ماي 2003 ص 118. منشور على الموقع: http://slconf.uaeu.ac

Brun (W), les mécanismes De Paiement Sur Internet, Juriscom.net, 20Bernard, 1999, P303.

[2]- **عبد الفتاح بيومي حجازي**، حماية المستهلك عبر شبكة الإنترنت، دار الفكر الجامعي، الإسكندرية، 2006، ص38.

[3]- تحتوي كل أنواع بطاقات الدفع الإلكتروني شرائط ممغنطة توجد عليها بيانات تخص صاحبها، هذه البيانات يتحدد لها رقم سري أثناء ترحليها من الحساب ألآلي إلى هذا الشريط، وهذا الرقم يمثل -كما أسلفنا- توقيعا الكترونيا.

أولا: التوقيع الإلكتروني في بطاقات الدفع الإلكتروني.

تتمثل بطاقات الدفع الإلكتروني في بطاقات الدفع والتي تسمّى عادة ببطاقات الوفاء، وبطاقات السحب الآلي والبطاقات الائتمانية أو المصرفية، سنحاول أن نتناول هذه البطاقات فيما يلي:

1: بطاقات الدفع.

يطلق عليها أيضا اسم بطاقات الوفاء،وهي بطاقات تعتمد على وجود رصيد للعميل لدى البنك المسوق لها في صورة حسابات جارية بغرض مساواة سحوبات للعميل أولا بأول،من هذه البطاقات الزرقاء في فرنسا (la Carte Bleue) وبطاقة الفيزا إلكترونيك (visa Electronique) في مصر والأردن، حيث تسمح هذه البطاقة لحاملها بدفع ثمن السلع والخدمات التي يبتاعها من المحلات التجارية التي تقبل الدفع إلكترونيا ويتم ذلك بتحويل قيمة السلع أو الخدمات من رصيد حاملها (المشتري) إلى رصيد البائع[1]تتم عملية التحويل بإحدى الطريقتين:

أ- الطريقة غير المباشرة (Off-Line):

في هذه الطريقة يستخدم التوقيع الإلكتروني من أجل تحويل ثمن السلع أو الخدمات من رصيد حامل البطاقة (المشتري) إلى رصيد البائع، وبهذه الطريقة يسلم المشتري بطاقته التي تحتوي بيانات خاصة عن حاملها والبنك المسوق لها إلى تاجر والذي بدوره يدون هذه البيانات إضافة لقيمة السلعة أو الخدمة على فاتورة، ثم يوقع المشتري عدة نسخ من هذه الفاتورة، وبعد ذلك ترسل إحداها للجهة المسوقة للبطاقة لتحويل القيمة من رصيد المشتري إلى رصيد البائع[2].

[1]- **عبد الفتاح بيومي حجازي**، النظام القانوني لحماية التجارة الإلكترونية، الكتاب الثاني، الحماية الجنائية لنظام التجارة الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2002، ص113.

[2]- **محمد أمين الرومي**، المرجع السابق، ص 132.

ب - الطريقة المباشرة (On –Line):

في هذه الطريقة يستخدم التوقيع الإلكتروني، حيث يسلم المشتري بطاقته إلى البائع الذي يمرّرها داخل جهاز ألي خاص للتأكد من صحة البيانات الموجودة على البطاقة ومن وجود رصيد للمشتري يكفي لتسديد قيمة السلع أو الخدمات، بعد ذلك يدخل المشتري الرقم الخاص به ليعلن موافقته على إتمام العملية، وقد أسلفنا القول بأن الرقم السري يعدّ أحد أشكال التوقيع الإلكتروني.

بمجرد الانتهاء من هذه الإجراءات يحول البنك المسوق للبطاقة المبلغ المطلوب من رصيد المشتري إلى رصيد البائع، حيث تتمّ العملية مباشرة وكأنّها بمثابة دفع فوري، لذا تعد طريقة (On-Line) من أعلى درجات ضمان الوفاء للتاجر بعكس طريقة (Off-Line) التي تعدّ بمثابة تعهد للتاجر من البنك المسوق للبطاقة بتسديد ثمن السلع أو الخدمات له.

2: بطاقة السحب الآلي.

تعدّ بطاقة السحب الآلي أكثر أنواع البطاقات الإلكترونية شيوعا واستخداما، فهي تسمح لحاملها بسحب مبالغ نقدية من رصيده هو بحد أقصى يتفق عليه في البداية مع البنك المسوق لها، حتى في خارج أوقات الدوام الرسمي والعطل الرسمية، كما تمكّنه من الاستفسار عن رصيده كلما طلب كشف حساب مختصر، وتحويل كل أو جزء من رصيده إلى رصيد أي شخص آخر[1].

يشترط لاستخدام هذا النوع من البطاقات الإلكترونية وجود رصيد لحاملها بالقيمة المطلوبة، فإذا لم يكن له رصيد بالقيمة المطلوبة أو كان له رصيد غير كاف فإنّه لا يستطيع إتمام ما زعم القيام به كون البطاقة ليست بطاقة ائتمان، حيث أنّ البنك المسوق

[1]- **عبد الله أحمد الله غرابية**، حجية التوقيع الإلكتروني في التشريع المعاصر، دار الراية للنشر والتوزيع، الأردن 2009، ص ص 73،83.

لها لا يوفر للعميل تسهيلا ائتمانيا، وإنّما عمله يقتصر على رد النقود الموجودة بحساب العميل بطريقة إلكترونية[1]. كما تمنح هذه البطاقة للعميل حق الدخول إلى آلات الصرف المؤتمنة وإلى الشبكات المرتبطة بها العائدة للمصارف الأخرى، كما يستطيع أيضا إجراء العديد من المعاملات المصرفية النمطية مثل: تحويل الأموال، الإيداع، السحب وتسديد بعض الفواتير، وكانت هذه البطاقة من أوائل البطاقات التي ظهرت وهي منتشرة بشكل كبير في جميع البنوك.

أمّا عن كيفية تطبيق التوقيع الإلكتروني من خلال بطاقة السحب الآلي، فإنّه يتمّ تسليم البنك المسوق لبطاقة السحب الآلي ورقم يتكون من أربع خانات (يفترض أن يكون سريا)، حيث يستخدمه العميل بدلا من التوقيع التقليدي، ولكي تتم العملية المراد إجرائها يجب إتباع عدّة إجراءات متسلسلة، وهي كالأتي:

- إدخال بطاقة السحب الآلي في المكان المخصص لها في جهاز الصراف الآلي[2].

- إدخال الرقم السري الخاص بالبطاقة، إذ يحتوي شريط البطاقة الممغنط مفتاح الرقم السري، وبهذه الخطوة يعبر العميل عن إرادته في إتمام التصرف إذ يعد الرقم السري بمثابة توقيع ولكن بشكل إلكتروني تحديد العملية المصرفية (سحب، إيداع، تحويل من رصيد إلى رصيد آخر...)[3].

3: البطاقات الائتمانية (المصرفية).

تقوم بطاقة الائتمان على القرض الذي يمنحه البنك لحاملها (العميل)، ليسدد به ثمن السلعة أو الخدمة التي اشتراها، ولكن حامل البطاقة لا يحصل على النقود من البنك مباشرة لتسديد المبلغ المطلوب منه، وإنّما بواسطة البطاقة وبإتباع إجراءات محددة يسدد

---

[1]-**FAUSSE-Arnaud,** Op cit, p22.

[2]- هذه الأجهزة يوفرها البنك المسوق للبطاقة في أماكن مختلفة كالأماكن العمومية، الشوارع، الجامعات، المطارات أين يمكن لكل شخص استعماله بكل سهولة.

[3]- **عبد الفتاح بيومي حجازي**، النظام القانوني لحماية التجارة الإلكترونية، المرجع السابق، ص112.

البنك ثمن السلعة أو الخدمة للتاجر مقابل فائدة يتفق عليها مع عميله، وعلى هذا الأخير سداد الثمن.يجب أن يتوفر لدى العميل ما يعرف باسم مدخل الدفع الآمن، وهو نظام تشفير عمله يشبه عمل السيارة المصفحة التي تنقل البيانات، إذ ينقل هذا النظام البيانات الخاصة ببطاقة الائتمان ويكشف هذا النظام عن بيانات البطاقة ويتأكد من صلاحيتها ويحول المبلغ المستحق من رصيد المشتري إلى رصيد البائع بطريقة إلكترونية[1] ويخصص لكل شخص يملك برنامج مدخل الدفع الآمن توقيع رقمي يستخدمه عند الحاجة.

هناك أيضا العديد من بطاقات الدفع الالكتروني التي يمكن من خلالها تطبيق التوقيع الإلكتروني مثل: بطاقة الشيكات، والبطاقة المدفوعة مسبقا مثل: بطاقة الهاتف وبطاقة النقل والبطاقة المدنية (وهي قريبة من بطاقة الائتمان).

ثانيا: التوقيع الإلكتروني في الأنظمة الحديثة للدفع الإلكتروني.

إذا كان تطور التجارة الإلكترونية يرجع إلى التقدم التقني والتكنولوجي في قطاع الاتصالات ومجال المعلوماتية، فإن سبب انتشارها يعود إلى تطور أنظمة الدفع بين المتعاملين فيها الذين يعتمدون على الوسائط الإلكترونية في إتمام تصرفاتهم،إذ تتمتع أنظمة الدفع الإلكتروني بالسرعة والسهولة في تسوية المدفوعات، حيث تعتبر عملية تحويل أثمان السلع أو الخدمات حجر الزاوية في نجاح وتطور التجارة الإلكترونية[2].

ظهرت مؤخرا وسائل مختلفة للدفع الإلكتروني، منها ما يتم بواسطة التحويلات البنكية،فعندما يتخذ المشتري قراره بشراء سلعة أو خدمة يصدر أمرا للبنك الذي يتعامل معه لإجراء عملية تحويل مبلغ معين من رصيده لرصيد البائع، تتطلب هذه الوسيلة وقتا طويلا لإتمام عملية التحويل، وهذا يتناقض مع ميزة التجارة الإلكترونية وهي الفورية،كما

---

[1]- من المواقع التي ظهرت على شبكة الانترنت التي تقدم خدمة مدخل الدفع الأمن موقع أنظر موقعها الإلكتروني: http://www.HyperMart .com.

[2]- **إبراهيم الدسوقي أبو الليل**، الجوانب القانونية للتعاملات عبر وسائل الاتصال الحديثة، دار النهضة العربية، القاهرة 1999، ص 160، وانظر: **محمد أمين الرومي**، المرجع السابق، ص139.

أنها تثقل عاتق المشتري بمصاريف إضافية، لهذا تم البحث عن وسائل أخرى تتمتع- إضافة إلى السرعة في الإنجاز –بقدرة المحافظة على بيانات الوسيلة المستخدمة في الدفع. وهو ما سنتطرق إليه في النقاط التالية:

1/ النقود الرقمية:

يمكن لنا أن نعرف النقود الرقية هي تلك الوسيلة الوحيدة التي يمكن بموجبها الدفع عبر الاتصال المباشر، فوسائل الدفع الأخرى كالتحويلات البنكية والبطاقات البنكية والشيكات الإلكترونية هي وسائل معالجة عبر الاتصال المباشر الدفع بمعنى أن النقود الإلكترونية ترسل قيمتها النقدية عبر شبكة الإنترنت وليس بواسطة نقل البيانات الخاصة بوسيلة الدفع -تحتفظ بطبيعتها-،يكمن الاختلاف فقط في الطريقة المستخدمة،أي يتم الانتقال من الطريقة اليدوية إلى الإلكترونية،وهكذا-من الناحية القانونية-لا يوجد سبيل لإنشاء طريق دفع جديد.

هناك العديد من التسميات للنقود الرقمية، منها النقود الإلكترونية، العملة الإلكترونية، النقود الافتراضية، وكلّها مصطلحات مترادفة تعبر عن مفهوم واحد ونفضل تسميتها بالنقود الرقمية لأنها مؤلفة من سلسلة الوحدات (Bits)[1] الرقمية تنظمها خوارزميات حسابية شديدة التعقيد لمنع تزويرها.

تعدّ النقود الرقمية أكثر أنظمة الدفع الحديثة تماشيا مع التجارة الإلكترونية، لأن طبيعتها اللامادية تسمح بتمريرها عبر قنوات الاتصال كشبكة "الانترنت"، تنقل من المشتري إلى البائع دون أن تمرّ على حساب المشتري بمعنى أنّها تمتاز بالتسليم المباشر من الدافع إلى المتلقي، كما في النقود الورقية التي تصدر عن البنوك المركزية، كما تتمتّع

[1]- **Bits**: هي وحدات إلكترونية تخزن إمّا على كرت البطاقة الذكية أو على ذاكرة الحاسب الآلي للمشتري وهذه الوحدات تمثل قيما مالية مختلفة تستخدم لدفع ثمن السلع أو الخدمات, وفي حال نفاذها يشحنها البنك بناء على رغبة العميل وبالقيمة التي يريدها أنظر: **عيسى غسان ربضي**، المرجع السابق، ص 214.

النقود الرقمية بخاصية تجعلها غير قابلة للتزييف أو السرقة، إذ ليس لها كيان مادي ملموس، فمصدرها إحدى مؤسسات الأموال الرقمية كمؤسسة[1]Pay Pal بالاشتراك مع بنك حقيقي كبنك (Mark Twain Bank).

2/ الشيكات الإلكترونية:

عملت بعض البنوك على ابتكار شكل جديد من الشيكات سميت بالشيكات الإلكترونية[2]، والشيك الإلكتروني عبارة عن:"**بيانات يرسلها المشتري إلي البائع عن طريق البريد الإلكتروني المؤمن والتلكس أو أية وسيلة إلكترونية أخرى، وتتضمن هذه الشيكات ذات البيانات التي يتضمنها الشيك البنكي من اسم المستفيد والبنك المسحوب عليه والمبلغ وتاريخ الصرف وأخيرا اسم وتوقيع الساحب ورقمه المصرفي**"[3]، واستخدام الشيك الإلكتروني كوسيلة دفع يتطلب وجود وسيط (جهة تخليص)، مابين المشتري والتاجر لمراجعة الشيكات الإلكترونية والتحقق من صحة الأرصدة والتوقيعات الإلكترونية.

يلزم لتحرير شيك إلكتروني أن يكون لكلا طرفيه (المستفيد والساحب) حسابات جارية في بنك واحد يقبل التعامل بالشيكات الإلكترونية، إذ يحدد توقيعا إلكترونيا لكلّ من المشتري والبائع يسجلهما في بيانات البنك. فعندما يحدد المشتري (الساحب) السلعة أو الخدمة التي يرغب في شرائها يحرر شيكا إلكترونيا باسم البائع يتضمن ثمنها، ثم يوقعه ويشفره ثم برسله إلكترونيا[4]. وبعد تسلم البائع الشيك وفتح الشفرة والإطلاع على بياناته يتحقق من الساحب والمبلغ، يضع توقيعه على الشيك الإلكتروني ويرسله إلى البنك، حيث يراجع هذا الأخير الشيك ويتحقق من صحة البيانات والأرصدة،فإذا كانت البيانات جميعها

---

[1] -**تعد مؤسسة** (Pay Pal) من أكبر المؤسسات العاملة في مجال تقديم النقود الرقمية، وتقدم هذه المؤسسة للأشخاص والشركات خدمة البريد الإلكتروني لتبادل النقود الرقمية بسرعة وأمان وتكلفة زهيدة، وتعتمد هذه المؤسسة في عملها على البنية التحتية للبنوك التي تنظم الحوالات وبطاقات الدفع.

[2] - أهم البنوك التي أصدرت هذه الشيكات بنك (بوسطن) و(سيتي دينك) والبنك الاحتياطي الأمريكي.

[3] - **عيسى غسان ربضي**، المرجع السابق، ص ص 108، 110.

[4] - في الواقع العملي يمكن تشفير بيانات الشيك والتوقيع معا أو توقيعه دون تشفير البيانات.

صحيحة، يحول قيمة الشيك من رصيد المشتري (الساحب) إلى رصيد البائع (المستفيد) وأخيرا يخطر الطرفين بإتمام العملية المصرفية.

3/ الدفع عبر الوسائط الإلكترونية المصرفية:

لم تتوقف وسائل الدفع الإلكتروني التي أفرزها التقدم التقني عند الوسائل المذكورة أعلاه، فقد أوجد التقدم التقني وسائل دفع إلكترونية أخرى تخدم التجارة الإلكترونية وتساعد على انتشارها وتطورها، من هذه الوسائل نذكر ما يلي:

أ-**الهاتف المصرفي**: توجد عدة طرق للدفع الإلكتروني عبر الهاتف المصرفي، الطريقة الأولى هي اتصال العميل مباشرة مع البنك الذي يتعامل معه، فبعد أن يتأكد البنك من هوية المتصل عن طريق رقم حسابه أو رقم بطاقته الإلكترونية يعمل على إتمام العملية المطلوبة[1].

أمّا الطريقة الثانية فتتمثل في إرسال العميل رسالة قصيرة (SMS) إلى البنك الذي يتعامل معه، محتوية بعض البيانات الخاصة بالعميل والمبلغ المراد تحويله.

الطريقة التي يطبق فيها التوقيع الإلكتروني هي الهاتف المصرفي، حيث عند تعاقد العميل مع البنك الذي يتعامل معه على تقديم خدمة الدفع عبر الهاتف يخصص له توقيعا على شكل رقم يستخدمه عند الحاجة إليه، أو بواسطة رقمه الخاص بالبطاقة الإلكترونية أو عن طريق توقيعه الرقمي الخاص بالشيكات الإلكترونية أو النقود الرقمية[2].

---

[1]- **عيسى غسان ربضي**، المرجع السابق، ص ص106-110.

[2]- شرعت مؤسسة بريد الجزائر بداية جويلية2011 في إنشاء مؤسسة "المتعامل الافتراضي للهاتف النقال"، حيث ستعمل على شراء مبلغ مالي كبير من المكالمات الهاتفية من شركة "**موبيليس**" كتجربة أولية، يتم تعبئتها في بطاقات خاصة بالاسم التجاري لمؤسسة بريد الجزائر بما يمكن أزيد من 13 مليون زبون من الإطلاع على كشف رصيد حسابه الجاري وإجراء تحويل الأموال عبر النقال وفي هذا السياق، كشف المدير العام لمؤسسة بريد الجزائر **عمر زرارقة** في تصريح لـــ"**الشروق**"، أن هذه الخطوة تندرج ضمن إستراتيجية التنويع الرامية إلى ضمان الجودة والسرعة وآنية الخدمة لزبائن بريد الجزائر، مؤكدا على أن "المتعامل الافتراضي للهاتف النقال" سيتم الشروع في تطبيقه مع مؤسسة "موبيليس" في جويلية المقبل، قبل أن يتم تعميمه مع متعاملي الهاتف النقال "**جازي ونجمة**"، حيث سيتم شراء مبلغ مالي كبير من

ب/ الانترنت المصرفي: شجع اتساع شبكة الانترنت البنوك على توفير وسيلة الدفع الإلكتروني المباشرة للعميل إذ شيدت بعض البنوك مقرات لها شبكة الانترنت تمكن العميل من الدخول إليها ودفع ثمن السلع أو الخدمات مباشرة دون الرجوع إلى موظف البنك أو الاستعانة بوسائل الدفع الإلكتروني الأخرى، وتتمّ عملية الدفع مباشرة وفورا بواسطة رقم حساب خاص بالعميل إضافة إلى التوقيع بشكل سري.

يعتبر القانون رقم 03-15 المتضمن الموافقة في الأمر 03-11 المتعلق بالنقد والقرض[1] أول قانون جزائري تضمن التعامل لإلكتروني الحديث في القطاع المصرفي ويتضح ذلك من خلال المادة 69 التي تتضمن نصها "**تعتبر وسائل الدفع كل الأدوات التي تمكن كل شخص من تحويل أموال مهما يكون السند أو الأسلوب التقني المستعمل**" ويتبين من خلال هذا النص رغبة المشرع الجزائري الانتقال من وسائل الدفع الكلاسيكية إلى وسائل الدفع الإلكترونية، وبعد ذلك صدر الأمر 05-06 المؤرخ بتاريخ 32 أوت 2005 المتعلق

=المكالمات الهاتفية، وسيتم تعبئته في بطاقات تحمل الاسم التجاري لبريد الجزائر، وهذه العملية ستمكن حسب محدثنا أزيد من 13 مليون زبون من استعمالها في المكالمات الهاتفية، وفي العمليات المصرفية على غرار معرفة الرصيد طلب كشف الحساب الجاري وتحويل الأموال من حساب إلى حساب عبر الهاتف، أي دون التنقل إلى مراكز ومكاتب البريد، وهو ما سيجنّب الاكتظاظ التي تشهدها مختلف النقاط التابعة لمؤسسة "بريد الجزائر" بالإضافة إلى المساهمة في حل مشكلة السيولة. وكشف زرارقة "عن تهيئة" مكاتب البريد بتصميم حديث ورد الاعتبار لها لاستقبال الزبائن، تماشيا مع روح التنافس الذي تفرضه السوق والتحكم في مجالات النشاط باستحداث مؤسسات فرعية تحوّل مؤسسة البريد إلى مجمع يضم 3 مؤسسات قريبا، حيث سيتم إنشاء مؤسستين جديدتين وهما مؤسسة "البريد الهجين" ومؤسسة المتعامل الافتراضي للهاتف النقال، إلى جانب مؤسسة البريد السريع "البطل"، التي تم استحداثها في الفاتح من الشهر الجاري والتي ستسمح لبريد الجزائر بمنافسة الشركات الكبرى المختصة في هذا المجال على غرار شركة "دياشال"، "يو بي أس" إلى جانب الشركة الأمريكية "فيدكس". وفي مواجهة العجز المسجل في السيولة النقدية عبر كامل الولايات، كشف محدثنا عن موافقة وزارة الدفاع الوطني، على تغيير موعد ضخ أجور مستخدميها، من 22 إلى 18 من كل شهر، بعد أن كانت العملية قد دخلت حيز التنفيذ بالنسبة للصندوق الوطني للمتقاعدين في النواحي التسع إلى جانب موظفي قطاع الاكتظاظ. جريدة الشروق الاثنين 30 ماي 2011 /الموافق ل27 جمادي الثانية 1432هـ / العدد 3309 أنظر الموقع الالكتروني: www.alchourouk.com

[1]- **أمر رقم 03-11**، المؤرخ في 26 أوت سنة 2003 المتعلق بالنقد والقرض، ج ر عدد 52 لـــ 2003/08/27 والذي ألغى الأمر 90- 10 المؤرخ في 14 أفريل 1990، المعدل والمتمم والملغى، والذي تمت الموافقة عليه بالأمر03- المؤرخ في 25 أكتوبر 2003، ج ر عدد 2003/64.

بمكافحة التهريب[1]، بذلك انتقل المشرع السند أو الأسلوب التقليدي الوارد في نص المادة 69 إلى مصطلح أكثر دقة يتمثل في وسائل الدفع الإلكتروني الوارد في النص 03 من الأمر المذكور.

وبموجب القانون رقم 05-02 المؤرخ في 06 فيفري 2005[2]، أضافت فقرة ثالثة للمادة 414 في وفاء بالسفتجة نص على أنّه: "... **يمكن أن يتم التقديم أيضا بأية وسيلة تبادل إلكترونية محددة في التشريع والتنظيم المعمول بهما**" ولقد تم إضافة نفس هذه الفقرة إلى المادة 502 بمناسبة تقديم الشيك للوفاء كما أضاف المشرع بموجب القانون 05-02 من القانون التجاري والمعنون بالسندات التجارية، الفصل الثالث منه يتضمن بطاقات السحب والدفع وذلك في المادة 543 مكرر 23، أما عن الطبيعة القانونية لهذه البطاقات، فقد اعتبرها المشرع الجزائري أوراق تجارية جديدة إضافة إلى الأوراق التجارية الكلاسيكية وهي السفتجة والشيك والسند لأمر.

يتّضح ممّا تقدم, أن المشرع الجزائري استحدث نظام الوفاء الإلكتروني في المعاملات التجارية لمفهومه الواسع، ويتضح ذلك من خلال نص المادة 69 من قانون النقد والقرض وذلك من خلال عبارة "**... مهما يكن السند أو الأسلوب التقني المستعمل**".

[1]- **أمر05-06**، المؤرخ في 2005/08/23، المتعلق بمكافحة التهريب، ج ر عدد 59.

[2]- **أمر 05-02**، المعدل والمتمم للأمر 75-59 لـــ 26 سبتمبر 1975 المتضمن القانون التجاري ج رعدد11.

ثالثًا: المعاملات المستثناة من تطبيق التوقيع الإلكتروني.

استثنت بعض القوانين تطبيق الوسائل الإلكترونية والتي من بينها التوقيع الإلكتروني على بعض المعاملات بسبب الطبيعة الخاصة التي يتميز بها،التي تقضى بعدم خضوعها للتوقيع الإلكتروني[1] لذا لا يجوز أن تتم بوسائل إلكترونية، وهذا ما أكّدته نصوص القوانين التي حددت هذه المعاملات، وتتعلق هذه المعاملات إجمالا بما يلي:

أ- الأمور المتعلقة بالأحوال الشخصية: كالزواج والطلاق والوصايا.

ب- سندات ملكية الأموال غير المنقولة والسندات القابلة للتداول والمعاملات المتعلقة ببيع وشراء الأموال غير المنقولة وأي مستند يتطلب القانون المصادقة عليه أمام القضاء.

فعلى الصعيد العربي وعلى سبيل المثال نجد المادة (6) من قانون المعاملات الإلكترونية الأردني رقم 2001/85 تنص: "لا تسري أحكام هذا القانون على ما يلي:

- العقود والمستندات والوثائق التي تنظم وفقا لتشريعات خاصة بشكل معين أو تتم بإجراءات محددة ومنها:

- إنشاء الوصية وتعديلها.

- إنشاء الوقف وتعديل شروطه.

- معاملات التصرف بالأموال غير المنقولة بما في ذلك الوكالات المتعلقة بها وسندات ملكيتها وإنشاء الحقوق العينية عليها باستثناء عقود الإيجار الخاصة بهذه الأموال.

- الوكالات والمعاملات المتعلقة بالأحوال الشخصية.

- الإشعارات المتعلقة بإلغاء أو فسخ عقود خدمات المياه والكهرباء والتأمين الصحي والتأمين على الحياة.

[1]- **عبد الفتاح بيومي حجازي**: مقدمة في التجارة الإلكترونية العربية، (الكتاب الثاني)، دار الفكر الجامعي، الإسكندرية 2004، ص 131.

-لوائح الدعاوى والمرافعات وإشعارات التبليغ القضائية وقرارات المحاكم.

- الأوراق المالية إلاّ ما تنص عليه تعليمات خاصة تصدر عن الجهات المختصة استنادا لقانون الأوراق المالية النافذ المفعول.

نص قانون دبي المتعلق بالمعاملات والتجارة الإلكترونية رقم 2 لسنة 2000 في مادته الخامسة على ما يلي: "**يسري هذا القانون على السجلات والتواقيع الإلكترونية ذات العلاقة بالمعاملات والتجارة الإلكترونية ويستثني:**

أ- المعاملات والأمور المتعلقة بالأحوال الشخصية كالزواج والطلاق والوصايا.

ب- سندات ملكية الأموال غير المنقولة.

ج- السندات القابلة للتداول.

د- المعاملات التي تتعلق ببيع وشراء الأموال غير المنقولة والتصرف فيها وتأجيرها".

أمّا بالنسبة للتشريعات الأجنبية نجد المادة 3/ب/1 من القانون الأمريكي الموحد للتجارة الأمريكية ينص:" **هذا القانون لا ينطبق على معاملة من المعاملات بقدر ما يخضع تنظيمها لقانون يحكم إنشاء وتنفيذ الوصايا أو ملاحقها أو الإئتمانات الإيصالية".**

أمّا التوجيه الأوربي الصادر في 8 يوليو 2000 فقد قرر أنّه: "**لا ينطبق هذا التوجيه على العقود المنشئة أو الناقلة لحقوق الملكية العقارية فيما عدا حقوق الإيجار والعقود التي تتطلب تدخلا من المحاكم والسلطة العامة وعقود الكفالة والعقود التي يحكمها قانون الأسرة أو قانون الميراث مثل عقود الوصية والهبة والزواج وإشهار الطلاق والتبني**"[1].

نخلص إلى أنّه نظرا للأهمية الكبيرة التي تتسم بها هذه المعاملات من الناحية الشرعية وبالخطورة من الناحية العملية، فقد عنيت بعض التشريعات العربية والأجنبية باستثنائها من مجال تطبيق قوانين المعاملات الإلكترونية وهذا خلافا للتشريع الفرنسي

[1]- **سعداوي سليم**، عقود التجارة الإلكترونية، دراسة مقارنة، دار الخلدونية للنشر، الجزائر، 2008، ص63.

الذي أقر باعتماد الكتابة الإلكترونية في التصرفات القانونية التي يشترط فيها الشكلية كالبيوع العقارية (بيع الأرض) والسيارة.

المطلب الثاني

القوة الثبوتية للتوقيع الإلكتروني

لا تعدّ 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 المعد أصلا للإثبات، وهو شرط أساسي لصحة الوثيقة سواء كانت إلكترونية أو ورقية، وعليه فإنّ العنصر الثاني الذي به يكون الإثبات الإلكتروني تاما والذي يحدد هوية الشخص ويعبر عن قبوله للالتزامات الواردة في المحرر الإلكتروني هو التوقيع الإلكتروني، لذا كان لزاما وضع القواعد التي تكفل قبوله وتضمن حجيته وقوته القانونية في الإثبات، ولهذا السبب رصدت التشريعات التي نظمت الإثبات الإلكتروني للتوقيع الإلكتروني بعداً قانونيا يعادل بقوته الحجية المقررة للتوقيع التقليدي ويساويه به، وذلك بما يتفق مع مقتضيات التجارة الإلكترونية.

سوف نتناول شروط حجية التوقيع الإلكتروني **(الفرع الأول)**، ولبيان هذه الحجية نعرض نصوص التشريعات المختلفة التي نظمت الإثبات الإلكتروني والتي أقرت بحجية التوقيع الإلكتروني وساوت بينه وبين التوقيع التقليدي **(الفرع الثاني)**.

الفرع الأول

شروط حجية التوقيع الإلكتروني

لا تعتبر الحجية المقررة للتوقيع الإلكتروني التي أضفتها عليه التشريعات المختلفة التي نظمت الإثبات الإلكتروني مطلقة، وإنما معلقة على توافر متطلبات وشروط معينة فلكي يتمتع التوقيع الإلكتروني بذات الحجية المقررة للتوقيع التقليدي في أحكام قانون الإثبات، يجب أن تتوافر فيه الشروط القانونية والضوابط الفنية والتقنية، التي تجعله توقيعا موثوقا به، أو معززا، أو محميا، أو جديرا بالتعويل عليه، كما عبرت التشريعات المختلفة على ذلك.

اشترطت المادة (1316-4) من القانون المدني الفرنسي، أن يتم التوقيع الإلكتروني باستخدام وسيلة آمنة لتحديد هوية الموقع وضمان صلته بالتصرف الذي وقع عليه[1].

نصت المادة (14) من قانون التوقيع الإلكتروني المصري على أنّه: "**للتوقيع الإلكتروني في نطاق المعاملات التجارية والمدنية 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 نصّت المادة (18) من نفس القانون على أنّه: "**يتمتع التوقيع الإلكتروني والكتابة الإلكترونية والمحررات الإلكترونية بالحجية في الإثبات إذا ما توفرت فيها الشروط التالية:**

[1] ارتباط التوقيع الإلكتروني بالموقع وحده دون غيره.

[2] سيطرة الموقع وحده دون غيره على الوسيط الإلكتروني.

[3] إمكانية كشف أي تعديل أو تبديل في بيانات المحرر الإلكتروني أو التوقيع الإلكتروني.

وتحدد اللائحة التنفيذية لهذا القانون الضوابط الفنية والتقنية اللازمة لذلك"[1].

[1]- أنظر المادة الثانية من المرسوم الفرنسي رقم 272 الصادر في 30 مارس 2001.

يتضح من هذه النصوص أنه يجب أن يتوافر في التوقيع الإلكتروني شروط ثلاثة حتى يتمتع بالحجية في الإثبات وهي:

1) ارتباط التوقيع الإلكتروني بالموقع وحده دون غيره.

2) سيطرة الموقع وحده دون غيره على الوسيط الإلكتروني.

3) إمكانية كشف أي تعديل أو تبديل في بيانات المحرر الإلكتروني أو التوقيع الإلكتروني.

أولاً: ارتباط التوقيع الإلكتروني بالموقع وحده دون غيره.

هو شرط بديهي يفرضه الدور أو الوظيفة التي يقوم بها التوقيع، فقد سبق أن رأينا أن التوقيع – إلكترونيا أو تقليديا – ما هو إلا وسيلة لتحديد هوية الموقع الذي يسند إليه الدليل أو المستند، والتعبير عن إرادته في الالتزام بما وقع عليه. من ثم يجب أن يكون للتوقيع طابعا مميزا ومنفرداً يسمح بتحديد شخصية الموقع وهويته، فقد استلزمت المادة (4/1316) من القانون المدني الفرنسي لحجية التوقيع، أن يتم باستخدام وسيلة آمنة لتحديد هوية الموقع وضمان صلته بالتصرف الذي وقعه. كما أفصحت المادة (1/ج) من قانون التوقيع الإلكتروني المصري رقم 15 لسنة 2004 عن حقيقة التوقيع الإلكتروني بأنّه يكون له طابع متفرد يسمح بتحديد شخص الموقع ويميزه عن غيره.

إذا ما تفحصنا التوقيع الإلكتروني، وجدناه يقوم بذلك في شكل رموز أو أرقام أو حروف أو أية إشارة تدل على شخصية الموقع وتميزه عن غيره، فشخصية الموقع تعد

[1]- انظر المادة (3/6) من قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية 2001، والمادة (2/2) من التوجيه الأوربي رقم 1999/93، وكذا المادتين (10) و (31) من قانون المعاملات الإلكترونية الأردني رقم 85 لسنة 2008 المادتين (10) و (20) من قانون المعاملات والتجارة الإلكترونية لإمارة دبي العربية رقم 2 لسنة 2002، المادة 323 مكرر 1 من القانون المدني الجزائري.

مضمونة بمجرد وجود التوقيع الإلكتروني، وهذا في الحقيقة هو الهدف من اعتماد التوقيع الإلكتروني[1]، كما وضحته المواد السابقة الذكر.

كي يرتبط التوقيع الإلكتروني بالموقع وحده دون غيره، يجب أن يعبر عن إرادة الموقع في الالتزام بالتصرف القانوني الذي يتضمنه المحرر الإلكتروني ويدلّ على رضائه به وإقراره له[2]، ويستفاد رضا الموقع وقبوله الالتزام بمجرد وضع توقيعه بالشكل الإلكتروني على البيانات التي يحتويها المحرر الإلكتروني[3].

فحين يأخذ التوقيع الإلكتروني شكل أرقام سرية أو رموز محددة، وتكون محفوظة لدى صاحبها ولا يعلمها غيره، فإذا استخدمت هذه الأرقام أو الرموز للتوقيع من طرف صاحبها، فإن مجرد توقيعه هذا يدل على موافقته على البيانات التي وقع عليها ورغبته الالتزام بها.

وعليه فإنّ التوقيع بالرقم السري المقترن بالبطاقة الإلكترونية والتوقيع القائم على التشفير يحققان هاتين الوظيفتين، فمثلاً بواسطة المفتاح العام العائد للمرسل يستطيع المرسل إليه التحقق من هوية الشخص الموقع وذلك بالرجوع إلى شهادة التصديق الإلكترونية المبعوثة مع المحرّرات الإلكترونية، أمّا عن نية التعبير عن الرضا بالالتزام بمحتوى المحرر الإلكتروني فتتحقق من خلال استخدام الموقع مفتاحه الخاص، فعندما يقوم هذا الأخير بتفعيل بيانات إنشاء التوقيع تتجه إرادته إلى الالتزام بما وقع عليه.

هذا وقد نص المشرع المصري في المادة (9) من اللائحة التنفيذية لقانون التوقيع الإلكتروني على أن ارتباط التوقيع الإلكتروني بالموقع وحده دون غيره يتحقق من الناحية الفنية والتقنية إذا توافرت الشروط التالية:

---

[1]- **نجوى أبو هيبة**، المرجع السابق، ص107

[2]- **ممدوح محمد علي مبروك**، المرجع السابق، ص140.

[3]- **نجوى أبو هيبة**، المرجع نفسه ، ص111.

أ/ استناد التوقيع إلى منظومة تكون بيانات إنشاء التوقيع الإلكتروني مؤمنة على النحو الوارد في المواد 4.3.2 من اللائحة التنفيذية.

ب/ توافر إحدى الحالتين:

1) أن يكون التوقيع الإلكتروني مرتبطا بشهادة تصديق إلكتروني معتمدة ونافذة المفعول صادرة من جهة تصديق إلكتروني مرخص لها ومعتمدة.

2) أن تقوم هيئة تنمية صناعة تكنولوجيا المعلومات بفحص التوقيع الإلكتروني من خلال التحقق من إمكانية تحديد مضمون المحرر الإلكتروني الموقع بدقة.

سهولة العلم بشخص الموقع، سواء في حالة استخدام اسمه الأصلي أم استخدامه لاسم مستعار أم اسم شهرة.

سلامة شهادة التصديق الإلكتروني، وتوافقها مع بيانات إنشاء التوقيع الإلكتروني إن وجدت.

فإذا ما تمّ التحقق من هذه العناصر أصدرت الهيئة شهادة فحص التوقيع الإلكتروني، سواء قامت الهيئة نفسها بأداء هذه الخدمة أو عهدت للغير بتقديم هذه الخدمة تحت إشرافها[1].

ثانيًا: سيطرة الموقع وحده دون غيره على الوسيط الإلكتروني.

يشترط لتمتع التوقيع الإلكتروني بالحجية في الإثبات أن يسيطر الموقع وحده دون غيره على الوسيط الإلكتروني[2]، أي أن يتم إنشاء التوقيع الإلكتروني بواسطة أدوات تكون خاصة بالشخص الموقع، وأن تكون خاضعة لسيطرته وحده دون غيره.

[1]- أنظر المادة (7) من اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري.

[2]- أنظر المادة (18/ب) من قانون التوقيع الإلكتروني المصري، المادة (31/ج) من قانون المعاملات الإلكترونية الأردني، المادة (1/20) من قانون المعاملات والتجارة الإلكترونية لإمارة دبي، المادة (3/2) من التوجيه الأوربي.

يقصد بالموقع الشخص الحائز على بيانات إنشاء التوقيع، ويوقع عن نفسه أو عن من يمثله قانونا[1]، كما يقصد بالوسيط الإلكتروني أداة أو أدوات أو أنظمة إنشاء التوقيع الإلكتروني[2].

أمّا إذا فقد الموقع سيطرته على الوسيط الإلكتروني وأصبحت بيانات إنشاء التوقيع الإلكتروني غير سرية، بحيث يعلمها أشخاص آخرون غير الموقع فإن التوقيع الإلكتروني لا يعتبر حجة في الإثبات، لأنّ تميز هوية الموقع وتحديد شخصيته بالرجوع إلى هذا التوقيع يكون مشكوك فيه[3]. توافر هذا الشرط – سيطرة الموقع وحده دون غيره على الوسيط الإلكتروني- يحول دون تنصل الموقع من توقيعه وما يترتب عليه من آثار بحجة عدم سيطرته وحده على الوسائل الخاصة بإنشاء التوقيع.

تتحقّق من الناحية الفنّية والتقنية سيطرة الموقع وحده دون غيره على الوسيط الإلكتروني من خلال إسناد أدوات أو منظومة إنشاء التوقيع الإلكتروني إلى تقنية شفرة المفتاحين العام والخاص، وأن يحوز الموقع على أداة حفظ المفتاح الشفري الخاص متمثلة في البطاقة الذكية المؤمنة والكود السري المقترن بها[4].

ويحصل العميل الموقع على المفتاحين العام والخاص من جهة التصديق الإلكتروني التي تتولى عادة عملية إصدار هذه المفاتيح بناء على طلب العميل، وبحيازة العميل أيضاً على أداة حفظ المفتاح الشفري الخاص، وهي البطاقة الذكية التي يخزن عليها المفتاح الشفري الخاص وكلمة السر المقترن بها، فإنه يكون مسيطرا على الوسيط الإلكتروني وبتحقق هذا الشرط يعتد بالتوقيع الإلكتروني وتكون له حجية في الإثبات.

---

[1]- المادة (2/د) من قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية 2001، المادة (16/2) من قانون المعاملات والتجارة الإلكترونية لإمارة دبي العربية.

[2]- أنظر المادة (1/د) من قانون التوقيع الإلكتروني المصري، المادة (11/2) من قانون المعاملات الإلكترونية الأردني المادة (18/2) من قانون المعاملات والتجارة الإلكترونية لإمارة دبي العربية.

[3]- **ممدوح محمد علي مبروك**، المرجع السابق، ص 164.

[4]- أنظر المادة (3) والمادة (10) من اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري، رقم 2004/15.

ثالثاً: إمكانية كشف أي تعديل أو تبديل في بيانات المحرر الإلكتروني أو التوقيع الإلكتروني.

يعدّ هذا الشرط على قدر كبير من الأهمية، إذ لا يكفي التحقق من صحة وسلامة إجراءات التوقيع من خلال التأكد من هوية الموقع، وموافقته على مضمون المحرر الإلكتروني الذي وقعه فقط، بل يجب أيضاً التحقق من أن التوقيع لم يتعرض لأيّ تلاعب أو تعديل أو تبديل، وهو الأمر الذي لا يمكن معرفته إلا إذا كان البرنامج المستخدم يسمح بكشف مثل هذا التعديل أو التبديل، والذي قد يمس التوقيع ذاته أو قد يكون في محتوى الرسالة الإلكترونية الموقعة، ويفقد التوقيع في كلتا الحالتين قيمته القانونية ولا يحتج به[1] فتمتع التوقيع الإلكتروني بالحجية في الإثبات يرتبط ارتباطاً وثيقا بدرجة الأمان والثقة التي يوفرها التوقيع الإلكتروني لدى المتعاملين به خاصة في مجال التجارة الإلكترونية فأساس هذه التجارة هو الثقة والائتمان المتبادل بين أطرافها.

يلزم لتحقق الثقة والأمان في التوقيع الإلكتروني أن يتم كتابة المحرر الإلكتروني والتوقيع عليه باستخدام دعائم أو وسائل ونظم من شأنها أن تحافظ على صحة المحرر الإلكتروني المشتمل على التوقيع، وتضمن سلامته وتؤدي إلى كشف، أي تعديل أو تبديل في بيانات المحرر الإلكتروني أو التوقيع الإلكتروني.

هذا وقد نصت المادة (11) من اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري رقم 15 لسنة 2004 على أنّه "**مع عدم الإخلال بما هو منصوص عليه في المواد (2، 3، 4) من هذه اللائحة يتم من الناحية الفنية والتقنية كشف أي تعديل أو تبديل في بيانات المحرر الإلكتروني الموقع إلكترونيا، باستخدام تقنية شفرة المفاتيح العام والخاص، وبمضاهاة شهادة التصديق الإلكتروني وبيانات إنشاء التوقيع بأصل هذه الشهادة وتلك البيانات أو بأي وسيلة مشابهة**".

[1]- **محمد المرسي زهرة**، المرجع السابق، ص260.

يتّضح من خلال نص هذه المادة أنّه يتمّ من الناحية الفنية أو التقنية كشف أيّ تعديل أو تبديل قد يحصل في التوقيع الإلكتروني أو المحرر الإلكتروني عن طريق استخدام تقنية شفرة المفتاحين العام والخاص، أو عن طريق الاستعانة بسلطة التصديق الإلكتروني وشهادة التصديق التي تصدرها، أو بأية وسيلة مشابهة.

نخصّ ممّا سبق أنّه إذا ما توافرت الشروط السابق بيانها في التوقيع الإلكتروني فإنه يتمتع بالحجية الكاملة في الإثبات أمام القضاء في نطاق المعاملات المدنية والتجارية.

الفرع الثاني

حجية التوقيع الإلكتروني وفقا للتشريعات المنظمة للإثبات الإلكتروني

تكتسي الحجية القانونية للتوقيع الالكتروني أهمية بالغة في الإثبات الالكتروني وبالتالي في حماية حقوق المتعاملين عبر الوسائط الالكترونية، لذلك كانت محل اهتمام المشرعين سواءا على الصعيد الدولي أو الوطني.

أولاً: الاعتراف التشريعي بحجية التوقيع الالكتروني في التشريعات الدولية.

حظي التوقيع الإلكتروني باهتمام دولي كبير فمنحت له مختلف التشريعات الحجية القانونية في الإثبات، نتطرق لهذا الموضوع فيما يلي:

***1*: منح التوقيع الالكتروني الحجية في الإثبات وفقا لقوانين اليونسيترال.**

تنص المادة (1/6) من قانون اليونسيترال بشأن التوقيعات الإلكترونية على أنه **"عندما يشترط القانون وجود توقيع من شخص، يعدّ ذلك الشرط مستوفيا في رسالة البيانات إذا أستخدم توقيع إلكتروني موثوقا به بالقدر المناسب للغرض الذي أنشئت أو أبلغت من أجله رسالة البيانات، في ضوء كل الظروف بما في ذلك أي اتفاق ذي صلة".**

فوفقا لهذا النص يعد التوقيع الإلكتروني صالحا لإنشاء الالتزامات حينما يتطلب القانون وجود توقيع على مستند معين، بشرط أن يكون هذا التوقيع الإلكتروني موثوق به[1]، ويمكن التعويل عليه بالقدر المناسب للغرض الذي أنشئت من أجله رسالة البيانات[2].

2: منح التوقيع الالكتروني الحجية القانونية في الإثبات وفقا لتوجيهات الاتحاد الأوروبي.

أمّا التوجيه الأوروبي رقم 93-1999 بشأن التوقيع الإلكتروني أضفى على هذا النوع من التوقيع نفس الحجية القانونية في الإثبات الممنوحة للتوقيع التقليدي وذلك في الفقرة الأولى من المادة الخامسة[3] من هذا التوجيه والتي نصت على أنّه "**على الدول الأعضاء مراعاة أن التوقيع الإلكتروني المتقدم، المستند إلى شهادة تصديق إلكتروني والمنشأ بوسيلة آمنة:**

1) يحقق الشروط القانونية للتوقيع بالنسبة للمعلومات المكتوبة إلكترونيا، بذات الحجية التي يحقها التوقيع اليدوي بالنسبة للمعلومات المكتوبة يدويا أو المطبوعة على الورق.

2) يكون مقبولا كدليل أما القضاء".

هذا وقد نصت أيضا الفقرة الثانية[4] من ذات المادة على أنّ: "**على الدول الأعضاء مراعاة أن التوقيع الإلكتروني لا يفقد أثره القانوني أو حجيته كدليل إثبات بسبب:**

---

[1]- أنظر الفقرة 3 من نفس المادة –المادة 6- من قانون الأونسيترال بشأن التوقيعات الإلكترونية لسنة 2001م.

[2]- أنظر نص المادة (7) من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية 1996م.

[3]-نصها في النسخة الفرنسية كما يلي: Effets juridiques des signatures électronique

Article N.5 : « 1-les Etats membres veillent à ce que les signatures électroniques avancées basées sur un certificat qualifie et crée par un dispositif sécurise de création de signatures.
a) Répondent aux exigences légales d'une signature à l'égard de données électroniques de la même manière qu'une signature manuscrite répond á ces exigences á l'égard de données manuscrites au imprimées sur papier et
b) soient recevables comme preuves en justice.

[4]-وجاء نصها في النسخة الفرنسية كالتالي:

2- les Etats membres veillent à ce que l'efficacité juridique et la recevabilité comme preuve en justice ne soient pas refuses à une signature électronique au seul motif que:
- la signature se présente sous forme électronique.

- **أن التوقيع جاء في شكل إلكتروني.**
- **لأنه لم يستند إلى شهادة تصديق إلكتروني.**
- **لأنه لم يستند إلى شهادة تصديق إلكتروني معتمدة من جهة مرخص لها بذلك.**
- **لأنه تم إنشاؤه أو إصداره من خلال تقنيات تجعله توقيعا إلكترونيا آمنا".**

وقد حذت العديد من الدول حذو قانون اليونسيترال النموذجي بشأن التوقيع الإلكتروني ونصوص التوجيه الأوربي، وذلك بإصدار تشريعات أو تعديلات في قوانينها تتناول الاعتراف بحجية التوقيع الإلكتروني في الإثبات.

كرّس في هذا الشأن المشرّع الفرنسي قرينة صحة التوقيع الإلكتروني وذلك في المادة (1316-4)، إذ بعد أن عرف التوقيع الإلكتروني بأنّه ما ينتج عن استخدام إجراء آمن يكفل تحديد هوية الشخص الموقع، وتضمن صلته بالتصرف الذي يحمل توقيعه المرتبط به، أضاف أن هذا الإجراء الآمن يعد مفترضا طالما أنّه جرى وفقا لشروط معينه، ترك تحديدها لمجلس الدولة بحسبان أنها شروط ترتبط بطابع تقني[1].

وبالفعل صدر مرسوم من مجلس الدولة الفرنسي رقم 272 في 30 مارس 2001 ومرسوما معدلا ومكملا له برقم 535 في 18 إبريل 2002[2]، وقد حدد هذا المرسوم القرينة التي افترضها المشرع بالمادة (1316-4)، حيث نصت المادة الثانية منه على توافر قرينة بسيطة على صحة التوقيع الإلكتروني متى توافرت عدّة شروط عددتها المادة المذكورة، وهذه الاشتراطات هي أن يكون الإجراء المستخدم في التوقيع الإلكتروني آمنا

- qu'elle ne repose pas sur un certificat qualifié par un prestataire accrédite de service de certification, qu'elle n'est pas créée par un dispositif sécurise de création de signature.

[1]- **محمد محمدأبو زيد**، المرجع السابق، ص 246.

[2]- **عبد التواب مبارك**، المرجع السابق، ص33.

وأن يتم استحداث التوقيع الإلكتروني بفضل أجهزة آمنه في إنشاء التوقيعات، وأن يستند التحقق من التوقيع إلى شهادة معتمدة تصدرها الجهة المختصة[1].

يتّضح من النصوص السابقة أن المشرع الفرنسي قد منح الحجية الكاملة في الإثبات للتوقيع الإلكتروني كالتوقيع التقليدي، طالما أنه جرى وفقا للشروط المنصوص عليها.

ثانيا: منح التوقيع الالكتروني الحجية القانونية في الإثبات وفقا لتشريعات الوطنية.

أ- التشريعات الغربية:

اقتداءا منها بالجهود الدولية، ومحاولة منها لتحقيق الأمن القانوني لاقتصادها ككل وللتوقيع الإلكتروني خاصة، قامت بمنح الحجية القانونية للتوقيع الإلكتروني في مختلف تشريعاتها.

***1*: القانون الفرنسي:**

لقد طبق المشرع الفرنسي الأحكام والتوجيهات الواردة بالتوجيه الأوربي رقم 93-1999 بشأن التوقيع الالكتروني، لاسيما المادة 2/5، التي تنص على أن تلتزم الدول الأعضاء في الاتحاد الأوروبي بتطبيق أحكام هذا التوجيه فيما يتعلق بالتوقيعات الالكترونية المتقدمة التي تعتمد على شهادة التوثيق، واتخاذ الإجراءات التي توفر الأمن لبيانات التوقيع[2]. تطبيقا لذلك صدر القانون الفرنسي رقم 230-2000 والذي منح الحجية للتوقيع الالكتروني وبتاريخ 30 مارس 2001 صدر المرسوم رقم 272-2001 والذي يتضمن القواعد والأحكام بشأن حماية وأمن بيانات التوقيع الالكتروني وبتاريخ 18

[1]- **محمد محمدأبو زيد**، المرجع السابق، ص 247.

[2]- **سمير حامد عبد العزيز الجمال**، المرجع السابق، ص 210.

أفريل2002 صدر أيضا المرسوم رقم 535-2002 الذي تضمن القواعد والأحكام الخاصة بحماية وأمن المنتهجات وأنظمة المعلومات[1].

كما أقرّ القضاء الفرنسي أقر بصلاحية التوقيع الالكتروني وحجيته في الإثبات من خلال حكم صدر بتاريخ 8 نوفمبر 1989 عن محكمة النقض الفرنسية، أقر بصلاحية التوقيع الرقمي الذي يتم بواسطة شخص من خلال الرقم المستخدم في البطاقات الرقمية وهذا بالنسبة للاتفاقات المتعلقة بالإثبات.

تكون الثقة في التوقيع الالكتروني والتي يستمد منها حجية الإثبات مفترضة عندما تراعي الشروط التي يتولى تحديدها مرسوم يصدر من مجلس الدولة الفرنسي[2].

من خلال ما سبق يمكن القول بأنّ المشرّع الفرنسي قد وضع مفهوما موسعا للتوقيع، ولم يفرق بين التوقيع التقليدي والتوقيع الالكتروني حيث يكون لكل منهما نفس الحجية القانونية في الإثبات طالما كان هذا التوقيع يميز صاحبه، ويتم بإجراءات آمنة تضمن سرية بيانات التوقيع[3].

2: القانون الأمريكي:

أوردت المادة (101) من الباب الأول الذي جاء بعنوان السجلات والتوقيعات الإلكترونية في التجارة الإلكترونية من التشريع الفدرالي الأمريكي بشأن التوقيعات الإلكترونية والتجارة الإلكترونية، قاعدة عامة تتعلّق بصحة وقانونية المحررات والتوقيعات الإلكترونية، حيث نصت الفقرة (أ) على أنّه رغما عن أيّ تنظيم أو قانون في أيّة ولاية أو أيّ قاعدة قانونية في أي قانون في أية معاملات مالية، سواء في داخل

[1] - **سمير حامد عبد العزيز الجمال**، نفس المرجع، ص 210.

[2] - **سعيد السيد قنديل**، المرجع السابق، ص 58.

[3] -Article 1108-1 du Code civil français : « Lorsqu'un écrit exigé pour la validité d'un acte juridique, il peut être établi et conservé sous forme électronique », in: Olive Leclerc, La reconnaissance de la signature électronique : Étude comparée des législations françaises et allemandes, par : Caroline Riet, http://m2bde.u-paris10.fr, 23 juin 2008, p.05.

الولايات أو في التجارة الأجنبية، يجب مراعاة أنه عقد خاص بالمعاملات المالية، لا ينكر أثره القانوني أو حجيته أو قابليته للتنفيذ بسب استخدام التوقيع الإلكتروني أو السجل الإلكتروني في كتابته أو صياغته، ويلاحظ أن التشريع الفيدرالي الأمريكي لم يشترط في التوقيع الإلكتروني ضوابط فنية أو تقنية معينة، كما لم يستلزم توثيق التوقيع الإلكتروني من جهة تصديق إلكتروني معتمدة[1].

3: في القانون الألماني:

أصدر المشرّع الألماني قانوني التوقيع الرقمي في 1997/11/01 وقانون خدمة المعلومات والاتصالات 1997/11/05، حيث اعترف بالتوقيع الالكتروني ومنحة حجية الإثبات.

ب- التشريعـــات الـــعربية:

قامت التشريعات العربية مثلها مثل التشريعات الغربية بمنح التوقيع الإلكتروني الحجية في الإثبات، سنتعرض لمختلف هذه التشريعات فيما يلي:

1: القانون الأردني:

أورد المشرع الأردني مادتين في قانون المعاملات الإلكترونية رقم 85 لسنة 2001م، ساوى فيهما حجية التوقيع الإلكتروني بحجية التوقيع التقليدي، حيث نصّ في مادته (7/أ) على: "**يعتبر السجل الإلكتروني والعقد الإلكتروني والرسالة الإلكترونية والتوقيع الإلكتروني منتجاً للآثار القانونية ذاتها المترتبة على الوثائق والمستندات الخطية والتوقيع الخطي بموجب أحكام التشريعات النافذة من حيث إلزامها لأطرافها أو صلاحيتها في الإثبات**"، ونص في المادة (10) على أنّه: "**إذا استوجب تشريع نافذ توقيعاً على المستند أو نص على ترتيب أثر على خلوه من التوقيع فإن التوقيع الإلكتروني على السجل الإلكتروني يفي بمتطلبات ذلك التشريع**".

2: القانون المصري:

[1]- **عبد التواب مبارك**، المرجع السابق، ص 37.

أضفى المشرّع المصري على التوقيع الإلكتروني الحجية الكاملة في الإثبات، عند استخدامه في نطاق المعاملات الإلكترونية، ليكون له نفس الحجية المقررة للتوقيعات التقليدية في أحكام قانون الإثبات في المواد المدنية والتجارية، بشرط أن يتم هذا التوقيع طبقاً للشروط والضوابط الفنية والتقنية التي حددها القانون رقم 2004/15 في شأن تنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات. حيث تنص المادة (14) منه على أنّه: "**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**".

هذا وقد وضع المشرع المصري قاعدة عامّة بشأن إثبات صحة التوقيع الإلكتروني والكتابة الإلكترونية والمحررات الإلكترونية، وذلك بالرجوع إلى قواعد وأحكام قانون الإثبات في المواد المدنية والتجارية، في حالة عدم وجود نص في القانون رقم 15 لسنة 2004م ولائحته التنفيذية بشأن إثبات صحة هذه المحررات الإلكترونية وهذا التوقيع الإلكتروني، حيث نص في المادة (17) من هذا القانون على أنّه: "**تسري في شأن إثبات صحة المحررات الإلكترونية الرسمية والعرفية، والتوقيع الإلكتروني والكتابة الإلكترونية، فيما لم يرد بشأنه نص في هذا القانون أوفي لائحته التنفيذية، الأحكام المنصوص عليها في قانون الإثبات في المواد المدنية والتجارية**"[1].

كما نصّت المادة (18) أيضاً على أنّه: "**يتمتع التوقيع الإلكتروني والكتابة الإلكترونية والمحررات الإلكترونية بالحجية في الإثبات إذا ما توافرت فيها الشروط الآتية:**

- **ارتباط التوقيع الإلكتروني بالموقع وحده دون غيره.**
- **سيطرة الموقع، وحده دون غيره على الوسيط الإلكتروني.**

[1]- **مناني فراح**، أدلة الإثبات الحديثة في القانون، المرجع السابق، ص، 132، 142.

- إمكانية كشف أيّ تعديل أو تبديل في بيانات المحرر الإلكتروني أو التوقيع الإلكتروني وتحدّد اللائحة التنفيذية لهذا القانون الضوابط الفنية والتقنية اللازمة لذلك"[1].

يتّضح ممّا سبق أن المشرع المصري قد أقرّ في هذا القانون على أنّ للتوقيع الإلكتروني في نطاق المعاملات المدنية والتجارية والإدارية ذات الحجية المقررة للتوقيع التقليدي في أحكام قانون الإثبات في المواد المدنية والتجارية، بشرط أن تتوافر الشروط القانونية والضوابط الفنية والتقنية التي تضمن صحة وسلامة التوقيع الإلكتروني وتوفر الثقة في نسبته للموقع.

كما نجد أنّ القانون المصري الخاص التوقيع الإلكتروني قد نص في المواد الرابعة عشر والخامسة عشر على أن التوقيع الإلكتروني يكون له الحجية في الإثبات المنصوص عليها في قانون الإثبات إذا تمّ استخدامه في المعاملات التجارية والمدنية والإدارية فقط ولم ينص على حجية التوقيع الإلكتروني في الإثبات إذا تم استخدمه في التعاملات الأخرى التي تخرج عن نطاق المعاملات المدنية والتجارية والإدارية.

3: القانون الجزائري:

نصّت المادة (2/327)[2] من القانون المدني الجزائري على أنّه: "**يعتد بالتوقيع الإلكتروني وفقا للشروط المذكورة في المادة 323 مكرر 1**"، ويكون بذلك قد ساوي في الحجية بين التوقيع الإلكتروني والتوقيع التقليدي، أي أنّه أضفى على التوقيع الإلكتروني نفس الحجية المقررة للتوقيع التقليدي وفقاً للأحكام المنصوص عليها في القانون المدني، غير أنه وفي نفس الوقت اشترط المشرع الجزائري للاعتداد بالتوقيع الإلكتروني ومنحه الحجية الكاملة، أن تتوافر فيه الشروط المنصوص عليها في المادة (323 مكرر1)، وهذه

[1]- انظر المواد (2)، (3)، (4)، (9) من اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري رقم 15 لسنة 2004م.

[2]- أضيفت الفقر الثانية من المادة (327) من القانون المدني بالقانون رقم05-10، المؤرخ في 20 يونيو 2005م منشور بالجريدة الرسمية رقم 44، ص 25.

الشروط هي إمكانية التأكد من هوية الشخص الذي أصدر التوقيع وأن يكون هذا التوقيع معدا ومحفوظ في ظروف تضمن سلامته.

إلاّ أنّ تحقّق هذين الشرطين يتوقف على وجود طرف ثالث يتمثّل في جهة وسيطة تصادق على هذا التوقيع، وتضمن صدوره من الشخص المنسوب إليه، مع عدم إحداث أيّ تحريف أو تعديل فيه، وفي غياب نص تنظيمي للمسألة تظل مشكلة تحديد الشخص الذي يصدر عنه هذا التوقيع قائمة حتى مع وجود توقيع إلكتروني[1].

نخلص من عرضنا للنصوص السابقة أن التشريعات المختلفة التي أولت اهتماما بالإثبات الإلكتروني، قد اتجهت إلى مساواة التوقيع الإلكتروني بالتوقيع التقليدي أقرّت له حجية مساوية لحجية هذا الأخير، غير أن إقرار هذه الحجية مرتبط بتوافر شروط قانونية ومتطلبات وضوابط فنّية وتقنية تضمن صحة وسلامة التوقيع الإلكتروني وتوفر الثقة في نسبته للموقع[2]، وبهذا لم يعد إحداث التوقيع الإلكتروني بواسطة الوسائل الإلكترونية عقبة أمام الاعتراف به وقبوله كعنصر في دليل الإثبات، فقد أصبح التوقيع الإلكتروني أداة تصلح لتوثيق التصرفات التي تتم بواسطة الوسائط الإلكترونية، خاصة في مجال عقود التجارة الإلكترونية، كما أنّ هذه المساواة بين التوقيع الإلكتروني والتوقيع التقليدي قد أنهت سلطة القاضي التقديرية في الأخذ بالتوقيع الإلكتروني أو رفضه.

[1]- لم يصدر لحد الساعة نص أو مرسوم تنظيمي يبين الضوابط الفنية والتقنية للتوقيع الإلكتروني أو الجهة المخولة بتوثيقه والمصادقة عليه.

[2]- **إبراهيم الدسوقي أبو الليل**، المرجع السابق، ص176.

تعرضنا في هذا الفصل إلى تحديد المقصود بالتوقيع الالكتروني فتبين لنا أن هذا الأخير يقوم على استخدام التقنيات الحديثة من حاسوب وأنترنيت، فهو يتخذ شكل بيانات الكترونية كما أنه في مجال التطبيقات رأينا أن التوقيع الالكتروني يستخدم فعلا في العديد من المجالات المهمة مثل البطاقات البلاستيكية الواسعة الانتشار، وكذلك في بعض الأوراق التجارية، وضف إلى ما سبق فلقد تعرضنا لشروط التوقيع الالكتروني أين لاحظنا ظهور أشخاص جديدة تكلف بالتوثيق مع إناطتهم وتخويلهم أدوارا ووظائف عديدة.

كما بحثنا في مدى قبول التوقيع الالكتروني كدليل إثبات قانوني، وذلك بتناولنا لحجيته في قانون الاونيسترال وكذا بالنسبة للقوانين المقارنة وما خلصنا إليه هو أن أغلب القوانين اتجهت إلى إعطاء التوقيع الالكتروني أثرا قانونيا كاملا في الإثبات، بشرط أن يكون موثقا وفق الإجراءات المحددة قانونا هذا من جهة ومن جهة أخرى لاحظنا اختلاف بين التشريعات في طريقة تنظيم التوقيع الالكتروني فيوجد من فضّلت تفريده بقانون خاص به ويوجد من قامت بإضافة مواد خاصة به في قوانينها المدنية.

صدرت تشريعات دولية وإقليمية ووطنية نظمت أحكامها التوقيع الإلكتروني لإزالة الغموض على هذا المفهوم الحديث والمستجد على الفكر القانوني، وبينت ماهيته واعترفت به ومن بين هذه القوانين التي حددت الطبيعة القانونية للتوقيعات الإلكترونية، قانون الأونسيترال النموذجي لعام 1996م بشأن تنظيم التجارة الإلكترونية، وقانون الأونسيترال النموذجي لعام 2001م بشأن التوقيعات الإلكترونية، وكذلك أصدرت المفوضية الأوربية أحكام التوجيه الأوربي رقم 93 لسنة 1999م بشأن التوقيعات الإلكترونية، وفضلاً على ذلك واسترشادا بالقوانين النموذجية والتوجيها الدولية، صدرت العديد من التشريعات الوطنية اعترفت بالتوقيع الإلكتروني وأضفت عليه حجية قانونية مساوية لحجة التوقيع التقليدي في الإثبات، ومن أهم هذه التشريعات الوطنية، التشريع الفدرالي الأمريكي لعام 2000م بشأن التوقيعات الإلكترونية في التجارة الداخلية والدولية، والقانون الفرنسي رقم 230 لسنة 2000م بشأن تطويع قواعد الإثبات لتكنولوجيا المعلومات والتوقيع الإلكتروني. والقانون التونسي رقم 83 لسنة 2000م في شأن المبادلات والتجارة الإلكترونية، والقانون الأردني المتعلق بالمعاملات والتجارة الإلكترونية رقم 85 لسنة 2001م وقانون إمارة دبي رقم 02 لسنة 2002م، والقانون المصري رقم 15 لسنة 2004م المتعلق بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات. وقد عرضنا نصوص التشريعات المختلفة التي نظمت الإثبات الإلكتروني والتي أقرت بحجية التوقيع

الإلكتروني وساوت بينه وبين التوقيع التقليدي، وشروط حجيته إن توفرت هذه الشروط فإنه يتمتع بالحجية الكاملة في الإثبات أمام القضاء في نطاق المعاملات المدنية والتجارية.

نخلص أن التوقيع الالكتروني في بيئة المعاملات الالكترونية له طابعه الذي يميزه عن التوقيع التقليدي، والذي يجعله توقيعا ذا طابع خاص كونه يتم بطريقة تكنولوجية حديثة تتلاءم مع طبيعة المعاملات الالكترونية وتمكن من تحديد هوية الوقع والتعبير عن إرادته في بيئة غالبا ما تكون افتراضية يجهل فيها المتعاملون أحيانا بعضهم البعض كون العقد لا يتم في مجلس واحد، وإنّما بين غائبين من حيث المكان وأحيانا من حيث الزمان، إن التوقيع الالكتروني يتمتع ببعض المزايا تجعله يفوق التوقيع التقليدي من حيث أدائه لوظائفه بدقة بالغة،لكن مع ذلك ولغرض منح الحجية الكاملة للتوقيع الالكتروني في إثبات المعاملات الالكترونية، لا تكفي النصوص القانونية لوحدها، إنما كانت هناك ضرورة ملحة لحماية التوقيع الالكتروني من التزوير والتحريف وكان ذلك باعتماد جهات التوثيق الالكتروني التي تعمل تخت رقابة الدولة وتقوم بمنح شهادات ضمان للتوقيع الالكتروني وتقوم بدور الوسيط في المعاملات الالكترونية عبر الشبكات، إضافة لذلك يتم اعتماد طريقة التشفير لحماية التوقيع الالكتروني والبيانات الالكترونية، ولقد مكن ذلك من إضفاء الثقة في التعامل الالكتروني والتوقيع الالكتروني، هذه الثقة هي التي تعطي للتوقيع مصداقية وتجعل القاضي يأخذ به كوسيلة إثبات هذا سنتناوله بالتفصيل في الفصل الثاني تحت إشكالية هامة تتمثل في وسائل أو آليات حماية التوقع الإلكتروني فما هي هذه الوسائل ومن هي الجهة المخولة بذلك؟

الفصل الثاني

آليـــات حمـــــاية

الـــتوقيع الإلكتروني

الفـــصل الثاني

آليـــات حمـــاية الـــتوقيع الإلكـــتروني

ترتب عن اعتماد الإنترنت في إبرام عقود التجارة الإلكترونية زيادة الطلب على أنظمة التشفير من أجل حمايتها من مخاطر القرصنة، ويتم ذلك عادة باستخدام برامج خاصة لهذه الانتهاكات، الأمر الذي يعرض المتعاقدين عبر شبكة الإنترنت إلى أخطار عديدة كإفشاء أسرار هامة مثل الإطلاع على بيانات شخصية أو اختلاسها، وهذا يؤدي إلى إلغاء عنصر الثقة والائتمان في هذه المعاملات، وللقضاء على هذه المخاطر ومواجهتها تمّ استخدام تقنية التشفير كإحدى وسائل حماية سلامة وسرية المعلومات المرسلة عبر شبكة الإنترنت، وإيجاد ضمانات كفيلة بإرساء الأمن القانوني من قبل جهات أخرى محايدة تسمى بجهات التصديق الإلكتروني.

يعتبر التوقيع الإلكتروني العنصر الرئيسي الذي تقوم عليها إجراءات التجارة الإلكترونية، كونه مرتبط بتوثيق التصرفات القانونية الإلكترونية وتحديد هوية المرسل والمستقبل، والتأكد من صحة البيانات - وسيلة مدنية لحماية معاملات التجارة الإلكترونية-. إزاء هذه الأهمية بات من الضروري وجود حماية جنائية له ضدّ كلّ تصرف يهدّده، بالاعتداء أو الضرر، فإنّ أيّ اعتداء على التوقيع الإلكتروني يمثل اعتداء على مضمون التجارة الإلكترونية عموما، وعلى كل جهة تستخدم التوقيع الإلكتروني للتوثيق وإثبات الهوية، سواء كانت عامة أم خاصة هذا ويعدّ من أكثر الجرائم تهديدا للتوقيع الإلكتروني جريمة تزوير التوقيع الإلكتروني وقد عالجت ذلك التشريعات والقوانين في دول العالم.

لبيان أهمية كل هذه النقاط، سوف نتطرق لدراسة موضوع الحماية التقنية والوقائية للتوقيع الإلكتروني **(المبحث الأول)**، ثم نتناول موضوع الحماية الجنائية له **(المبحث الثاني)**.

المبحث الأول

الحماية التقنية والوقائية للتوقيع الإلكتروني

غياب العلاقة المباشرة بين الأطراف في التصرفات الإلكترونية خاصة التي تتم عبر شبكة الانترنت، تطلبت توفر عنصر الثقة والأمان في هذه التصرفات، خاصة فيما يتعلق بالتوقيعات الإلكترونية للأطراف المتعاقدة، ولهذا كان من الضروري إيجاد وسائل تقنية لحماية هذا التوقيع من أي مخاطر قد يتعرض إليها من جهة، ولبث الثقة والأمان في التصرفات التي تتم عبر الوسائط الإلكترونية من جهة أخرى[1]، ومن أهم هذه الوسائل تقنية تشفير البيانات لضمان إرسال الرسائل ونقل المعلومات بطريقة سرية لا يمكن للغير الإطلاع عليها أو تغير بياناتها **(المطلب الأول)**، إلى جانب وجود طرف ثالث محايد بين أطراف التصرف يعمل كجهة مصادقة وهذا من خلال شهادة الكترونية يصدرها تحتوي على مجموعة من البيانات وظيفتها تأكيد العلاقة ما بين الموقع وتوقيعه الإلكتروني، لذلك ارتأت التشريعات الدولية والإقليمية والوطنية إيجاد وسيط (طرف ثالث) قصد تحقيق الحماية الوقائية **(المطلب الثاني)**.

المطلب الأول

الحماية التقنية لتوقيع الإلكتروني

تأمين المعاملات الإلكترونية من الضرورات التي يسعى إليها دائما المتعاملون في مجال التوقيع الإلكتروني، وكلّما كان المتبع يوفر الثقة بين المتعاملين كلّما ازدادت كمية المعاملات الإلكترونية. كما تتعرض المؤسسات المتعاملة في التجارة الالكترونية الناتجة عن التكنولوجيا الجديدة والأنظمة الجديدة التي تعتمد عليها كي تتم المعاملة بشكل مؤمن نظرا لتدخل قنوات الاتصال على الإنترنت مفتوحة للجميع، ممّا يعرض المعلومات

[1]- **خالد مصطفى فهمي**، المرجع السابق، ص ص100-103.

الشخصية للخطر. ردع هذه المخاطر أدى إلى ظهور عدة تقنيات للتقليل من المخاطر التي تعاني منها المؤسسات ومستهلكي في الوقت الذي تتم فيه معاملة التجارة الالكترونية[1].

نقصد بالحماية التقنية للتوقيع الإلكتروني المحافظة على المعلومات وسلامتها، هي الطرق والوسائل المعتمدة للسيطرة على كافة أنواع ومصادر المعلومات وحمايتها من السرقة، التشويه، الابتزاز، التلف والضياع، التزوير والاستخدام غير المرخص وغير القانوني، حماية وتأمين كافة الموارد المستخدمة في معالجة المعلومات[2]، حيث يتمّ تأمين المنظمة نفسها الأفراد والعاملين فيها والأجهزة والحسابات ووسائط المعلومات التي تحتوي على بيانات المنظمة وذلك بإتباع إجراءات ووسائل عديدة تضمن سلامة المعلومات.

ويعرفها محمد دباس الحميد أنّها: **"حماية جميع أنواع المعلومات ومصادر الأدوات التي يتعامل مها وتعالجها من منظمة وغرفة تشغيل أجهزة، والأجهزة ووسائط التخزين والأفراد من السرقة والتزوير والتلف والضياع والاختراق"[3]**

---

[1]- **JEFFREY F,Rayport et Jaurorski Bernard**, commerce électronique (Traduit de l'américain port) Francine Nézina, Johanne champoux et élisabéth Rochette, Edition cheneliere/ McGram-Hill, Montréal – Toronto, 2003,P. 56.

[2]- يعتبر التشفير حلا تنتهجه جميع القنوات التلفزيونية الفضائية من أجل حماية المواد التي تبثها وأرباحها من القرصنة وهذه المواد تتنوع بين بطولات كرة القدم والرياضات المتنوعة والأفلام والبرامج الوثائقية والبرامج الحصرية، وما يدفع القنوات لهذا الأمر هو سياسة الحقوق التلفزية المتعارف عليها في منظومة القنوات الفضائية في أيامنا هذه. حيث أن القناة التي تمتلك مالا أكثر تدفع وتحصل على أي مادة من المواد المذكورة سابقا حصريا، بمعنى أن القناة المشترية لديها الحق في احتكار بث تلك المادة والإنفراد بعرضها وبالطبع كل هذا يجعل الحرب بين القنوات الفضائية فيما بينها من جهة، وبين القنوات الفضائية والقراصنة من جهة أخرى تشتعل، وهذا ما يتسبب في انتهاج القناة لمبدأ التشفير حماية لنفسها ولمشتركيها الرسميين، الذين يشتركون في القناة باقتناء البطاقة الأصلية وكذلك تحقيق الربح المادي وراء ثمن الاشتراك الرسمية، والتشفير بصفة عامة وحجب البث ومنعه من الظهور للجميع إلا لمن يمتلك بطاقة الاشتراك، والتي تقوم بفك التشفير وتشغيل القناة بطريقة شرعية وقد سمي بالتشفير لأنه يتم وضع شفرة مكونة من عدة أرقام لكل قناة وتكون هذه الشفرة مخفية متغيرة باستمرار. وقد ظهر سنة 1994 عندما انتهجته باقة SKY DIGITALالبريطانية لتكون أول باقة تدخل عالمالتشفير، فتبعتها باقات .Première, ART, CANAL Plus ومع اشتعال هذه الحرب ظهرت عدة شركات للتشفير طرحت في السوق عدة أنظمة، تختلف مميزاتها فيما بينها، وقامت بعرضها على كبرى القنوات الفضائية لاستخدامها.

[3]- **محمد دباس الحميد**، حماية أنظمة المعلومات، دار الحامد للنشر والتوزيع، الأردن، 2007، ص 34.

يعتبرالتشفير أفضل تقنية لحماية البيانات والمعلومات المرسلة عبر الشبكات المفتوحة من أي تعديل أو تغير غير مرغوب فيه[1]، ولذلك تأتي تقنيات التشفير في مقدمة الوسائل والأدوات المبتكرة في مجال توفير الأمن وسلامة وسرية المعلومات والمعاملات والصفقات المتبادلة عبر شبكة الإنترنت، إضافة إلى كون هذه التقنية لا تقتصر وظائفها على تأدية وظائف الحماية فقط بل تمتد إلى وظائف أخرى تساهم في تدعيم الإثبات الإلكتروني، أهمها التحقق من هوية مرسل الرسالة والمصادقة على مضمونها وعلى توقيع أصحابها إلكترونيا والتأكد من سلامتها, وبالتالي عدم قابليتها للإنكار[2].

لبيان حقيقة هذه التقنية المتمثلة في تقنية التشفير التي تعتبر في مقدمة الوسائل والأدوات في مجال توفير الحماية وسلامة وسرية البيانات والمعلومات المرسلة عبر شبكة الإنترنت، نتطرق إلى التعريف القانوني للتشفير في مختلف التشريعات العربية والأجنبية والفقه **(الفرع الأول)**، وإلى أنواع التشفير وطرقه **(الفرع الثاني)**، ومستوياته **(الفرع الثالث)**.

الفرع الأول

التشفير طريقة لحماية التوقيع الإلكتروني

تقنية التشفير عملية قديمة استعملت لإرسال رسائل القادة العسكريين خلال الحروب بكلّ أمان[3]، بحيث ثبت استخدمه منذ حوالي عام قبل الميلاد لحماية الرسائل السرية[4] ولأهميته حظي باهتمام العديد من التشريعات بتنظيم استخدام تكنولوجيا التشفير.

---

[1]- **وسيم شفيق الحجار**، الإثبات الإلكتروني، المنشورات الحقوقية، بيروت، 2002، ص 198.

[2]- **طوني ميشال عيسى**، التنظيم القانوني لشبكة الإنترنت، دراسة مقارنة في ضوء القوانين الوضعية والاتفاقات الدولية، المنشورات الحقوقية، بيروت، 2001، ص197.

[3]- راجع: **ثروت عبد الحميد**، المرجع السابق، ص،75، **و: سعيد السيد قنديل**، المرجع السابق،ص 73، وكذا: **محمد السعيد رشدي**، المرجع السابق، ص 58 .

[4]- إن الدراسات التحليلية التي عنيت بالتشفير توصلت إلى أول استخدام للتشفير يعود إلى قبل أربعة سنة تقريبا، فقد استخدم المصريون القدماء التشفير كعلامة لتزين قبور الملوك، إلا أن غايتهم من التشفير لم تكن حماية سر معين وإنّما كنوع من الفخامة

يمكن تعريف التشفير بأنّه:" **مجموعة من الوسائل التي تهدف لحماية سرية البيانات والمعلومات بحيث لا يستطيع فهمها وقراءتها إلا المرسل والمرسل إليه فقط، ذلك عن طريق استخدام رموز خاصة تعرف عادة باسم المفتاح** PIN".

يعرف التشفير بأنّه: "**كل العمليات التي تؤدي بفضل بروتوكولات سرية إلى تحويل معلومات أو إشارات مفهومة (مقروءة)، أو القيام بالعكس وذلك باستخدام برامج مصممة لهذه الغاية**"، **ويعرف أيضا بأنّه: "آلية يتمّ بمقتضاها ترجمة معلومة مفهومة إلى معلومة غير مفهومة عبر تطبيق بروتوكولات سرية قابلة للانعكاس أي يمكن إرجاعها إلى حالتها الأصلية**"[1].

كما عرف بأنّه تقنية تعتمد على خوارزميات رياضية تسمح لمن يمتلك مفتاحا سريا أن يُحول رسالة مقروءة إلى رسالة غير مقروءة، وبالعكس اعتبر كذلك بأنها النظرية الأكثر انتشارا لتأكيد هوية الشخص المرسل باستخدام مفاتيح ترميز من قبل طرفين[2].

حرصا من التشريعات المهتمة بازدهار التجارة الإلكترونية، أباحت تشفير البيانات والمعاملات التي يتم تدوينها أو التعامل بها من خلال الوسائط الإلكترونية، هذا في وقت كانت فيه بعض هذه التشريعات تقيد استخدام الأفراد والشركات للتشفير لأغراض سرية

=والقدسية لقبور الملوك، هذه البداية الأولى البسيطة لاستخدام التشفير ثم استخدم لنقل العبارات العسكرية والدبلوماسية، فقد استخدامه الأسبان القدماء لتشفير عباراتهم العسكرية واستخدمه أيضا الحكام في الهند للتواصل مع جواسيسهم، ومع توالي الحضارات تطورات طرق التشفير فقد استعمل الرومانيون آليات متعددة للتشفير ككتابة النص على ورقة على قطعة من الخشب ذات قطر معين، ولكي يفتح النص يجب إعادة لف الورقة على قطعة من خشبية قطرها مساو لقطر الخشبة الأولى، وقد شهد علم التشفير تطورا ملحوظا مع اختراع الكهرباء وأجهزة التلغراف والبت اللاسلكي، وفي الحربين العالميتين الأولى والثانية كان للتشفير دور فعال إذ استخدمته الدول التي خاضت الحرب لضمان عدم تسرب المعلومات السرية إلى العدو، وفي المقابل سعت الدول إلى كسر رموز التشفير لكشف خطط العدو العسكرية، ويشكل التشفير في وقتنا للحاضر حربا باردة بين الدول العظمى كالولايات المتحدة وروسيا والصين، إذ تسعى هذه الدول إلى كسر شفرات السفن الحربية والأقمار الصناعية التجسسية، ومع دخول العالم عصر تكنولوجيا المعلومات والاتصالات وابتداع شبكة الانترنت واستخدامها في نقل البيانات، فقد استخدام التشفير للمحافظة على سرية البيانات وحمايتها من تطفلات الغير.

[1]- أنظر تقنية التشفير تاريخيا:**سمير حامد عبد العزيز الجمال**، المرجع السابق، ص218، و**عايض راشد عايض المري** المرجع السابق، ص96. ولمزيد من التفاصيل القانونية والتقنية والتاريخية بخصوص التشفير راجع:

DIMITRIOU Philippe, «l'application du droit de la cryptologie en matière de sécurité des réseaux informatique » D.E. Afac des sciences juridique, politiques et socials, école doctorale N°74, université de LILLE, 2002, p:9.

[2]- **عمر خالد زريقات**، المرجع السابق، ص ص 269، 271.

لها صلة بالسياسة العامة المنطوية على اعتبارات الأمن والدفاع الوطني[1]، غير أنّه مع تعميم استخدام التشفير أصبح هذا الأخير من أهم الضمانات في مجال التجارة الإلكترونية وذلك لتوفير وضمان الثقة في هذه التجارة والتي بدونها لن تعرف أي تطور أبدا.

مر التشفير بمراحل عديدة من التطور ومازال هذا النظام في تطور مستمر حتى الآن، فعندما يضع المشفرون نظام تشفير يأتي آخرين ويحاولون فك هذا النظام ومعرفة سر الشفرة،فيلجأ المشفرون لنظام جديد، حيث كان في الستينات حكرا على الحكومات غير أنه في أواخرها قامت شركة **IBM** بتطوير نظام للتشفير أطلقت عليه اسم **Lucifer** تحفظت عليه الحكومة الأمريكية بحجة عدم حاجة المؤسسات والشركات الخاصة لنظام التشفير، غير أن ذلك لم يمنع هذا النظام من أن يحقق انتشارا واسعا، ولم يظهر له إطارا تشريعيا إلا حديثا في بعض الدول المتقدمة وعددها محدود، ومن بين التشريعات التي اهتمت بتنظيم وتحديد أسلوب التشفير منها على سبيل المثال:

أولاً: التعريف القانوني للتشفير في البلدان الغربية.

يعتبر نظام التشفير أكثر تقدما في الدول الغربية، حيث أصبحت جل المعاملات اليومية في هذه الدول تتم عبر الوسائل الإلكترونية، وبالتالي اعتماد نظام التشفير لإضفاء السرية عليها، سنتناول مسألة تعريفه في تشريعات مختلف الدول الغربية كما يلي:

***1*: القانون الفرنسي:**

صدر أوّل مرسوم فرنسي بشأن التعامل بوسيلة التشفير بتاريخ 18 أفريل 1939 ثم صدر تعديل له بالمرسوم الصادر في 18 أبريل 1982، ثمّ صدر القانون الفرنسي رقم 90/1170 بتاريخ 29 ديسمبر 1990، حيث تضمنت المادة (27) منه على تعريف التشفير بأنّه: "**كل الأعمال التي تهدف إلى تحويل معلومات أو إشارات واضحة باستخدام وسائل**

[1] **عيسى غسان ربضى**، المرجع السابق، ص ص 72،73 .

مادية أو معالجة آلية إلى معلومات أو إشارات غامضة للغير، أو إلى إجراء العملية العكسية عبر وسائل مادية أو معلوماتية مخصصة لهذا الغرض"[1].

سمح هذا القانون للمشروعات الصغيرة والأفراد باستخدام التشفير بعد أن كان مقصورا على المجالات العسكرية والحكومية فقط، وبتاريخ 24 فبراير 1998 صدر المرسوم رقم 98/101 الذي وضع الضوابط المتعلقة باستخدام التشفير[2]، كما أنّه وبموجب القانون رقم 616 بتاريخ 18 يونيو 2001 أدخلت تعديلات على المادة (27) من القانون رقم 1170-90 تجيز تصدير وسائل التشفير التي تؤمن وظيفة السرية لرسالة المعلوماتية، وهذا التعديل التشريعي كان بناء على توصيات البرلمان الأوربي بتاريخ 2000/6/22 التي ترمي إلى إلغاء القيود القائمة على تبادل تقنيات ومنتجات التشفير فيما بين الدول الأوربية الأعضاء[3]. أما الفقرة الأولى من المادة 28 فقد عرفت أدوات التشفير ووسائله في مجال المعلوماتية بأنها "**أعمال ترمي عبر اتفاقية سرية إلى تحويل معلومات أو إشارات غامضة، أو القيام بالعملية المعاكسة،وذلك باستخدام وسائل أو برامج مخصصة لهذه الغاية**"[4].

ثانيًا: التعريف القانوني للتشفير في البلدان العربية.

اقتداءا منها بالدول الغربية قامت بتنظيم التشفير، وسنتناول تعريف التشفير في مختلف تشريعات الدول العربية فيما يلي:

[1]- **سمير حامد عبد العزيز الجمال**، المرجع السابق، ص219.

[2]- لمزيد من التفاصيل حول تطور نظام التشفير، راجع: **سمير حامد عبد العزيز الجمال**، المرجع السابق، ص ص 218 و 219. **ومحمد السعيد رشدي**، المرجع السابق، ص ص 55، 56.

[3]-**THIERRY PIETTE-COUDOL, échange électroniques certification et sécurit**é, édition LITEC ? Paris, 2000, pp 60. 61

[4]-« toutes prestations visant a transformer a l'aide de convention secrets des information ou signaux claires en information ou signaux inintelligibles ou a réaliser l'opération inverse grâce a des moyens matériels ou logiciels conçus a cet effet »

1: القانون التونسي:

عرف المشرّع التونسي التشفير وحدد مفهومه في الفصل الثاني من الباب الأول من القانون التونسي رقم 83 لسنة 2000 في شأن المبادلات والتجارة الإلكترونية، حيث نص على أن التشفير هو "**استعمال رموز أو إشارات غير متداولة تصبح بمقتضاها المعلومات المرغوب تمريرها أو إرسالها غير قابلة للفهم من قبل الغير أو استعمال رموز أو إشارات لا يمكن الوصول إلى المعلومات بدونها**"، كما نص أيضا على بعض الشروط التي يجب مراعاتها عند استعمال التشفير، حيث جاء في الفصل الثالث من نفس القانون على أنّه "**يخضع استعمال التشفير في المبادلات والتجارة الإلكترونية عبر الشبكات العمومية للاتصالات، إلى التراتيب الجاري بها العمل في ميدان الخدمات ذات القيمة المضافة للاتصالات**".

هذا وقد نص في الفصل (48) من القانون رقم 2000/83م في حالة الاعتداء على البيانات المشفرة على أنه "**يعاقب كل من استعمل بصفة غير مشروعة عناصر تشفير شخصية المتعلقة بإمضاء غيره بالسجن لمدة تتراوح بين ستة أشهر وعامين وبخطية تتراوح بين 1000 و10000 دينار أو بإحدى العقوبتين**"[1].

2: القانون المصري:

أباح المشرع المصري أيضا تشفير البيانات والمعلومات التي يتم تدوينها أو التعامل عليها من خلال الوسائط الإلكترونية، وذلك كأسلوب يحقق تأمين المعاملات التجارية وبالتالي ازدهارها رغم أن قانون التوقيع الإلكتروني المصري رقم 2004/15 جاء خاليا من تعريف التشفير، إلاّ أنّه ترك هذه المسألة ليتم تنظيمها بأحكام اللائحة التنفيذية للقانون بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات، وذلك بوضع القواعد والضوابط الخاصة بتشفير المحررات والبيانات الإلكترونية، وكذلك وضع القواعد الخاصة بتشفير التوقيع الإلكتروني وبيانات الائتمان وغيرها من البيانات التي يتمّ

[1]-يمكن مراجعة نصوص هذا القانون لدى: **وائل أنور بندق**، المرجع السابق، ص51، أو على الموقع:
http// :arabegov.com/news/news.asp

تحريرها أو نقلها أو تخزينها على وسائط إلكترونية، وفقا للمعايير الفنية والتقنية المنصوص عليها في اللائحة التنفيذية للقانون والمشار إليها في الملحق الفني والتقني لهذه اللائحة[1].

عرفت المادة (9/1) من اللائحة التنفيذية لقانون التوقيع الإلكتروني التشفير بأنّه: **"منظومة تقنية حسابية تستخدم مفاتيح خاصة لمعالجة وتحويل البيانات والمعلومات المقروءة إلكترونيا بحيث تمنع استخلاص هذه البيانات والمعلومات إلا عن طريق استخدما مفتاح أو مفاتيح فك الشفرة".**كما عرف منظومة أو تقنية شفرة المفتاحين العام والخاص- تقنية المفتاح العام-، والتي يستخدم فيها مفتاحان مختلفان ولكن مرتبطان رياضيا، ويتم توزيع المفتاح العام بشكل حر على أيّ شخص يطلبه، أمّا المفتاح الخاص فيحتفظ به الشخص سرا لاستخدامه في التشفير والتوقيع الإلكتروني على المحررات الإلكترونية المرسلة، حيث نصت المادة (10/1) من اللائحة ذاتها بأنّه: **"تقنية شفرة المفتاحين العام والخاص هي منظومة تسمح لكل شخص طبيعي أو معنوي بأن يكون لديه مفتاحين متفردين أحدهما عام متاح إلكترونيا والثاني خاص يحتفظ به الشخص ويحفظه على درجة عالية من السرية".** عرفت نفس اللائحة كل من المفتاحين العام والخاص وكذلك المفتاح الشفري الجذري التي تستخدمه جهات التصديق الإلكتروني لإنشاء شهادات التصديق وبيانات إنشاء التوقيع الإلكتروني، حيث نصت في الفقرات (13/12/11) من المادة الأولى من اللائحة التنفيذية على ما يلي:

"-المفتاح الشفري العام: أداة إلكترونية متاحة للكافة، تنشأ بواسطة عملية حسابية خاصة، وتستخدم في التحقق من شخصية الموقع على المحرر الإلكتروني، والتأكد من صحة وسلامة محتوى المحرر الإلكتروني الأصلي.

-المفتاح الشفري الخاص: أداة إلكترونية خاصة بصاحبها، تنشأ بواسطة عملية خاصة وتستخدم في وضع التوقيع الإلكتروني على المحررات الإلكترونية ويتم الاحتفاظ بها على بطاقة ذكية مؤمنة.

[1]-أنظر الفقرة (أ) و (ب) من الملحق الفني والتقني للائحة التنفيذية لقانون التوقيع الإلكتروني المصري رقم 15 لسنة 2004م.

-المفتاح الشفري الجذري: أداة إلكترونية تنشأ بواسطة عملية حسابية وتستخدمها جهات التصديق الإلكتروني لإنشاءاتها ذات التصديق الإلكتروني وبيانات إنشاء التوقيع الإلكتروني".

يرى جانب من الفقه في هذا الخصوص أنّ التوقيعات الرقمية يستعان بها على نطاق واسع، وذلك على أنها أكبر وسيلة لتحقيق مستوى الثقة المطلوبة بين الأطراف في المعاملات التجارية من حيث الفعالية وإمكانية التطبيق، حيث تنشأ التوقيعات الرقمية باستخدام علم التشفير، إما باستخدام الشفرة غير المتماثلة، أو المفتاح العام[1]، حيث نصت المادة الثالثة من اللائحة التنفيذية لقانون التوقيع الإلكتروني رقم 15 لسنة 2004 على أنّه:

"يجب أن تتضمن منظومة تكوين بيانات إنشاء التوقيع الإلكتروني المؤمنة الضوابط الفنية والتقنية اللازمة وعلى الأخص ما يلي:

1) أن تكون المنظومة مستندة إلى تقنية شفرة المفتاحين العام والخاص، وإلى المفتاح الشفري الجذري الخاص بالجهة المرخص لها والذي تصدره لها الهيئة، وذلك كله وفقا للمعايير الفنية والتقنية المشار إليها في الفقرة (أ) من الملحق الفني والتقني لهذه اللائحة.

2) أن تكون التقنية المستخدمة في إنشاء مفاتيح الشفرة الجذرية لجهات التصديق الإلكتروني من التي تستعمل مفاتيح تشفير بأطوال لا تقل عن 2048 حرف إلكتروني (bit)".

يوجد **ثلاثة أنواع من التشفير[2] يتمّ استخدامها في التجارة الإلكترونية وهي:**

<u>التشفير المتماثل</u>: ويقصد به المفتاح الخاص Clé privée، يقوم على وجود مفتاح واحد من أجل تشفير البيانات وكذلك حل التشفير، وهو النظام المعروف بـــ "السيمتري" وقد أخذ على هذا النظام أنه غير آمن لأن مرسل المعاملة أو البيانات ومستقبلها يملكان نفس المفتاح[3].

1- **BRAZELL Lorna**, Electronic signatures, law and Regulation Sweet Maxwell, London, 2004, P 50.

[2]- **عيسى غسان ربضى**، المرجع السابق، ص ص 80 -81.

[3]- **إبراهيم سليمان عبد الله**، التجارة الالكترونية أمن المعلومات، مقال منشور على البريد الإلكتروني:
www.kau.edu.sa/iabdullah

التشفير غير المتماثل: يقوم على وجود مفتاحين هما مفتاح عام "clé Publique" معروف ومتاح للجميع يتمّ استخدامه في عملية التشفير ومفتاح خاص "clé privée" غير معروف لأي شخص إلا الشخص مرسل الرسالة، وهو النظام المعروف بـــ "الاسميتري" فالمفتاح العام يتميز عن المفتاح الخاص كونه معروفا ومتاح إلكترونيا لطرفين أو أكثر غير أنّ هذا التميز الذي يخص المفتاح العام لا يفصله عن المفتاح الخاص، لأنّهما مترابطان في عملهما، ويكمل كلّ منهما الآخر، فإذا استعمل المفتاح الخاص لتشفير الرسالة فلا يمكن فك التشفير إلا بالمفتاح العام كما أنّه لو عرف أحد المفتاحين فلا يمكن معرفة المفتاح الآخر حسابيا.

التشفير المزدوج: هو نظام خليط بين المتماثل وغير المتماثل، وفيه يتم تشفير الرسالة بمفتاح خاص ثم تشفير المفتاح الخاص بمفتاح عام وإرسال كل من الرسالة المشفرة والمفتاح الخاص المشفر إلى المرسل إليه باستخدام أي شبكة اتصالات[1].

ثالثا: التعريف الفقهي للتشفير.

عرفه البعض بأنّه:" **تغيير في شكل البيانات عن طريق تحويلها إلى رموز أو إشارات لحماية هذه البيانات من إطلاع الغير عليها من تعديلها أو تغييرها**".(2)

وعرفه البعض الأخر بأنه :"**عملية الحفاظ على سرية المعلومات الثابت منها والمتحرك باستخدام برامج لها القدرة على تحويل وترجمة تلك المعلومات إلى رموز بحيث إذا ما تم الوصول إليها من قبل أشخاص غير مخول لهم بذلك لهم لا يستطيعون فهم أي شيء، لأن ما يظهر لهم هو خليط من الرموز والأرقام والحروف غير مفهومة**"[3].

من خلال ما سبق يمكن لنا تعريف التشفير بأنه كتابة المعلومات في شكل رموز غير مفهومة من الغير سواء بوسائل مادية أو معالجة آلية تتمّ لتحقيق ذلك، ويعطي

---

[1]-**قدري عبد الفتاح الشهاوي**، المرجع السابق، ص 416.

[2]-PGP 6.5.1, Introduction à la cryptographie, 1999, Network associate, in: http://laurent.falcaum.fre.fr, p.02.

[3]-**محمد أمين الرومى المحامى**، النظام القانوني للتوقيع الإلكتروني، المرجع السابق، ص ص 31، 32.

استخدام هذه الوسائل شكلاً للمعلومة لا يتسنى للغير التعرف عليه، حيث يكون التطبيق العملي لذلك بواسطة مفتاحين: الأول مفتاح خاص لا يعرفه إلا المنشئ له، أما الآخر فهو مفتاح عام يكون معلوماً لغيره من المتعاملين معه، ويتم تشفير الوثيقة بواسطة المفتاح الخاص بالمرسل والـــذي نرمز له بالرمز ((س))، ثم تشفر بواسطة المفتاح العام للمرسل إليه الذي نشير إليه بالرمز ((ص)) والغرض من التشفير الأول التحقق من أن الرسالة من ((س)) أما الثاني فإنـــه لضمان سريتها، بحيث لا يتسنى فتحها إلا بالمفتاح الخـــاص عند ((ص)) وعند وصول الرسالة يستطيع ((ص)) فك التشفير الأول بواسطة المفتاح العـــام للتعرف على أنها مـــن عند ((س))، كما يستطيع أيضاً فك مضمونها عن طريق المفتاح الخاص به وهذا ما يطلق عليه التشفير المزدوج.

الفرع الثاني

مستـــويات التشفـــير

توجد عدّة مستويات للتشفير, فقد يكون على مستوى الإرسال، أو على مستوى التنقل أو التصفح، كما قد يكون على مستوى التطبيق أو التنفيذ، وأخيرا التشفير على مستوى الملفات، وسنتطرق لدراسة كل هذه المستويات على النحو التالي:

<u>أولاً</u>: التشفير على مستوى الإرسال.

يتمّ في هذا المستوى تشفير جميع المعلومات والبيانات بين نقطة الإرسال ونقطة الاستقبال، ويتم عن طريق الشبكات الافتراضية الخاصة[1]، وهي شبكات جزئية من شبكة الإنترنت، تقوم فيه إحدى المنشآت أو المشروعات بتخصيصه لخدمتها عن طريق إحاطته بالاحتياطات التأمينية المطلوبة لإرسال واستقبال المعلومات من خلاله بشكل آمن، أي

[1]- **أحمد محمد الهواري**، عقود التجارة الإلكترونية في القانون الدولي الخاص، بحث مقدم للمؤتمر العملي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، مركز البحوث والدراسات بأكادمية شرطة ذبي، الإمارات العربية المتحدة، الفترة 26-28 أفريل 2003، ص، ص25، 30.

تبادل المعلومات والبيانات بشكل آمن على شبكة الإنترنت، ويتم عن طريق تشفير جميع البيانات والمعلومات من نقطة الإرسال إلى نقطة الاستقبال[1].

ثانيًا: التشفير على مستوى التصفح أو التنقل.

وفقا لهذا المستوى يتم تشفير جميع الاتصالات بين نوافذ الشبكة أو أحد برامج التصفح وأحد مقار المعلومات أو المواقع الموجودة عليها، مما يؤدي إلى حماية البيانات أثناء انتقالها، وقد أعلنت شركة نت سكيب Netscape أحد البروتوكولات التأمينية عام 1995 وهو بروتوكول securesochatlayer والمعروف اختصارا بـ SSL، وتتصرف مهمة هذا البروتوكول نحو تشفير جميع الاتصالات على النحو المذكور سابقا، الأمر الذي يقلل من فرصة نسخ أو وصول البيانات إلى أيدي أي شخص غير مرغوب فيه وقصر وصولها للمستقبل النهائي، ممّا قد يعطي هذا الأمر شكلا من أشكال الثقة والائتمان للعملاء، لأنّ المعلومات والبيانات الخاصة بهم بما فيها أرقام بطاقة الائتمان، لن تكون متاحة سوى للتاجر، أو المنشأة أو المؤسسة المراد التعامل معها عن طريق هذه الشبكة دون غيرها.

عندما يرغب أحد المستهلكين في شراء سلعة عن طريق الإنترنت، يقوم بالدخول على الموقع أو الصفحة الخاصة بالمؤسسة المراد التعامل معها (web site)، وبعد اختيار الشيء المراد شراءه، يدخل إلى القناة أو الطريق الآمن لإتمام عملية الشراء، ممّا يؤدّي إلى انتقال الموقع على المقر أو الخادم الآمن(secure server)، عندها يتم تشفير جميع قنوات الاتصال والإرسال بين نافذة شبكة المعلومات ومقر المعلومات، ويتغير بداية اسم مقر المعلومات من http إلى http[2]- برتوكول SSL قد بدأ عمله أثناء إتمام الصفقة

---

[1]-**قدري عبد الفتاح الشهاوي**، المرجع السابق، ص 418.

[2]- بعد ظهور نظام الويب العالمي (www) وكانت الحاجة إلى لغة تسمح بربط مواقع الويب الموصولة بشبكة الانترنت فيما بينها وبالتجول داخلها، وهنا ظهر بروتوكول (HTTP) تعمل على حمل ونقل البيانات مباشرة بين الأطراف

L'application la plus connue d'internet est HTTP: Ce sont les pages webque Le protocole HTTP (utilisé par votre navigateur) utilise internet pour transporter des pages HTML, des images (jpeg, gif...musiques (MP3...) sur le site web: http://sebsauvage.net/comprendre/internet/index.html

التجارية-، وبمجرد وصول تلك البيانات إلى مقر المعلومات يتم حل الشفرة بواسطة برنامج خاص لاستخراج أمر الشراء، ويعتبر هذا البروتوكول الأكثر انتشارا واستخداما[1].

يوجد بروتوكول آخر لتأمين البيانات أثناء انتقالها بين أحد نوافذ شبكة الإنترنت وأحد مقار المعلومات، ويسمى هذا النظام ببروتوكول الاتصال الآمن S-http[2]، ويختلف هذا النظام عن نظام نت سكيب للتأمين، في أنّ النظام الأول –نظام بروتوكول الاتصال الآمن S-http- يقوم بحماية البيانات المنقولة ذاتها، بينما النظام الثاني –بروتوكول SSL- مهمته حماية قناة الاتصال أثناء انتقال البيانات من المرسل إلى المستقبل.

قامت بعض المؤسسات والشركات العاملة في مجال الإنترنت بضم النظامين السابقين، بروتوكول الاتصال الآمن ونظام نت سكيب للتأمين ليعمل كلاهما على توفير أكبر قدر من نظم التأمين للمعاملات التجارية التي تتم عبر الشبكة.

ثالثًا: التشفير على مستوى التطبيق أو التنفيذ.

يتمّ فيه تشفير طلب الشراء وعملية الدفع عبر شبكة online، وهو نظام تأمين المعاملات الإلكترونية SET[3]، ويعتبر هذا النظام من أهم البروتوكولات المتعلقة بالنواحي التي ظهرت في مجال منظومة التجارة الإلكترونية.

يتطلب العمل بنظام SET فتح حساب بنكي لكل من البائع والمشتري بأحد البنوك المستخدمة له، واستخدام المشتري لأحد برامج التصفح –نوافذ شبكة المعلومات- المدعم لنظام SET، واستخدام البائع لمقر معلومات SERVER يدعم هو الآخر ذلك النظام.

---

[1]-**قدري عبد الفتاح الشهاوي**، المرجع السابق، ص ص 419، 420.

[2]-اختصارا لـــ: Secure Hyper Text Transport Protocol .البروتوكول الأمن والعالمي المدى في نقل البيانات أنظر **عمر خالد زريقات**، المرجع السابق، ص ص40، 56.

[3]-اختصارا ل Secure Electronic Transaction بروتوكول الإخفاء المزدوج والدفين الأمن أنظر: **قدري عبد الفتاح الشهاوي**، المرجع السابق، ص 421.

عندما يقوم المشتري بفتح حساب في البنك يقوم هذا الأخير بإرسال كل من شهادة خاصة بالمشتري ومفتاحين للتشفير أحدهما خاص والآخر عام، يستخدم الأول لتشفير طلب الشراء وتوقيعه، بينما يستخدم الثاني لتوثيق وإرسال بيانات عملية الدفع، ويقوم البنك بتسليم كل من البائع والمشتري الشهادة الدالة على شخصية كل منهما بملف من ملفات الحساب الآلي، ويتم تبادل ملفات الشهادات بين البائع والمشتري أثناء الصفقة التجارية بصورة مشفرة بحيث لا يستطيع أي شخص من الخارج الإطلاع عليها، وبعد تأكد كلا من التاجر والمشتري من هوية الآخر، بتبادل الشهادات المشفرة وحل شفرتها تأتي الخطوة الأخيرة وهي عملية الدفع مقابل السلعة أو الخدمة المراد شرائها، ويتم ذلك عن طريق تشفير المشتري لرقم بطاقة الائتمان الخاصة به، ولا يستطيع حل هذه الشفرة سوى البنك الضامن لكل من البائع والمشتري، ويلزم أن يتأكد البائع من أن طلب الشراء الذي قام باستقباله هو نفس الطلب الذي تم إرساله من قبل المشتري عن طريق بصمة خاصة يحملها طلب الشراء، ويقوم البائع بعد ذلك بإرسال نسخة من طلب الشراء والبيانات الخاصة بإجراءات عملية الدفع إلى البنك، حيث ينتظر اعتماد البنك للصفقة بعد التأكد من هوية البائع وصحة الرسالة، وكذلك التأكّد من رصيد المشتري الذي يسمح بإتمام الصفقة، وهكذا يسمح للبائع بتكملة الصفقة التجارية على هذا الأساس، ويستطيع البائع أن يقوم بإرسال ما هو مطلوب شرائه إلى المشتري، سواء كان عبر شبكة المعلومات Online أو عن طريق إرساله بالطرق التقليدية التي تعتمد على النقل أو الشحن[1].

هذا وقد قامت شركة Visa في جمهورية مصر العربية خلال مارس 1999م بالإعلان عن إدخالها نظام SET لبنك مصر، بحيث يتم تأمين المعاملات التجارية والمالية

[1]-**قدري عبد الفتاح الشهاوي**، المرجع السابق، ص 423.

التي تجري عبر شبكة المعلومات من خلاله، ومن ثم أضحى هو البنك الضامن أو الطرف الثالث الموثوق به في إجراء المعاملات التجارية في مجال التجارة الإلكترونية[1].

رابعًا: التشفير على مستوى الملفات.

يتمّ التشفير هنا على مستوى الرسائل الإلكترونية والملفات التي يتم تداولها، فوفقا للبرنامج التأميني الذي وضعه فليب زيمرمان Philip Zimmerman لحماية الرسائل الإلكترونية عام 1995، والذي يطلق عليه اختصارا PGP[2]، يتم تشفير البيانات التي تحتويها الرسائل باستخدام أسلوب المفتاح العام Public Key، ويتميز هذا البرنامج بسهولة استخدامه، وفي نفس الوقت صعوبة الهجوم عليه.

يعتمد نظام PGP في حل الشفرة الخاصة بالرسالة المشفرة به على استخدام المفتاح الملائم لحل الشفرة، وهكذا فإن أي تجربة لأي مفتاح آخر غير المفتاح المطلوب لحل الشفرة يعتبر من المهام المستحيلة التي لا يمكن أن تنجح[3].

المبحث الثاني

التصديق الإلكتروني

تأتي الثقة والأمان في مقدمة الضمانات التي يجب توافرها لازدهار التجارة الإلكترونية، وهو الأمر الذي يستوجب توفير الوسائل التي تكفل تحديد هوية المتعاقدين والتعبير عن إرادتهم على نحو صحيح وبطريقة يمكن معها نسبة التصرف إلى صاحبه وهذه المشكلة هي الأخرى تتطلب إيجاد حلول تقنية لاسيما في ظلّ تنامي مخاطر القرصنة الإلكترونية وإساءة استخدام أسماء الغير وانتحالها في أنشطة غير مشروعة عبر شبكة الإنترنت.

---

[1]-**قدري عبد الفتاح الشهاوي**، نفس المرجع، ص 424.

[2]-اختصارا لـــ Pretty Good Privacy .

[3]- **قدري عبد الفتاح الشهاوي**، المرجع السابق، ص 421 .

لتفادي هذه المخاطر تم الاستعانة بطرف ثالث محايد موثوق به، يتمثل في جهة مختصة تقوم بدور الوسيط بين المتعاملين لتوثيق تعاملاتهم الإلكترونية، بإصدار شهادة تسمى بشهادة التصديق الإلكتروني، وذلك بعد التحقق من هوية الأطراف ومضمون التصرف وسلامته من العيوب[1].

نظرا لهذا الدور المهم الذي تقوم به هذه الجهات، فقد صدرت العديد من التشريعات التي تناولت تنظيمها بأحكام خاصة تجعلها خاضعة لإشراف الدولة ورقابتها، كما حدّدت مجموعة من الشروط يجب أن تلم بها هذه الجهات لمنحها ترخيص مهنة التصديق الإلكتروني، وهذه الشروط منها ما هو خاص بهذه الجهة المختصة بإصدار شهادات التصديق الإلكتروني، ومنها ما هو خاص بعملها، وقد اختلفت هذه الشروط من تشريع إلى آخر.

وبناءا على ما سبق نتطرق للجهة المختصة بإصدار شهادة التصديق الإلكتروني **(المطلب الأول)**، ثم نتناول خصوصيات شهادة التصديق الإلكتروني **(المطلب الثاني)**.

المطلب الأول

الجهة المختصة بإصدار شهادة التصديق الإلكتروني

تعتمد التجارة الإلكترونية في إجراءاتها على شبكة اتصال مفتوحة، كما أن غالبية العقود التي تتم بين أطرافها تعتبر من العقود المبرمة بين غائبين، وذلك بسبب اختلاف زمان ومكان التعاقد، وغياب الحضور المادي للمتعاقدين[2]، ممّا استلزم وجود طرف ثالث محايد يتمثل في أفراد أو شركات أو جهات مستقلة، تقوم بإصدار شهادات تسمى "شهادات

[1]- **سمير حامد عبد العزيز الجمال**، المرجع السابق، ص 320.

[2]- **المنزوالي صالح**، القانون الواجب التطبيق على عقود التجارة الإلكترونية: دار الجامعة الجديدة، 2006، ص 18.

التصديق الإلكتروني" تؤكّد فيها صحة هوية وتوقيعات الأطراف المتعاقدة إلكترونيا، تسمى هذه الجهات "بجهات التصديق أو التوثيق الإلكتروني"[1].

لبيان المزيد عن الجهات المختصة بإصدار شهادات التصديق الإلكترونية، نقسم هذا المطلب إلى: تعريف الجهة المختصة بإصدار شهادات التصديق الإلكتروني **(الفرع الأول)**، دور الجهة المختصة بإصدار شهادات التصديق الإلكترونية **(الفرع الثاني)** وأخير مسؤولية جهات التصديق الإلكتروني **(الفرع الثالث)**.

الفرع الأول

تعريف الجهة المختصة بإصدار شهادات التصديق الإلكتروني

إختلف الفقه والقانون المقارن في الاصطلاح الذي يطلق على الجهة المختصة بإصدار شهادات التصديق الإلكتروني، حيث يستخدم جانب من الفقه اصطلاح "سلطة الإشهار" ويعرفها بأنها "**هيئة عامة أو خاصة تسعى إلى ملء الحاجة الملحة لوجود طرف ثالث موثوق،يقدم خدمات أمنية في التجارة الإلكترونية، بأن يصدر شهادات تثبت صحة حقيقة معينة متعلقة بموضوع التبادل الإلكتروني لتوثيق هوية الأشخاص المستخدمين لهذا التوقيع الرقمي، وكذلك نسبة المفتاح العام المستخدم إلى صاحبه**"[2].

يطلق عليها جانب ثان من الفقه اصطلاح "مقدم خدمات التصديق" ويعرفه بأنه: "**هيئة أو مؤسسة عامة أو خاصة تستخرج شهادات إلكترونية، وتكون هذه الشهادات بمثابة سجل إلكتروني يؤمن التوقيع الإلكتروني ويحدد هوية الموقع، ومعرفة المفاتح العام، وتعتبر شهادة**

---

[1]- **الدسوقي أبو الليل**، توثيق التعاملات الإلكترونية ومسؤولية جهة التوثيق تجاه الغير المضرور، بحث مقدم إلى مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، الذي نظمته كلية الشريعة والقانون في جامعة الإمارات العربية المتحدة، بالتعاون مع غرفة التجارة وصناعة ذبي، في الفترة ما بين 10 و 12 ماي 2003، المجلد الخامس، ص 1856، الموقع:
http://www.unue.banque.com/imarat/arab/12/3398.pdf

[2]-**عايض راشد عايض المري**، المرجع السابق، ص 100.

التصديق بمثابة بطاقة هوية إلكترونية تستخرج من شخص مستقل ومحايد ومرخص له بمزاولة هذا النشاط"[1].

يرى جانب أخر من الفقه استخدام اصطلاح "مقدم خدمات التصديق الإلكتروني" وذلك لتميزه عن جهات التصديق التقليدية، ويعرف بأنه:" **شخص طبيعي أو معنوي يستخرج الشهادات الإلكترونية، ويقدم الخدمات الأخرى المرتبطة بالتوقيعات الإلكترونية، ويضمن تحديد هوية الأطراف المتعاقدة والاحتفاظ بهذه البيانات لمدة معينة، ويلتزم باحترام القواعد المنظمة لعمله، والتي يتم تحديدها بمعرفة السلطة المختصة"**[2].

يعرف جانب آخر من الفقه مقدم خدمات التصديق بأنه:"**جهة أو منظمة عامة أو خاصة، تستخرج شهادات إلكترونية والشهادة هذه تؤمن صلاحية الموقع وحجية توقيعه وكذلك التأكد من هوية الموقع، وتوقع هذه الشهادة من شخص له الحق في مزاولة هذا العمل"**[3].

استخدم قانون الأمم المتحدة النموذجي بشأن التوقيعات الإلكترونية لسنة 2001م اصطلاح "مقدم خدمات التصديق" ووفقا للمادة (2/هـ) التي تطرقت إلى تعريف مقدم خدمات التصديق فإنه يقصد به "**شخصا يصدر الشهادات ويجوز أن يقدم خدمات أخرى ذات صلة بالتوقيعات الإلكترونية**".

أما التوجيه الأوربي رقم 93 لسنة 1999م بشأن التوقيع الإلكتروني فقد استخدم اصطلاح "مقدم خدمة التصديق" وفقا للمادة (11/2) منه فإنه يقصد بمقدم خدمة التصديق" **كل كيان أو شخص طبيعي أو معنوي يصدر شهادات توثيق التوقيع الإلكتروني، أو يتولى تقديم خدمات أخرى متصلة بالتوقيعات الإلكترونية** "[4] ، والمقصود بالخدمات المتصلة بالتوقيع

---

[1]- أنظر **SEDALLIAN Valerie**, Preuve et signature électroniqu eop. cit. P5. على موقع:
http://www.juriscom.net/chr2/fr20000509.htm

[2]-**سمير حامد عبد العزيز الجمال**، المرجع السابق، ص 322.

[3]-**سعيد السيد قنديل**، المرجع السابق، ص 75.

[4]-نص المادة (11/2) من التوجيه الأوربي 93 لسنة 1999م:
"Prestataire de service de certification " toute entité ou personne Physique ou morale qui délivre des certificats ou fournit d'autres services lies aux signatures électroniques. http://www.ec.europa.eu.

الإلكتروني، التقنيات التي من خلالها يتم إصدار خدمات النشر أو الإطلاع أو إصدار توقيع مؤرخ أو إصدار الخدمات المعلوماتية الأخرى كالحفظ في الأرشيف[1].

ووفقا للمادة (13/2) من هذا التوجيه، والتي نظمت الجهة المختصة بمنح تراخيص مزاولة نشاط خدمات التصديق، حيث يمنح هذا الترخيص بناء على طلب مقدم خدمات التصديق، يتقدم به إلى الجهة التي تعهد إليها الدولة بمنح هذه التراخيص سواء كانت هيئة عامة أو خاصة، ويتعين على مقدم خدمة التصديق حتى يكون مؤهلاً لإصدار شهادات تصديق معتمدة، أن تتوافر فيه الشروط والضوابط التي تفيد كفاءته المهنية في هذا المجال.

رغم تنظيم التوجيه الأوربي لجهات التوثيق الإلكتروني أو مقدم خدمة التصديق إلاّ أنّه لم يجعل هذا التصديق إلزاميا وإنّما ترك للأطراف حرية اللجوء إليه[2].

أمّا في القانون التونسي رقم 83 لسنة 2000م بشأن المبادلات والتجارة الإلكترونية، استخدم المشرّع التونسي اصطلاح "مزود خدمات المصادقة الإلكترونية" بالنسبة للجهة المختصة بإصدار شهادات التصديق الإلكترونية، ووفقا للفصل الثاني من الباب الأول من هذا القانون فإنه يقصد بمزود خدمات المصادقة الإلكترونية: "**كل شخص طبيعي أو معنوي يحدث ويسلم ويتصرف في شهادات المصادقة ويسدي خدمات أخرى ذات علاقة بالإمضاء الإلكتروني**".

كما أنشأ المشرع التونسي "الوكالة الوطنية للمصادقة الإلكترونية" واعتبرها مؤسسة عامة، تتمتع بالشخصية المعنوية وبالاستقلال المالي وتخضع في علاقاتها مع الغير إلى

[1]- **ثروت عبد الحميد**، المرجع السابق، ص 163 .

[2]- **إبراهيم الدسوقي أبو الليل**، المرجع السابق، ص180.

التشريع التجاري التونسي، ومقرها بتونس العاصمة[1]، وقد حدّد في الفصل التاسع من الباب الثالث من القانون السابق الذكر أهداف هذه الوكالة والتي تتلخص في ما يلي[2]:

1) منح تراخيص مزاولة نشاط خدمات المصادقة الإلكترونية على كامل تراب الجمهورية التونسية.

2) السهر على مراقبة احترام مزود خدمات المصادقة الإلكترونية للقانون.

3) تحديد مواصفات منظومة إحداث التوقيع الإلكتروني.

4) إصدار وتسليم وحفظ شهادات المصادقة الإلكترونية الخاصة بالأطراف المؤهلة للقيام بالمبادلات التجارية.

5) المساهمة في أنشطة البحث والتكوين والدراسة المتعلقة بالمبادلات والتجارة الإلكترونية.

6) إبرام اتفاقيات الاعتراف المتبادل الخاص بمزودي خدمات التصديق الإلكتروني مع الأطراف الأجنبية[3].

هذا ويتعيّن على كلّ من يرغب في ممارسة نشاط مزود خدمات المصادقة الإلكترونية الحصول على ترخيص مسبق من الوكالة الوطنية للمصادقة الإلكترونية ويشترط فيه للحصول على هذا الترخيص توافر العديد من الشروط[4].

أمّا قانون المعاملات الإلكتروني الأردني رقم 85 لسنة 2001 فلم يورد أي تعريف للجهة المختصة بإصدار شهادات التصديق الإلكترونية، حيث خول المشرع الأردني مجلس الوزراء إصدار الأنظمة والأحكام التي تحدد الجهة التي تشرف على ترخيص

---

[1]-انظر الفصل الثامن من الباب الثالث من القانون التونسي رقم 83 لسنة 2000م بشأن المبادلات والتجارة الإلكترونية متوفر على الموقع الإلكتروني: http://www.tunisia-cafe.com/vb/showthread.php?t=8878

[2]- انظر الفصل التاسع نفس القانون على الموقع: http://www.tunisia-cafe.com/vb/showthread.php?t=8878

[3]-أنظر الفصل الثالث والعشرون من الباب الرابع من نفس المرجع

[4]- أنظر الفصل الخامس عشر من الباب الرابع من نفس المرجع

مقدمي خدمات التصديق، وطرق وإجراءات إصدار الشهادات، وسائر الأمور المرتبطة بها[1].

أمّا عن المشرّع الإماراتي فقد استخدم اصطلاح "مزود خدمات التصديق" على الجهة المختصة بإصدار شهادات التصديق الإلكتروني وذلك في قانون المعاملات والتجارة الإلكترونية رقم 2002/2، ووفقا للمادة (20/2) من الفصل الأول من هذا القانون يقصد بمزود خدمات التصديق "**أي شخص أو جهة معتمدة أو معترف بها تقوم بإصدار شهادات تصديق الكترونية أو أية خدمات أو مهمات متعلقة بها وبالتوقيع الإلكتروني بموجب أحكام الفصل الخامس من هذا القانون**".

يقوم بمهمة الإشراف على خدمات المصادقة الإلكترونية مراقب لخدمات التصديق يتم تعيينه بقرار يصدره رئيس سلطة منطقة دبي الحرة للتكنولوجيا والتجارة الإلكترونية وذلك وفقا لما نص عليه المشرّع الإماراتي في المادة (23) من الفصل الخامس من القانون السابق الذكر، وحسب هذه المادة أيضاً يقوم مراقب خدمات التصديق بمنح تراخيص أنشطة مزودي خدمات التصديق، ومراقبتها والإشراف عليها. كما يجوز لمراقب خدمات التصديق أن يفوض كتابيا غيره في القيام ببعض مسؤولياته، هذا وقد اعتبر المشرّع الإماراتي كلّ من المراقب والمفوض من قبله موظفاً عاماً بشأن ممارسة مهام وظيفته، وهذا لإعطاء القرارات الصادرة عنهما القوة التنفيذية الخاصة بالقرارات الصادرة بموظفي الدولة[2].

أمّا قانون التوقيع الإلكتروني المصري رقم 2004/15، فلم يضع تعريفا لهذه الجهة المختصة بإصدار شهادات التصديق الإلكتروني، إلاّ أنّ اللائحة التنفيذية لهذا القانون قد عرفت هذه الجهة وذلك في المادة (6/1)، التي تنص على أن جهة التصديق الإلكتروني

[1]-أنظر المادة (40/ب) من القانون الأردني رقم 2001/85 بشأن المعاملات الإلكترونية على الموقع الإلكتروني: http://old.openarab.net/ar/node/250

[2]- **عبد الفتاح بيومي حجازي**: التوقيع الإلكتروني في النظم القانونية المقارنة، المرجع السابق، ص 202.

هي:"**الجهة المرخص لها بإصدار شهادة التصديق الإلكتروني، وتقدم خدمات تتعلق بالتوقيع الإلكتروني**".

أنشأ المشرّع المصري هيئة عامة تسمّى "هيئة تنمية صناعة تكنولوجية المعلومات"[1] تكون لها الشخصية الاعتبارية العامة وتتبع وزير الاتصالات والمعلومات مقرها الرئيسي محافظة الجيزة، ويجوز لها إنشاء فروع في جميع أنحاء جمهورية مصر العربية[2].

وفقاً لنص المادة (3) من قانون التوقيع الإلكتروني المصري رقم 2001/15 تهدف هيئة تنمية صناعة تكنولوجيا المعلومات إلى تحقيق الأغراض التالية:

- تشجيع وتنمية صناعة تكنولوجيا المعلومات والاتصالات.
- نقل التكنولوجيا المتقدمة للمعلومات، وتحقيق الاستفادة منها.
- زيادة فرص تصدير خدمات الاتصال، وتكنولوجيا المعلومات ومنتجاتها.
- الإسهام في تطوير، وتنمية الجهات العامة في مجال تكنولوجيا المعلومات والاتصالات.
- توجيه وتشجيع، وتنمية الاستثمار في مجال تكنولوجيا المعلومات والاتصالات.
- رعاية المصالح المشتركة لأنشطة تكنولوجيا المعلومات.
- دعم البحوث والدراسات في مجال تكنولوجيا المعلومات والاتصالات وتشجيع الاستفادة بنتائجها.
- تشجيع ودعم المشروعات الصغيرة والمتوسطة في مجال استخدام وتوظيف آليات المعاملات الإلكترونية.
- تنظيم نشاط خدمات التوقيع الإلكتروني وغيرها من الأنشطة في مجال المعاملات الإلكترونية و صناعة تكنولوجيا المعلومات.

[1]- الموقع الإلكتروني لهيئة تنمية صناعة تكنولوجيا المعلومات: http://www.itida.gov.eg/E-signature-root-ca.agp

[2]-أنظر المادة (2) من القانون المصري رقم 2004/15م بشأن تنظيم التوقيع الإلكتروني.

أقرّ المشرّع المصري في هذا القانون العديد من الاختصاصات لهيئة تنمية صناعة تكنولوجيا المعلومات، أهمّها منح وتجديد تراخيص مزاولة نشاط خدمات التوقيع الإلكتروني، متابعة ومراقبة نشاط مقدمي خدمات التصديق الإلكتروني[1]، الذين يعهد إليهم بإنشاء منظومة التوقيع الإلكتروني، تحديد معاييرها، ضبط مواصفاتها الفنية، وإصدار شهادة تصديق بصحة التوقيع الإلكتروني وكذلك التصديق على المعاملات الإلكترونية[2].

كما ألزم المشرّع المصري جهات التصديق الإلكتروني قبل مزاولة نشاط إصدار شهادات التصديق الإلكتروني، ضرورة الحصول على ترخيص من هيئة تنمية صناعة تكنولوجيا المعلومات[3]، نظير مقابل يحدده مجلس إدارتها، وفقا للإجراءات والقواعد والضمانات المقررة قانوناً، دون التقيد بأحكام قانون إلتزامات المرفق العام رقم 1974/129 ، مع مراعاة ما يلي:

1) أن يتم اختيار المرخص له في إطار من المنافسة والعلانية.

2) أن يحدد مجلس هيئة تنمية صناعة تكنولوجيا المعلومات مدة الترخيص بحيث لا تزيد عن تسعة وتسعين عاماً.

3) أن تحدد وسائل الإشراف، والمتابعة الفنية والمالية التي تكفل حسن سير المرفق بانتظام و اطراد[4].

---

[1]-أنظر المادة (4) من القانون المصري رقم 15 لسنة 2004 بشأن تنظيم التوقيع الإلكتروني.

[2]-**سمير حامد عبد العزيز الجمال**،المرجع السابق، ص333.

[3]-تم منح الترخيص لأربعة شركات لتقديم خدمات التوقيع الإلكتروني، وهي (التسجيل وإصدار شهادات التصديق الإلكتروني، إصدار أدوات إنشاء وتثبت التوقيع الإلكتروني، خدمة حفظ مفاتيح الشفرة الخاصة المصدرة لمستخدمي الخدمة)، وذلك بعد التقييم الفني والمالي للعروض المقدمة من الشركات من طرف هيئة تنمية وصناعة تكنولوجيا المعلومات وهذه الشركات وهي:

-شركة المحاسبة المتقدمة (Advanced computer technology [ACT])-

-شركة مصر المقاصة (Misr for clearance, Depositary and central Registry, [MCDR])-

-شركة إيجبت ترست (Egypt TRUST) -

-الشركة المصرية لخدمات الشبكات وتأمين المعلومات (Security & Network services [SNS])

أنظر الموقع الإلكتروني: http://www.itida.gov.eg/e-signature-root.

[4]-أنظر المادة (19) من قانون التوقيع الإلكتروني المصري رقم 2004/15م.

ويكون لهيئة تنمية صناعة تكنولوجيا المعلومات كامل السلطة في إلغاء الترخيص بمزالة نشاط إصدار شهادات التصديق الممنوح لجهات التصديق الإلكتروني، عند مخالفتها لشروط الترخيص حتى يتم إزالة أسباب المخالفة[1].

كما تختص الهيئة باعتماد الجهات الأجنبية المختصة بإصدار شهادات التصديق الإلكتروني، مقابل النظير الذي يحدده مجلس إدارة الهيئة، وهذا الاعتماد يتم وفقا للقواعد والإجراءات والضمانات التي تقررها اللائحة التنفيذية.

الفرع الثاني

دور الجهة المختصة بإصدار شهادات التصديق الإلكترونية

يكمن الهدف الأساسي من إنشاء جهات مختصة في إصدار شهادات التصديق الإلكتروني في الدور الذي تقوم به، من خلال التحقق من هوية الشخص الموقع (المرسل) وصلاحية توقيعه وتحديد أهليته القانونية للتعامل والتعاقد[2].

لا يقتصر دور جهات التصديق أو التوثيق الإلكتروني على تحديد هوية المتعاملين أو تحديد أهليتهم القانونية، بل يتعدى إلى التحقق من مضمون هذا التعامل أو التبادل الإلكتروني، وسلامته وكذلك جديته وبعده عن الغش والاحتيال[3].

كما تقوم هذه الجهات بإصدار التوقيع الرقمي وإصدار المفاتيح الإلكترونية سواء المفتاح الخاص الذي يتم بواسطته تشفير البيانات والمعاملات الإلكترونية، أو المفتاح العام الذي يتم بمقتضاه فك التشفير. إذن فلجهات التصديق الإلكتروني عدة أدوار، يمكن إجمالها فيما يلي:

---

[1]-أنظر المادة (26) من قانون التوقيع الإلكتروني المصري رقم 2004/15م والمادة (23) من اللائحة التنفيذية لهذا القانون.

[2]- **سعيد السيد قنديل**، المرجع السابق، ص75.

[3]-**إبراهيم الدسوقي أبو الليل**، المرجع السابق، ص178.

أولاً: التحقق من هوية الشخص الموقع.

يتمثّل الدور الرئيسي لجهات التصديق الإلكتروني في تمكين المرسل إليه التأكد من هوية المرسل وصلاحية توقيعه، حيث تقوم بإصدار شهادة تصديق إلكترونية تفيد التصديق على التوقيع الإلكتروني المستخدم في تعاقد معين، كما تفيد أيضا بموجب هذه الشهادة صحة التوقيع ونسبته إلى من صدر عنه (الشخص الموقع).

عندما يضع أحد الأطراف توقيعه الإلكتروني على محرر إلكتروني ويقوم بإرساله إلى شخص آخر، فإن جهة التصديق الإلكتروني تصدر شهادة إلكترونية وظيفتها الربط بين الموقع ومفتاحه العام، بحيث تحتوي هذه الشهادة على البيانات الخاصة بصاحبها كاسمه وسلطته في التوقيع بحيث أن هذه البيانات التي تحتويها الشهادة تحدد للمرسل إليه هوية المرسل – الموقع –، وبعد أن يتأكّد المرسل إليه من صلاحية الشهادة الإلكترونية المرسلة له – من خلال الجهة التي أصدرتها – يعول على المحرر الإلكتروني، وهكذا يتم التبادل بين المرسل والمرسل إليه حتى يتم التوصل إلى الاتفاق النهائي[1].

يمكن أن يمتدّ دور جهة التصديق الإلكتروني في التحقق إلى تحديد الأهلية القانونية للمتعاقد، وكذا التحقق من مسألة سلطة هذا الشخص في إبرام التعاقد، فقد يتجاوز هذا الشخص حدود اختصاصاته وسلطاته[2].

كما يقع على عاتق جهة التصديق الإلكتروني إنشاء سجل إلكتروني لشهادات التصديق الإلكتروني توضح فيه ما هو قائم من هذه الشهادات وما ألغي أو أبطل منها وما تمّ إيقافه أو علق العمل بها[3].

---

[1]- **وسيم شفيق الحجار**، المرجع السابق، ص211.

[2]- **محمد محمد أبو زيد**، المرجع السابق، ص203.

[3]- **إبراهيم الدسوقي أبو الليل**، المرجع السابق، ص 179، أنظر الفصل الرابع عشر القانون التونسي رقم 38 لسنة 2000م.

ثانياً: إثبات مضمون التبادل الإلكتروني.

تقوم الجهة المختصة بإصدار شهادات التصديق الإلكتروني كذلك بالتحقق من مضمون التعامل أو التبادل الإلكتروني بين الأطراف المتعاقدة، وكذلك التيقن من سلامته وجديته وبعده عن الغش والاحتيال، إضافة إلى إثبات وجوده ومضمونه[1]، حماية للمتعاملين من أيّ غش قد يقعون فيه أثناء تعاملاتهم، حيث نجد أنّ جهات التصديق الإلكتروني تقوم بتعقب المواقع التجارية على الإنترنت للتحري عن جديتها أو مصداقيتها فإذا اتضح لها أن هذه المواقع غير حقيقية أو غير جدية فإنّها تقوم بتوجيه رسائل تحذيرية للمتعاملين توضح فيها عدم مصداقية هذه المواقع[2].

كما تتولى جهة التصديق الإلكتروني تحديد وقت ولحظة إبرام العقد، والقاعدة العامة أنّه عند عدم وجود نص خاص فلا يعد تاريخ إبرام العقد شرط ضروريا لصلاحية التصرف، فتحديد لحظة إبرام العقد تعد مؤشرا لتحديد موعد ترتيب الآثار القانونية لهذا العقد[3]، كتحديد لحظة تمام عملية التحويل المصرفي الإلكتروني له عدّة آثار، من ذلك تحديد إنهاء أو عدم إنهاء التحويل عند إفلاس أحد الأطراف، وأيضا تحديد جواز رجوع الأمر في تحويله مادام المبلغ لم يخرج من ذمته إلى ذمة المستفيد. أمّا عند التحويل، فإنّ ذلك يؤدي إلى عدم جواز التصرف في المبلغ المالي محل الأمر بالتحويل[4].

لتحديد لحظة إبرام التعامل أو التبادل الإلكتروني أهمية أخرى تتمثل في تحديد مدّة التقادم، التي يمكن أن ترد على مثل هذه التصرفات القانونية، وما يترتب من إجراءات قاطعة أو موقفة لهذا التقادم، لذا فإنّ تحديد لحظة إبرام العقد يتعين أن يتمّ من خلال جهات التصديق الإلكتروني والتي تعمل على تحديد تاريخ واحد لإبرام العقد الإلكتروني[5].

---

[1]- **إبراهيم الدسوقي أبو الليل**، المرجع السابق ، ص178.

[2]- **إبراهيم الدسوقي أبو الليل**، المرجع نفسه، أنظر هامش رقم 193 الصفحة رقم 178.

[3]-**سعيد السيد قنديل**، المرجع السابق، ص105.

[4]-**إيمان مأمون أحمد سليمان**، المرجع السابق، ص314.

[5]-**سعيد السيد قنديل**، المرجع نفسه، ص106.

ثالثاً: إصدار المفاتيح الإلكترونية.

تقوم جهات التصديق الإلكتروني بإصدار مفاتيح التشفير الإلكتروني، سواء المفتاح الخاص الذي من خلاله يتم تشفير المعاملة الإلكترونية الذي يكون خاصا بصاحبه ولا يعلمه غيره، أو المفتاح العام الذي يتمّ بواسطته فك هذه الشفرة، يكون هذا المفتاح متاحا للكافة. كما تصدر جهات التصديق الإلكتروني المفتاح الشفري الجذري الذي ينشأ بواسطة عملية حسابية، تستخدمه لإنشاء شهادات التصديق الإلكتروني وبيانات إنشاء التوقيع الإلكتروني[1].

تتولّى جهات التصديق الإلكتروني إصدار التوقيع الرقمي، وتكون إجراءات إصدار هذا التوقيع بتقديم البيانات اللازمة من طالب تصديق التوقيع إلى جهة التصديق، مع بيان الأشخاص المخولين بالتوقيع، ليصدر لكل منهم مفتاح خاص، وبعد هذا الإجراء يتم إصدار المفتاح الخاص بحيث يتم تثبيت نصف هذا المفتاح بجهاز الحاسب الآلي لطالب تصديق التوقيع الإلكتروني، أمّا النصف الآخر من المفتاح فيتم تثبيته ببطاقة إلكترونية ذكية، لذلك فإن المفتاح الخاص الذي يتم استخدامه في التوقيع لا يمكن العمل به إلاّ من جهاز حاسب آلي واحد فقط، حتى يمكن التأكّد من أنّ التوقيع الرقمي صادر بالفعل من صاحبه، ويحتفظ الموقع بالمفتاح الخاص لديه ولا يطلع عليه أي شخص بحيث يكون سريا لا يعلمه إلى صاحبه، أما المفتاح العام والذي تحتفظ به عادة جهة التصديق، فتقوم هذه الأخيرة بإرساله عن طريق البريد الإلكتروني إلى من يرغب في التعامل مع صاحب التوقيع الإلكتروني، إذ بمقتضى هذا المفتاح العام يتم التحقق من هوية الشخص ومن صحة توقيعه[2].

---

[1]- أنظر المادة (1) من اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري أنظر الموقع الإلكتروني:
http://ar.jurispedia.org/index.php/

[2]-**إبراهيم الدسوقي أبو الليل**،المرجع السابق، ص178.

إزاء الأدوار المنوطة بها جهات التصديق الإلكتروني، فإن هناك شروط يجب أن تتوافر لدى هذه الجهات كي تتمكن من أداءها، تتميز معظم هذه الشروط بالطابع الفني والتقني، مثل التزام الجهة المختصة عند إصدار شهادات التصديق الإلكتروني باستعمال وسائل وأنظمة موثوق بها في إصدار هذه الشهادات واتخاذ كافة الوسائل اللازمة لحمايتها من أي تقليد أو تدليس أو استعمال غير مشروع[1].

كما تلتزم الجهة المختصة بإصدار شهادات التصديق بالبيانات المقدمة لها من أصحاب الشأن، ويقع على عاتقها الالتزام بالمحافظة على سرية هذه البيانات والمعلومات الخاصة بهؤلاء الأشخاص المشتركين[2].

كذلك على الجهة المختصة بإصدار شهادات التصديق الإلكتروني أن توفر لمن يعول على الشهادة الإلكترونية الوسائل التي تؤكد له أن الموقع المحددة هويته في الشهادة الإلكترونية، كان لديه وقت التوقيع السيطرة على الأداة الفنية اللازمة للتوقيع، وأنها كانت وقت التوقيع سارية المفعول[3].

---

[1]-أنظر المادة (2/9) من قانون الأونسيترال بشأن التوقيعات الإلكترونية 2001م/ المادة (24/ب) من قانون إمارة دبي رقم 2002/2، الفصل (13) من الباب الرابع من قانون المبادلات والتجارة الإلكترونية التونسي رقم 2000/83، المادة (3) والمادة (12/ز) من اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري رقم 2004/15 أنظر على الموقع الإلكتروني:
http://www.uncitral.org/pdf/arabic/texts/electcom/ml-elecsig-a.pdf

[2]-المادة (21) من قانون التوقيع الإلكتروني المصري رقم 2004/15م والمادة (2/12) من لائحته التنفيذية.

[3]-المادة (4/9) من قانون الأونسيترال بشأن التوقيعات الإلكترونية 2001م، المادة (24/ج/2) من قانون إمارة دبي رقم 2002/2م، على الموقع الإلكتروني http://www.ecipit.org.eg/arabic/pdf/Dubi_low.pdf المادة (3/هـ) من اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري.

الفرع الثالث

مسؤولية جهات التصديق الالكتروني

يطرح الحديث عن مسؤولية مقدم خدمة التصديق نفسه عندما يخل القائم بهذه الخدمة بأحد الالتزامات المفروضة عليه، هذه المسؤولية تكون غاية في الأهمية عندما يوجد خطأ في الشهادة، مع ذلك يكون القائم على خدمة التصديق مسؤولا عن صحة البيانات التي صدق عليها، وعن نسبة التوقيع لصاحبه في تاريخ تسليم الشهادة لمن يتسلمها[1]، تقوم هذه المسؤولية طبقا للمادة 1/8 من التوجيه الأوربي المتعلق بالتوقيع الالكتروني، وتقريبا من ذلك المادة 8 من القانون النموذجي للجنة القانون التجاري الدولية التابعة للأمم المتحدة[2]، إلا أنه يجوز لمقدم خدمات التصديق إثبات عدم وجود أي خطأ من جهته، وأنه قام بواجبه كما ينبغي من حفظ لسرية البيانات الشخصية الخاصة بعملائه وصحة البيانات المدونة على الشهادة التي يصدرها ونسبتها لصاحبها، ولا ريب في أنّ عبء الإثبات الذي يقع على عاتق مقدم خدمة التصديق هو أمر في غاية الدقة والتعقيد.

لكي يضمن مقدم خدمة التصديق صحة المعلومات التي تتضمنها الشهادة التي يصدرها، فإنه يقع على عاتقه التحقق من هوية الأطراف الموقعة، وله في سبيل ذلك أن يطلب من الأطراف ما يفيد صحة البيانات والمعلومات، بيد أنه عند ثبوت حدوث تزوير من صاحب الشأن في هذه البيانات، فإن مقدم خدمة التصديق لا يكون مسئولا في هذه الحالة. كما أنه يقع على عاتق صاحب الشأن أن يخطر مقدم خدمة التصديق بكل تغيير أو تعديل في هذه البيانات التي تحتويها الشهادة، وإلاّ فإنّه يكون هو المسئول عن صحتها، إلاّ

[1] - **سعيد السيد قنديل**، المرجع السابق، ص92. أنظر كذلك:
ESNAULT Julien, la signature électronique, op cite, p47.

[2] - **حمودي ناصر**، المرجع السابق، ص319.

أنّ مقدم خدمة التصديق الالكتروني يكون مسئولا في حالة نسيانه تسجيل إلغاء الشهادة أو في حالة وجود أي إهمال من جانبه يؤدي إلى إلحاق ضرر بالغير[1].

كي يضمن مقدم خدمة التصديق صحة البيانات الواردة في الشهادة له عند إصدارها أن يطلب من طالبها كل ما يفيد من وثائق تأكد هويته، والتي لا يتحمل مسؤولية تزويرها من قبل مقدمها[2]، كما أنّه يجب على الغير أن يتأكد من صلاحية شهادة التصديق من حيث مدتها وما لحقها من تعديل أو إلغاء، والغرض من استخدامها، وذلك بالرجوع إلى السجل الالكتروني الذي ينشره مقدم خدمة التصديق عبر الانترنت[3].

نظرا لأهمية شهادةالتصديق الالكتروني، وخطورة المعلومات التي تتضمنها والتي يعول عليها الغير لدى إتمام تعاملاتهم، فإنّ دور جهات التصديق الالكتروني أصبح على قدر واسع من الأهمية، لكونها تؤمن حلقة الوصل بين المتعاملين الذين قد لا يتعارفون ويبرمون تعاملاتهم على أساس الثقة التي توفرها لديهم جهات التصديق الالكتروني، فإنّه كان لزاما تحديد المسؤوليات في حالة حدوث إخلال بالالتزامات المناطة بجهات التوثيق الالكتروني[4]، حيث بقدر المسؤولية التي تتحملها هاته الجهات تكون الثقة التي تؤمنها لدى المتعاملين.

---

[1]- **سمير حامد عبد العزيز الجمال**، المرجع السابق، ص346. أنظر كذلك:

CONDOUThierry Piette, Op Cit, p28.

[2]- **سعيد السيد قنديل**، المرجع السابق، ص95.

[3]- **سمير حامد عبد العزيز الجمال**، المرجع نفسه، ص 346.

[4]- ويرجع عدم صحة المعلومات التي تتضمنها شهادات التوثيق الالكتروني إلى العديد من الأسباب، منها فشل هذه الجهات في الحصول على دليل صحيح يوضح هوية صاحب التوقيع، أو عدم دقة وسائل التشفير المستخدمة في ربط صاحب المفتاح العام الموجود لدى جهة التوثيق، من ذلك أيضا عدم إمساك جهاتالتوثيق لدفاتر وسجلات ملائمة لحفظ المعلومات، أو عدم متابعة هذه السجلات ومراجعتها وتحديثها أول بأول، وقد يرجع ذلك أيضا إلى استخدام جهات التوثيق لموظفين وعمال غير مهرة أو غير مدربين أو غير أمناء، مشار إليه لدى: **إبراهيم الدسوقي أبو الليل**، الجوانب القانونية للتعاملات الالكترونية، المرجع السابق، ص188. أنظر كذلك:

THIEFRY Patrick : l'émergence d'un droit européen du commerce électronique, revue trimestrielle du droit européen, p672.

إنّ المسؤولية عن الأضرار التي تحدث للغير بصفة عامة، هي أحد أهم الموضوعات القانونية التي تتعرض لها الأنظمة القانونية وتضع لها قواعد عامة تحكمها. لكن كثيرا ما يتدخل المشرع بالنسبة لحالة خاصة من حالات المسؤولية، حيث يرى عدم كفاية القواعد في المسؤولية لتنظيمها ويضع لها قواعد خاصة بها يخالف فيها القواعد والأحكام العامة وجه أو أكثر، سواء فيما يتعلق بشروط قيام المسؤولية أو الأضرار التي تعوض، أو قدر التعويض وكيفيته، أو الإعفاء من المسؤولية.

هذا ما حدث فعلا بالنسبة لمسؤولية جهات التوثيق عن الأضرار التي تلحق الغير الذي يعود على صحة شهادات التوثيق الالكترونية التي تصدرها، فأمام عدم كفاية القواعد العامة في المسؤولية المدنية لتنظيم مسؤولية هذه الجهات، تدخل المشرع في بعض الأنظمة ووضع قواعد خاصة بمسؤولية جهات التصديق الالكتروني حديثة للغاية، حيث أنها ترتبط بالاعتراف بالتوقيع الالكتروني في الكتابة الالكترونية[1].

نجد المشرع الفرنسي لم يورد أي نص يتعلق بالتزامات مقدمي خدمة التصديق الالكتروني ولم يحدد نطاق مسؤوليتهم، لكن هذا الأمر لا يخرج عن نطاق الأحكام الواردة في التوجيه الأوربي المتعلقة بالمسؤولية، كون أحكام التوجيه تشمل دول الاتحاد الأوربي ومنها فرنسا[2].

بينما نجد المشرع التونسي قد جعل صاحب الشهادة المسئول الوحيد عن سرية وسلامة منظومة إحداث التوقيع الالكتروني التي يستعملها، وكل استعمال لهذه المنظومة يعد صادرا منه، كما يكون مسئولا عن كل ضرر يلحق أو يحصل لشخص وثق عن حسن نية في الضمانات المنصوص عليها في هذا القانون، غير أنّه لا يكون مسئولا عن عدم احترام صاحب الشهادة للقيود الواردة بها، وهو تقريبا ما ذهب إليه المشرع الأردني

[1] - **إبراهيم الدسوقي أبو الليل**، الجوانب القانونية لتعاملات الالكترونية، المرجع السابق، ص189.

[2] -**سمير حامد عبد العزيز الجمال**، المرجع السابق، ص348.

والمشرع الإماراتي قريبا من ذلك المشرع المصري في المواد من 12 إلى 16 من قانون التوقيع الالكتروني المصري، بينما لم ينظم المشرع الجزائري ذلك[1].

على العموم فإنّ تحميل القانون جهات التصديق الالكتروني مسؤولية جراء الإخلال بالواجبات المناطة لها يساهم في بعث الاطمئنان لدى المتعاملين في مجال التجارة الالكترونية، ويلزم الجهات الوسيطة (التصديق الالكتروني) ببذل أقصى مجهود لأجل ضمان سلامة المعاملات الالكترونية والاستخدام الصحيح للتوقيع الالكتروني.

المطلب الثاني

شهادة التصديق الإلكتروني

إنّ الدور الأساسي الذي تقوم به الجهة المختصة بإصدار شهادات التصديق الإلكترونية هو دور الوسيط المؤتمن بين الأشخاص والأطراف المعتمدين على الوسائط الإلكترونية في إتمام تصرفاتهم القانونية، وذلك من خلال شهادة التصديق الإلكترونية التي لها دور فعال وأثر هام في مجال المعاملات الإلكترونية وخاصة عقود التجارة الإلكترونية.

شهادة التصديق الإلكترونية من شأنها التأكد من شخصية الموقع – المرسل– لتشهد بأن التوقيع الإلكتروني هو توقيع صحيح ينسب إلى من أصدره، ويستوفى الشروط والضوابط المطلوبة فيه من أجل الأخذ به واعتباره دليل إثبات يعول عليه. حيث تؤكد الشهادة أن البيانات الموقع عليها هي بيانات صحيحة لم يطرأ عليها أي تعديل سواء بالحذف أو بالإضافة أو التغيير، وبهذا تصبح هذه البيانات موثقة، ولا يمكن إنكارها[2].

نظرا لأهمية شهادة التصديق الإلكترونية، كونها أهم دور تقوم به جهات التصديق الإلكتروني من خلال إصدارها من جهة، ومن جهة أخرى لكونها أداة توفر وتبث الثقة

[1]- **حمودي ناصر**، المرجع السابق، ص320، راجع كذلك: **سمير حامد عبد العزيز الجمال**، المرجع السابق، ص ص 352-353.

[2]-**إبراهيم الدسوقي أبو الليل**، المرجع السابق، ص184.

والأمان لدى المتعاملين في مجال التجارة الإلكترونية عبر الإنترنت، فقد قسمنا هذا المطلب إلى فرعين نتعرض لتعريف شهادة التصديق الإلكترونية **(الفرع الأول)، ثم** لمدى حجية شهادة التصديق الأجنبية **(الفرع الثاني)**.

الفرع الأول

تعريف شهادة التصديق الإلكترونية

نظراً لطبيعة شهادة التصديق الإلكترونية في إبرام التصرفات عبر الوسائط الإلكترونية خاصة في مجال الإثبات، فقد اهتمت العديد من التشريعات التي نظمت التجارة الإلكترونية والتوقيع الإلكتروني بتعريف هذه الشهادة مبينة المقصود بها، وحددت وظيفتها المتمثلة في تحديد هوية الموقع والربط بينه وبين مفتاحه العام الذي يكون مذكورا في الشهادة نفسها[1].

فقد عرفت المادة (2/ب) من قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية لسنة 2001م شهادة التصديق الإلكترونية بأنها: "**رسالة بيانات أو سجلا آخر يؤكدان الارتباط بين الموقع وبيانات إنشاء التوقيع**". وقد نصت المادة (9) من ذات القانون في الفقرتين (ج) و(د) على ضرورة أن تتضمن شهادات التصديق بيانات معينة حتى تتمكن من آداء مهمتها في التصديق وبث الثقة والأمان لدى المتعاملين بها، وهذه البيانات هي[2]:

1/هوية مزود خدمات التصديق.

2/ أن الموقع المعينة هويته في الشهادة كان يسيطر على بيانات إنشاء التوقيع في الوقت الذي أصدرت فيه الشهادة.

3/ أن بيانات إنشاء التوقيع كانت صحيحة في الوقت الذي أصدرت فيه الشهادة أو قبله.

4/ وجود أي تقييد على الغرض أو القيمة التي يجوز أن تستخدم من أجلها بيانات إنشاء التوقيع أو تستخدم من أجلها الشهادة.

---

[1]-**إبراهيم الدسوقي أبو الليل**، نفس المرجع، ص184.

[2]-أنظر نص المادة (9) الفقرتين (ج) و(د) من قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية لسنة 2001م.

5/ أن بيانات إنشاء التوقيع صحيحة ولم تتعرض لما يثير الشبهة.
6/ وجود أي تقييد على نطاق أو مدى المسؤولية التي اشترطها مقدم خدمات التصديق.

أمّا التوجيه الأوربي رقم 1999/93م فقد ميز في المادة (2) منه في الفقرتين التاسعة والعاشرة ما بين الشهادة الإلكترونية البسيطة والشهادة الإلكترونية الموصوفة المؤكدة، وعرفت الأولى بأنها: "**الشهادة الإلكترونية التي تربط البيانات الخاصة بفحص التوقيع الإلكتروني والشخص المعين وتؤكد هوية هذا الشخص**"، أمّا الشهادة الثانية فهي: "**شهادة مؤهلة تستوفي الشروط أو المتطلبات المنصوص عليها في الملحق 1، وتقدم بواسطة مقدم خدمات التصديق المستوفي للمتطلبات المنصوص عليها في الملحق 2**"[1].

حدّد الملحق الأول من التوجيه الأوروبي تحت عنوان "متطلبات الشهادات المؤهلة" البيانات التي يجب أن تتضمنها شهادة التصديق الإلكتروني، حيث نص على: "**إشارة إلى أن الشهادة صدرت كشهادة مؤهلة.**

- **التعرف على مقدم خدمة التصديق والدولة التي يوجد فيها مقره.**
- **اسم الموقع، أو أسمه المستعار، والذي يكون معروفا به.**
- **تقديم سمة خاصة للموقع بحيث تدرج عند الضرورة، حيث يعتمد ذلك على غرض إصدار الشهادة.**
- **بيانات التحقق من التوقيع المناظر لبيانات إنشاء التوقيع في ظل سيطرة الموقع.**
- **إشارة إلى بداية مدة ونهاية صلاحية الشهادة.**
- **رمز هوية الشهادة.**
- **التوقيع الإلكتروني الخاص بمقدم خدمة التصديق الذي أصدرها.**
- **القيود على نطاق استخدام الشهادة إذا كانت موجودة.**
- **قيود على قيمة الصفحة التي تستخدم فيها الشهادة عند وجودها**".

[1]-نظم المرسوم الفرنسي رقم 272 الصادر في 30 مارس 2001م من مجلس الدولة الفرنسي نموذجين من شهادات التصديق على التوقيع الإلكتروني، أحدهما عادي – بسيط – Le Certificat Électronique Simple يستخدم هذا النموذج في التصديق على صحة المراسلات الإلكترونية التي تتم عبر البريد الإلكتروني. أما الآخر وهو نموذج التصديق الإلكتروني Le Certificat électronique qualifie يتضمن عدة بيانات وهو يضمن صحته بيانات التوقيع الإلكتروني وصلته بالموقع، هذا وقد حددت المادة (6) من هذا المرسوم البيانات التي يجب أن يشتمل عليها هذا النموذج الصادر من الجهة المختصة، للإطلاع أكثر على هذا الموضوع أنظر: **ممدوح محمد على مبروك**، المرجع السابق، ص ص145-146.

كما عرف القانون التونسي رقم 2000/83م بشأن المبادلات والتجارة الإلكترونية، شهادة التصديق الإلكترونية في الفصل الثاني من الباب الأول بأنّها: "**الوثيقة الإلكترونية المؤمنة بواسطة الإمضاء الإلكتروني للشخص الذي أصدرها والذي يشهد من خلالها أثر المعاينة على صحة البيانات التي تتضمنها**". حدد كذلك في الفصل (17) من الباب الرابع منه أهم البيانات التي يجب أن تتضمنها شهادة التصديق الإلكتروني وهي:

- هوية صاحب الشهادة.
- هوية الشخص الذي أصدرها وإمضائه الإلكتروني.
- عناصر التدقيق في إمضاء صاحب الشهادة.
- مدة صلاحية الشهادة.
- مجالات استعمال الشهادة.

أمّا قانون المعاملات والتجارة الإلكترونية رقم 2002/2 الخاص بإمارة دبي فقد عرف شهادة التصديق الإلكترونية في المادة (22/2) التي نصت بأن: "**شهادة المصادقة الإلكترونية هي شهادة يصدرها مزود خدمات التصديق يفيد فيها تأكيد هوية الشخص أو الجهة الحائزة على أداة توقيع معينة، ويشار إليها في هذا القانونبـــ "الشهادة**"[1].كما حددت المادة (3/24) منه البيانات التي يجب أن تتضمنها شهادة المصادقة الإلكترونية وهذا لإخفاء الثقة والآمان على مضمونها بالنسبة للمتعاملين بها، ولكي يكون للشهادة قيمة قانونية كاملة في الإثبات[2].

أمّا المشرّع المصري فقد بين المقصود بشهادة التصديق الإلكتروني معرفا إياها في المادة الأولى فقرة (و) من قانون التوقيع الإلكتروني رقم 2004/15 بأنّها: "**الشهادة التي تصدر من الجهة المرخص لها بالتصديق، وتثبت الارتباط بين الموقع وبيانات إنشاء التوقيع**". وفيما

[1]- **بالنسبة للمشرع الأردني** عرف شهادة التصديق الإلكترونية – شهادة التوثيق – بأنها الشهادة التي تصدر من جهة مرخصة أو معتمدة لإثبات نسبة توقيع الكتروني إلى شخص معين إسناداً إلى إجراءات توثيق معتمدة" المادة (14/2) من قانون المعاملات الإلكترونية رقم 85 لسنة 2008م.

[2]- أنظر المادة (24) من قانون المعاملات والتجارة الإلكترونية لإمارة دبي رقم 2 لسنة 2002م.

يخصّ البيانات التي يجب أن تتضمنها كي يكون لها حجية قانونية في الإثبات، فقد نص المشرع المصري في المادة (20) من قانون التوقيع الإلكتروني على أن: "**تحدد اللائحة التنفيذية لهذا القانون البيانات التي يجب أن تشمل عليها شهادة التصديق الإلكتروني**".

وقد حدّدت المادة (20) من اللائحة التنفيذية لقانون التوقيع الإلكتروني البيانات التي بجب أن تشتمل عليها نماذج شهادات التصديق الإلكترونية بنصها على أنّه: "**يجب أن تشتمل نماذج شهادات التصديق الإلكتروني التي يصدرها المرخص له على البيانات الآتية، وذلك على نحو متوافق مع المعايير المحددة في الفقرة (أ) من الملحق الفني والتقني:**

1. **ما يفيد صلاحية هذه الشهادة للاستخدام في التوقيع الإلكتروني.**
2. **موضوع الترخيص الصادر للمرخص له، موضحا فيه نطاقه ورقمه وتاريخ إصداره وفترة سريانه.**
3. **اسم وعنوان الجهة المصدرة للشهادة ومقرها الرئيسي وكيانها القانوني والدولة التابعة لها إن وجدت.**
4. **اسم الموقع الأصلي أو اسمه المستعار أواسم شهرته، وذلك في حالة استخدامه لأحدهما.**
5. **صفة الموقع.**
6. **المفتاح الشفري العام لحائز الشهادة المناظرة للمفتاح الشفري الخاص به.**
7. **تاريخ بدء صلاحية الشهادة وتاريخ انتهائها.**
8. **رقم مسلسل الشهادة.**
9. **التوقيع الإلكتروني لجهة إصدار الشهادة.**
10. **عنوان الموقع الإلكتروني (Web site) المخصص لقائمة الشهادات الموقوفة أو الملغاة ويجوز أن تشتمل الشهادة على أي من البيانات الآتية عند الحاجة:**

- **ما يفيد اختصاص الموقع والغرض الذي تستخدم فيه الشهادة.**
- **حد قيمة التعاملات المسموح بها بالشهادة.**
- **مجالات استخدام الشهادة.**

يتّضح لنا أنّ جميع هذه التشريعات قد استندت في تعريفها لشهادة التصديق الإلكترونية على الجانب الوظيفي لهذه الشهادة، المتمثل في تأكيدها على صحة التوقيع الإلكتروني وارتباطه بالموقع، وأنّه قد صدر ممن ينسب إليه ولم يشبه أي تزوير أو

تحريف، وأنّ البيانات الموقع عليها هي بيانات صحيحة صادرة من الموقع ولم يتم التلاعب فيها بالتغير أو التعديل، ويتمّ التحقق من هذه المعلومات عن طريق استخدام المفتاح العام لمن صدرت عنه الشهادة الإلكترونية والذي يكون مذكورا في الشهادة نفسها نظر للارتباط بين هذا المفتاح العام والمفتاح الخاص لصاحب الشهادة[1].

هكذا تنشئ شهادة التصديق الإلكترونية علاقة ثلاثية بين كل من جهة مقدم خدمات التصديق والموقع –المرسل– والمرسل إليه، ولاشك أن هذه العلاقة توفر الآمان والثقة لدى المتعاملين في إبرام معاملاتهم التجارية بطريقة الكترونية، هذا يؤدي إلى تطور وازدهار التجارة الإلكترونية.

تتعدد شهادات التصديق الإلكترونية في الوقت الحالي، فإلى جانب شهادة تصديق التوقيع الإلكتروني التي سبق عرضها، فهناك شهادات أخرى تتنوع بحسب الهدف منها ومن أمثلة ذلك:

***شهادة:** التي تقوم بتصديق تاريخ ووقت إصدار التوقيع الرقمي، حيث يقوم صاحب الرسالة بعد التوقيع عليها بإرسالها إلى الجهة المختصة بالتصديق التي تقوم بتسجيل التاريخ عليها وتوقيعها من جهتها ثم تعيدها إلى مرسلها.

***شهادة الإذن:** يتم بموجبها تقديم معلومات وبيانات عن صاحب التوقيع، كمؤهلاته ومحل إقامته.

***شهادة البيان:** تفيد بيان صحة واقعة معينة ووقت وقوعها[2].

استعمل المشرع الجزائري مصطلح الشهادة الإلكترونية في المادة الثالثة من المرسوم التنفيذي رقم 07-162 حيث نص على أن " **الشهادة الإلكترونية: وثيقة في شكل تثبت الصلة بين معطيات فحص التوقيع الإلكتروني والموقع". والشهادة الإلكترونية الموصوفة: شهادة إلكترونية تستجيب للمتطلبات المحدّدة.**

[1]- **إبراهيم الدسوقي أبو الليل**،المرجع السابق، ص184.

[2]-**عايض راشد عايض المري**، المرجع السابق، ص344.

الفرع الثاني

شهادة التصديق الأجنبية

تتجاوز المعاملات الإلكترونية أو العقد في نطاق التجارة الإلكترونية الحدود الإقليمية للدولة التي ابرم فيها أو التي يقيم فيها أحد أطرافه، فغالبا ما يكون فيه عنصر أجنبي وذلك لأنّ التجارة عبر شبكة الانترنت هي تجارة غير محدودة بموقع جغرافي إنما تجعل العالم بمثابة قرية صغيرة، بحيث يمكن لطرفي المعاملة التباحث والتعاقد فيما بينهما رغم بعد المكان واختلاف الزمان في وقت قصير وبتكاليف قليلة.

لهذه الاعتبارات فإن التوقيعات الإلكترونية الأجنبية وكذلك شهادات التصديق الصادرة عن مقدمي خدمات تصديق أجانب قد حضت بأهمية بالغة من طرف التشريعات الدولية والإقليمية والوطنية، من خلال الاعتراف بها وتنظيمها. فهذه التشريعات قد ساوت بين التوقيع الإلكتروني والشهادة الصادرة من مقدم خدمات تصديق وطني، وبين التوقيع الإلكتروني والشهادة الصادرة خارج الدولة –مقدم خدمات تصديق أجنبي-، وفقا للضوابط والشروط التي يشترطها كل تشريع بأن تتوافر في التوقيع الإلكتروني الأجنبي أو الشهادة الأجنبية أو مقدم خدمات التصديق الأجنبي.

نظّمت المادة (12) من قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية لعام 2001م، الاعتراف بالشهادات والتوقيعات الإلكترونية التي تصدر من جهات التصديق الإلكتروني الأجنبية، حيث تضمنت ما يفيد بأن شهادة التصديق الأجنبية لها نفس المفعول القانوني للشهادة التي يصدرها مقدم خدمة التصديق في الدولة المشرعة، طالما استوفت الشروط التي تضفى عليها الموثوقية اللازمة للتعويل عليها، وأن تتمتع بالكفاءة التي تخضع في تقديرها للمعايير الدولية المعترف بها ولأية عوامل أخرى ذات صلة نفس الحكم يسري أيضا بالنسبة للتوقيع الإلكتروني الأجنبي.

كما أقرّ هذا القانون في نفس المادة على أنه يجوز للأطراف الاتفاق فيما بينهم على استخدام أنواع معينة من التوقيعات الإلكترونية أو الشهادات، ويكون هذا الاتفاق معترف به وساري المفعول عبر حدود الدول المختلفة بشرط أن يكون صحيحا وغير مخالف للقانون المطبق[1].

كما اعترف التوجيه الأوربي رقم 1999/93م بمقدم خدمات التصديق الأجنبي في حالة توافر الشروط الخاصة التي حددها التوجيه، تمّ اعتمادها وفق نظام تصديق أو توثيق اختياري[2] معمول به داخل الدول الأعضاء، أمّا إذا كانت شهادة التصديق الأجنبية معتمدة من قبل أحد مقدمي خدمات التصديق الإلكتروني المعتمد داخل المجموعة الأوربية، وتوفرت فيه الشروط التي يتطلبها التوجيه الأوربي في مقدم خدمات التصديق بوجه عام[3]، إضافة إلى حالة الاتفاقات الثنائية أو الجماعية مع الالتزام بالشروط الواردة في التوجيه الأوربي رقم 1995/46 حول معالجة البيانات ذات الصفة الشخصية[4].

اعترفت العديد من التشريعات الوطنية بشهادة التصديق الأجنبية ومنها على سبيل المثال قانون المبادلات والتجارة الإلكترونية التونسي رقم 2000/83 الذي أعتبر الشهادات الصادرة من مزود خدمات المصادقة الإلكترونية الموجود بدولة أجنبية كالشهادات الصادرة من مزود خدمات المصادقة الإلكترونية الموجود بالجمهورية التونسية، متى تم تنظيم هذا الاعتراف في إطار اتفاقية اعتراف متبادل تبرمها الوكالة الوطنية للمصادقة الإلكترونية مع الدول الأجنبية[5].

---

[1]- أنظر المادة (12) من قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية لسنة 2001م .

[2]- يقصد بنظام التصديق الاختياري وفقا للمادة (13/2) من التوجيه الأوربي رقم 93 لسنة 1999م كل ترخيص يصدر لتحديد الحقوق والالتزامات الخاصة بتوريد خدمة التصديق والتي تمنح بناء على طلب مقدم خدمات التصديق الإلكتروني بواسطة هيئة عامة أو خاصة يعهد إليها بتحديد هذه الحقوق والالتزامات والتأكد من احترامها، ومراقبتها إذا كان مقدم خدمة التصديق غير مؤهل بمراعاة الحقوق المحددة في التراخيص طوال المدة اللازمة للحصول على موافقة الهيئة المختصة.

[3]- أنظر المادة (7) من التوجيه الأوربي رقم 93 لسنة 1999م أنظر على الموقع: europa.eu.http://www.ec

[4]- **ثروت عبد الحميد**، المرجع السابق، ص 167.

[5]-أنظر الفصل (23) من الباب الرابع من قانون المبادلات والتجارة الإلكترونية التونسي رقم 2000/83.

كذلك اعترف القانون الإماراتي رقم 2002/2 بشأن المعاملات والتجارة الإلكترونية بشهادات التصديق الإلكترونية والتوقيع الإلكتروني التي تصدر في الدول الأجنبية، واعتبرها نافذة قانونا دون وضع أي اعتبار بالنسبة للمكان الذي صدرت فيه هذه الشهادة أو التوقيع الإلكتروني. من جهة أخرى يجب عدم التمسك بالاختصاص القضائي الذي يوجد فيه مقر عمل الجهة التي أصدرت الشهادة أو التوقيع الإلكتروني، فقد نصت المادة (1/26) من القانون السابق الذكر على أنه: "**لتقرير ما إذا كانت الشهادة أو التوقيع الإلكتروني نافذا قانونا لا يتعين إيلاء الاعتبار إلى المكان الذي صدرت فيه الشهادة أو التوقيع الإلكتروني ولا إلى الاختصاص القضائي الذي يوجد فيه مقر عمل الجهة التي أصدرت الشهادة أو التوقيع الإلكتروني**".

كي تمنح الشهادات التي يصدرها مزود خدمات التصديق الأجانب الحجية كشهادات صادرة من مزودي خدمات التصديق بالدولة، يجب أن يكون مزودي خدمات التصديق الأجانب على درجة من الوثوق تعادل على الأقل المستوى الذي تطلبه المادة (24) من ذات القانون من مزودي خدمات التصديق العاملين بالدولة، إضافة إلى ضرورة توافر المعايير الدولية المعمول بها في مثل هذا الخصوص[1]، التي تعني تطبيق المبادئ المستقر عليها حسب القانون والعرف الدولي في علاقات الدول ببعضها البعض في مثل هذه الأحوال، حيث أنه لا يمكن لمشرع وطني أو سلطات وطنية أن تعترف بالوثائق الأجنبية لإنتاج أثار قانونية على أرضها ما لم تكن معاملة بالمثل من طرف هذه الدولة الأجنبية، أي أن تشريعات هذه الأخيرة تعترف بذات الوثائق الوطنية بالقوى التنفيذية على أراضيها هي أيضا[2]، كما يجب أيضا إضافة إلى ما سبق أن يوضع في الاعتبار أي اتفاق بين

[1]-أنظر المادة (2/26) من القانون رقم 2002/2 الإماراتي بشأن المعاملات والتجارة الإلكترونية أنظر على الموقع الإلكتروني: http://www.uaeec.com/articles-action-show-id-34.htm

[2]-د/**عبد الفتاح بيومي حجازي**، المرجع السابق، ص 307.

الأطراف محل المعاملة التي تستخدم فيها شهادة التوثيق الإلكتروني وذلك لتقرير مدى حجيتها القانونية[1].

كما أقرّ المشرّع الإماراتي للأطراف في المعاملات التجارية أن يحددوا في عقودهم وجوب اللجوء إلى مزودي خدمات تصديق معينين، أو فئة معينة منهم، أو فئة معينة من الشهادات فيما يتعلق بالرسائل والتوقيعات الإلكترونية المقدمة لهم. كما أنه في الحالات التي يتفق فيها الأطراف فيما بينهم على استخدام أنواع معينة من الشهادات أو التوقيعات، فإن ذلك الاتفاق يعتبر كافيا للاعتراف به أمام الجهات القضائية للدول المختلفة،شرط ألا يكون هذا الاتفاق غير مشروع وفقا لأحكام القوانين المطبقة في إمارة دبي[2].

اعترف قانون تنظيم التوقيع الإلكتروني المصري كذلك بشهادات التصديق الصادرة من جهات أجنبية، حيث منح هيئة تنمية صناعة تكنولوجيا المعلومات سلطة اعتماد الجهات الأجنبية التي تزاول إصدار شهادات التصديق الإلكتروني نظير مقابل يحدّده مجلس إدارتها، ويكون ذلك في الحالات ووفقا للقواعد والإجراءات والضمانات التي تحددها اللائحة التنفيذية لقانون التوقيع الإلكتروني[3]. وقد بينت اللائحة التنفيذية لقانون التوقيع الإلكتروني الحالات التي يمكن للهيئة أن تعتمد فيها الجهات الأجنبية المختصة بإصدار شهادات التصديق الإلكتروني حيث نصت المادة (21) على أنّه: "**للهيئة اعتماد الجهات الأجنبية المختصة بإصدار شهادات التصديق الإلكتروني في أحدى الحالات الآتية:**

- **أن يتوافر لدى الجهة الأجنبية القواعد والاشتراطات المبينة في هذه اللائحة بالنسبة للجهات التي ترخص لها الهيئة بمزاولة إصدار شهادات التصديق الإلكتروني.**

---

[1]- أنظر المادة (5/26) من القانون الإماراتي رقم 2002/2 بشأن المعاملات والتجارة الإلكترونية أنظر الموقع الإلكتروني:
http://shabab20.net/index.php?option=com_kunena&func=view&id=815&catid=39&Itemid=194
أنظر: **حسن محمد عرب**، منظومة التشريعات الإلكترونية في الإمارات، مقال على الموقع الإلكتروني:
http://www.uaeec.com/articles-action-show-id-34.htm

[2]-أنظر المادة (6/26) المرجع نفسه

[3]-أنظر المادة (22) من القانون المصري رقم 2004/15 بشأن تنظيم التوقيع الإلكتروني.

- **أن يكون لدى الجهة الأجنبية وكيل في جمهورية مصر العربية مرخص به من قبل الهيئة في إصدار شهادات التصديق الإلكتروني ويتوافر لديه كل المقومات المطلوبة للتعامل بشهادات التصديق الإلكتروني وأن يكفل تلك الجهة فيما تصدره من شهادات تصديق إلكتروني وفيما هو مطلوب من اشتراطات وضمانات.**
- **أن تكون الجهة الأجنبية ضمن الجهات التي وافقت جمهورية مصر العربية بموجب اتفاقية دولية نافذة فيها على اعتمادها باعتبارها جهة أجنبية مختصة بإصدار شهادات التصديق الإلكتروني.**
- **أن تكون الجهة الأجنبية ضمن الجهات المعتمدة أو المرخص لها بإصدار شهادات تصديق إلكتروني من قبل جهة ترخيص بلدها وبشرط أن يكون هناك اتفاقا بين جهة الترخيص الأجنبية و بين الهيئة على ذلك...".**

كما أوجبت اللائحة التنفيذية على الجهة الأجنبية المعتمدة أن تطلب من الهيئة اعتماد أنواع أو فئات شهادات التصديق الإلكتروني التي تصدرها، وذلك نظير المقابل الذي يحدده مجلس إدارة الهيئة [1].

بمجرد اعتماد الهيئة شهادات التصديق الإلكتروني الصادرة من جهة أجنبية فإنها تتمتع بذات الحجية في الإثبات المقررة لشهادات التصديق الإلكتروني النظيرة الصادرة في داخل مصر من جهة وطنية مرخص لها.

ممّا سبق يلاحظ أن المشرع المصري قد عالج مسألة الاعتراف بالشهادات الصادرة من جهات أجنبية دون التوقيع الإلكتروني الصادر عن جهات أجنبية، وما إن كان يسمح باعتماده هو الآخر أم لا، وهو نفس المسلك الذي تبناه القانون التونسي بشأن المبادلات والتجارة الإلكترونية.

هذه المسألة ذات أهمّية كبيرة سيما أنّ التوقيعات الإلكترونية قد تكون لازمة بالنسبة للمعاملات الإلكترونية خاصة في مجال عقود التجارة الإلكترونية التي غالبا ما يكون فيها أحد أطرافها أجنبي.

[1]- أنظر المادة (22) من اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري رقم 2004/15.

هذا ما جاءت به المادة 12 من قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية لسنة 2001، حيث نصت على الاعتراف بالتوقيع الإلكتروني وشهادات التصديق الإلكترونية حسب ضوابط يصفها المشرع الوطني عند التشريع للتوقيع الإلكتروني.

المبحث الثاني

الحماية الجنائية للتوقيع الإلكتروني

مع تزايد العمليات التجارية الالكترونية على المستوى العالمي والمحلي والتطور الكبير في الوسائل التقنية المستعملة لحماية التجارة الالكترونية، كان من الإلزامي توفير الحماية التشريعية والقانونية لهذا النوع من التجارة.فالقاعدة العامة تنص على أنّ التوقيع الإلكتروني الذي لا يتمتع بالحجية في الإثبات ليس محلا للتزوير، بينما التوقيع الإلكتروني المتمتع بالحجية في الإثبات يقع محلا للتزوير، وعليه فالتمتع بالحجية في الإثبات شرط لحصول التوقيع على الحماية الجنائية[1] إذ ما تمّ تزويره، كونه مصلحة يرى المشرع أنها جديرة بالحماية التشريعية، وبالتالي ينص على حمايتها بتجريم الاعتداء عليها.لذا سنتطرق إلى جرائم الاعتداء على التوقيع الإلكتروني **(المطلب الأول)**.

اشتدت الحاجة إلى التوقيع الإلكتروني أمام عجز التوقيع التقليدي الذي يتطلب جهدا ووقت وأقلّ أمن من التوقيع الإلكتروني، فأصبح من أولويات المتخصصين في علوم القانون توفير حماية قانونية وذلك بعرض مجموعة من النماذج للقوانين التي تبنتها الدول في تشريعاتها الداخلية سواء كانت حماية مدنية أو جنائية.كما امتدت هذه الاهتمامات إلى ضرورة تضافر الجهود الدولية، ومن المعلوم أن التوقيع الإلكتروني قد وكبه تطور تشريعي ينظمه ويحدد مصداقيته ويحميه بالتجريم والعقاب، وفي ظل تزايد الاعتماد عليه

[1]- الحماية في اللغة: من يحمى حماية أي: دفع عنه، وهذا شيء حمى أي محظور لا يقرب الجنائية في اللغة: من الجناية وأصلها من جني يجني جناية. ويرد بالحماية الجنائية إضفاء الشارع وصف التجريم على كافة الأفعال التي تهدد مصلحة معينة أو حق من الحقوق وقيام الجهات التشريعية في دول العالم بإصدار قوانين تضفي صفة التجريم على الأفعال التي تهدد مصلحة معينة.

والتحول إليه وهل تمكنت التشريعات من إحاطته بالحماية الجنائية؟ أي معرفة الحماية التي توفرها التشريعات المقارنة لذلك سوف نتعرض إلى تجريم الاعتداء على التوقيع الإلكتروني في التشريعات الوطنية والدولية **(المطلب الثاني)**.

المطلب الأول

جرائم الاعتداء على التوقيع الإلكتروني

أصبح التوقيع الإلكتروني إحدى وسائل الحماية المدنية للمعاملات المتعلقة بالتجارة الإلكترونية[1]، فالتحول التدريجي إلى التوقيع الإلكتروني وقبوله في الإثبات لابد أن يسبقه تنظيم تشريعي يكفل الضوابط والشروط اللازمة لإضفاء المصداقية عليه، وحمايته من العبث ووصول المجرمين إليه، خاصة أنهم يعملون على تطوير أنفسهم وجرائمهم تبعا لتطور التقنية، حتى تظل الفرصة سامحة لهم لارتكاب جرائمهم،فتولدت جرائم مستحدثة تحدث في البيئة الإلكترونية، أو ترتكب بوسائل إلكترونية تسمى الجريمة المعلوماتية **(الفرع الأول)**، ولا يخفى على أحد ما تتسم به الجريمة في البيئة الإلكترونية من صعوبة في إثباتها، وصعوبة الوقوف على طبيعة الاعتداء ذاته، كما أن الدليل على ارتكابها يغلب عليه الطابع الإلكتروني، لذلك فالبيانات المتعلقة بالتوقيع الالكتروني، والمعلومات من أرقام سرية وغيرها من الأسرار الخاصة بأصحابها لا يجوز لأحد الاطلاع عليها حتى لو لم يستخدمه، وعليه سوف نتعرض إلى جريمة التزوير **(الفرع الثاني)**، كما هنالك جرائم الاعتداء على التوقيع وأهمها جريمة صنع أو حيازة برنامج لإعداد توقيع إلكتروني مزور **(الفرع الثالث)**، وجريمة الدخول بطريق الغش على قاعدة بيانات تتعلق بالتوقيع الإلكتروني**(الفرع الربع)**، وجريمة فض مفاتيح التشفير **(الفرع الخامس)**.

الفرع الأول

[1] - **عبد الفتاح بيومي حجازي**، النظام القانوني لحماية التجارة الإلكترونية، مرجع سابق، ص ص 294، 305.

تعريف الجريمة المعلوماتية

تعرف الجريمة عموما في نطاق القانون الجنائي أنها فعل غير مشروع صادر عن إرادة جنائية تقرر له القانون عقوبة أو تدبيرا احترازيا.

أمّا جرائم الحاسب فيعرفها مكتب تقسيم التقنية بالولايات المتحدة الأمريكية بأنها:"**الجريمة التي تلعب فيها البيانات الحاسوبية والبرامج المعلوماتية دورا رئيسيا من هنا يمكن أن نقول بأن جرائم الحاسب هي كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسب**"[1].

تُعرف الجريمة في القوانين الوضعية بأنها كل فعل يعاقب عليه القانون أو امتناع عن فعل يقضي به القانون، ولا يعتبر الفعل أو الترك جريمة إلا إذا كان مجرماً في القانون. حيث حدّد القانون الوضعي عقوبات محددة للمخالفات، بمعنى أنه لا يمكن معاقبة أي فعل ما لم يكن هناك نص محدد له في القانون وإلا لا يعتبر جرماً. من ناحية أخرى الجريمة هي كلّ فعل ضار يأتيه المواطن ويكون لهذا الفعل أثر ضار على غيره من المواطنين وبالتالي فالجرائم الإلكترونية "**هي كل فعل ضار يأتيه المواطن عبر استعماله لوسائط الإلكترونية مثل الحواسيب، أجهزة الموبايل، شبكات الاتصالات الهاتفية، شبكات نقل المعلومات، شبكة الإنترنت أو الاستخدامات غير القانونية للبيانات الحاسوبية أو الإلكترونية عموماً**".

تطور الانترنت وازدياد عدد المستخدمين لها في العالم (حوالي 1.6 مليار مستخدم يمثلون ربع سكان العالم)،جعل منها وسطاً ملائماً للتخطيط وتنفيذ الجرائم بعيداً عن رقابة وأعين الجهات الأمنية.

كما يعرف البعض الجريمة الإلكترونية الرقمية أنها" **نشاط إجرامي تستخدم فيه التقنية الإلكترونية الرقمية و(الحاسوب الآلي الرقمي وشبكة الإنترنت) بطريقة مباشرة أو غير مباشرة كوسيلة لتنفيذ الفعل الإجرامي المستهدف**[1].

[1] **محمد دباس الحميد**، المرجع السابق، ص 60.

نص المشرع الفرنسي في القانون رقم 1988/19 ضمن نصوصه الخاصة ببعض الجرائم الإلكترونية المرقمة (المعلوماتية)، في نص المادة 2/462 والتي تنص: "**كل من توصل لنظام المعالجة الآلية للبيانات بطريق التحايل ويقصد بالتحايل تدخّل غير مشروع**"[2]. وقد نصت نفس المادة أنّه: "**يترتب على جريمة التوصل إلى نظام المعالجة آليا للبيانات بطريق التحايل أحد الآثار الثلاثة:**

- **محو البيانات** la suppression de données
- **تعديل البيانات** la modification de données
- **تعطيل تشغيل النظام** l'altération du fonctionnement de system"[3].

ذهب تيار من الفقه إلى تعريف الجريمة المعلوماتية أنّها: المصطلح المترجم من الفرنسية crime informatiqueالذي يتضمن المعالجة الآلية للبيانات، فغرفها بأنها: "**أي جريمة يكون متطلبا لاقترافها أن تتوافر لدى فاعلها معرفةتقنية الحاسب**" أو هي "**أي فعل غير مشروع**[4] **تكون المعرفة بتقنية المعلومات أساسية لمرتكبه**" **أو هي كل سلوك إجرامي بمساعدة الحاسب الآلي أو تحدث في محيطه**".

كما عرفت منظمة التعاون الاقتصادي والتنمية[5] (OCDE) الجريمة المعلوماتية بأنّها: "**كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية**".

من التعريفات السابقة نجد أن الجريمة المعلوماتية تستهدف في جوهرها المعلومات بمفهومها الواسع، من بيانات ومعلومات وبرامج تطبيقية. تقوم هذه الجريمة على اعتبارين

---

[1]- **مصطفى محمد موسى**، أساليب إجرامية بالتقنية الرقمية ماهيتها...مكافحتها، دراسة مقارنة، دار الكتب القانونية 2005، ص 56.

[2]- **مصطفى محمد موسى**، نفس المرجع، ص 57.

[3]- **المرجع نفسه**، ص 58.

[4]- **إيهاب فوزي السقا**، الحماية الجنائية والأمنية لبطاقات الائتمان، دار الجامعة الجديدة، الإسكندرية 2007، ص 115.

[5]-ORGANISATION DE COOPERATION ET DE DEVELOPPEMENT ÉCONOMIQUE (OCDE), «The Economic and Social Impacts of Electronic Commerce: Preliminary Findings And Research Agenda », disponible à : http://www.onlineaustralia.net.au/publications/other/OECD/ottawa98/e_simpact.p

مهمين أولهما أن تكون المعلوماتية وسيلة للغش والتحايل والاعتداء، والثاني أن تكون المعلوماتية نفسها محلا للاعتداء[1].

كما يمكننا الإشارة إلى عدة محاولات فقهية لوضع تعريف للجريمة المعلوماتية، فعرفها الأستاذ الفرنسي MASSA أن المقصود بها "**الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق الربح**".

أمّا الأستاذة l'estançvivant عرفتها بأنها "**مجموعة من الأفعال المرتبطة بالمعلوماتية و التي يمكن أن تكون جديرة بالعقاب**".

كما يعرف الفقيه الألماني تاديمان الجرائم المعلوماتية بأنّها: "**كل أشكال السلوك غير المشروع أو الضار بالمجتمع الذي يرتكب باستخدام الحاسب**"[2].

يعرف المشرع الجزائري الجريمة المعلوماتية في المادة 2 من القانون 09-04[3] المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بأنها: "**جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات ألإلكترونية**".

يمكننا الاستخلاص من هذه التعاريف أن الجريمة المعلوماتية هي التي يكون موضوعها النظام المعلوماتي، أي البيانات نفسها التي تتداول عبر قنوات الاتصال، ممّا يعرّض التوقيع الإلكتروني لخطر التزوير والغش وعرضة للعديد من الجرائم التي سيتم التطرق إليها فيما يلي، وبفضل خصوصية مهارة المجرم المعلوماتي، حيث يمكنه اقتراف هذه الجرائم بالمعالجة الدقيقة غير المشروعة لهذه الوسائل، ومن أهم خصائص الجريمة المعلوماتية.

---

[1]- **إيهاب فوزي السقا**، المرجع نفسه، ص 116.

[2]- **محمد علي العريان**، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، الإسكندرية، 2004، ص 44.

[3]- **قانون رقم: 09-04**، مؤرخ في 5 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج، ر عدد47.

أولاً: خصائص الجريمة المعلوماتية.

جعلت طبيعة المعالجة الالكترونية للبيانات من المخاطر التي تتعرض لها والجرائم التي تتعرض لها ذات طابع خاص وبالتالي يمكن تمييزها عن غيرها بتبيان خصائص الجريمة المعلوماتية:

1- الجاني في الجرائم المعلوماتية:

قد يكون الجاني في جرائم المعلوماتية شخصاً طبيعياً يعمل لحسابه، ويهدف إلى تحقيق مصلحة خاصة به من وراء الجريمة التي يرتكبها ضد أحد نظم المعالجة الآلية للبيانات والمعلومات، أو عن طريق الاستعانة بأحد نظم المعالجة الآلية للبيانات والمعلومات. لكن يحدث كثيراً أن يقترف الشخص الطبيعي الفعل المؤثم جنائياً ليس لحسابه الخاص, وإنّما لحساب أحد الأشخاص المعنوية كشركة عامة أو خاصة تعمل في مجال المعلوماتية، أو تعمل في مجال آخر، تقوم بالسطو على أحد أنظمة المعلوماتية، أو تحدث ضرراً للغير عن طريق اللجوء لأحد نظم المعالجة الآلية للمعلومات، وبذلك ترتكب من مجرم غير عادي.

إذا كان المجرم المعلوماتي يتوافق مع المجرم التقليدي بكونه إنسان اجتماعي، فإنّه يتميز عنه من حيث المعرفة والمهارة والوسيلة الخاصة بهذه الجريمة، وهذا الاكتساب يتم عن طريق الدراسة المخصصة في هذا المجال حيث يتمتع بالذكاء، إذ أنه يستغل ذكائه في تنفيذ جريمته، أي أن المجرم من ذوي المستويات العملية غالبا سعيا لتحقيق الربح من جراء تنفيذ جريمته عاديا.

2- جرائم المعطيات ناعمة مغرية للمجرمين:

فإذا كانت الجرائم التقليدية تحتاج من مرتكبيها إلى قوة عضلية لتنفيذها فإن جرائم المعطيات لا تحتاج إلى مثل تلك القوة العضلية وإنما إلى قوة عملية وقدرة من الذكاء ومهارة في توظيف ذلك، والجاني في سبيل تنفيذها لا يحتاج من الوقت إلا ثوان أو دقائق

معدودات[1] ونعومة هذه الجريمة وما تدركه من أرباح ومن إشباع للفضول عند البعض جعلها من الجرائم المغرية والجذابة للمجرمين.

3- جرائم المعطيات جرائم عابرة للحدود:

ليس هناك في عالم اليوم حدود تقف حائلا أمام نقل المعطيات بين الحسابات الآلية الموزعة في مختلف دول العالم عبر شبكات المعلومات، فيمكن في بعض دقائق نقل كم هائل من المعطيات بين حساب وآخر ببعده عن آلاف الكيلومترات، كما يمكن أن تقع الجريمة من جاني في دولة معينة على مجني عليه في دولة أخرى في وقت قصير جدا لاسيما مع تعاظم الدور الذي تقدمه شبكة الإنترنت خاصة في مجال التجارة الإلكترونية وازداد اعتماد البنوك عليها.

تثير الطبيعة الدولية لهذه الجرائم العديد من المشاكل كمشكلة السيادة، الاختصاص القضائي وقبول الأدلة المتحصل عليها في دولة ما أمام قضاء دولة أخرى، ولهذا مكافحة هذه الجرائم تتطلب تعاونا كثيفا بين الدول وتوافقا كبيرا بين تشريعاتها[2]. وفي هذا المجال يمكننا ذكر قضية RN Toinpson وفيها قام مبرمج إنجليزي يعمل لدى بنك بالكويت بالتلاعب في معطيات بنظام الحاسب الآلي الخاص بالبنك، وذلك عن طريق الخصم من أرصدة العملاء ثم الإيداع في حسابه الخاص، وبعد عودته إلى إنجلترا طلب من البنك تحويل الحساب الخاص إلى عدة حسابات بنكية في إنجلترا فقام البنك بذلك، حوكم الفاعل بتهمة الحصول على أموال الغير بطريق الاحتيال، وحكم عليه بعقوبة السجن.

4- صعوبة اكتشاف جرائم المعلوماتية وإثباتها:

لا تحتاج جرائم المعلوماتية إلى أي عنف, أو سفك للدماء, أو أثار اقتحام لسرقة الأموال, وإنما هي أرقام وبيانات تتغير أو تمحى تماما من السجلات المخزونة في ذاكرة

[1]- **أشرف توفيق شمس الدين**، الحماية الجنائية للمستند الإلكتروني, بحث مقدم لمؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، ذبي، الفترة من 10-12 ماي2003، ص 100-120.

[2]- **محمد خليفة**، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، 2005، ص 37.

الحاسبات الآلية, كونها في أغلب الأحيان جرائم لا تترك أي أثر خارجي مرئي لها، فإنها تكون صعبة الإثبات.

يزيد من صعوبة إثبات هذه الجرائم ارتكابها عادة في الخفاء, وعدم وجود أي أثر كتابي لما يجرى خلال تنفيذها من عمليات أو أفعال إجرامية, حيث يتمّ بالنبضات الالكترونية نقل المعلومات, أضف إلى ذلك إحجام مجتمع الأعمال عن الإبلاغ عنها تجنبا للإساءة إلى السمعة وهز الثقة في كفاءة المنظمات والمؤسسات المجني عليها, فضلاً عن إمكانية تدمير المعلومات التي يمكن أن تستخدم كدليل في الإثبات في مدّة قد تقل عن الثانية الزمنية. إضافة إلى عدم ملائمة الأدلة التقليدية في القانون الجنائي في إثباتها, ومن ثم يلزم البحث عن أدلة جديدة حديثة ناتجة من ذات الحاسب, ومن هنا تبدأ صعوبات البحث عن الدليل, وجمع هذا الدليل, وتبدأ مشكلات قبوله إن وجد, ومدى موثوقيته أو مصداقيته على إثبات وقائع الجريمة.

بعد استعراضنا لأهم عناصر الجريمة المعلوماتية، يمكننا إسقاطها أو تطبيق مبادئها كذلك في حالة تزوير التوقيع الإلكتروني والسطو على أرقام البطاقات الائتمانية واختلاس من البنوك، أو تزوير وثائق ومستندات مالية.

الفرع الثاني

جريمة تزوير التوقيع الإلكتروني

يعتبر تزوير التوقيع الإلكتروني شكلا من أشكال الغش المعلوماتي، وقد عالجت التشريعات والقوانين في دول العالم المختلفة حتى الشريعة الإسلامية[1] كافة أشكال جريمة التزوير في المحررات التقليدية، لكنها انقسمت اتجاه التزوير الذي يقع في مجال المعلوماتية، حيث يرى فريق من الفقه عدم إمكانية تطبيق النصوص التقليدية على جرائم تزوير المعلوماتي، بينما يرى غيرهم إمكانية تطبيقها وفقا للمفهوم السائد والمستقر[2] للتزوير المعلوماتي، ولابدّ من تشريع نصوص خاصة بجرائم التزوير التي تقع في مجال المعلوماتية، نحاول أن نلقي البحث على مفهوم التزوير[3] بصفة عامة، أي جريمة التزوير المعلوماتي بصفة خاصة ثم نرى كيفية تزوير التوقيع الإلكتروني.

أولاً: تعريف جريمة التزوير.

تعتبر جريمة التزوير في المحررات من أهم الموضوعات في قانون العقوبات لأنّها من أخطر الجرائم التي تخل بالثقة الواجب توافرها في هذه المحررات، ومن ناحية أخرى فإن جريمة التزوير تعتبر من الجرائم الحديثة إذا ما قورنت مع جريمة السرقة والقتل كونها نشأت وتطورت مع نشوء وتطور الكتابة ونظام التوثيق وبروز المحررات بنوعيها الرسمية والعرفية، الأمر الذي استدعى وضع قواعد ونصوص قانونية رادعة من أجل

---

[1]- اهتمت الشريعة الإسلامية بحفظ الأموال، وأمرت باتخاذ الوسائل الكفيلة بحفظها، وشرَّعت العقوبات الرادعة لمن يتجرأ أو يحاول الاعتداء عليها بالتزييف أو التزوير أو غير ذلك من طرق الاعتداء.وقد حرَّم الله عز وجل أكل الأموال بالحيل الماكرة والطرق الملتوية, قال تعالى: [وَلا تَأْكُلُوا أَمْوَالَكُمْ بَيْنَكُمْ بِالْبَاطِلِ وَتُدْلُوا بِهَا إِلَى الْحُكَّامِ لِتَأْكُلُوا فَرِيقًا مِنْ أَمْوَالِ النَّاسِ بِالْإِثْمِ وَأَنْتُمْ تَعْلَمُونَ] [البقرة 188]، وأباحت الشريعة الإسلامية للإنسان المدافعة عن ماله إذا اعتدى عليه ولو باستعمال القوة.

[2]- المزيد حول الموضوع: http://ns1.lawjo.net/vb/showthread.php?t=10381#ixzz1XD4u7JxD

[3]- لم يعرف القانون الجزائري جريمة تزوير المحررات، بل اقتصرا كالقانون الفرنسي على بيان الطرق التي يقع بها ولهذا فقد أورد الفقهاء، عدة تعاريف حاولوا فيها تحديد معنى التزوير المعاقب عليه وبيان ماهيته وإحاطته بحدود تمنع دخول ما ليس منه أو خروج ما هو منه، وأشهر هذه التعارف هو التعريف الذي وضعه الأستاذ: جارسون بقوله: "**التزوير في المحررات هو تغيير الحقيقة في محرر بقصد الغش بإحدى الطرق التي عينها القانون تغييرا من شأنه أن يسبب ضررا**". وعرفه الفقه الفرنسي بأنه "**تغير للحقيقة في محرر لإثبات واقعة متى وقع بقصد الإضرار**"، إدماج المشرع الجزائري القسم الخاص بالجرائم الماسة بالأنظمة المعلوماتية بالجنايات والجنح ضد الأموال واعتبر المعلوماتية مالا من نوع خاص لكنه لم يستحدث نصا خاصا بالاعتداء على سير نظام المعالجة الآلية لم يتعرض المشرع الجزائري إطلاقا التزوير المعلوماتي لا باستحداث نص خاص به ولا بتوسيع مجال التزوير ومفهوم المحرر ليشمل أية دعامة أخرى ليمتد ليشمل كافة صور التزوير الحديث أي المعلوماتي.

حماية هذه الوثائق من العبث في مضمونها والمحافظة على مصداقيتها وسلامة تداولها ببعث الثقة في محتواها ومضمونه.

لم يضع المشرع الجزائري تعريفا محددا لجريمة التزوير في المحررات ولم يقم بتحديد أركانها، وإنما اكتفى بتحديد الطرق التي تقع بها، على غرار المشرّع الفرنسي تاركين هذه المهمة للفقه والقضاء[1].

يعتبر تغيير الحقيقة أساس جريمة التزوير، فلا يتصور وقوع التغيير إلا بإبدال الحقيقة بما يغايرها، فإذا انعدم تغيير الحقيقة لا تقوم جريمة التزوير، ولكي يعتبر التغيير تزويرا، يشترط فيه ألا يؤدي إلى إتلاف ذاتية المحرر أو قيمته، إذ يتحقق الركن المادي للتزوير بتغيير الحقيقة في محرر بطريقة من الطرق التي نص عليها القانون أو النظام تغيرا من شأنه إحداث ضرر للآخرين. من خلال هذا التعريف يتضح أن الركن المادي يقوم على أربعة عناصر يتمثل الأول فيتغير الحقيقة، أما الثاني أن يكون ذلك في محرر والركن الثالث أن يكون التغير بإحدى الطرق التي حددها القانون، وأخيرا أن يكون من شأن التغير الإضرار بالآخرين.

أمّا بالنسبة للركن المعنوي لجريمة التزوير يتطلب وجود قصد جنائي، عليه لابدّ من انصراف إرادة الجاني إلى ارتكاب الفعل المكون للجريمة، واتجاه نيته إلى تحقيق غاية معينة هي استعمال المحرر فيما زور من أجله، لذلك فإنّ الركن المعنوي في جريمة التزوير، يتكون من عنصرين هما: إرادة الفعل المكون للجريمة، ونية استعمال المحرر المزور[2].

---

[1]- قانون العقوبات الفرنسي الحالي (الذي دخل حيز التنفيذ ابتداء من 01-03-1994 بموجب القانون رقم 1336-92 المؤرخ في 16-12-1992) ينص في المادة 441-1 منه على: "**يشكل تزويرا كل تغيير احتيالي للحقيقة، من شأنه إحداث ضرر، و ينجز بأية وسيلة كانت، وينصب على محرر أو على أية دعامة للتعبير عن الأفكار يكون موضوعها أو يكون من آثارها إقامة الدليل على حق أو على واقعة ذات نتائج قانونية**". هذا التعريف ينطبق عموما على جريمة التزوير وفقا للقانون الجزائري إلا في نقطة واحدة وهي حدوث التزوير على الدعائم الحديثة لتلقي البيانات التي لا يشملها القانون الجزائري.

[2]-**إيهاب فوزي السقا**، جريمة التزوير في المحررات الإلكترونية، دار الجامعة الجديدة ، القاهرة، 2008، ص58.

قد يكون التزوير ماديا أو معنويا، حيث يقع التزوير المادي بوسيلة مادية يترتب عنها أثار في مادة المحرر أو في شكله، أما التزوير المعنوي فهو الذي يقع بتغير الحقيقة دون أن يترك ذلك أثرا يدرك بالحس. قد يقع التزوير المادي وقت أو بعد إنشاء المحرر،بينما التزوير المعنوي لا يقع إلا وقت إنشاء المحرر[1]، فتذهب الغالبية العظمى من الفقه القانوني إلى عدم انطباق نصوص التزوير التقليدية على التعديل أو التغيير الواقع على المعطيات والبيانات المختزنة بشكل غير مرئي في كونها بيانات الكترونية ومغناطيسية وحجته في ذلك كالآتي:

- لا يمكن أن ينطوي تزوير البيانات المخزنة بشكل الكتروني تحت النصوص التقليدية لأن هذه الأخيرة إنما تفترض إمكانية القراءة البصرية لمحتويات المحرر المدونة فيه، وهذا غير متحقق بالنسبة للمعطيات الإلكترونية المخزنة على شريط ممغنط.
- إن تغيير الحقيقة الذي يقع على البيانات المعالجة الكترونيا أيّا كان الوعاء المحفوظة فيه لا يمكن أن تقوم جريمة التزوير بمفهومها التقليدي لانتفاء الكتابة، فطبيعة البيانات المسجلة على الشريط المغناطيسي المعالجة بطريقة الكترونية لا تسمح بقراءتها ولا التعرف بصريا على دلالتها لذلك لا يمكن اعتبارها كتابة.
- إن البيانات المثبتة على الشريط المغناطيسي للبطاقة لا تتيح فرصة قراءتها إلا بجهاز معين لذلك فالمعالجة الالكترونية لهذا النوع من البيانات لا يعبر عن فكرة بشرية وإنما عن محض فكرة إلكترونية خاصة بالآلة القارئة.

بخلاف المشرّع الجزائري نجد أن حماية بطاقة الوفاء من التزوير حظيت باهتمام المشرع الفرنسي، بموجب نصوص خاصة، ما دام أن أغلب الفقه اتجه إلى عدم اعتبار التغيير الذي يقع على البطاقة وعلى بياناتها تزويرا بالمفهوم المنصوص عليه في قانون

[1]-**منير محمد الجنبيهي، ممدوح محمد الجنبيهى**، تزوير التوقيع الإلكتروني، دار الفكر الجامعي، الإسكندرية، 2006، ص ص 98، 101.

العقوبات، خاصة بالنسبة للبيانات المشفرة، ممّا يجعل تدخل المشرع بنصوص جديدة وملائمة ضرورة حتمية لحماية البطاقات الالكترونية من هذه الجريمة المتفاقمة[1].

تغيّر الحقيقة سواء كان في محرر رسمي أو عرفي يمكن تصور حصوله في هذه المحررات في نطاق المعلوماتية، وفي هذه الحالة تسمى جريمة التزوير بأنها "تزوير معلوماتي".

ثانيًا: التزوير في المجال المعلوماتي.

لا يثير مفهوم التزوير صعوبة حيث ورد في كافة القوانين والتشريعات العقابية التقليدية، ولكن بظهور تكنولوجيا وتقنية الحاسبات الآلية قد اكتسب بعدا جديداً أضاف عليه أهمية تفوق ما كان عليه قبل ذلك، كما أكسبته شكلاً جديداً بل تسمية جديدة حيث أصبح يشار إليه بالمعلوماتية إشارة يرتبط بها بتقنية تكنولوجيا الحاسبات.

يبدو مما تقدم أن التزوير المعلوماتي يرد على بيانات في وثائق معلوماتية، تلك الوثائق يتم الحصول عليها بوسائل معلوماتية، بعبارة أدق تلك الوثائق التي يتم الحصول عليها بواسطة جهاز الكتروني أو كهرومغناطيسي أو أشرطة ممغنطة، وإن كان هنالك جانب من الفقه يرى ضرورة عدم الخلط بين الوثائق المبرمجة والوثائق المعلوماتية.

على الرغم ممّا ذكر فإنّ التزوير المعلوماتي يعادل في خطورته التزوير التقليدي، فهو كل تغيير للحقيقة في محرر بكل الطرق التي يقرها القانون المادية والمعنوية تغيراً من شأنه إحداث ضرراً للغير بواسطة استخدام الحاسب الآلي، وتأسيساً على ذلك فإن التزوير المعلوماتي يتكون من ثلاثة أركان الركن المادي المتمثل في تغيير الحقيقة

[1]- تناول المشرع الجزائري جريمة التزوير في المحررات في الفصل السابع من الباب الأول من الكتاب الثالث من الجزء الثاني من قانون العقوبات تحت عنوان التزوير، وقد تناول القسم الثالث من هذا الفصل موضوع تزوير المحررات العرفية أو التجارية أو المصرفية في المادة 219 من قانون العقوبات "كل من ارتكب تزوير بإحدى الطرق المنصوص عليها في المادة 216 في المحررات التجارية أو المصرفية أو شرع في ذلك يعاقب بالحبس من سنة إلى خمس سنوات و بغرامة من 500 إلى 2000 دج. أنظر: **عبد الله ليندة**، النظام القانوني لبطاقة الدفع، مذكرة ماجستير في القانون الخاص، تخصص قانون الإصلاحات الاقتصادية، جامعة جيجل، 2007، ص 141143.

والركن المعنوي المتمثل بالقصد الجنائي والركن الخاص ينصب على الضرر الذي يسببه الركن المادي ويصيب المصلحة العامة أو مصلحة شخص من الأشخاص.

يقع التزوير في مجال المعلوماتية عندما يكون التلاعب وتغيير الحقيقية منصبا على المعلومات المخزنة بالنظام المعلوماتي، فتغيير الحقيقة يقع على المعلومات يتمّ التعامل بها من خلال شبكة الانترنت، ويتخذ التزوير في المحررات الإلكترونية إحدى الصورتين:

الصورة الأولى:تتمثل في التلاعب في معلومات داخل نظام الحاسب الآلي، وذلك لتغيير الحقيقة في المحرر، سواء بتعديل المعلومات أو محوها أو جزء منها.

الصورة الثانية: تتمثل في إدخال معلومات غير صحيحة لخلق محرر غير صحيح.

كلتا الطريقتين تتم بنية استعمال المحرر لما زور لأجله، فالتزوير في صورته المستحدثة يعتمد على التلاعب في المعلومات الخزنة داخل النظام المعلوماتي، ويتم ذلك بطرق ثلاث[1]:

الطريقة الأولى: من خلال عمليات الإدخال المعلوماتي أيا كانت وسيلته، سواء مباشرة بالاتصال المباشر بين مدخل المعلومات والنظام، كأن يكون من الأشخاص المسموح لهم بالتعامل معه وفقا لاختصاصات وظيفية، أو بطريقة غير مباشرة بالاتصال بالنظام المعلوماتي، ومن الأمثلة عن هذه الطريقة قيام موظف بنك بإدخال رصيد وهمي لعميل في البنك، مما يترتب على ذلك إمكانية تحويل مالي حقيقي لحساب أخر.

الطريقة الثانية: يتم التلاعب فيها في مرحلة المعالجة الآلية للمعلومات من خلال برامج التلاعب في نظم عملها كي تقوم بإحداث هذا التلاعب في معلومات النظام ومثال هذه الطريقة تلاعب موظف البنك بالبرامج البنكية عن طريق تغير بعض الأوامر التي تعمل

[1]- لمزيد من التفاصيل أنظر: **محمد أمين الرومي:** جرائم الكمبيوتر والانترنت، الدار المطبوعات الجامعية الإسكندرية، مصر 2003، ص 109، 130 وكذا: **مصطفى محمد موسى،** التحقيق الجنائي في الجرائم الإلكترونية مطابع الشرطة، القاهرة، 2008 ص 632، 646.

بها البرامج ، كأن يجعل النظام يجبر الكسر في الرصيد للرقم الأدنى تاركا مبالغ فائضة من حسابات العملاء[1].

الطريقة الثالثة:تتم في مرحلة الإخراج المعلوماتي وهي لا تكون منفصلة عن الطريقتين السابقتين، بل متممة لهما من خلال ما حدث من تلاعب في مرحلة الإخراج المعلوماتي على الدعامة سواء كانت تقليدية، متمثلة في مخرجات ورقية أو دعامة.

ثالثًا: كيفية تزوير التوقيع الإلكتروني.

يكون التزوير أسهل من غيره، وذلك لضعف إجراءات الأمان والثقة في التوقيع الإلكتروني، فالتوقيع البيومتري كما سبق القول يعتمد على الخواص الفيزيائية والطبيعية للإنسان، مثل بصمة العين، وبصمة الأصبع، وبصمة معالم الوجه وخاصية الصوت حيث يتمّ عن طريق تخزين صورة دقيقة لهذه الصفة أو الخاصية في ذاكرة النظام في الكمبيوتر، ويتم مقارنتها مع بصمة صاحبها عند إجراء أي تصرف أو تعامل، فإنّ كانت مطابقة يخول صاحبها بإجراء التصرف.

يسهل تزوير هذه الطرق، بعد أن يتم مهاجمتها أو نسخها من قبل قراصنة الحاسب الآلي أو كما يطلقوا عليهم الهايكرز[2] يتم فك شفرتها ثم استخدامها بطريقة غير مشروعة ومن أهم الصور الأكثر عرضة لتزوير نجد التوقيع بالرقم السري وكذلك التوقيع الرقمي.

---

[1]-**إبراهيم بن سطم بن خلف العنزي**، المرجع السابق، ص 109.

[2]-هايكرز عموما كلمة تصف المختص المتمكن من مهارات في مجال الحاسوب وأمن المعلوماتية. والهاكر (بالإنجليزية: Hacker) أساسا كلمة أطلقت على مجموعة من المبرمجين الأذكياء الذين كانوا يتحدوا الأنظمة المختلفة ويحاولوا اقتحامها، وليس بالضرورة أن تكون في نيتهم ارتكاب جريمة أو حتى جنحة، ولكن نجاحهم في الاختراق يعتبر نجاحا لقدراتهم ومهارتهم، إلا أن القانون اعتبرهم دخلاء تمكنوا من دخول مكان افتراضي لا يجب أن يكونوا فيه والقيام بهذا عملية اختيارية يمتحن فيها المبرمج قدراته دون أن يعرف باسمه الحقيقي أو أن يعلن عن نفسه، ولكن بعضهم استغلها بصورة إجرامية تخريبية لمسح المعلومات =والبعض الآخر استغلها تجاريا لأغراض التجسس والبعض لسرقة الأموال، وجدت الكثير من الشركات مثل مايكروسوفت ضرورة حماية أنظمتها ووجدت أن أفضل أسلوب هو تعيين هؤلاء الهاكرز بمرتبات عالية مهمتهم محاولة اختراق أنظمتها المختلفة وإيجاد أماكن الضعف فيها واقتراح الوقاية اللازمة، في هذه الحالة بدأت صورة الهاكز في كسب الكثير من الايجابيات. إلا أن المسمى الأساسي واحد. وقد أصبحت كلمة هاكز تعرف مبرمجا ذا قدرات خاصة يستخدمها في الصواب كما يمكن استخدامها في الخطأ. ينظر كثيرون للهاكر على أنه شخص مدمر وسلبي، ويقرن البعض كلمة هاكر مع قرصان الحاسوب. وذلك

1- تزوير التوقيع الإلكتروني الذي يتم بالرقم السري:

أكثر تطبيقات هذه الصورة وأهمّها بطاقات الصرف البنكي بأنواعها المختلفة ويعدّ أهمّ صور الاستخدام غير المشروع للبطاقات البنكية كما يلي:

1. استخدام بطاقات بنكية مزيفة جزئيا أو مزيفة كليا.
2. استخدام بطاقات بنكية مسروقة.
3. استخدام بطاقات بنكية صحيحة صدرت بطريقة غير مشروعة.

إنّ المبدأ الأساسي لتزوير البطاقة البنكية هو سرقة بياناتها من خلال جهاز الحساب الآلي،باستخدام أدوات معينة يتم نقش هذه البيانات على بطاقة أخرى تكون معدة لهذا الغرض أو تكون بطاقة منتهية أو مسروقة ويتم استخدامها بعد ذلك في عمليات الدفع أو السحب.

كما سبق القول في الفصل الأول من أكثر تطبيقات التوقيع الإلكتروني نجد بطاقات الدفع يمكن أن تكون هذه البطاقة مزورة، أي يمكن أن يكون هنالك اعتداء من قبل الغير بالتزوير أو السرقة أو النصب[1] فإن صور إساءة استعمال بطاقات الدفع كثيرة نتناولها فيما يلي:

أ-تزوير بطاقة الدفع:

بتأثير من بعض ما ورد في الإعلام، حيث يرجع السبب لقلة فهمهم حقيقة الهاكر، وخلطهم لها بكلمة القرصنة (بالإنجليزية: Piracy) التعبير الذي يصف البيع غير المشروع لنسخ من أعمال إبداعية، أما الكراكر مصطلح أطلق فيما بعد للتمييز بين الهاكر الصالح والهاكر المفسد، وبالرغم من تميز الإثنين بالذكاء وروح التحدي وعدم خوفهم من مواجهة المجهول. إلا أن الكراكر يقوم دائما بأعمال التخريب والاقتحام لأسباب غير ايجابية. بينما الهايكر يبتكر الحلول للمشاكل ويحاول أن يبدع في عمله. أنظر على الموقع: http://ar.wikipedia.org/wiki

(1)-**إيهاب فوزي السقا**، المرجع السابق، ص187.

جرمت المادة 1/323 من قانون العقوبات الفرنسي المساس بأنظمة المعالجة الرقمية للبيانات التي يمكن الاعتماد عليها لردع بعض الممارسات غير المشروعة باستعمال بطاقات الدفع المستعملة بنظام معتمد على أجهزة وميكانيزم إلكتروني.

تمّ التأكيد على قرار التجريم هذا من طرف محكمة الاستئناف بباريس في 6 ديسمبر 2000، كما يوجد في قانون النقد والمال تجريم خاص والمتعلق بالممارسات الإجرامية المتعلقة باستعمال بطاقات الدفع في نص المادة 4-163[1].

كما تم التأكد من ذلك في قانون 15 نوفمبر 2001 أضاف لقانون النقد والمال للمادة 1-4-163 والتي وسعت من الأفعال المجرمة إلى صنع، الاستحواذ، ترك، منح أو وضع تحت تصرف الغير الوسائل والبرامج الرقمية أو كل البيانات الخاصة بتزوير بطاقات الدفع، كما يعاقب على مجرد محاولة القيام بهذه الممارسات[2].

فيتم التزوير عندما تفقد بطاقة الائتمان من العميل، وقد تسرق منه فيتلقاها الغير ويقوم باستبدال ما بها من بيانات ومعلومات، ليقوم باستخدامها في عمليات الشراء والسحب، فيشكل اعتداء ليس على البنك المصدر للبطاقة فحسب ولكن يمتد الاعتداء ليشمل حامل البطاقة أيضا.هذا الاعتداء يشكل في رأي جمهور الفقهاء جريمة تزوير على اعتبار أن التزوير هو تغيير الحقيقة وتغيير ما على الشريط الممغنط الخاص بالبطاقة، يعدّ تزويرا لأنّه يغيّر ما على البطاقة من بيانات ومعلومات[3]. تتمّ هذه العملية عن طريق ما يسمى بعملية skimming devis للحصول على خصائص الهوية الإلكترونية من

---

[1]-**GOVALDA Ch, STOUFFELT J**, Droit du crédit, effets de commerce chèques carte de paiement transfert de fonts, 6ème édition, Ed. litec, 2006, p389.
La falsification ou contrefaçon de carte de paiement ou de retrait l'usage en connaissance de cause de titre ainsi trafiques, ainsi que l'acceptation en connaissance de cause de tels titres sont punissable pénitent, art. L163-4 du code monétaire et financier.

[2] -Ch. Govalda, J. stoufflet, idem, p 389.

[3] - **إيهاب فوزي السقا**، المرجع السابق، ص 188. في نفس المرجع توجد العديد من تقنيات التزوير منها: kimming devise، inposing، scannar وعملية الصقل أو Buffer أو استعمال قارئ الكتروني مغناطيسي electronic magnitic reader.

القطاعات المغناطيسية من إحدى البطاقات الصحيحة، ثم نقلها بنفس خصائصها إلى بطاقة أخرى.

قد يكون تزوير البطاقة الائتمانية ذاتها كليا أو جزئيا، حيث يتمّ التزوير الكلي باصطناع البطاقة بالكامل وتقليد ما عليها من كتابات وحروف وعلامات وأشرطة، أو من خلال بيانات بطاقة صحيحة يتم الحصول عليها بتصويرها فوتوغرافيا بواسطة التاجر بعيدا عن أعين العميل، وقد يكون بتغيير بعض بيانات البطاقة كنزع الشريط الممغنط الأصلي ووضع الشريط الخاص بالفاعل القائم بعملية التزوير[1]. كل هذه الأحوال والأنماط لا تدخل في حيز تعريف الفقه للتزوير، حيث يعرفه أنه: "**تغيير الحقيقة في محرر بإحدى الطرق التي تنص عليها القانون تغييرا من شأنه إحداث ضرر ومقترن بنية استعمال المزور فيها أعد له**".

إذا كان تعريف الفقه ينطوي على التزوير في المحررات المادية الملموسة، فإن التزوير في مجال المعالجة الآلية للبيانات عبر شبكة الإنترنت يعد من أخطر طرق الغش التي تقع في هذا المجال، خاصة بحلول الحساب الآلي والمحررات الإلكترونية محل الأوراق في كافة المجالات، ممّا يزيد من صعوبة اكتشاف وإثبات التزوير الذي يقع في هذا المجال[2].

---

[1] - **إيهاب فوزي السقا**، المرجع نفسه ، ص 192.

[2] - أعطيكم مثالاً هنا وهو تيم كورادو أشهر لصوص البطاقات الائتمانية على شبكة الانترنت الذي لا يزال حراً طليقاً لأنّه كلما اقتادته الشرطة إلى المحكمة كلما ازدادت ضحكته ذلك لأنه لا يوجد دليل واحد ضده، قام هذا البريطاني باقتحام عشرات المواقع في شبكة الانترنت واستولى على أرقام وبيانات ما يزيد على (124) ألف بطاقة ائتمانية تخص عملاء هذه المواقع، وقام بنشر أرقامها وبياناتها على شبكة الانترنت، وقام أيضاً بإرسال بعض بيانات هذه البطاقات إلى بعض المواقع الشخصية لأفراد آخرين لا يعرفهم ولا يعرفونه، وقال (تيم كوراد و (حين إلقاء القبض عليه للمرة الأولى، إنّ رهان رجال الشرطة ضده هو رهان خاسر لأنهم لا يملكون دليلاً واحداً ضده، وقال أيضاً أنّ هدف من قام بهذه العمليات التي يتهم بها هو إيقاظ الشركات التجارية التي يوجد لها مواقع على شبكة الانترنت من سباتها العميق ودفعها لإنجاز المزيد من إجراءات الحماية لمواقعها الالكترونية وبالتالي حماية أموال زبائنها، وأفلت كورادو من العقاب بسبب واحد وهو أن الموقع الذي تقول الشرطة أنّه استعمله في عملياته مسجل في شركة (Great solution) التي يوجد مقرها في مقاطعة ويلز البريطانية، ولكن كل البيانات الموجودة في هذا الموقع لا تدل أبداً على أي شيء يتعلق بشخصية تيمكورادو للمزيد أنظر على الموقع: http://hewar.kacnd.org/vb/showthread.php?t=153

يأخذ تزوير بطاقات الائتمان في نطاق شبكة الإنترنت والمعلوماتية صورة تحليق أرقام بطاقات ائتمان خاصة ببنك معين، من خلال تزويد الحاسب بالرقم الخاص بالبنك مصدر البطاقة بواسطة برنامج تشغيل خاصة[1].

ب- استعمال الغير لبطاقة دفع مزورة أو مسروقة:

إن منتحل الصفة سارقا كان أو مزورا والذي يستعمل البطاقة لسحب الأموال من الموزعين الالكترونيين للأوراق النقدية معاقبون جنائيا d'escroquerie، ومسئولون مدنيا اتجاه الضحايا (البنك والعميل صاحب البطاقة) جراء هذا الاختلاس[2]، في جميع الحالات فإن سرقة البطاقة أو ماكنة السحب يعد اختلاسا لمنقول مملوكا للغير بنية تملكه طبقا لنص المادة 311 عقوبات مصري[3].

تختلف جريمة تزوير المحررات عن جريمة استعمال المحررات المزورة، فهما جريمتان مستقلتان عن بعضهما البعض، وجريمة استعمال المحررات المزورة إنّما يقصد بها دفع هذه المحررات إلى التعامل وفي مجال بطاقة الوفاء قيام الجاني باستعمال بطاقة دفع مزورة في الحصول على السلع والخدمات لدى التاجر المورد، ثم إن العقاب على استعمال محرر مزور وارد حتى ولو لم يكن المستعمل هو نفسه المزور، كما يعاقب المزور حتى ولم يعقب فعله هذا استعمال المحرر المزور[4].

ج- الحصول على بطاقة الدفع بمستندات مزورة:

الأصل أن الحصول على بطاقة الائتمان يتم طبقا للقواعد المعمول بها في البنك مصدر هذه البطاقة وحسب المستندات المطلوبة، شرط أن تكون مستندات صحيحة غير

---

[1] - **محمد أمين أحمد الشوابكة**، جرائم الحاسوب و الانترنت،دار الثقافة للنشر و التوزيع ، الأردن ،2004 ، ص 201.

[2] - Ch. Govalda, J. stoufflet, op-cit, Ed2. p480.

[3] - **إيهاب فوزري السقا**،المرجع السابق ، ص 197.

[4] - فثار جدل فقهي حول طبيعة جريمة استعمال بطاقة الدفع فذهب فريق إلى تكييفها أنها جريمة سرقة باستعمال مفتاح مصطنع وذلك على أساس أن البطاقة المزورة تدخل في مفهوم المفتاح المصطنع، وذهب فريق آخر إلى تكييف استعمال بطاقة دفع مزورة من قبل الغير جريمة نصب، فإذا ما قدم هذا الشخص البطاقة المزورة للتاجر يكون قد أوهمه بصحة هذه البطاقة مما يؤدي بالتاجر إلى الاعتقاد بوجود رصيد وهمي لهذا الحامل غير الشرعي للبطاقة المزورة. أنظر: **عبد الله ليندة** ، المرجع السابق، ص 144.

مخالفة للحقيقة، فلا يجوز أن يتقدم طالب بطاقة الائتمان بأسماء منتحلة وعناوين وهمية، أو أي ضمانات غير حقيقية وإلا تعرض للعقوبات الجنائية، فضلا عما قد يتحمله البنك من خسائر نتيجة استخدام البطاقة في شراء السلع والخدمات بمبالغ كبيرة ثم يقوم حامل البطاقة بالهرب، فلا يستطيع البنك الاستدلال عليه، فيضطر إلى دفع قيمة المستحقات الناتجة عن استعمال طالب البطاقة بمستندات مزورة[1].

تقوم هذه الجريمة حين يتقدم الجاني إلى البنك بمستندات شخصية مزورة منتحلا فيها صفة الغير أو بيانات غير صحيحة، فيصدر البنك له بطاقة صحيحة يستخدمها في شراء سلع وخدمات ولا يتمكن البنك من استرداد قيمتها بعد ذلك، إما لعدم الاستدلال على صاحب البطاقة وإما لأن الضمانات غير كافية، وفي إحدى القضايا حدث أن قام أحد البنوك برفع –دعوى جنحة مباشرة- ضد أحد الأشخاص استنادا للمادة 336 عقوبات مصري، بتهمة الاستيلاء على مبلغ 459.90 دولار ومبلغ 7904.30 جنيها تخص البنك نفسه، حيث قام المدعي عليه باستخراج بطاقة "فيزا كارد" من البنك المدعي لاستخدامها في السوق المحلية[2]، بعد أن قدم مستندات تثبت دخله السنوي لا يقل عن مبلغ 2400 جنيه مصري، حتى يتم خصم قيمة المشتريات منه شهريا فضلا عن تعهده بعدم استخدام البطاقة ما لم يكن رصيده كافيا[3]. حيث لم يقم بسداد مشترياته إلى التجار الذين رجعوا على البنك بوصفه ضامنا لهم، قام البنك بالسداد، وطالب بعقاب المدعي عليه بوصفه قد استعمل طرقا احتيالية.

---

[1]- **بيار إميل طوبيا**، بطاقة الاعتماد والعلاقات التعاقدية المنبثقة عنها، منشورات الحلبي الحقوقية، 2000، ص، ص 57-58.

[2]- **مصطفى محمد موسى**، التحقيق الجنائي في الجرائم الإلكترونية، في قضية الاستيلاء على معلومات بطاقات الائتمان ص633، وتزوير كروت الفيزاكارت، ص634.

[3]- **عبد الفتاح بيومي حجازي**، الدليل الجنائي والتزوير في جرائم الحساب الآلي والانترنت، دار الكتب القانونية، الإسكندرية 2002، ص، ص 180، 260.

يوجد نوع آخر من الأساليب غير المشروعة يقوم بها بعض حاملي البطاقات الملغاة[1]نتيجة عدم استعماله للبطاقة بالشكل الجيد، فقد يرغب الشخص في استخراج بطاقة ائتمانية جديدة ولكن لا يستطيع، نظرا لتاريخه الائتماني السيئ لدى جهات إصدار البطاقات، فيذهب إلى بعض العصابات الإجرامية والتي تطلق على نفسها قيادات الإصلاح الائتماني والتي تحصل على مبالغ مالية تصل إلى ألفي دولار، حتى يتمكن طالب البطاقة من استخراج بطاقة ائتمان دون[2] اعتراض البنك المصدر، بعد تغيير المستندات التي تدل على سوء استخدامه للبطاقة من قبل[3].

2-تزوير التوقيع الرقمي:

التوقيع الرقمي يتم بواسطة منظومة إلكترونية تتخذ شكل حروف أو أرقام أو رموز أو إشارات...الخ، حيث لا يمكن تقليدها إنما يمكن استعمالها دون علم مالكها، عن طريق الحصول على منظومة التوقيع بطريق التجسس الإلكتروني أو الدخول غير المشروع[4]، فالتوقيع بهذه الطريقة سليما إلاّ أنه استخدم من غير صاحبه. وعليه يتم الكشف عن التوقيع الرقمي المزور بإثبات أنّه لم يصدر من مالك المنظومة، وإنّما من شخص آخر، قام بسرقتها.

تعتبر جرائم تزوير البيانات المنظومة على شبكة الإنترنيت أكثر الجرائم شيوعا, حيث يكون تزوير البيانات بالدخول إلى قاعدة البيانات وتعديلها، سواء بإلغاء بيانات

---

[1]- **أمجد حمدان الجهني**، الاستخدامات غير مشروعة لبطاقات الدفع الالكتروني من قبل الغير، مركز الدراسات القضائية في:06.2009/01، المملكة الأردنية الهاشمية، ص 4، مقال منشور على الموقع: www.coiss.com/replay.php

[2]- **عبد الفتاح بيومي حجازي**، المرجع السابق، ص 167.

[3]- بالرغم أن النسبة العالمية لتقديم مستندات مزورة لاستخراج بطاقة ائتمان، قد يشكل نسبة صغيرة بالنسبة لجمالي الاعتداءات الواقعة على البطاقة، إلاّ أنّها تتزايد في الفترة الأخيرة بسبب إمكانية تزوير وثائق ومستندات الشخصية بجودة وسهولة، حقق هذا النوع من الاحتيال عام 2001 ما يقارب من 6% من إجمالي الخسائر الناتجة عن الاعتداءات الخاصة ببطاقة الائتمان مقارنة بـ 1% عام 1994، أنظر: **إيهاب فوزي السقا**، المرجع السابق، ص 168-169.

[4]-أنظر **منير محمد الجنبيهي، ممدوح محمد الجنبيهى**، المرجع السابق، ص54

موجودة بالفعل أو بإضافة بيانات لم تكن موجودة من قبل[1]. كما تتميز جريمة تزوير التوقيع الإلكتروني الرقمي بكونها جريمة مركبة تتكون من جريمتين هما:جريمة سرقة منظومة التوقيع الإلكتروني الرقمي فإنها قد تتم بطريقة تقليدية كالتجسس، والدخول غير المشروع للنظام المعلوماتي عن طريق القرصنة الإلكترونية[2]، من الجدير بالذكر أنّ لجريمة تزوير التوقيع الإلكتروني، يصعب اكتشافها إلاّ بعد حصول الجريمة الثانية وهي الاستخدام غير المشروع لمنظومة التوقيع الإلكتروني.

رابعًا: تزوير شهادة التصديق.

توجد جهات يُرخص لها سواء كانت شخصية أو اعتبارية باعتماد التوقيعات الإلكترونية بشهادات مصدق عليها منهم، وهذه الشهادات يترتب عليها آثارا قانونية تتمثل في إنشاء التزامات وإثبات حقوق بالنسبة لطرفي العقد في التجارة الإلكترونية في حالة اعتماد التوقيع الإلكتروني بينهما، لذلك فإن تزوير أو تقليد شهادات التصديق على التوقيع الإلكتروني يعادل في خطورته تزوير أو تقليد التوقيع الإلكتروني ذاته. وجهات التصديق الالكتروني تعمل تحت رقابة الدولة، تقوم بمنح شهادات ضمان للتوقيع الالكتروني وتقوم بدور الوسيط في المعاملات الالكترونية، لكن هذه الشهادات تنشأ وتعالج وتسلم وتحفظ بطريق إلكتروني وأنها أصلا عبارة عن بيانات ومعلومات إلكترونية تخزن عبر وسيط إلكتروني، فقد يتمكن أحدهم من اخترق هذا الوسيط ويقوم بتقليد أو تزوير أو نشر شهادة التصديق مزورة، هنا تقوم جريمة تزوير شهادة التصديق الإلكتروني التي تكون عادة لأغراض احتيالية أو تقديم بيانات مزورة لمزود خدمات التصديق. نرى أن هذه الجريمة تقترب إلى حد ما إلى التزوير التقليدي حين يقوم الجاني بوضع أسماء أو صور أشخاص مزورة، فقد ينتحل هوية غيره -انتحال لشخصية الآخرين- بتقديم بيانات خاطئة وغير

---

[1] - **عصمت سعد**، خسائر بالمليارات...جريمة الإلكترونية كل ثلاث دقائق على الانترنت، مقال منشور على الموقع:
http://www.ensan.net/news/212/ARTICLE/3596/2008-04-22.htm

[2] - **عصمت سعد**، نفس المرجع، ص98.

صحيحة عن هويته إلي مزود خدمات التصديق، هذا الأخير يصدر الشهادة طبقا لهذه البيانات.

يتمثل الركن المادي في تزييف الطلب، ذلك أنّ الجاني أو نائبه يقدّمان بيانات غير صحيحة أيا كان موضوع هذه البيانات سواء كانت تتعلق بهوية صاحب الشهادة أو هوية الشخص المفوض، هذه البيانات تحدد شخص صاحب التوقيع الإلكتروني وصاحب الشهادة تحديدا دقيقا. يتعين كذلك تقديم هذه البيانات الكاذبة أو المضللة إلى مزود خدمات التصديق، ويكون الغرض من ذلك هو استصدار شهادة التصديق الإلكتروني أو وقف لشهادة صادرة وقائمة بالفعل أو إلغائها[1]، وهذه الجريمة من الجرائم العمدية، فصورة الركن المعنوي فيها القصد الجنائي العام بعنصريه العلم والإرادة.

الفرع الثالث

جريمة صنع أو حيازة برنامج لإعداد توقيع إلكتروني مزور

يتمثّل الركن المادي لهذه الجريمة في صور عديدة هي: صناعة نظام معلوماتي برنامج لإعداد توقيع إلكتروني، حيازة النظام أو البرنامج وذلك بغرض إعداد توقيع إلكتروني دون موافقة صاحبه.أما محل الجريمة هنا هو إعداد توقيع إلكتروني، الأمر الذي يقربنا من فكرة الاصطناع أو التقليد في التزوير بمفهومه التقليدي، ووسيلة الجاني في هذه الجريمة نظام معلوماتي أو برنامج يساعده في إنجاز مشروعه الإجرامي وهو التوقيع الإلكتروني[2] رغما عن إرادة صاحبه، يخرج من نطاق هذه الجريمة، قيام الجهة المرخص لها حسب القانون بإعداد توقيع إلكتروني للشخص طالما أن ذلك برضاه وبموافقته.

الفاعل في هذه الصورة من التعدي على التوقيع الإلكتروني قد يقوم بصناعة البرامج أو النظام المعلوماتي، بمعنى خلقه من العدم، أي تم تصميمه حسب مواصفات فنية

[1]-**هدى حامد قشقوش**، المرجع السابق، ص588.

[2]-**عبد الفتاح بيومي حجازى**: الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، مرجع سابق ، ص 228.

وتقنية معينة بنفس الأدوات التي يعد بها البرامج أو النظام المشروع لهدف التوصل في النهاية إلى عمل ذلك التوقيع الإلكتروني.

يمكن أن يكون الجاني شخص طبيعي أو اعتباري مرخص أو غير مرخص له بالعمل في هذا المجال، طالما لا توجد موافقة لذوي الشأن لاستخراج هذا التوقيع من صاحبه، فمناط التجريم هنا أن يتم عمله رغما عن إرادة صاحبه ولو تم ذلك من طرف الشخص المرخص له بالعمل في هذا المجال،أما الوسيلة التي يستخدمها الجاني مجموعة من الأجهزة والأدوات التي يختلس بها معلومات عن توقيعات قائمة بالفعل ليحصل على نسخة منها دون موافقة أصحابها، أو عمل برنامج معلوماتي جديد[1] غير النظام القائم وذلك حتى يساعده في تحقيق غرضه الإجرامي غير المشروع، لا تقوم الجريمة إذا لم يكن للنظام أو البرنامج القدرة الفنية على عمل التوقيع الإلكتروني، لذلك يجب توفر الشروط[2] الثلاثة لقيام الجريمة، أمّا الصورة الثانية للركن المادي في هذه الجريمة فهي حيازة برنامج أو نظام معلوماتي لإعداد توقيع إلكتروني دون موافقة صاحبه، والحيازة المشروعة لهذا البرنامج أو النظام المعلوماتي لا عقاب عليها طالما أن الشخص مرخص له بهذه الحيازة من الجهة المختصة، بهدف توثيق هذه التوقيعات طالما لم يثبت أن نيته قد اتجهت إلى استخراج توقيع إلكتروني رغما عن إرادة صاحبه.

أمّا الحيازة المعاقب عليها في هذا الفرض، فهي حيازة البرنامج أو النّظام المعلوماتي القادر على عمل توقيع إلكتروني رغما عن إرادة صاحب الشأن، والفرض أن حيازة الجاني للبرنامج المعلوماتي غير مشروعة، أي غير مالكا له أو مستأجرا أو

---

[1]- راجع في ذلك**عبد الفتاح بيومي حجازي**،" التجارة الإلكترونية في القانون العربي النموذجي لمكافحة جرائم الكمبيوتر والانترنت مرجع سابق، ص161- 166. وأيضا في "**النظام القانوني لحماية التجارة الإلكترونية** مرجع سابق، ص ص310،294.

[2]- شروط العقاب: **أولا** صناعة برنامج أو نظام معلوماتي **ثانيا**: البرنامج أو النظام له القدرة الفني لعمل توقيع إلكتروني **ثالثا**: أن يكون ذلك رغما عن إرادة صاحب التوقيع ذاته.لا عقاب على الشروع ولا على الأعمال التحضرية، للمزيد من التفاصيل أنظر: **عبد الفتاح بيومي حجازي**، التجارة الإلكترونية في القانون العربي النموذجي لمكافحة جرائم الكمبيوتر والانترنت، المرجع السابق ص 163.

مستعيرا من آخر، حيث ألزم المشرع المصري الحصول على الترخيص من الجهات المختصة، وقد خول مركز المعلومات ودعم القرار بمجلس الوزراء منح الترخيص للجهات أو الأشخاص الراغبة في إعداد هذه البرامج أو صناعتها أو استرداها وإلاّ عدت الحيازة للبرنامج أو النظام المعلوماتي غير مشروعة[1].

الفرع الرابع

جريمة الدخول بالغش على قاعدة بيانات التوقيع الإلكتروني

نقصد بقاعدة البيانات التي تتعلق بالتوقيع الإلكتروني البيانات المخزنة داخل الحساب الآلي أو قرص منفصل، مثل البيانات المتعلقة باسم صاحب التوقيع ومهنته وكافة بياناته الشخصية وكافة المعلومات المتعلقة بذلك التوقيع والتي يفترض سريتها.

يتمثل الدخول غير المشروع في نظم وقواعد معالجة البيانات، سواء تلاعب بهذه البيانات بتعديلها، إلغاءها أولا- مجرد الدخول غير المشروع يعتبر جريمة الكترونية-، أو إعاقة تشغيل النظام باستخدام أي وسيلة تقنية للدخول علي نظام معالجة البيانات، فمثلا يمكن الدخول عن طريق كلمة السر الحقيقية إذا لم يكن للجاني حـــق استخدامها أو باستخدام برنامج أو شفرة خاصة، ويستوي أن يكون الدخول علي النظام بطريقة مباشرة أو غير مباشرة والدخول من الجرائم الوقتية. أمّا البقاء داخل النظام فيفترض اختلاس وقت النظام ويتخذ صورة الجريمة المستمرة[2]، ويمكن أن يكون البقاء لاحقا على دخول

[1]- تناول المشرع الفرنسي مجموعة من الجرائم التي تقع علي أنظمة معالجة البيانات 1-323 إلى 7-323، وتعاقـــب المادة الأولي علي الدخول بطريق الغش أو التدليس Frauduleusement علي أو إبقاء الاتصال بطريقة غير مشروعة نظام لمعالجة البيانات بالحبس لمدة سنة وبغرامة مائة ألف فرنك فرنسي، وتكونت العقوبة الحبس لمدة سنتين وغرامـــة 000, 200 ألف فرنك فرنسي إذا ترتب على نشاط الجاني إلغـــاء أو تعديـــل البيانات الموجودة بالنظام أو تعديل تشغيل النظام (م323-1)، وتعاقب المادة الثانية بالحبس لمـــدة ثلاثة سنوات وغرامة 300,000 ألف فرنك فرنسي على إعاقة أو التسبب فـــي تحريف تشغيل نظـــام معالجـــة البيانات (م 323-2).

[2]-نجد أن المشرع المصري قد نصفي المادة 26 منه على تجريم أفعال الغش أو التدليس التي تقع على نظام معلومات أو قاعدة بيانات تتعلق بالتوقيعات الإلكترونية، وكذلك فقد جرمت هذه المادة أفعال الاتصال أو الإبقاء على الاتصال بنظام المعلومات أو قاعدة البيانات بصورة غير مشروعة. أيضا فإن المادة 27 من هذا المشروع قد جرمت أفعال الصنع أو الحيازة أو الحصول على

غير مشروع، ويمكن أن يكون البقاء لاحقا على دخول مشروع والدخول يكون عن طريق الغش أو التدليس[1].

يتمثل الركن المادي في هذه الجريمة في قيام الجاني بالاتصال بنظام البيانات والمعلومات المتعلق بالتوقيع، حيث أنّ الجاني ليس له حق الاتصال بهذين النظامين المتعلقين بالتوقيع الإلكتروني،فقام بالاتصال بمها تحققت عدم المشروعية،أو يكون له حق الاتصال بمها خلال المدة محددة أو في أوقات محددة وانتهت المدة المحددة للاتصال أو الفترة التي يجوز له فيها الاتصال، ومع ذلك أبقى الاتصال قائما، ومن هنا تتحقق عدم مشروعية هذا الفعل، ويتوافر به السلوك الإجرامي الذي يقوم بيه الركن المادي في هذه الجريمة[2]، وهذه الجريمة من الجرائم العمدية، الركن المعنوي فيها هو القصد الجنائي العام بعنصريه العلم والإرادة، وذلك بأن يعلم الجاني بحقيقة سلوكه الإجرامي، وأنّ ذلك محضور بنص القانون لقد نص المشرع الجزائري على هذه الجريمة في المادة[3]394 ق ع ج الفقرة الأولى لم يقصد به التوقيع الإلكتروني بل النظام المعلوماتي، حيث يجب لقيام الجريمة اشتمالها على:

=نظام معلومات أو برنامج لإعداد توقيع الكتروني دون موافقة صاحب الشأن.كذلك فإن المادة 28 منه قد جرمت أفعال التزوير أو التقليد لمحرر أو توقيع إلكتروني أو شهادة اعتماد توقيع إلكتروني، وكذا فقد جرمت هذه المادة الاستعمال للمحرر المزور أو للتوقيع الإلكتروني المزور أو للشهادة المزورة باعتماد التوقيع الإلكتروني بشرط ثبوت علم الجاني بذلك.

[1]- يقصد بالغش أو التدليس المعلوماتي أن يكون الدخول إلى قاعدة البيانات قد تم بوسيلة إلكترونية يكون مجرد من المشروعية أي بدون إذن قضائي، أو ليس من قبل الأشخاص الذين يحق لهم الإطلاع على هذا النظام أو قاعدة البيانات المتعلقة بالتوقيع الإلكتروني.

[2]-**عبد الفتاح بيومي حجازي**، التجارة الإلكترونية في القانون العربي النموذجي لمكافحة جرائم الكمبيوتر والانترنت، مرجع سابق 159.

[3]-**قانون 15/04** المؤرخ في 10 /2004/11 المعدل والمتمم للأمر 156/66المؤرخ في 1966/06/08 المتضمن قانون العقوبات ج ر عدد 71 صادر في 10نوفمبر2004.

أولا: فعل الدخول: ذهب الفقه الفرنسي إلى أن الدخول له مدلول معنوي، حيث يشبه الدخول إلى النظام بمثابة الدخول في ذاكرة الإنسان، كما له مدلول مادي يتمثل في كون الشخص قد حاول الدخول أو دخل بالفعل إلى النظام المعلوماتي[1].

لم يحدد المشرع وسيلة الدخول إلى النظام، فيمكن الدخول بأية وسيلة كانت، وذلك عن طريق كلمة السر الحقيقية متى كان الجاني غير مخول في استخدمها أو باستخدام برنامج أو شفرة خاصة أو عن طريق استخدام الرقم الكودي لشخص آخر[2].

ثانيا: فعل البقاء: يقصد بفعل البقاء "**التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام**"، أي الدخول غير المشروع إلي حاسب آلي بقصد ارتكاب جريمة أو تسهيل ارتكاب جريمة سواء بواسطته أو بواسطة شخص آخر، والواضح هنا أن الاختراق المعاقب عليه يكون محله جهاز الحاسب الآلي من جهة،من جهة أخري نجد أن هذه الجريمة يشترط لقيامها توافر القصد الجنائي العام والخاص معا وبالتالي فإن توافر القصد العام فقط لا يكفي لقيام الجريمة.

الفرع الخامس

جريمة فض مفاتيح التشفير

تقع هذه الجريمة على موضوع التجارة والضرر محقق الوقوع في المستقبل من جرائم الخطر وليس من جرائم الضرر، لقد أصبغت الحماية الجنائية على البيانات المشفرة والمودع شفرتها لدى مكتب التشفير الذي حدده القانون مثل مركز المعلومات ودعم القرار التابع لمجلس الوزراء في مصر، ولعل السبب في قصر هذه الحماية على بيانات الجهات الخاضعة في تشفيرها لمكتب التشفير لكون التشفير كما سبق القول من الأمور الخطرة التي يكون فيها مساسا بسلامة الدولة وأمنها القومي، لذلك لابدّ من توحيد الجهة المختصة

[1] -للمزيد **انظر**: **خثير مسعود**، الحماية الجنائية لبرامج الكومبيوتر أساليب وثغرات، دار الهدى للطباعة والنشر والتوزيع، الجزائر 2010، ص، ص139،108.

[2] - **بوعمرة أسيا**:النظام القانوني لقواعد البيانات، رسالة ماجستير، جامعة الجزائر، 2005، ص، ص 90،65.

باعتماد الشفرات وحفظها[1]. ومن ناحية أخرى فإن الركن المادي لهذه الجريمة يتمثل في كشف مفاتيح الشفرة أو فض المعلومات المشفرة في غير الأحول المصرح بها. لكن إذا تم فض التشفير عن طريق إذن قضائي أي في الحالات التي يجيزها القانون لا تعتبر جريمة[2]، ويمكن القول أن تجريم فض المعلومات حماية للتجارة الإلكترونية عامة وسرية التوقيع الإلكتروني خاصة.

تشفير المعلومات أو البيانات دليل على أنها ذات طابع خاص –سرية- لا ينبغي الاطلاع عليها من الغير معني. بعد كسر الشفرة و الوصول إلى الأرقام الخاصة بالتوقيع واستخدمه في تحقيق أغراضه[3]، يقوم الجاني باستنساخ التوقيع.

رغم أن التشفير هو الوسيلة الفعالة لحماية بيانات التوقيع إلاّ أنّه لا يؤمنه، حيث يمكن فك أو كشف مفتاح التشفير الذي نعني به المفتاح الخاص والحصول عليه من قبل أشخاص غير مخولين باستخدامه، لذلك وضعت الشركات المصدرة للتوقيع الإلكتروني سياسات خاصة يجب إتباعها للحفاظ على المفتاح الخاص حيث يجب أن يكون وحيدا Unique بحيث يحمل بصمة شخص واحد فقط حامله إتباع سياسة آمنة وفاعلة.

---

[1]-**عبد الفتاح بيومي حجازي**، التجارة الإلكترونية في القانون العربي النموذجي لمكافحة جرائم الكمبيوتر والانترنت، المرجع السابق، ص 180.

[2]-**قضية Bourquin:** تتلخص وقائعها في قيام اثنين من العاملين بمطبقة Bourquin، ومن أجل إنشاء مؤسسة منافسة، ينسخ سبعة وأربعين قرصا ممغنطا تحتوى على معلومات بالغة الهمية خاصة بعملاء المطبعة وذلك داخل مؤسسة Bourquin والاستعانة بمعداتها، كما قاموا بالاستلاء على سبعين قرصا ممغنطا من ناحية، ومن جهة أخرى بسرقة المحتوى المعلوماتي لسبعة وأربعين قرصا، خلال المرة اللازمة لإعادة إنتاجها وذلك إضرارا بالمؤسسة المالكة لجميع هذه الأقراص، ولقد أبدت محكمة النقيض ما ذهبت إليه محكمة الاستئناف من إدانة المهتمين من سرقة سبعين قرصا، والمحتوى المعلوماتي لسبعة وأربعين قرصا من جهة أخرى، كما رفضت الطعن المقدم من المهتمين مقررة أن قضاة الموضوع قد أثبتوا توفر كافة العناصر المكونة للجريمة، ويعد هذا الحكم على جانب كبير من الأهمية، من جهة يأتي هذا الحكم أكثر وضوحا من حيث تحديد المجال الذي تنصب عليه جريمة السرقة، ألا وهو المعلومات في حد ذاتها، ومن جهة أخرى فهو يتعرض لنسخ المعلومات المسجلة على الأقراص الممغنطة بصفة خاصة.

[3]-**عصام عبد الفتاح مطر**، المرجع السابق، ص 362، 365.

المطلب الثاني

تجريم الاعتداء على التوقيع الإلكتروني في التشريعات الأجنبية والوطنية

يحظى التوقيع الإلكتروني بحماية قانونية، إضافة إلى تلك التي يضيفها القانون الخاص به،الحماية التي يستمدها من القوانين التقليدية القائمة، وقد أطلقت الدول التي أصدرت قانون خاص اسم قوانين التوقيع الإلكتروني، والاتجاه الثاني من الدول الأخرى قامت بإدخال تعديلات على النصوص التشريعية القائمة على نحو يؤدي إلى استيعابها الصور المستحدثة من الجرائم الإلكترونية.

سنقوم بدراسة الحماية القانونية في بعض الدول الأوربية الدول الغربية **(الفرع الأول)**، كما انتهجت الدول العربية نفس الحذو بتبنيها نصوص تشريعية وقوانين خاصة بالحماية القانونية من المخاطر والجرائم التي تمس التوقيع الإلكتروني **(الفرع الثاني)** ونظرا لخصوصية الجريمة المعلوماتية العابرة للحدود تضافرت الجهود الدولي لإيجاد تعاون أمني دولي لمكافحة الجرائم الالكترونية **(الفرع الثالث)**.

الفرع الأول

تجريم الاعتداء على التوقيع الإلكتروني في القوانين الغربية

لقد تضمّنت الكثير من التشريعات الغربية نصوصا خاصة تتعلّق بالاستعمال التعسفي وغير المشروع للتواقيع الإلكترونية والبطاقات الائتمانية، والأمثلة التالية توضح ذلك:

أولا:الحماية الجنائية للتوقيع الإلكتروني في القانون الفرنسي:

تعتبر فرنسا من أوائل الدول الغربية التي سارعت بإصدار تشريعات تهتم بحماية المعلوماتية والتصدي لبعض صور الجرائم التي سببها التقدم في استعمال الحساب الآلي،وكذلك شبكة المعلومات الدولية انترنت، أو بعض الشبكات المحلية، كما هو الحال

في شبكة، مانتيل، الفرنسية[1]. وقد أجرى المشرع الفرنسي عدة تعديلات قانونية تصب جميعها في مجال مكافحة جرائم المعلوماتية وحماية التجارة الإلكترونية، أحدث تعديلات بالنسبة لتوقيع الإلكتروني في قانون العقوبات الفرنسي لعام 1995، حيث استحدث المشرع نصوصا تتعلّق بحماية المعلومات المعالجة،كما جرم التزوير المعلوماتي، الأمر الذي يسبغ حماية جنائية متكاملة على نظام التجارة الإلكترونية، والتوقيع الإلكتروني ومن أوجه الحماية التي أثبتها المشرع الفرنسي:

1- تجريم الدخول بطريق الغش أو التدليس على نظام المعلومات أو إبقاء الاتصال بطريقة غير مشروعة به (المادة 323-1).

2- تجريم إدخال البيانات بطريقة غير مشروعة في نظام معالجة البيانات أو إلغاء أو تعديل البيانات التي يحتوي عليها النظام بطريقة غير مشروعة (المادة 323-3).

3- التعديلات التي تضمنها القانون رقم 1382 والصادر في 30 ديسمبر 1991 والتي تضمنت المادة رقم 1/67 التي تنص على تجريم تقليد أو تزوير بطاقات الوفاء أو السحب الآلي، وعاقب عليها بالحبس من 1-8 سنوات والغرامة[2].

4- أجرى المشرع الفرنسي تعديلاته على النصوص التقليدية بالتزوير لتشمل التزوير في المحررات الإلكترونية، وهذا ما يحقق الحماية الجنائية للتوقيع الإلكتروني ضد جرائم التزوير المعلوماتي بأنواعها التي تقع على التوقيع الإلكتروني.

بصدور قانون العقوبات الفرنسي الجديد، جُرّم التزوير في المحررات الرسمية أو العرفية، الذي يقع بأي طريقة، على خلاف قانون العقوبات الفرنسي القديم، بموجب نص المادة 441 التي حلت محل المواد 145-152، وأصبح النص بعموميته يغطي التزوير

---

[1]- التوقيع الإلكتروني خطوة إلى الأمام: Electronic Signature متوفر على الموقع:
http://www.egovs.com/egovs_webo2/news.php?main=7&detailsid=

[2]-**هدى حامد قشقوش**، الحماية الجنائية للتوقيع الإلكتروني، بحث مقدم لمؤتمر الأعمال المصرفية الإلكترونية من الشريعة والقانون، المنعقد برعاية كلية الشريعة بجامعة الإمارات بالتعاون مع غرفة تجارة وصناعة دبي، للفترة 10-13ماي 2003، ج2 ص 584، 585.

المعلوماتى والتزوير بالطرق التقليدية، حيث نصت الفقرة الأولي من المادة 441 على أنّه "**يعد تزويرا كل تغيير تدليسي للحقيقة، يكون من شأنه أن يحدث ضررا، ويقع بأي وسيلة كانت سواء وقع في محرر أو سند معبرا عن الرأي أيا كان موضوعه والذي أعد مسبقا كأداة لإنشاء حق أو ترتيب أثر قانوني معين، ويعاقب على التزوير واستعمال المحرر المزور بالسجن ثلاث سنوات وبالغرامة التي لا تتجاوز 300.000 يورو**"[1]،الواضح من النص أن المشرع الفرنسي أقلع عن الإشارة لتحديد طريقة معينة للتزوير، حيث ذكر عبارة " أي وسيلة" "Par quelques moyen" والعلة في ذلك تكمن في رغبته أن يكون النص عاما يشمل التزوير بكل وسائله العادية مادي أو معنوي، بطريق التقليد أو الاصطناع أو تغير إقرار أولى الشأن وفي الوقت نفسه يشمل صور التزوير المعلوماتى.

وفّر المشرّع الفرنسي حماية جنائية للمواقع الإلكترونية ومحتوياتها، حيث جرم العديد من الأفعال كالدخول غير المشروع على مواقع الإنترنت، وإعاقة تشغيل نظام المعالجة الآلية للمعلومات، وتدمير البيانات والمعطيات الإلكترونية، وفي جانب آخر نجده يقرر حماية جنائية خاصة لبطاقات الائتمان بموجب القانون رقم 1383-91 المؤرخ في 1991/12/30م في المادة11 منه التي عدلت المادة 67 من المرسوم بالقانون الصادر في 1935/10/30م لتضيف مادتين هما 1/67 و2/67 وذلك بعد المادة 67 من المرسوم بالقانون آنف الذكر، حيث جرّمت المادة 1/67 ثلاث جرائم تتعلق بالبطاقات الائتمانية هي:الأولى تقليد أو تزوير بطاقة وفاء أو سحب، والثانية استعمال أو محاولة استعمال لبطاقة وفاء أو سحب مقلدة أو مزورة مع العلم بذلك، والثالثة قبول الدفع عن طريق الوفاء ببطاقة مقلدة أو مزورة وهو على علم بذلك في حين أن المادة 2/67 نصت على وجوب

[1]-**Un faux** selon l'article 441-1 du code pénal français, « une altération frauduleuse de la vérité, de nature à causer un préjudice et accomplie 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 juridiquessur.http://perlpot.net/cod/penal.pdf

مصادرة وتدمير البطاقات المقلدة ومصادرة الأدوات التي استخدمت أو المعدة للاستخدام في التزوير أو التقليد إلا إذا استخدمت بدون علم مالكه.

ومن التعديلات أيضا التي تحمي التجارة الإلكترونية والتوقيع الإلكتروني في القانون الفرنسي، تلك التي أجريت وأضيفت بموجبها المادتان (425/462)، في شأن الغش المعلوماتي، لتستوعب تجريم التزوير في الوثيقة المعلوماتية ويرى الفقه الجنائي أن أهمية هذا التعديل الأخير تتجلى في مساواة التوقيع الإلكتروني، حيث أن اللبنة الأولى لتنظيم وحماية نظام المعلوماتية في فرنسا والذي انعكس إيجابا على التجارة الإلكترونية كان في صدور القانون رقم 78-81 الصادر في 6 جانفي 1987 في شأن الحريات والمعلوماتية، وقد عالج فيه مسألة تخزين البيانات في الحساب الآلي، وأنواع البيانات ومدتها، وتلك التي تخزن وتلك التي لا يجوز تخزينها، وكذلك الجهة المختصة بالرقابة والإشراف على تطبيق ذلك القانون، حيث أنشأت بمقتضاه "**اللجنة القومية للمعلوماتية والحريات**"[1]، تختص بإجراء رقابة سابقة ورقابة لاحقة للتأكد من الحماية الكاملة للحريات في مواجهة نظم المعلومات، وتسهر على تطبيق أحكام قانون المعلوماتية وإبلاغ ذوي الشأن بحقوقهم وواجباتهم، والتحقق من احترام نظام المعلومات لأحكام القانون، وإصدار الإذن -الترخيص السابق- للإدارة من أجل إنشاء نظم المعلومات أو تلقى الإخطارات من الأفراد في هذا الشأن[2]، وهذه اللجنة مستقلة في عملها،وتعد تقريرا سنويا عن عملها يقدم

---

[1]- فرضت اللجنة الوطنية للمعلوماتية والحريات في فرنسا غرامة قدرها 100 ألف يورو على شركة Google لجمعها بيانات شخصية عبر برنامجها "streetview المثير للجدل.وأوضح الأمين العام للجنة يان بادوفا في مقابلة مع journal le parisien أنها "غرامة قياسية منذ حصولنا في العام 2004 على الحق بفرض عقوبات مالية، وقد أطلق برنامج "ستريت فيو" العام 2007 وهو يوفر صوراً بانورامية بالأبعاد الثلاثة للشوارع، ما يسمح لمستخدميه بالتنقل افتراضياً فيها، إلا أن هذه الخدمة أثارت سلسلة من المشاكل والجدل في عدة دول. وفي أيار/ مايو 2010، كشفت Google أن السيارات التي تجوب الشوارع لحسابها لالتقاط صور جمعت خطأ بيانات شخصية (رسائل إلكترونية وأشرطة فيديو..) واعتبرت اللجنة الوطنية الفرنسية أن "قاعدة المعلومات التي جمعتها streetview تمت بطريقة غير قانونية تجاه الأفراد لأنها حصلت من دون علمهمللمزيد أنظر الموقع الإلكتروني لتلفيزيون: بنادي فرانس 24 ومونت كارلو الدولية: http://www.france24.com/ar/node

[2]- **وعلي محمود علي حموده**، الجوانب القانونية والأمنية للعمليات الإلكترونية،أكاديمية شرطة دبي، مركز البحوث والدراسات، - كلية الحقوق – جامعة حلوان دبي.

لرئيس الدولة وللبرلمان، وأعضاء اللّجنة لا يخضعون لأي تعليمات أو توجيهات في ممارسة أعمالهم، لذلك يطلق عليها سلطة إدارية مستقلة une autorité administrative indépendante.

ثانيًا: الحماية الجنائية للتوقيع الإلكتروني في القانون الأمريكي.

تعدّ الولايات المتحدة الأمريكية من أولى الدول التي أصدرت تشريعات تعترف فيها بالتوقيع الإلكتروني وتوفير الحماية الجنائية له، وتمنحه حجية كاملة في الإثبات شأنه في ذلك شأن التوقيع التقليدي. حيث أصدر في 30 يونيه 2000 قانونا اتحاديا "**للتوقيع الإلكتروني العالمي والتجارة الوطنية**" أجاز بموجبه قبول واستخدام التوقيع والسجلات الإلكترونية في التعاملات التجارية الدولية وبين الولايات، وقد أبقى هذا القانون الاتحادي على كافة التشريعات الصادرة من الولايات للتوقيع والسجلات الإلكترونية، وفي حال عدم صدور مثل هذه التشريعات فإن القانون الاتحادي للتوقيع الإلكتروني هو الذي يطبق، ما يعني أن الغطاء التشريعي للمستندات الإلكترونية يمتد إلى كافة الولايات الأمريكية، حتى ولو لم تصدر قانونا خاصة به[1].

يوجد فيما يتعلق بحماية البطاقات الائتمانية في الولايات المتحدة الأمريكية منذ عام 1984م نصٌ خاصٌ تناول الاستعمال غير المشروع لبطاقات الائتمان يجرم الاستعمال التعسفي للأدوات التي تسمح بالدخول إلى حساب بنكي يمكن من خلاله الحصول على أموال أو أشياء أو خدمات أو أي شيء آخر له قيمه، تشمل الأدوات البطاقات المسروقة أو المفقودة أو تلك التي انتهت مدة صلاحيتها أو تم إلغاؤها، إضافة إلى تجريمه الاتجار في البطاقات غير المصرح باستعمالها، وكذا تقليد وتزوير البطاقات الائتمانية. وفي عام 1994م عدل هذا النص بإضافة جريمة أخرى إليه تتمثل في حيازة الأجهزة التي تساعد

[1]-**Edward H, Freeman J .D**, «Digital signature and Electronic Contracts», Information Systems Security, 2004 p.p 130.192

على تقليد وتزوير البطاقات الائتمانية متى ارتبط ذلك بنية غير مشروعة[1]، وفيما يتعلق بالنشر غير المشروع لأرقام البطاقات الائتمانية والبيانات الخاصة بها عبر شبكة الإنترنت، فقد جرّمها القانون الفيدرالي للاحتيال عبر وسائل الاتصال، الذي جرّم النقل غير المصرح به للمعلومات أو الإشارات أو العلامات أو الصور أو التسجيلات الصوتية عبر وسائل الاتصالات، وإزاء انتشار هذه الظاهرة في العديد من الولايات الأمريكية، تقدم السناتور الديمقراطي رياني فينشتين عضو مجلس الشيوخ عن ولاية كاليفورنيا بمشروع قانون إلى المجلس يطالب فيه الشركات إصدار البطاقات الائتمانية في مختلف أنحاء البلاد، بإخطار عملائها عن أي اختراق لسجلاتها المخزنة أو ملفاتها المشفرة، وتناول المشروع أيضا فكرة استحداث مكتب خاص بجرائم سرقة الهوية يتبع المفوضية الفيدرالية للتجارة في الولايات المتحدة الأمريكية، كما دعا المشروع إلى ضرورة التحقق من هوية أي طرف ثالث يريد الدخول على معلومات شخصية خاصة بمواطنين أمريكيين[2].

الفرع الثاني

تجريم الاعتداء على التوقيع الإلكتروني في التشريعات العربية

نظرا لما تمثله التجارة الإلكترونية من أهمية كبرى في عصر عرف بعصر المعلومات والاتصالات، سارعت الكثير من الدول العربية إلى توفير الحماية الجنائية لهذه التجارة من الاعتداءات التي قد تتعرض لها، وفيما يلي بيان لبعض الأمثلة:

أولاً: الحماية الجنائية للتوقيع الإلكتروني في القانون التونسي.

تضمن قانون المبادلات والتجارة الإلكترونية التونسي رقم 2000/73 العديد من الأحكام المتعلقة بالحماية الجنائية للتجارة الإلكترونية وكذلك التوقيع الإلكتروني، إضافة إلى العديد من الأحكام الواجبة على مزودي خدمات المصادقة وكذلك ما يجب على

[1]-**ABA** Section Creates First Digital Signature Guidelines To Aid In Security Of The Internet, 1996.http:/www.abanet.org/media/home.html.

[2] -Report to the Governor and legislature on New York States « Electronic Signatures and records Act ,p.9. **united Nations (UN CITRAL (Commission on Internationcel Trade Law**

المستفيد من الخدمة، من اتخاذ كافة الإجراءات الاحتياطية اللازمة لمنع وقوع أي فعل غير مشروع سواء على التجارة الإلكترونية أم على التوقيع الإلكتروني، فقد جرم الاعتداء على التوقيع الإلكتروني في المادة (48) منه التي نصت على أنه "**يعاقب كل من استعمل بصفة غير مشروعة عناصر لتشفير شخصيته، المتعلقة بإمضاء غيره، بالسجن لمدة تتراوح بين 6أشهر إلى عامين وبخطية تتراوح بين 1000 و10.000 دينار أو بإحدى هاتين العقوبتين**"، كذلك فإنّ المشرع التونسي قد اهتمّ بحماية التوقيع الإلكتروني وبيان حجيته وفصل في هذه الحماية لأنّه بمطالعة المادة الثانية الفقرات (3، 6، 7) نجد أن الفقرة (3) نصت على أن شهادة المصادقة الإلكترونية شهادة مؤمنة بواسطة التوقيع الإلكتروني، أمّا الفقرة (6) فهي خاصة بعناصر التشفير التي تؤدي إلى تمام "في مجال الحماية الجنائية للتوقيع الإلكتروني جرم المقنن التونسي العديد من الأفعال نذكرها فيما يلي:

أ- عدم مراعاة مزود خدمات المصادقة الإلكترونية لمقتضيات كراس شروط الخدمة المنصوص عليها في المادة 44 منه[1]، هذه الجريمة لا تقع إلا بطريق العمد[2] بمجرد عدم مراعاة الشروط والمقتضيات تقع الجريمة دون النظر في مدى توفر القصد الجنائي.

ب- ممارسة نشاط مزود خدمات المصادقة الإلكترونية دون الحصول على ترخيص مسبق، حيث جرمت المادة 46 هذا الفعل وعاقبت عليه بالسجن لمدة تتراوح بين 6 أشهر وثلاثة سنوات وبغرامة مالية.

---

[1] -تنص المادة 44 على ما يلي "**يسحب الترخيص من مزود خدمات المصادقة الإلكترونية ويتم إيقاف نشاطه، إذا أخل بواجباته المنصوص عليها بهذا القانون أو بنصوص التطبيقية، وتتولى الوكالة للمصادقة الإلكترونية سحب الترخيص بعد سماع المزود المعني بالأمر**". كما عاقبت المادة 45 منه بالغرامة من 1000 إلى 10000 دينار تونسي لكل مزود خدمات تصديق إلكتروني لم يراع المواصفات والشروط التي نص عليها القانون.

[2] -**عبد الفتاح بيومي حجازي**، النظام القانوني للتوقيع الإلكتروني، المرجع السابق، ص 490.

جـ-جريمة التصريح عمدا بمعطيات خاطئة لمزود خدمات المصادقة الإلكترونية بموجب المادة 74 وعاقبت عليه بالسجن لمدة تتراوح بين ستة أشهر وعامين، مع غرامة مالية تتراوح بين 1000 و10000 دينار.

د-جريمة استعمال عناصر تشفير شخصية متعلقة بإمضاء الغير بصفة غير مشروعة نصت المادة 48 على معاقبة كل من استعمل بصفة غير مشروعة عناصر تشفير شخصية متعلقة بإمضاء الغير بالسجن لمدة تتراوح بين 6 أشهر وعامين وبغرامة مالية تتراوح بين 1000 و10000 دينار.

جرم المشرّع التونسي من خلال المواد كافة الأعمال التي يراها الأخطر، والأكثر تهديدا، لذلك يمكن القول أنّ المشرّع التونسي تولى بالفعل مكافحة هذه الظاهرة وأقر عقوبات جنائية.

ثانيًا: الحماية الجنائية لتوقيع الإلكتروني في القانون المصري.

نهج المشرّع المصري ذات المسلك الذي انتهجته التشريعات المقارنة الأوروبية والعربية فيما يتعلق بالحماية الجنائية للتوقيع الإلكتروني، بصدور قانون تنظيم التوقيع الإلكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات2004/15م[1]، وتجريمه لبعض الانتهاكات التي يتعرض لها التوقيع الإلكتروني، حيث نصت المادة 23 من القانون على: **"مع عدم الإخلال بأية عقوبة أشد منصوص عليها في قانون العقوبات أو في أي قانون آخر، يعاقب بالحبس وبغرامة لا تقل عن عشرة الآلف جنيه ولا تجاوز مائة ألف جنيه أو بإحدى هاتين العقوبتين كل من:**

أ-أتلف أو عيّب توقيعا أو وسيطا أو محررا إلكترونيا، أو زور شيء من ذلك بطريق الاصطناع أو التعديل أو التحويل أو بأي طريق آخر[2].

---

[1]-**محمد أمين الرومي**، النظام القانوني للتوقيع الإلكتروني، مرجع سابق، ص 99 -153.

[2]-**عماد محمد علي البلوي**، جريمة تزوير التوقيع الإلكتروني دراسة وصفية لأساليب الكشف والتحقيق والتجريم المرجع السابق، ص99-101.

ب -توصل بأية وسيلة إلى الحصول بغير حق على توقيع أو وسيط أو محرر إلكتروني أو اخترق هذا الوسيط أو أعترضه أو عطله عن أداء وظيفته".

يلاحظ من النص أن المشرع المصري يجرم نوعين من الانتهاكات الواقعة ضد التواقيع، اعتبرهما المشرع من جرائم الخطر التي لا يتوقف تجريم السلوك فيها على تحقق نتيجة معينة،أما طرق التزوير الواردة في الفقرة (ب) من المادة سالفة الذكر جاءت على سبيل المثال وليس الحصر بدليل أن المشرع وفي نهاية هذه الفقرة أورد عبارة " بأي طريق آخر"، وهي من الجرائم العمدية لا يتصور ارتكابها بطريق الخطأ، والقصد الجنائي فيها هو العام بعنصريه العلم والإرادة.

أمّا فيما يتعلق بالاعتداء على المواقع الإلكترونية وأسماءها نلاحظ خلو القانون السالف الذكر وكذلك المدونة العقابية المصرية من أيّ نص يجرمها، لذلك نرى أنّه من الضرورة بمكان شمولها بالحماية اللازمة مثلها مثل المستندات والتواقيع الإلكترونية[1].

بالنسبة لجريمة السطو على أرقام البطاقات الائتمانية وهي إحدى الجرائم التي تهدد التجارة الإلكترونية فإننا نلاحظ أن النصوص المستحدثة الواردة في قانون الجزاء العماني أو قانون مكافحة جرائم تقنية المعلومات الإماراتي 2006/2 أو قانون العقوبات القطري2004/11 والتي تنطبق تماما على شبكة الإنترنت، لا يوجد لها نظير في التشريع المصري، حيث لم يرد في التشريع المصري ما يخص هذه الجريمة، بالتالي يجب الرجوع إلى النصوص التقليدية الواردة في قانون العقوبات كنصوص تجريم السرقة أو النصب أو الاختلاس.

إزاء ذلك كان على المشرع المصري في ظل هذه الطفرة المعلوماتية وحتى يكون بمنأى عن القياس الذي يتعارض مع مبدأ المشروعية وليتجنب مشقة تطويع النصوص

[1] -**عبد الفتاح بيومي حجازي**، النظام القانوني للتوقيع الإلكتروني، المرجع السابق، ص 538.

القانونية التقليدية أن يلحق بالركب ويستحدث نصوصاً تجرم السطو على أرقام البطاقات الائتمانية.

ثالثاً: الحماية الجنائية لتوقيع الإلكتروني في القانون الجزائري.

تماشيا مع التطور التكنولوجي في مجال الاتصالات وانتشار استخدام النظم المعلوماتية، أصدر المشرع الجزائري نصوص قانونية بموجب ق.ع.ج 04-15 تحت عنون جرائم المساس بأنظمة المعالجة الآلية للمعطيات والاستعمال للإعلام الآلي من خلاله جرم كل أنواع الاعتداءات التي تستهدف الدخول غير المشروع لأنظمة المعلوماتية، تغيير أو إتلاف المعطيات، محددا بذلك الأفعال والسلوكات التي تدخل ضمن مجال هذا النوع الجديد من الجرائم والتي يمكن حصرها في الأتي:

1- جريمة الدخول أو البقاء في المنظومة عن طريق الغش المادة 349 مكرر ق ع ج تقوم هذه الجريمة بمجرد الدخول غير المرخص به وعن طريق الغش إلى المنظومة المعلوماتية، سواء مسّ الدخول أو البقاء كل أو جزء من المنظومة، ويكفي إثبات المحاولة لتطبيق أحكام المادة، ولا يشترط لقيام هذه الجريمة إلحاق أضرار بالمنظومة المعلوماتية[1].

2- جريمة إدخال معطيات في منظومة المعالجة الآلية أو إزالة أو حذف أو تعديل معطيات منظومة المعالجة الآلية عن طريق الغش المادة 349 مكرر، ف1[2] ق،ع،ج، تقوم هذه الجريمة بمجرد ارتكاب أحد الأفعال المذكورة أعلاه بغض النظر عن المجال المستهدف، سواء كانت البرامج أو المعطيات أو قاعدة البيانات لتوقيع الإلكتروني.

3- جريمة القيام عمدا أو عن طريق الغش بتصميم، توفير، نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية أخرى، أو حيازة أو إفشاء أو

---

[1]- اجتهاد القضاء الفرنسي بعد تم الدخول غير المرخص به إلى منظومة شركة TATI الفرنسية عدة مرات من طرف شركة أخرى، قامت شركة TATI بمقاضاة تلك الشركة بأن موقع TATI لم يكن محميا، وبتالي ليس لهذه الأخيرة (TATI) الحق في الاحتجاج على الدخول إلى موقعها، فقضى القضاء الفرنسي بأنه ليس من الضروري أن تكون الأنظمة محمية.

[2]- المادة 394 مكرر1 على أنه: "**يعاقب بالحبس من ستة أشهر إلى ثلاثة سنوات وبغرامة من 500.000 د.ج إلى 2.000.000 د.ج كل من أدخل بطريقة الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها**".

استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى جرائم المعلوماتية، المادة 394 مكرر ف 3 من ق،ع،ج، ويلاحظ بأن كل الجرائم هي جرائم عمديه وترتكب عن طريق الغش.

4- جريمة المشاركة ضمن جماعة أو في اتفاق لغرض ارتكاب إحدى جرائم المعلوماتية المادة 349 مكرر ف 5 من ق،ع،ج وتقوم بالانتماء أو الاشتراك في جماعة أو اتفاق.

5- جريمة الشروع في ارتكاب إحدى جرائم المعلوماتية:المادة 349 مكرر7 من ق، ع ج وتكون العقوبة المقررة عن الشروع، بطبيعة الحال هي نفس العقوبة المقررة للجريمة التامة[1].

تبنى المشرّع الجزائري مثله مثل المشرّع الفرنسي الحماية الجنائية للبرامج من خلال تعديله الأخير لقانون 04-15، بهدف حماية النظام ككل، إلاّ أنّه لم يتعرض إلى جل الجرائم التي نص عليها المشرع الفرنسي، وإن كانت على قدر من الأهمية كجريمة تزوير المستندات المعلوماتية، رغم تداركه من خلال ق، ع الفراغ القانوني في مجال الإجرام المعلوماتي كما سبق القول وذلك بتجريم الاعتداءات الوردة على الأنظمة المعلوماتية، إلاّ أنّه أغفل تجريم الاعتداءات الواردة على منتجات الإعلام الآلي نقصد من ذلك نصا خاصا بالتزوير المعلوماتي، بحيث نص على تزوير المحررات بمعزل عن جريمة استعمالها فجعل كل منها مستقلة عن الأخرى، بحيث نص على استعمال الأوراق العمومية أو الرسمية في المادة 218 ق،ع واستعمال الأوراق العرفية أو التجارية أو المصرفية في المادة 221، وكذا استعمال الوثائق الإدارية والشهادات في المواد 222 1/ و223 و 2227/ و228/3 ق،ع،[2]، ولم يتعرض إلى جريمة استعمال المستندات

[1]- **الأرزاق بن عبد الله، وأحمد عمراني**، نظام المعلوماتية في القانون الجزائري واقع وأفاق، المؤتمر السادس لجمعية المكتبات والمعلومات السعودية، المنعقد بمدينة الرياض، البيئة المعلومات الأمنية للمفاهيم والتشريعات والتطبيقات المنعقد بمدينة الرياض خلال الفترة 21-22 أفريل 2010، ص 1،83 مقال منشور على الموقع الإلكتروني:
http://www.4shared.com/file/W4F2rGal

[2] -أنظر المواد من 222 إلى 228 ق. ع. ج السالف الذكر.

المعلوماتية المزورة، بخلاف نظيره الفرنسي الذي نص على هذه الجريمة في المادة 462/6ق،ع،ف: "**كل من استخدم - بتبصر –المستندات المعلوماتية المنصوص عليها في المادة 5/462 فإنّه سيعاقب بالسجن من سنة إلى خمس السنوات وبغرامة من 20000 فرنك إلى 200000 فرنك أو بإحدى هاتين العقوبتين**".

لسدّ الفراغ القانوني الذي عرفه المجال المعلوماتي بصدور قانون رقم 04-15 اصدر المشرع قانون مكافحة الجرائم المعلوماتية تحت عنوان "**القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها** " قانون رقم 09-04[1].

الفرع الثالث

التعاون الدولي من أجل حماية التوقيع الإلكتروني

تعدّ المعاهدات الدولية النموذج الأمثل الذي يجسد التعاون الدولي في هذا المجال بحيث لم يتوقف عند التشريعات الداخلية للدول لتجاوز إلى تضافر الجهود الدولية ووضع إطار قانوني يضمن حماية هذا النوع من المعاملات وحماية المستهلك خاصة عند الدفع عبر الخط.لذلك أصبحت الحاجة ماسة إلى وجود آليات أمنية دولية تنظم التعاون لإحداث قوانين نموذجية لمكافحة الجرائم المعلوماتية عموما وجرائم التوقيع الإلكتروني خصوصا وسنقوم بدراسة بعض النماذج الإقليمية والدولية لترسيخ وحماية التوقيع الإلكتروني.

أولاً: اتفاقية مجلس أوروبا بشأن الإجرام "السيبيري".

شهدت بودابست في أواخر عام 2001 أولى المعاهدات الدولية التي تكافح جرائم الانترنت والتي افتتح باب التوقيع عليها في 23 نوفمبر 2001، هذه الاتفاقية هي الوحيدة المُتعدِدة الأطراف في مجال الجرائم التي تتم باستعمال الكمبيوتر، الأمر الذي شكل دافعًا للعديد من الدول من خارج مجلس أوروبا والقارة الأوروبية إلى الانضمام إليها، وأبرزُها الـــ و م أ التي صادقت عليها في 22 سبتمبر2001، حيث تهدف هذه الاتفاقية إلى بناء

[1]- قانون رقم 04/09، السابق الذكر.

سياسة جنائية مشتركة من أجل مكافحة الجرائم المعلوماتية في جميع أنحاء العالم من خلال تنسيق وموائمة التشريعات الوطنية بعضها البعض، وتعزيز مقدرات القضاء والتشديد في تطبيق القانون وتقوية وتحسين التعاون الدولي في هذا الإطار،وكذلك العمل على تعريف وتحديد العقوبات من جرائم المعلوماتية في إطار قوانينهم المحلية، وباستقراء هذه الاتفاقية نجد في ديباجتها تجد الكثير من الجرائم المعلوماتية ومنها الخاصة بحماية البيانات الشخصية في مجال الخدمات المتعلقة بالاتصالات السلكية واللاسلكية.

وقد عبرت اتفاقية المجلس الأوروبي حول الإجرام السيبيري عن إدراك دول المجلس للمخاطِ الجديدة التي تعرضها شبكات الكمبيوتر وسُرعة تطورها وانتشارها، إذ جاء في ديباجتها ما يلي: "**اقتناعًا منا لدول أعضاء مجلس الاتحاد الأوروبي بضرورة منح الأولوية للسعي من أجل تنفيذ سياسة جنائية مُشتركة تهدف إلى حماية المُجتمع من أخطار جرائم الإنترنت وهي التي تشمل أمورًا من بينها تبني التشريع المُناسب ودعم التعاون الدولي – وإدراكُ العُمق التغيرات التي أحدثها التحول إلى الرقمية وارتباط شبكات الكمبيوتر مع بعضها البعض مع استمرار عولمته – وانشغلا بمخاطر احتمال استخدام شبكات الكمبيوتر والمعلومات الاليكترونية أيضًا في ارتكاب جرائم جنائية**"[1]. وقد تم تحديد الجرائم التي تمس سرية، وأمن وسلامة وتوافر بيانات الكمبيوتر ومنظوماته في المادة الثانية منها، التي حصرت خذه الجرائم في:

- الدخول غير مشروع على منظومة الكمبيوتر كليا أو على جزء منها دون وجه حق.
- الاعتراض غير مشروع لحظ سير البيانات دون وجه حق وعن قصد باستخدام الوسائل الفنية لقطع عمليات البث والإرسال (المادة 03).
- التدخل في البيانات عن قصد، وذلك من حيث إتلاف، أو إلغاء، أو إفساد، أو تغيير، أو تدمير البيانات الموجودة بالكمبيوتر دون وجه حق (المادة 04).

[1]- للاطلاع على النص الكامل لاتفاقية الإجرام السيبيري، يرجى مراجعة الموقع الالكتروني الخاص بالمجلس الأوروبي:
http://conventions.coe.int/treaty/fr/Treaties/Html/185.htm

ذكرت المادة 07[1] الجرائم المتعلقة بالكمبيوتر وذلك عند ارتكابه عن قصد وبدون وجه حق بتزويد الكمبيوتر ببرامج خاصة بمعلومات وببيانات، أو تبديل أو تغيير أو إلغاء المعلومات والبيانات الخاصة بالكمبيوتر، ممّا ينتج عنه وجود معلومات وبيانات غير صحيحة بقصد دراستها أو الاهتمام بها أو العمل بها لأغراض قانونية كما لو كانت صحيحة[2]، وقصد حماية النشاط الإلكتروني وردع الجرائم التي تتم بالطرق الإلكترونية. أصرت الاتفاقية على ضرورة قيام الدول الأطراف فيها بإقرار الإجراءات التشريعية وغيرها من الإجراءات الأخرى كلما كان ذلك ضروريا للحفاظ على السير الحسن والقانوني للنشاطات والاستعمالات لأجهزة الحواسيب والنشاطات التي تتم بواسطتها.

بينت اتفاقية المجلس الأوروبي في المادة 23 منها على الأسس العامة المتعلقة بالتعاون الدولي، بحيث ذكرت تعاون الدول الأطراف فيما بينها لتطبيق الاتفاقيات الدولية ذات الصلة والخاصة بالتعاون الدولي في الشؤون الجنائية والإجراءات المتفق عليها بمقتضى التشريع الخاص المتعلق بمبدأ المعاملة بالمثل لأقصى درجة ممكنة للأغراض الخاصة بعمليات التحقيق والبحث، أو الإجراءات المتعلقة بالجرائم أو الخاصة بنظم وبيانات الكمبيوتر، أو لتجميع الأدلة الخاصة بالجريمة في صورة إلكترونية[3].

يمكن القول أن هذه الأسس المقررة من أجل تحقيق تعاون دولي لوضع حدّ للجرائم المعلوماتية وحماية مستعملي الإنترنت تستجيب لخصوصية التجارة الإلكترونية التي لا تخضع للمفهوم الكلاسيكي للحدود، ذلك راجع لتفتح قنوات الاتصالات على العديد من

---

[1]- **Article 7 – Falsification informatique** **النص باللغة الفرنسية**

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'introduction, l'altération, l'effacement ou la suppression intentionnels et sans droit de données informatiques, engendrant des données non authentiques, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient authentiques, qu'elles soient ou non directement lisibles et intelligibles. Une Partie peut exiger une intention frauduleuse ou une intention délictueuse similaire pour que la responsabilité pénale soit engagée.

[2]- اتفاقية المجلس الأوروبي الخاصة بالإجرام السيبيري، بودابست، المواد 2-4 و7 منها.

[3]- المادة 23 من اتفاقية المجلس الأوروبي الخاصة بالإجرام السيبيري، بودابست، 23-11-2001.

دول العالم في آن واحد وضرورة ردع هذه الجرائم ولو اختلف مكان آثارها عن مكان اقترافها، كسرقة بيانات أو تغييرها من بلد معيين وتضر بأشخاص موجودين في بلد آخر وبالتالي ضرورة تضافر جهود كافة الدول لتحقيق تعاون فعلي وفعال في عصر تكنولوجيا الاتصالات وثورة المعلوماتية.

جاء في المذكرة التفسيرية لاتفاقية بودابست الموقعة في 23 نوفمبر 2001: "... **كما أن الاستخدام العام للبريد الإلكتروني ووصول الجمهور لمواقع الويب عبر الإنترنت من أمثلة هذا التطور الذي قلب أوضاع مجتمعنا، كذلك فإن سهولة الوصول إلى المعلومات في النظم المعلوماتية مع الإمكانيات اللامحدودة لتبادلها وإرسالها بصرف النظر عن المسافات الجغرافية...ومن خلال الاتصال بخدمات الاتصالات والمعلومات يستطيع المستخدمون اصطناع فضاء جديد يسمى الفضاء المعلوماتي الذي يستعمل أساسا لآثار شرعية ولكن يمكن أن يخضع لسوء الاستخدام. إذ هناك احتمال استخدام شبكات الحاسوب والمعلومات الإلكترونية في ارتكاب أعمال إجرامية. وعلى ذلك يجب على القانون الجنائي أن يحافظ على مواكبته لهذه التطورات التكنولوجية التي تقدم فرصا واسعة لإساءة استخدام إمكانيات الفضاء المعلوماتي...**"[1].

أما فيما يخص العالم العربي، فلا يوجد حتى هذه اللحظة اتفاقية أو مشروع اتفاقية خاصة بالتعاون الإقليمي العربي في مجال مُكافحة الجرائم التي تتم باستخدام الكمبيوتر أو شبكة الإنترنت، ومن هُنا تنبُع أهمية نشر الوعي وزيادة المعرفة في هذا المجال في المنطقة العربية، كما تبرُز أيضًا ضرورة تدريب سُلطات إنفاذ القانون والملاحقة القضائية على هذا النوع من الجرائم لاسيما في ظِل التطورات السريعة التي يشهدها العالم وخاصةً ظاهرة العولمة، وسرعة انتقال المعلومات والبيانات عبر الحدود الدولية.

ثانيًا: جهود الاتحاد الدولي للاتصالات لحماية الفضاء الإلكتروني.

وضع مجموعة توصيات بين فيها مجموعة الأطر التنظيمية والإجراءات العملية الهادفة إلى منع الاستعمال غير المصرح به، مع تحيد السبل المسموح بها لاستعمال المعلومات وأنظمة الاتصالات الإلكترونية وشديد على مبادئ:

[1]- **جعفر حسن جاسم الطائى**، جرائم تكنولوجيا المعلومات، رؤية جديدة للجريمة الحديثة، دار البداية لنشر والتوزيع عمان، 2007، ص227، 240.

- تأمين استمرارية الخدمة.
- خصوصية المعطيات والمعلومات.
- الحرص على إيجاد السبل الكفيلة بحماية المواطنين والمستخدمين لهذه التقنيات من كافة المخاطر التي قد تتأتى من استعمالها واختراق الشبكات بهدف سرقة المعلومات والأسرار الحساسة.
- الأضرار المتأتية من الجهل وسوء الاستعمال من بعض المستخدمين المرخص لهم الذين يستغلون مراكزهم للقيام بأعمال غير مرخص لهم بها.

تهدف هذه التوصيات إلى حماية الاقتصاد بشكل عام والبيانات والمعلومات المخزنة وأنظمة المعلومات، كما تساهم على الحفاظ على ثقة المستخدمين، وتحقق هذه الأهداف برفع مستوى التوعية حول المخاطر الموجودة، إنشاء مؤسسات وإطارات وطنية تعتني بموضوع إيجاد وسائل الحماية والتوعية من المخاطر.

كما دعت التوصية إلى مواجهة التحديات عبر تضافر جهود وعوامل، الأفراد والقوانين والأطر التنظيمية، والإجراءات العملية والتكنولوجيا، كما يجب على الأفراد أن يكونوا حرصين على إتباع الإجراءات المرسومة من قبل المؤسسات المعنية.

- على المؤسسات وضع إجراءات حماية فعالة والتشدد في تطبيقها.
- على مؤسسات القطاعين العام والخاص أن تحرص على استخدام طبقات متعددة من تقنيات الحماية واعتماد تكنولوجيات متعدّدة للحد ما أمكن من المخاطر.
- تقييم وفهم المخاطر واستخدام وسائل خاصة للحماية.

ومن بين إجراءات الحماية كذلك أوصت بـــ:

- التركيب والصيانة بطرق سليمة.
- استخدام الجدران النارية مع كلمات السر.
- الترميز والتشفير، زيادة استخدام التشفير على شبكة الإنترنت، على سبيل المثال مع الشبكات الافتراضية الخاصة (VPNS) وبرامج حماية برتوكولات الإنترنت (IPSEC).
- إعطاء دور أمن أوسع لمديري الشبكات.

- الاستعانة بأصحاب الخبرة الأجنبيين.
- عمليات مراجعة وتدقيق دورية إجراءات الحماية والأمان.
- الحد ما أمكن من عدد الأشخاص الذين يحق لهم الوصول إلى غرف الحاسوب[1].

كما هدفت توصيات الاتحاد الدولي للاتصالات إلى سن مجموعة متكاملة من القوانين المتعلقة بالفضاء الإلكتروني وأمنه مع وضعها موضع التنفيذ، على أن تتوافق هذه القوانين مع أحكام الاتفاقات العالمية لمكافحة جرائم المعلوماتية، يترجم بإجراء تقييم لمدى كفاية المقدرات الراهنة للسلطات القضائية يدعي لمراجعة قوانينه الجنائية الراهنة لتحديد مدى كفايتها لمعالجة المشاكل المالية والمستقبلية لجرائم المعلوماتية.

- اعتماد قوانين إجرائية وأسس تعاونية وسياسات موضوعية لمكافحة فاعلة لجرائم المعلوماتية.
- إنشاء وحدات وطنية مختصة بمكافحة جرائم المعلوماتية[2].

ثالثًا: اليوم العربي للسلامة والأمن في الفضاء السيبيري.

كان للمركز العربي للبحوث القانونية والقضائية نشاطات عدّة التقت في مجملها مع الأهداف والمهام الملقاة على عاتقه لاسيما في تفعيل العمل العربي المشترك بما يتلاءم مع تطور العلوم والتقنيات، فساهم في إنشاء المرصد العربي لأمن الفضاء السيبراني بالتعاون مع العديد من الهيئات الحكومية ومؤسسات المجتمع المدني اللبنانية والعربية.

استكمالا لهذه الخطوة إنعقد في بيروت[3] اليوم العربي لأمن الفضاء السيبيري الذي يسعى إلى إلقاء الضوء على نقاط التلاقي بين المجتمعات العربية والإقليمية، حول

---

[1]- **عماد يوسف حب الله**، حماية الفضاء السيبراتي– الأمور التنظيمية لأمن المعلومات والاتصالات-، الهيئة المنظمة للاتصالات في لبنان: أمن الفضاء السيبراتي، 4-5 شباط 2009، مقال منشور على الموقع: http://www.tra.gov.lb/library.

[2]-**واقد يوسف**، النظام القانوني لدفع الإلكتروني، مذكرة لنيل درجة ماجستير في القانون ،تخصص قانون التعاون الدولي،جامعة مولود معمري، تيزي وزو، 2011. ص، ص182، 183. على الموقع الإلكتروني:
http://www.ummto.dz/IMG/pdf/THESE_OUAGUED.pdf

[3]- وقد عقب الاجتماع ورشة عمل بعنوان "إرشادات الإسكوا لتنسيق التشريعات السيبرانية في المنطقة العربية" اشتملت جلسات اليوم الأول على عرض لمشروع الإسكوا بعنوان تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة قدمتها الدكتورة نيبال

ضرورة إيجاد التشريعات والتنظيمات الملائمة التي تتناسب وحاجات تسخير تكنولوجيا المعلومات والاتصالات، لخدمة التنمية الاقتصادية والاجتماعية، والتأكيد على أهمية التنبه إلى مخاطر عدم التنسيق والتعاون في مجال خلق الانسجام التنظيمي والتشريعي في مجال الأمن السيبيري، بما يضمن انخراطا سليما في مجتمع المعلومات، لا يتعارض وتطلعات المجتمعات العربية على المستويات الثقافية والعلمية والاقتصادية والاجتماعية كافة مركزا لذلك على ضرورة الإفادة من التجارب الأوروبية والعربية الرائدة في مجالات التنظيم والتشريع، كما في المجالات التقنية،لاسيما لجهة حماية المعلومات الشخصية وحماية أمن الدول ومصالحها الحيوية، منع الاعتداءات على بنيتها التحتية والتعرض لأنظمة المعلومات لديها، على خط مواز، يطلق المرصد من خلال هذا اليوم العربي حملة إعلامية واسعة تهدف إلى نشر الوعي حول أهمية هذا اللقاء ومخرجاته المتوقعة، لاسيما منها، وضع مشاريع عربية وإقليمية تتناول مسائل الرد على التحديات التي تطرحها السلامة المعلوماتية وسلامة الفضاء السيبري.

=إدلبي، وقراءة عامة في تطور تقنيات الانترنت وتطور التشريعات السيبرانية مع عرض للمنهجية المعتمدة في صياغة الإرشادات التوجيهية للتشريعات للسيبرانية وقدمها الدكتور وسيم حرب مؤسس المركز العربي لتطوير أحكام القانون والنزاهة والمشرف العام على المركز،تلبية للدعوة الموجهة من الاسكوا إلى المنظمة العربية للتنمية الإدارية للمشاركة في الاجتماع المنعقد ببيروت في الفترة من 13-15 يوليو سبتمبر 2011.للمزيد إطلع على الموقع الإلكتروني:
http://css.escwa.org.lb/ICTD/1429/Day2/2.pdf

التوقيع الإلكتروني مصلحة من المصالح الجديرة بالحماية لكونه عنصر أساسي تقوم عليه التجارة الإلكترونية، بدأ الاعتماد عليه بشكل كبير في كافة المعاملات القانونية بل أصبح إحدى وسائل الحماية المدنية للمعاملات المتعلقة بالتجارة الإلكترونية، وإزاء هده الأهمية المتزايدة وجب توفر حماية تقنية وقانونية، لبث الثقة والأمان في القوقع الإلكتروني لجأ التقنيون إلى استعمال التشفير لحمايته من المخاطر التي قد يتعرض له، من تزوير، تخريب، إتلاف، سرقة وتشويه والابتزاز والتلف، والاستخدام غير المرخص وغير القانوني لذلك تم الاعتماد تكنولوجيا التشفير الذي يعتبر تقنية قديمة استعملت منذ الأزل شهد تطور عبر التاريخ ومازال في تطور مستمر حتى الآن فعندما يضع المشفرون نظام تشفير يأتي آخرين ويحاولون فك هذا النظام ومعرفة سرّ الشفرة فيلجأ المشفرون لنظام جديد، يعتمد على الخوارزميات الرياضية الذكية يمكننا تعريفه بأنه مجموعة من الوسائل التي تهدف لحماية سرية البيانات والمعلومات بحيث لا يستطيع فهمها وقراءتها إلا المرسل والمرسل إليه فقط، وذلك عن طريق استخدم رموز خاصة تعرف عادة بالمفتاح وتحويل يتم عن طريق بروتوكولات سرية تحويل على عبارات، معلومات ،إشارات غير مفهومة أو القيام بالعكس.

ظهر لتشفير إطار تشريعيا حديثا ،عرفته القوانين المحلية و الدولية إلى جانب الفقه حول وضع تعريف له ونص على ضرورة استعماله بعد أن كان حكرا على الحكومات، فصدر أول مرسوم فرنسي بشأن التعامل بوسيلة التشفير وقد سمح للمشروعات الصغيرة والأفراد باستخدام التشفير بعدما كان مقصورا على المجالات العسكرية والحكومية سنة 1982، عرفه المشرع التونسي وحدد مفهومه في القانون رقم 83 لسنة 2000 جرم كل اعتداء وكل استعمال غير مشروع، عكس المشرع المصري جاء خاليا من تعريف التشفير ترك هذه المسألة ليتم تنظميها بأحكام اللائحة التنفيذية للقانون رقم 15لسنة 2004، أما الفقه فقد عرفه البعض بأنه عملية الحفاظ على سرية المعلومات تغيير في شكل البيانات عن طريق تحويلها إلى رموز وإشارات لحماية هذه البيانات من إطلاع الغير عليها من تعديلها أو تغيرها.

تتنوع مستويات التشفير حسب النظام المستخدم قد يكون على مستوى الإرسال ونقطة الاستقبال، وقد يكون على مستوى التنقل أو التصفح، كما يمكن أن يكون على مستوى التطبيق أو التنفيذ يتم على جميع المستويات بغرض حماية البيانات أثناء تنقلها، أما عن أنوعه هنالك ثلاثة التشفير المتماثل، غير المتماثل والمزدوج، لكن التشفير وحده لا يكفي وحده لحل مشكلة أمن التوقيع الإلكتروني فقد حتم ذلك ضرورة تدخل طرف ثالث تكون مهمته التعريف بالأطراف وضمان صلة الشخص بتوقيعه، تسمّى بالجهات المختصة بإصدار شهادة التصديق الإلكتروني، لكون العقود الإلكترونية تبرم بين غائبين باختلاف الزمان والمكان عبر شبكة اتصال مفتوحة هذا الأمر استلزم وجود هذا الطرف الثالث المحايد يتمثل في أفراد أو شركات أو جهات مستقلة وتسمّى بجهات التصديق

أو التوثيق الإلكتروني وتعمل بترخيص من السلطات المختصة في الدولة وتحت إشرافها، ضمن أحكام تحدد ،نظامها وماهيتها والدور الذي تقوم به من خلال تقديم شهادات إلكترونية تحدد بها هوية الموقع وتتحقق من صحة التوقيع وارتباطه بصاحبه ،فقد صدرت العديد من التشريعات التي تناولت تنظيم هذه الجهة بأحكام خاصة تجعلها خاضعة لرقابة الدولة وتحمل مسؤولية أعمالها .

تلعب جهات التصديق أو التوثيق دور أساسيا، إصدار شهادات التصديق الإلكتروني وذلك التحقق أولا من هوية الشخص الموقع وثانيا إثبات مضمون التبادل الإلكتروني وثالثا إصدار مفاتيح التشفير ،كل خطأ في الشهادة تقوم مسؤولية مقدم خدمات التصديق كما يجوز لها إثبات عدم وجود أيّ خطأ من جهة، إذا أدت دورها من حفظ لسرية البيانات وصحتها ولا شكّ أن عبء الإثبات يقع عليها هو أمر في غاية التعقيد والدقة، نظرا لأهمية شهادة التصديق لقد عرفت التشريعات هذه الشهادة ونظمتها كما اعترفت بالشهادات التصديق والتوقيعات الإلكترونية التي تصدر من جهات التصديق الأجنبية فقد نظمت المادة 12 من قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية لعام 2000.

يجب توفير الحماية الجنائية للتوقيع الإلكتروني كونه مصلحة جديرة بالحماية، لذلك وكبه تطور تشريعي ينظمه ويحدد مصدقتيه، يحميه بالتجريم والعقاب، التزوير من أكثر الجرائم التي تهدده إلى جانب جرائم معلوماتية أخرى، فقد تبنت التشريعات الدولية والوطنية قوانين تجريم الإعتداء علية لزلت الجهود الدولية تتظافر المكافحة الجرائم الإلكترونية.

خاتمـــــة

تستلزم عقود التجارة الإلكترونية وجود توقيعات إلكترونية منسوبة لأطراف العقد وهذا نتيجة للطبيعة الإلكترونية التي تتميز بها هذه العقود، مما تعذر معها استخدام التوقيع التقليدي.

وبما أنّ التوقيع الإلكتروني واقعة مستجدة فرضتها مقتضيات التجارة الإلكترونية فقد صدرت تشريعات دولية وإقليمية ووطنية نظمت أحكامها التوقيع الإلكتروني لإزالة الغموض على هذا المفهوم الحديث والمستجد على الفكر القانوني، وبينت ماهيته واعترفت به ومن بين هذه القوانين التي حددت الطبيعة القانونية للتوقيعات الإلكترونية، قانون الأونسيترال النموذجي لعام 1996م بشأن تنظيم التجارة الإلكترونية، وقانون الأونسيترال النموذجي لعام 2001م بشأن التوقيعات الإلكترونية، كما أصدرت المفوضية الأوربية أحكام التوجيه الأوربي رقم 93 لسنة 1999م بشأن التوقيعات الإلكترونية، وفضلاً على ذلك واسترشادا بالقوانين النموذجية والتوجيهات الدولية، صدرت العديد من التشريعات الوطنية اعترفت بالتوقيع الإلكتروني وأضفت عليه حجية قانونية مساوية لحجة التوقيع التقليدي في الإثبات.

يعتبر التوقيع الإلكتروني مجموعة من الحروف أو الأرقام، أو الرموز أو الأصوات، أو أي معالجة إلكترونية أخرى، بحيث يمكن أن يعبر عن رضا أطراف التصرف القانوني، وأن يميز ويحدد هوية شخص موقعه، كما يرتبط بمضمون المحرر على أي دعامة إلكترونية.

للتوقيع الإلكتروني صور عديدة تتلف التقنية المستخدمة في تشغيل منظومة التوقيع الإلكتروني، ومن هذه الصور ما يعتمد على الأرقام أو الأحرف أو الرموز... مثل التوقيع بالرقم السري المقترن بالبطاقة الممغنطة، ومنها ما يعتمد على الخواص الطبيعية والفيزيائية للإنسان وهو التوقيع البيومتري، كذلك منها ما يعتمد على التشفير باستخدام المفتاح المتماثل –المفتاح العام– أو المفتاح غير المتماثل– المفتاح العام والخاص–، لكل صورة من هذه الصور قوة ثبوتية تختلف عن الأخرى، يرتكز قياس مستوى القوة الثبوتية

للتوقيع الإلكتروني على مدى قدرة منظومة تشغيله على تحقيق وظيفتي التوقيع التقليدي وهما التعبير عن إرادة الموقع في الالتزام بمحتوى المحرر، وتحديد هويته.

يصطدم إثبات التوقيعات الإلكترونية بكثير من العقبات من الناحية الفنية والقانونية في ظل غياب نصوص تشريعية تنظم الإثبات الإلكتروني، محاولة لإزالة هذه العقبات القانونية لجأ البعض إلى فكرة مرونة القواعد التقليدية في الإثبات، وهذا لإمكانية الأخذ بالتوقيع الإلكتروني كحجة ودليل في الإثبات من خلال محاولة الاستعانة بالاستثناءات الواردة على قاعدة وجوب الإثبات بالكتابة أو الاستعانة بالاتفاقات المبرمة بين أطراف العقد الإلكتروني التي تنظم حجية التوقيع الإلكتروني، تساهم في التوصل إلى حلول فعلية يمكن أن تزيل هذه العقبات القانونية إلا أنها حلول جزئية ومحدودة غير مستقرة تعجز على توفير بنية قانونية للتوقيع الإلكتروني، تكفل حماية كاملة لحقوق الأطراف المتعاقدة عبر شبكة الانترنت.

من أجل الاعتراف القانوني لعناصر الدليل الإلكتروني وتنظيم الإثبات الإلكتروني صدرت العديد من التشريعات التي صيغت مؤخرا – والتي بيناها سابقا – على المستوى الدولي والوطني نظمت الإثبات الإلكتروني واعترفت بعناصر الدليل الإلكتروني ومنحتها ذات الآثار القانونية التي ترتبها عناصر الدليل الكتابي، فقد اعترفت هذه التشريعات بحجية الكتابة الإلكترونية والتوقيع الإلكتروني والمحرر الإلكتروني ومنحتهم قوة في الإثبات تعادل قوة الكتابة التقليدية والتوقيع التقليدي والمحرر التقليدي.

لكي يتمتع التوقيع الإلكتروني بذات الحجية المقررة للتوقيع التقليدي يجب أن تتوافر فيه الشروط القانونية والضوابط التقنية التي تجعل منه توقيعا موثوقا به أو معززا أو محميا أو جديرا بالتعويل عليه، كما عبرت التشريعات المختلفة على ذلك، وهذه الشروط تتمثل فيما يلي:

1) تعريف التوقيع الإلكتروني بهوية صاحبه والتعبير عن رضائه بمحتوى المحرر الإلكتروني.
2) ارتباط التوقيع الإلكتروني بالموقع وحده دون غيره.
3) سيطرة الموقع وحده دون غيره على الوسيط الإلكتروني.

4) إمكانية كشف أي تعديل أو تبديل في بيانات المحرر الإلكتروني أو التوقيع الإلكتروني.

بسبب غياب العلاقة المباشرة بين الأطراف في معظم تصرفاتهم التي تتم عبر الوسائط الإلكترونية خاصة تلك التي تتم عن طريق شبكة الانترنت، فإن توفر عنصر الثقة والأمان في هذه التصرفات عنصر أساسي وضروري، خاصة فيما يتعلق بالتوقيعات الإلكترونية للأطراف المتعاقدة، لهذا كان من الضروري إيجاد وسائل تقنية لحماية هذا التوقيع من أي مخاطر قد يتعرض لها من جهة ، ولبعث الثقة والأمان في التصرفات التي تتم عبر الوسائط الإلكترونية من جهة أخرى، ومن أهم هذه الوسائل ما يلي:

1) تقنية تشفير البيانات لضمان إرسال الرسائل ونقل المعلومات بطريقة سرية، وهو وسيلة فنية تسمح بحماية البيانات والمحافظة على سريتها، بحيث لا يمكن للغير الإطلاع عليها أو تغيير بياناتها.

2) وجود طرف ثالث محايد بين أطراف التصرف يعمل كجهة مصادقة وهذا من خلال شهادة الكترونية يصدرها تحتوي على مجموعة من البيانات، وظيفتها تأكيد العلاقة ما بين الموقع وتوقيعه الإلكتروني والتحقق من مضمون التعامل أو التبادل الإلكتروني بين الأطراف المتعاقدة.

نهيب بالمشرع الجزائري سرعة إصدار قانون التجارة الإلكترونية وأن يكون تشريعا متكاملاً يتضمن القواعد المناسبة لنشاط هذه التجارة، وإصدار نص قانوني أو تعديل يبين به كيفية تنظيم التوقيع الإلكتروني ويحدد إطاره العام ويوضح مفاهيمه القانونية بعدما اعترف واعتد به في التعديل الذي أجراه على مواد القانون المدني، وضرورة إصدار قوانين تجرم كلّ اعتداء على التوقيع نظرا للأهمية التي يلعبها سواء في توثيق المحررات الإلكترونية بصفة خاصة أو حماية التجارة الإلكترونية بصفة عامة، فلقد منح الكتابة الالكترونية والتوقيع الالكتروني نفس الحجية في الإثبات مع الكتابة والتوقيع التقليدي وذلك بتوفر الشروط المحددة في نص المادة 323 مكرر 1 من القانون المدني إلاّ أنّه ورغم هذا فموقف مشرعنا يبقي موقف محتشم و سلبي وخاصة أمام الانفتاح الاقتصادي والتطورات التقنية السريعة إذ أنّنا نجد أنفسنا أمام نصوص غامضة تحتاج

لنصوص تنظميه لتوضيحها، ومع هذا فّن الجانب التشريعي وحده لا يكفي بل لابدّ من إطارات مؤهلة سواء من حيث اليد العاملة أو من حيث تخصص القاضي الذي لابد أن يوسع من مداركه ومعارفه لتحدي الإشكالات والمنازعات التي تطرح لنظرها.

تجدر الإشارة أن القضاء الجزائري لم تعرض عليه أية قضية تتعلق بالتوقيع الالكتروني وهو ما يفيد أن نصوصنا ما هي إلا نصوص نظرية لم تجد بعد موقعها الحقيقي في الجزائر بسبب التغيرات والمستجدات التي تطرأ بشكل مستمر وهذا ما جعل موضوع التوقيع الالكتروني موضوع غير ثابت وغير مكتمل من حيث مفاهيمه القانونية.

أخيرا يمكن القول أنّه لا يمكن أن نحقق الأمن الكامل في بيئة الإنترنيت، ويبقى الأمن نسبي، لأنّه كلما تطورت التكنولوجيا كلما تطورت وسائل القرصنة، ورغم ذلك نسعى دائما إلى توفير الجو القانوني الملائم واعتماد نظام معلوماتي عالي الثقة باستخدام أدوات التشفير قصد توفير بيئة آمنة وثقة في المعاملات الإلكترونية، وإزالة التخوفات التي تعرقل تطور التجارة الإلكترونية في بيئة افتراضية لازال يكتنفها الغموض ويهدد أصحابها الخوف

أخيرا يمكن القول لا يوجد نظام أمني كامل قطعي الأمن ليس قطعي أو مطلق خاصة في عصر المعلوماتية إذ أن هناك قيمة زمنية للمعلومات تماما كما هو الحال بالنسبة للنقود

قائمـــة المراجـع

قائمة المراجع

أولا: باللغة العربية:

1/ الكتب:

1- **إيهاب فوزي السقا**، الحماية الجنائية والأمنية لبطاقة الائتمان، دار الجامعة الجديدة، مصر، دون طبعة، 2007.

2- **ثروت عبد الحميد**، ماهيته، مخاطره، وكيفية مواجهتها، مدى حجيته في الإثبات دار الجامعة الجديدة، القاهرة، 2007.

3- **حسن عبد الباسط جميعي**، إثبات التصرفات القانونية التي يتم إبرامها عن طريق الإنترنت، دار النهضة العربية، 2000.

4- **خالد مصطفى فهمي**، النظام القانوني للتوقيع الإلكتروني في ضوء التشريعات العربية والاتفاقيات الدولية، دار الجامعة الجديدة، 2007.

5- **خالد ممدوح إبراهيم**، إبرام العقد الالكتروني، دراسة مقارنة، دار الفكر الجامعي الإسكندرية، 2006.

6- ـــــــــــــــــ، إبرام العقد الإلكتروني، دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، 2006.

7- ـــــــــــــــــ، أمن مراسلات البريد الالكتروني، الدار الجامعية، دون طبعة، 2008.

8- **رضا متولي وهدان**، النظام القانوني للعقد الإلكتروني والمسؤولية عن الاعتداءات الإلكترونية، دار الفكر والقانون، المنصورة، 2008.

9- **سعيد سيد قنديل**، "التوقيع الإلكتروني"، دار الجامعة الجديدة، الإسكندرية، 2006.

10- **سميحة القليوبي**، الأوراق التجارية (الكمبيالة، السند لأمر، الشيك، الشيك السياحي، الشيك المسطر، الشيك المعتمد، وسائل الدفع الحديثة)، الطبعة الخامسة، دار النهضة العربية، 2006.

11- **سمير حامد عبد العزيز الجمال**، التعاقد عبر تقنيات الاتصال الحديثة، دار النهضة العربية، القاهرة، 2006.

12- **سمير حامد عبد العزيز الجمال**، التعاقد عبر تقنيات الاتصال الحديثة، دار النهضة العربية، القاهرة، 2006.
13- **طوني ميشال عيسى**، التنظيم القانوني لشبكة الإنترنت، دراسة مقارنة في ضوء القوانين الوضعية والاتفاقات الدولية، المنشورات الحقوقية، بيروت، 2001.
14- **عبد الرازق السنهوري**، الوسيط في شرح القانون المدني الجديد، نظرية الالتزام بوجه عام الإثبات أثار الالتزام المجلد الثاني دار إحياء التراث، بيروت، 1981.
15- **عبد الفتاح بيومي حجازي**، الدليل الجنائي والتزوير في جرائم الحساب الآلي والانترنت، دار الكتب القانونية، الإسكندرية، مصر، 2002.
16- ـــــــــــــــــــ، النظام القانوني لحماية التجارة الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2002.
17- ـــــــــــــــــــ، النظام القانوني لحماية التجارة الإلكترونية، الكتاب الثاني الحماية الحنائية لنظام التجارة الإلكترونية، دار الفكر الجامعي الإسكندرية، 2002.
18- ـــــــــــــــــــ، حماية المستهلك عبر شبكة الإنترنت، دار الفكر الجامعى، الإسكندرية.
19- ـــــــــــــــــــ، مقدمة في التجارة الإلكترونية العربية، (الكتاب الثاني)، الإسكندرية، دار الفكر الجامعي، الإسكندرية، 2004.
20- ـــــــــــــــــــ، التوقيع الإلكتروني في النظم القانونية المقارنة ط1، دار الفكر العربي، الإسكندرية، مصر، 2005.
21- ـــــــــــــــــــ، الإلكترونية "الكتاب الثاني الحماية الجنائية لنظام التجارة الإلكترونية، دار الفكر الجامعي، مصر، 2007.
22- ـــــــــــــــــــ، الجريمة في عصر العولمة، دار الفكر الجامعي، الإسكندرية، 2007.
23- ـــــــــــــــــــ، "التجارة الإلكترونية في القانون العربي النموذجي لمكافحة جرائم الكمبيوتر والانتارنت"، دار شتات للنشر والبرمجيات الإسكندرية، مصر، 2008.

24- **علاء محمد نصيرات**، حجية التوقيع الإلكتروني في الإثبات (دراسة مقارنة) دار الثقافة للنشر والتوزيع، الأردن، 2005.
25- **عمر خالد زريقات**، عقود التجارة الالكترونية عقد البيع عبر الانترنت، ط1 دار الجامعة للنشر والتوزيع، الأردن،2007.
26- **عمرو عيسى الفقي**، الجرائم المعلوماتية – جرئام الحاسب الآلي في مصر والدول العربية، المكتب الجامعي الحديث، دون طبعة ، 2006.
27- **فيصل سعيد الغريب**، التوقيع الإلكتروني وحجيته في الإثبات، منشورات المنظمة العربية للتنمية الإدارية، مصر، 2005.
28- **لورنس محمد عبيدات**، إثبات المحرر الالكتروني، دار الثقافة لنشر والتوزيع عمان، 2005.
29- **محمد السعيد رشدي**، التعاقد بوسائل الاتصال الحديثة ومدى حجيتها في الإثبات، منشاة المعارف، الإسكندرية، 2008.
30- **محمد أمين أحمد الشوابكه**، جرائم الحاسوب والانترنت، دار الثقافة للنشر والتوزيع الأردن، 2004.
31- **محمد أمين الرومي**، التعاقد الإلكتروني عبر الأنترنت، دار المطبوعات الجامعية، الإسكندرية، 2004.
32- ـــــــــــــــ، النظام القانوني للتوقيع الإلكتروني، دار الكتب القانونية مصر، 2008.
33- **محمد حسين منصور**، المسؤولية الإلكترونية، دار الجامعة الجديدة للنشر والتوزيع، الإسكندرية، 2003.
34- **محمد خليفة**، الحماية الجنائية لمعطيات الحاسب الآلي، دار الجامعة الجديدة 2007.
35- **محمد دباس الحميد**، حماية أنظمة المعلومات، دار الحامد للنشر والتوزيع الأردن، 2007.
36- **محمد دباس الحميد، ماركو ابراهيم نينو**، حماية أنظمة المعلومات، دار الحامد للنشر والتوزيع، عمان، الأردن، 2007.

37- **محمد سعيد أحمد إسماعيل**، أساليب الحماية القانونية لمعاملات التجارة الإلكترونية، منشورات الحلبي الحقوقية، 2009.
38- **محمد عبد الرحيم الشريفات**، التراضي في تكوين العقد عبر الانترنت، دار الثقافة للنشر والتوزيع، الأردن، 2009.
39- **محمد علي العريان**، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، 2004.
40- **محمد فواز المطالقة**، الوجيز في عقود التجارة الإلكترونية، دراسة مقارنة، دار الثقافة للنشر والتوزيع، عمان، 2008.
41- **مصطفى محمد موسى**، أساليب إجرامية بالتقنية الرقمية ماهيتها، مكافحتها دراسة مقارنة، دار الكتب القانونية، 2005.
42- **ممدوح محمد خيري هاشم**، مشكلات البيع عن طريق الانترنت في القانون المدني دراسة مقارنة، دار النهضة العربية، 2000.
43- **ممدوح محمد على مبروك**، مدى حجية التوفيع الإلكتروني في الإثبات، دراسة مقارنة بالفقه الإسلامي دار النهضة العربية، 2005.
44- **مناني فراح**، العقد الإلكتروني وسيلة إثبات حديثة في القانون المدني الجزائري دار الهدى للطباعة والنشر والتوزيع، الجزائر، 2009.
45- **منير محمد الجنبيهي، ممدوح محمد الجنبيهي**، التوقيع الإلكتروني وحجيته في الإثبات، دار الفكر الجامعي، الإسكندرية، 2005.
46- **نضال إسماعيل برهم**، أحكام عقود التجارة الالكترونية، دار الثقافة للنشر والتوزيع الأردن، 2005.
47- **وائل أنور بندق**، موسوعة القانون الالكتروني وتكنولوجيا الاتصالات، دار المطبوعات الجامعية، الإسكندرية، 2007.

2/ الرسائل والمذكرات الجامعية:

1- **إيمان مأمون أحمد سليمان**، "الجوانب القانونية لعقد التجارة الإلكترونية، رسالة دكتوراه جامعة المنصورة، 2006.

2- **حمودي ناصر**، النظام القانوني لعقد البيع الدولي الإلكتروني المبرم عبر الإنترنيت، رسالة لنيل شهادة دكتوراه في العلوم، التخصص: القانون، كلية الحقوق، جامعة مولود معمري تيزي وزو، 2009.

3- **عايض راشد المري**: مدى حجية الوسائل التكنولوجية الحديثة في إثبات العقود التحارية رسالة دكتوراه، جامعة القاهرة، 1998.

4- **عيسى غسان ربضي**، القواعد الخاصة بالتوقيع الإلكتروني، رسالة دكتوراه، كلية الحقوق جامعة عين الشمس، مصر، 2006.

5- **محمد إبراهيم عرسان أبو الهيجاء**، القانون الواجب التطبيق على عقود التجارة الإلكترونية، رسالة دكتوراه، جامعة الدول العربية، القاهرة، 2004.

6- **محمد أحمد محمد نور جستينية**، مدى حجية التوقيع الإلكتروني في عقود التجارة الإلكترونية، رسالة دكتوراه، جامعة القاهرة 2005.

7- **محمد مرسي زهرة**، مدى حجية التوقيع الإلكتروني في الإثبات، رسالة دكتوراه، جامعة عين شمس فبراير 1994.

8- **حابت أمال**، استغلال خدمات الانترنت، مذكرة لنيل شهادة ماجستير في القانون، فرع قانون الأعمال، جامعة مولود معمري، تيزي وزو، 2004.

9- **صلاح عبد الحكيم المصري**، متطلبات استخدم التوقيع الإلكتروني في إدارة مراكز تكنولوجيا المعلومات في الجامعات الفلسطينية في قطاع غزة، رسالة لنيل شهادة الماجستير في إدارة الأعمال، كلية التجارة، الجامعة الإسلامية غزة، 2007.

10- **لملوم كريم**، الإثبات في معاملات التجارة الإلكترونية بين التشريعات الوطنية والدولية مذكرة لنيل شهادة الماجستير، جامعة مولود معمري، تيزي وزو، 2011.

3/ المقالات والبحوث العلمية:

1- **إبراهيم سليمان عبدا لله**، التجارة الالكترونية أمن المعلومات، مقال منشور على البريد الإلكتروني، www.kau.edu.sa/iabdullah

2- **أحمد محمد الهواري**، عقود التجارة الإلكترونية في القانون الدولي الخاص، بحث مقدم للمؤتمر العملي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، مركز

البحوث والدراسات بأكادمية شرطة ذبي، الإمارات العربية المتحدة، الفترة 26-28 أفريل 2003.

3- **الدسوقي أبو الليل**، توثيق التعاملات الإلكترونية ومسؤولية جهة التوثيق تجاه الغير المضرور، بحث مقدم إلى مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، الذي نظمته كلية الشريعة والقانون في جامعة الإمارات العربية المتحدة، بالتعاون مع غرفة التجارة الإلكترونية وصناعة ذبي، في الفترة ما بين 10 و12 ماي 2003، المجلد الخامس، ص1856 الموقع:http://www.unue.banque.com/imarat/arab/12/3398.pdf

4- **جميل حلمي**، مخاذير الشراء الإلكتروني، بحث منشور على الموقع الإلكتروني: www.islamonlaine.net/arabic/elonomics/2003/12/articale02.shtml.

5- **حسن محمد عرب**، مقال على الموقع الإلكتروني http://www.uaeec.com/articles-action-show-id-34.htm

6- **قارة مولود**، الإطار القانوني للتوقيع والتوثيق الإلكترونيين في قانون المعاملات والتجارة الالكترونية، **مقال منشور عبر الموقع** www.minshawi.com

7- **نادر شافي**، التوقيع الالكتروني، الاعتراف التشريعي له وتعريفه القانوني وشروطه وأنواعه والمصادقة عليه، مجلة الجيش اللبناني، عدد 249، مارس 2006، منشور عبر الموقع: www.lebarmy.lb/article.asp

4/ الوثائق:

جريدة الشروق الاثنين 30 ماي 2011 /الموافق لـ 27 جمادي الثانية 1432هـ / العدد 3309 أنظر الموقع الالكتروني: www.alchourouk.com

لقانون الأونسيترال النموذجي للتجارة الإلكترونية الإلكتروني: منشور باللغتين الإنجليزية والعربية على الموقع: http://www.uncitral.org

قانون التوجيه الأوربي، منشور على الموقعين: http://www.ec.europa.eu. http://www.fs.dk/uk/acts/eu/pdf/esign-fr.pdf

5/ النصوص القانونية:

الإتفاقيات الدولية:

إتفاقية الأمم المتحدة لاستخدام الخطابات الإلكترونية في العقود الدولية 2005م.

النصوص التشريعية:

1- الأمر رقم 59/75، مؤرخ في 26 سبتمبر 1975 والمتضمن القانون التجاري، المعدل والمتمم.

2- الأمر رقم 03-11، المؤرخ في 26 أوت سنة 2003 المتعلق بالنقد والقرض، ج ر عدد 52 مؤرخة في 2003/08/27، والذي ألغى الأمر90- 10 المؤرخ في 14 أفريل 1990 المعدل والمتمم والملغى، والذي تمت الموافقة عليه بالأمر03- المؤرخ في 25 أكتوبر 2003، ج ر عدد 64 مؤرخة في2003.

3- قانون رقم 15/04، مؤرخ في 14 نوفمبر 2004، يعدل ويتمم الأمر رقم 156/66 المؤرخ في 8 جوان 1966، والمتضمن قانون العقوبات، ج ر عدد 71، الصادرة في 10 نوفمبر 2004.

4- الأمر رقم 58/75 المؤرخ في 26 سبتمبر1975، المتضمن القانون المدني، معدل ومتمم بالأمر رقم 10/05 مؤرخ في 20 جوان 2005، ، ج ر عدد 44 الصادرة في 26 جوان 2005.

5- قانون رقم 23/06، المؤرخ في 20 ديسمبر 2006، يعدل ويتمم الأمر رقم 156/66، المؤرخ في 8 جوان 1966، والمتضمن قانون العقوبات، ج ر عدد 84 الصادرة في 20 ديسمبر 2006.

6- قانون رقم 04/09، مؤرخ في 5 أوت 2009، يتضمن القواعد الخاصة من الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج ر عدد 47، الصادرة في 16 أوت 2009.

7- أمر05-06، المؤرخ في 2005/08/23، المتعلق بمكافحة التهريب، ج ر عدد 59.

8- أمر 05-02 المعدل والمتمم للأمر 75-59 لـــ 26 سبتمبر 1975 المتضمن القانون التجاري ج ر عدد 11.

النصوص التنظيمية:

1- مرسوم تنفيذي رقم 123/01، مؤرخ في 09 ماي 2001، يتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية، وعلى مختلف خدمات المواصلات السلكية واللاسلكية، ج ر عدد 27، الصادرة في 13 ماي 2001.

2- مرسوم تنفيذي رقم 275/98، مؤرخ في 25 أوت 1998، يضبط شروط وكيفيات إقامة خدمات الأنترنيت واستغلالها، ج ر عدد 63، الصادرة في 26 أوت 1998.

القوانين النموذجية:

1- قانون اليونسيترال النموذجي بشأن التجارة الإلكترونية لسنة 1996، صادر في جلسة رقم 85 للجمعية العامة للأمم المتحدة بتاريخ 16 ديسمبر 1996، متوفر عبر الموقع:
http//www.uncitral.org/pdf/arabic…

2- قانون اليونسيترال النموذجي بشأن التوقيعات الإلكترونية، صادر في جلسة رقم 85 للجمعية العامة للأمم المتحدة بتاريخ 12 ديسمبر 2001، متوفر عبر الموقع:
http//daccess-ods.un.org/tmp/7958533.html

ب/ النصوص التشريعية للدول الأجنبية:

1-القرار 109-2005 خاص بإصدار اللائحة التنفيذية لقانون التوقيع الإلكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات رقم 15 لسنة 2004م، وقد صدر هذا القرار في 2005/5/15م، ونشر بالوقائع المصرية العدد 115 تابع بتاريخ 2005/5/25م متوفر عبر الموقع: http//www.cksu.com uoloade/vb/12536.

2- القانون التونسي بشأن المبادلات والتجارة الإلكترونية رقم 83-2000 الصادر في 9-9-2000 ونشر في الرائد الرسمي للجمهورية التونسية في الصدد 24من الصفحة رقم 2084 إلى غاية الصفحة 2089– أنظر الموقع:
http://www.infocom.th/fileadmin/documentation/juridiques/jortAR/jort 64 11 8 2000 pdf

3-المرسوم رقم 272-2001م، الصادر في 30 مارس 2001، الجريدة الرسمية الفرنسة صفحة 5070 الصادرة في 2001/03/31، والذي جاء تطبيقا للمادة (4/1316) من القانون المدني، للإطلاع على هذا المرسوم أنظر الموقع الإلكتروني:
www.journal.officiel.gouv.fr

4-قانون المعاملات الإلكترونية الأردني رقم 85 لسنة 2001 على الموقع:
http://www.lob.gov.jo/ui/laws/index.jsp.
5-القانون الإماراتي رقم 2 لسنة 2002م بشأن المعاملات والتجارة الإلكترونية انظر الموقع الإلكتروني:
http://shabab20.net/index.php?option=com_kunena&func=view&id=815&catid=39&Itemid=194
6-القانون الفدرالي الأمريكي أنظر الموقع الإلكتروني:
http://www.frwebgate.access.gpo.gov.cgibin/getdoc.cgi?dbname106-cong-public-laws.
http://www.gigalawcom/articles/2000-all/aston-2000-06-all.htm
7-التوجيه رقم 93/1999 والصادر بتاريخ 1999/12/13 بشأن التوقيع الإلكتروني
http//eur-lex.europa.eu/lex uriserv/…

ثانيا: باللغات الأجنبية:

1/ Ouvrages:

BRUN (W), les mécanismes du paiement sur Internet, Juriscom.net, 20 Bernard, 1999.

Ch. DEVYS. Du sceau numérique a la signature numérique, in, vers une administration sans papier (sous la direction de Christ: DHENIN) Paris, la documentation française, Paris 1996.

FAUSSE-Arnaud, la signature électronique: Transaction et confiance sur Internet, édition Dunod, Paris, 2001.

RAYPORT Jeffrey F et JAURORSKY Bernard, commerce électronique (Traduit de l'américain port) Francine Nézina Johanne champoux et Elisabeth Rochette, Edition cheneliere/ Mc Gram-Hill, Montréal – Toronto, 2003

LANCE Loeb, your right in the on- line, world, OSBORNE Mc GRAW-HALL, New-York, U S A, 1995.

BRAZELL LORNA, Electronic signatures, law and Regulation Sweet Maxwell. London 2004.

JEAN_BAPTISTE Michelle « créer et exploiter un commerce électronique », édition LITEC, Paris, 1998.

ROGER Larry-Miller and GQYLOURD A-Gentz, Law for electronic commerce, THOMSON LEARMING, New-York, 2000.

PIETTE-COUDOL Thierry, Echange électroniques certification et sécurité, édition LITEC, Paris, 2000**.**

TOERING Jean Pierre et BRIAN Français, Des moyens de paiements, Edition que sais-je ?, 1ère édition 1999.

2/ Thèses et mémoires :

DIMITRIOU Philippe, «l'application du droit de la cryptologie en matière de sécurité des réseaux informatique » D.U.E.A fac des sciences juridique, politiques et sociales, école doctorale N°74, université de LILLE, 2002.

Julien ESNAULT, mémoire de DESS de droit Multimidia et de l'informatique, l'Université de Paris, 2002.

3/ Articles:

CAPRIOLI, Eric et **CANTERO Anne**, aspects légaux et réglementaire de la signature électronique, disponible sur le site : www.caprioli-avocats.com

THIERY Patrick: l'émergence d'un droit européen du commerce électronique, revue trimestrielle de droit européenne, N°04, 2000, pp 649-674.

PGP 6.5.1, Introduction à la cryptographie, 1999, Network associate, in : http://laurent.falcaum.fre.fr, p.02.

ROJINSKY (c), Signature Electronique: « Le décret et le devront être complètes », sur le site:
http://www.jurcon.het/pro/2/ce2001/04/9.htm

- **VALERIE sédalian**: preuve et signature électronique, Paris, sur Le site: http://www.juriscom.net/chr2/fr20000509.htm

فهرس الموضوعات

ملخص

أدّى التطور التكنولوجي ودخول التجارة الالكترونية في المعاملات المالية، إلى ضرورة إيجاد وسيلة سريعة آمنة ومقبولة تستخدم في توثيق المعاملات الالكترونية غير الوسائل التقليدية التي قد تؤخر أو تعيق التعاقد بين الأطراف، فتمّ إدخال التوقيع الالكتروني ليحل محل التوقيع التقليدي، الذي هو وسيلة إلكترونية لتوثيق هذه المعاملات، يتم من خلاله التأكد من شخصية صاحب التوقيع وموافقته على الالتزام بها، وصحة الوثيقة التي تمّ تبادلها بين الأطراف، لذا يعتبر مخالفا للقانون كلّ تزوير أو تقليد أو كلّ أوجه الاعتداء عليه، سواء بموافقة صاحبه أو بدونها، إلاّ أنّ الحياة العملية ورغم الثقة الممنوحة للتوقيع الالكتروني، سواء للموقع أو الموقع له وحتى الغير، أفرزت العديد من المخاطر كالقرصنة الإلكترونية التي تعيق استخدام التوقيع الإلكتروني بشكل أمن مما يستدعي آليات تقنية ووقائية وقانونية لتأمين وحماية التوقيع الإلكتروني على المستوى الداخلي والدولي.

RESUME

Le développement technologique et l'entrée du commerce électronique dans les transactions financières, est un besoin urgent de trouver une utilisation rapide sûr et acceptable dans la documentation des transactions électroniques. Le moyen traditionnel peut retarder ou entraver le contrat entre les parties, C'est pour cela que la signature électronique remplace la signature traditionnelle,

La signature numérique est un mécanisme permettant de garantir l'intégrité d'un document électronique et d'en authentifier l'auteur.

pour documenter les transactions qui sont faites par Internet, la signature électronique assure l'identité des titulaires de cette signature et leur consentement, et l'authenticité du document qui sont échangés entre les parties, de sorte qu'il est contre la loi toute fraude, soit avec le consentement du propriétaire ou autrement, sauf que le processus de la vie et malgré la confiance accordée à la signature électronique, la plupart des risques comme le piratage, qui empêchent l'utilisation de cette signature ce qui exige des mécanismes techniques, et des mesures juridiques pour la sécuriser et la protéger au niveau national et international.