جامعة عبد المالك السعدي
الكلية المتعددة التخصصات
تطوان

ماستر قانون الأعمال
الفصل التاسع
مادة: التجارة الالكترونية

الموضوع

حجية التوقيع الالكتروني في إثبات العقود الالكترونية

تحت إشراف:

د. هشام الإدريسي العزوزي

من إعداد:

وردة الوردي
إيمان بوزينب
فدوى الشاط الصباغ
رفيعة حيون
هناء بنبراهيم

السنة الجامعية:2016-2017

مقدمة

يعرف العالم اليوم تطورا سريعا ومهولا في مجال الاتصالات ونظم المعلومات، ويرجع سبب ذلك إلى التطور التكنولوجي الذي قفز قفزة نوعية في كل المجالات ومن بينها مجال التجارة الالكترونية، والذي أثر أيضا بشكل واضح في المبادئ الراسخة في الفكر القانوني، خاصة عناصر دليل الإثبات(الكتابة والتوقيع)،التي تقوم على وسط مادي محسوس وملموس، وقد صاحب هذا التطور ظهور أنماط وأشكال متعددة للوسائل التي يتم من خلالها إبرام التصرفات القانونية، حتى أدى إلى قلب المعادلة في جميع المعاملات من الدعامة الورقية إلى الدعامة الالكترونية ، وحتى يتلاءم توثيق المعاملات القانونية مع هذه الاشكال الجديدة ، ظهر ما يسمى بالتوقيع الإلكتروني.

كانت أولى بوادر ظهوره بشكل خاص من خلال إرشادات التوقيع الالكتروني التي وضعتها نقابة المحامين الامريكيين سنة 1995، والتي تبعته قانون الاونسترال النموذجي للتوقيع الإلكتروني سنة 1996 رقم 85 ، الذي تم تحيينه سنة 2001 وبالضبط 2001/01/10، وقبل هذا التحيين صدر التشريع الفدرالي بشأن التوقيعات الالكترونية في التجارة الداخلية والدولية لعام 2000، ومعه التوجيه الاوروبي للتجارة الالكترونية لسنة 2000 الصادر في 2000/06/08،كذلك قانون رقم 230 لسنة 2000 الذي طور به المشرع الفرنسي قانون الإثبات مع تكنولوجيا المعلومات، ثم اللوائح البريطانية المنظمة للتوقيعات الالكترونية الصادرة بتاريخ 2002/03/08.[1]

أما بالنسبة للتشريعات العربية فقد أصدر المشرع المصري القانون المنظم للتوقيع الإلكتروني رقم 15 سنة 2004، أما المشرع المغربي فلم يؤطر التوقيع الالكتروني إلا سنة 2007 عند صدور قانون رقم 53.05 المتعلق بالتبادل الإلكتروني للمعطيات القانونية[2]، من خلال الفرع الأول من الباب الأول من القسم الثاني وبالضبط من المادة 6 إلى المادة 11 من القانون المذكور، كما أنه لم يقم بإعطاء تعريف له عكس باقي التشريعات[3]والتي نجد من بينها قانون الاونسترال الذي عرف التوقيع الإلكتروني بكونه: "بيانات في شكل إلكتروني مدرجة في رسالة بيانات أو مضافة إليها، ويجوز أن تستخدم لتعيين هوية الموقع والتدليل على موافقته على المعلومات الواردة في رسالة البيانات"[4].

---

[1]- زينب غريب، إشكالية التوقيع الالكتروني وحجيته في الإثبات، رسالة لنيل دبلوم الماستر في القانون الخاص، من كلية العلوم القانونية والاقتصادية والاجتماعية، جامعة محمدد الخامس السويسي الرباط، السنة الجامعية 2009-2010 الصفحة 4-5

[2]- انتصار اليعكوبي، مدى حجية المحررات لإلكترونية في الإثيات -دراسة مقارنة-بحث لنيل دبلوم الماستر في القانون الخاص، تخصص المدني والأعمال، السنة الجامعية 2010-2011، الصفحة:2

[3]- عرف المشرع المصري في المادة الأولى من القانون رقم 15 لسنة 2004 المتعلق بالتوقيع الإلكتروني بأنه:" ما يوضع على محرر إلكتروني ويتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها، ويكون له طابع منفرد يسمح بتحديد هوية الموقع ويميزه عن غيره "وفي مقابل هذا نجد قانون إمارة دبي رقم 2لسنة 2002 المتعلق بالمعاملات والتجارة الإلكترونية الذي عرف التوقيع الإلكتروني في مادته الثانية بأنه:" توقيع مكون من حروف أو أرقام أو رموز أو صوت أو نظام معالجة ذي شكل إلكتروني مكان وملحق أو مرتبط منطقيا برسالة إلكترونية"

[4]- محمد أطويف، إشكالية إثبات عقد التجارة الإلكترونية، مجلة الحقوق، العدد 15، مطبعة المعارف الجديدة، الرباط السنة 8، يونيو 2013-يناير 2014، الصفحة:69-70

-

وتتجلى أهمية التوقيع الإلكتروني في العقود الإلكترونية من خلال القوة الثبوتية والحجية التي يضفيها على المعاملات القانونية، باعتباره الأداة أو المفتاح الحقيقي التي يمكن بواسطته إثبات وحل المشاكل التي يمكن أن تواجه المتعاملين بهذا النوع من التعاقدات، ومنه يمكننا طرح الاشكالية التالية:

ما مدى نجاعة قانون رقم 05-53 في ضمان حجية التوقيع الالكتروني، وما مدى فعالية هذا الأخير؟

وللإجابة عن هذه الإشكالية، ارتأينا تقسيم الموضوع إلى مبحثين :

- **المبحث الأول :فعالية التوقيع الالكتروني في إثبات العقود الالكترونية**
- **المبحث الثاني: الآليات الحمائية للتوقيع الالكتروني في العقود الإلكترونية**

المبحث الأول: فعالية التوقيع الالكتروني في إثبات العقود الالكترونية

إن التوقيع الإلكتروني هو عبارة عن وسيلة يستعملها أحد الأشخاص للتعبير عن شخصيته وإرادته في الإلتزام بمضمون المحرر الإلكتروني، حيث يأتي في شكل معادلات رياضية وخوارزمية ورموز سرية يتم معالجتها من خلال الحاسب الآلي، فإن هذا الأمر يدفعنا إلى التساؤل عن فعالية هذا التوقيع وما مدى فدرته عل إثبات المعاملات الإلكترونية؟

للإجابة عن هذا السؤال سنحاول تقييم التوقيع الإلكتروني إذ يطرح السؤال حول الأمن الذي يوفره هذا التوقيع خاصة أمام التطور التقني السريع؟ (المطلب الأول).

كما أنه لابد من الوقوف على حجية هذا التوقيع عن طريق لابراز مدى فعاليته في مجال إثبات المعاملات الالكترونية وابراز مدى انسجامه مع التوقيع التقليدي (المطلب الثاني)

♦ المطلب الأول: تقييم التوقيع الالكتروني

لتقييم التوقيع الالكتروني لا بدة من الوقوف على وظائفه، وكذلك لا بدة من التطرق إلى أشكاله ودراسة مدى فعاليتها خاصة وأن المشرع المغرب اكتفى فقط بالإشارة إلى التوقيع الالكتروني دون تحديد أشكاله التي يمكن اعتمادها في الإثبات (الفقرة الأولى)، كما أنه نص على مجموعة من الشروط التي يجب أن تتوفر فيه، وانطلاقا من هذه الشروط نستخلص مجموعة من الوظائف يجب أن يوفرها التوقيع الالكتروني وهذا ما سنقف عليه في (الفقرة الثانية).

الفقرة الأولى: صور التوقيع الإلكتروني

تختلف أشكال التوقيع الالكتروني باختلاف الطريقة المتبعة في إظهاره، فقد يتخذ هيئة حروف أو أرقام أو رموز[5]، كما يمكن أن يأتي عبارة عن وحدات ضوئية أو رقمية أو كهرومغناطيسية، كما قد يكون مجرد نسخ للتوقيع العادي، ومن هنا يطرح التساؤل حول مدى فعالية هذه الصور، وما إذا كانت توفر الأمن كافي للعمل بها خاصة وأن المشرع المغربي نص على التوقيع الالكتروني المؤمن؟

للإجابة عن هذا الإشكال سنتطرق لبعض صور التوقيع الالكتروني مع تقييم فعاليتها:

أولا: التوقيع الرقمي

يعتبر التوقيع الرقمي من أهم صور التوقيع الالكتروني لما يحققه من أمان وموثوقية في مجال الانترنيت والتجارة الالكترونية[6]، نظرا لما يتمتع به من قدرة فائقة على تحديد هوية أطراف العقد تحديدا دقيقا ومميزا.

---

[5]-ماجد محمد سليمان أبا الخيل، العقد الاكتروني، مكتبة الرشد،المملكة العربية السعودية، الطبعة الأولى 2009، الصفحة 102

[6]- زروق يوسف، حجية وسائل الإثبات الحديثة، رسالة لنيل شهادة دكتوراه في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبوبكر بلقايد تلمسان، السنة الجامعية 2012 -2013، الصفحة: 247.

ووفقا لمعيار الايزو والمتعلق بالأمان الصادرة عن المنظمة الدولية للمقياس iso أنه يقصد بالتوقيع الرقمي بيان يتصل بوحدة البيانات أو هو التحويل التشفيري لوحدة من البيانات، بما سيسمح للمرسل إليه من التعرف على مصدر وحدة البيانات وإثباتها والتحقق من سلامة مضمونها وتأمينها ضد أي تعديل أو تحريف[7].

وقد جاء التوقيع الرقمي من خلال فكرة الرموز السرية والمفاتيح المتماثلة وغير المتماثلة، حيث يتم الاعتماد على اللوغاريتمات والخوارزميات والمعادلات الرياضية المعقدة فنيا[8]، ويتم التوقيع الرقمي عبر إنشاء رمز أو رقم سري باستخدام برنامج حاسب (الترميز)، الذي يقوم على تحويل الرسالة إلى صيغ غير مفهومة عن طريق تقنية التشفير، ثم إعادتها إلى صيغتها الأصلية بإستخدام المفتاح المناسب لفك تلك الشفرة.

فالمقصود بالتوقيع الرقمي مجموعة من البيانات أو المعلومات المتصلة بمنظومة بيانات أخرى، أو صيغة منظومة في صورة مشفرة حيث يتم تحويل الكتابة من أسلوبها العادي إلى معادلة رياضية وتحويل التوقيع إلى أرقام عن طريق تقنية التشفير، ولكي يتم إعادة المعلومات التي تم تشفيرها إلى وضعها الأصلي، يستخدم المفتاح المناسب لفك الشفرة. ويتم التوقيع الرقمي من الناحية التقنية عبر نمطين من التشفير:

- التشفير المماثل وهو تشفير يقوم على فكرة المفتاح واحد الذي يتبادله الطرفين لفك رموز الرسالة، حيث يستخدمه المرسل إليه قصد فك الشفرة والاطلاع على الرسالة، غير أن هذا النوع غير أمن لأن المرسل والمرسل إليه يملكان نفس المفتاح[9].
- التشفير غير المماثل وهو الذي يقوم على وجود زوجين من المفاتيح غير المتناسقة، مفتاح عام وأخر خاص، فالأول يكون غير سري ومعروف عند الجميع، فأما الثاني فيكون سريا خاص بصاحبه وبواسطته يشفر رسالته، حيث يسمح المفتاح العام لكل شخص بقراءة رسالة البيانات عبر شبكة الانترنيت دون أن يستطيع تعديلها، إذا رضي بمضمونها يستطيع التوقيع عليها بواسطة مفتاح خاص ثم إعادتها إلى مصدرها مرفقة بتوقيعه[10].

ويعتبر هذا النوع من التوقيع أكثر استخدام في إبرام التعاقدات بين التجار والشركات لما له من تحديد تام ومميز لهوية طرفي، وهو بذلك يكون محققا لكافة شروط التوقيع الإلكتروني التي يتطلبها القانون، فهل يوفر هذا التوقيع الأمن الكافي لتشجيع العمل به؟

لا إجابة واضحة حتى الأن، إلا أنه لا يمكن نفي دوره كوسيلة إثبات لهوية صاحب العمل شأنه في ذلك شأن التوقيع المكتوب بخط اليد بل وأكثر من هذا الأخير، كما يحقق سلامة لمحتوى الرسالة ويحميها من كل تغيير أو تزوير قد يطالها، ويضمن كذلك سرية المعلومات التي تتضمنها الرسائل الالكترونية، إلا أنه تعتريه في الوقت الحاضر مجموعة من العيوب، حيث مكن التطور التقني الحالي من القيام بعمليات تزوير التوقيع الرقمي يصعب اكتشافها، وهذا عن طريق كسر المفتاح الخاص برسالة البيانات حيث يمكن بعدها التغيير بسهولة تامة في مضمون الرسالة من جانب الشخص الذي أصدرها أو من جانب صاحب التوقيع ، بالإضافة إلى أنه يتطلب التدريب والمهارات على البرمجيات المستعملة في إنشائه.

---

[7] -virginie ETIENNE »le développement de la signature électronique », master 2, recherche droit des affaires, université PARIS 13 NORD, année universitaire 2010 – 2011, page 20 – 21.

[8]- محمد برادة غزيول، قراءة في القانون المتعلق بالتبادل الالكتروني للمعطيات القانونية، مجلة المعيار، العدد 39، يونيو 2008، الصفحة:16.

[9]- زروق يوسف، مرجع سابق، الصفحة: 246.

[10]- ماء العينين السعداني، الإطار القانوني للمصادقة على التعاملات الالكترونية، مجلة قانون وأعمال، المطبعة والوراقة الوطنية، العدد الثاني دجنبر 2011، الصفحة: 112.

ثانيا: التوقيع البيومتري

يعتمد التوقيع البيومتري على صفات ذاتية فزيائية وسلوكية للإنسان، لتميزه وتحديد هويته، عن طريق إدخال معلومات بطريقة بيومترية بذاكرة الحاسب الآلي [11](مثل بصمة الشخصية، قزحية العين، التعرف على الوجه البشري، خواص اليد البشرية، التحقق من نبرة الصوت ...).

ويتم التحقق من شخصية مستخدم التوقيع البيومتري عن طريق أجهزة إدخال المعلومات وتخزينها بطريقة مشفرة في ذاكرة الحاسوب، ليقوم بعد ذلك بمطابقة صفات المستخدم مع الصفات المخزنة[12].

أدى اختلاف الخواص المميزة لكل إنسان، إلى جعل من التوقيع البيومتري والذي يرتكز على هذه الخصائص، وسيلة إثبات موثوق بها لتمييز الشخص وتحديد هويته كموقع بشكل دقيق، وهو ما يفتح مجال واسعا لاستخدامه في إثبات التصرفات التي تم عبر الوسائط الإلكترونية.

إلا أن الاشكال المطروح هو هل تصلح خصائص الإنسان الذاتية كوسيلة من وسائل التوقيع الإلكتروني بإعتبار هذه الخصائص من المستحيل تحليلها والعبث بها، وهل توفر الأمن الكافي لهذا التوقيع؟

بالرغم من الإجابيات التي يحملها هذا التوقيع، وأمام تطور التقني السريع الذي يمكن خلاله نسخ التوقيع، حيث أن ما يعاب على هذه التقنية من التوقيع هو إمكانية مهاجمتها أو نسخها من قراصنة الحاسوب عن طريق فك شفرتها، لأنها تفتقر إلى الأمن والسرية[13]، وما يزيد من صعوبة اعتماد هذا التوقيع أيضا أن تقنية الخاصة بهذا الشكل مرتفعة الثمن ، كما أنه قد لا يعبر بشكل صحيح عن رضى الحقيقي للموقع بمضمون ما وقع عليه، أو بأحرى ألا تتوفر أية نية للتوقيع، فقد يجبر الشخص على الوقوف أمام الجهاز الخاص يعمل على مسح الخواص البيومترية، وبالتالي أخذ توقيعه دون رضاه إلا أن ذلك لا ينقص من حجية التوقيع البيومتري في الإثبات، حيث أن هذه التلاعبات قد تطال أيضا التوقيع اليدوي.

ثالثا: التوقيع باستخدام البطاقات الممغنطة والمقترنة بالرقم السري

يعتبر التوقيع باستخدام البطاقات الممغنطة من صور التوقيع الالكتروني الأكثر شيوعا لدى الجمهور، وتتولى البنوك ومؤسسات الائتمان إصدار هذه البطاقات[14].

ويتم التوقيع بإستخدام البطاقة الممغنطة عبر إتباع الخطوات التالية:

- إدخال البطاقة الخاصة بالعميل والتي تحتوي على بياناته الشخصية، في الجهاز الخاص بنقطة البيع أو في جهاز الصرف الآلي.
- إدخال الرقم السري الذي يعد بمثابة التوقيع، وهذا بكتابته عن طريق لوحة المفاتيح التي توجد في الجهاز[15].

وتأتي بطاقات الممغنطة على نوعين:

- فالنوع الأول يجمع بين طرفين (العميل والبنك)، يستخدم للسحب النقدي من خلال أجهزة الصرف الآلي.

---

[11]- إدريس النوازلي، حماية عقود التجارية الإلكترونية في القانون المغربي، دراسة مقارنة، المطبعة والوراقة الوطنية، الطبعة الأولى 2010، الصفحة:66.

[12]- زينب غريب، مرجع سابق -الصفحة: 34.

[13]-ماء العينين السعداني، مرجع سابق، الصفحة: 109 – 110.

[14]- طارق عبد الرحمان ناجي كميل، التعاقد عبر الأنترنيت وأثاره، دراسة مقارنة، بحث لنيل دبلوم الدراسات العليا في لقانون الخاص، كلية العلوم القانونية والاقتصادية والاجتماعية، جامعة محمد الخامس أكدال، السنة الجامعية 2003-2004 -الصفحة:131.

[15]- زروق سمير، مرجع سابق، الصفحة: 53.

- أما النوع الثاني فيكون بين ثلاث أطراف (العميل والبنك وطرف ثالث) حيث يخول هذا النوع من البطاقات للوفاء بثمن السلع والخدمات التي يحصل عليها العميل من بعض التجار والمحلات التي تقبلها.

فالتوقيع الإلكتروني عبر بطاقة الائتمان مثلا يتم عن طريق استخدام التوقيع الرقمي فكل شخص يستخدم هذا النوع من البطاقات في سداد ثمن السلعة أو الخدمة يجب أن يتوفر لديه ما يعرف باسم مدخل الدفع الأمن، وهو نظام تشفير يقوم بنقل بيانات الخاصة بالبطاقة والمعلومات بشكل أمن من الموقع إلى مراكز بطاقة الائتمان[16].

وقد استقر القضاء الفرنسي على قبول هذه الصورة من التوقيع الالكتروني في الإثبات بعدما رفضها في البداية، حيث أصدرت محكمة الاستئناف مونبيلييه في 9 أبريل 1987 قرارا أخذت فيه باستخدام الرقم السري والتوقيع الالكتروني، حيث قام بإلغاء حكم الصادر عن محكمة ستي الذي كان قد رفض الأخذ بالتوقيع الذي يصر عن جهاز الصرف الآلي على اعتبار أنه تابع للبنك وليس للعميل[17].

والملاحظة التي يمكن تسجيلها بخصوص هذا التوقيع هو أنه يتسم بالبساطة وبتوفير قدر كبير من الأمان والثقة لدى العميل نظرا لوجود ضمانات عند سرقة البطاقة، غير أن ما يعاب على هذا التوقيع هو اقتصار أثاره في الإثبات، على حالات وجود علاقة تعاقدية مسبقة بين الطرفين واتفاقهما بشأن ما يثور بسببها من نزاعات.

رابعا: التوقيع بالقلم الالكتروني

يتمثل التوقيع الالكتروني باستخدام قلم إلكتروني ضوئي وحساس يكمنه الكتابة على شاشة الحاسوب الآلي عن طريق برنامج هو المسيطر والمحرك لكل العملية[18].

بحيث يوجد برنامج خاص للالتقاط التوقيع والتحقق من صحته أو ما يطلق عليه خدمة التحقق من صحة التوقيع[19] ، إذ يقوم البرنامج بتلقي بيانات العميل عن طريق بطاقة خاصة تحتوي على بيانات كاملة عن هذا الشخص الذي يضعها في الأدلة المستخدمة، وتظهر التعليمات بعد ذلك على الشاشة الالكترونية ليتبعها الشخص من أجل التوقيع، ثم تظهر للشخص مفاتيح معينة تعطيه الاختيار من خلال الضغط عليها، ويقوم البرنامج بجمع المعلومات عن المستخدم وحساب التوقيع والوقت وعدد مرات المحاولة، وبعدها يقوم بتشفير كل هذه البيانات والاحتفاظ بها إلى وقت الحاجة إليها، وتسمى البيانات المشفرة بالشارة البيومترية[20].

ثم بعد ذلك يقوم برنامج بتحقق من صحة التوقيع حيث يقوم بفك رموز الشارة البيومترية، لتقارن معلومات الموجودة عليها مع احصائيات التوقيع المخزنة من قبيل بياناتها لتصدر بعد ذلك تقريرها إلى برنامج الكمبيوتر، الذي يعطي الرأي النهائي في صحة أو عدم صحة هذا التوقيع[21].

---

[16]- زينب غريب، مرجع سابق، الصفحة: 56.

[17]- زروق يوسف، مرجع سابق، الصفحة: 245.

[18]- إدريس النوازلي، مرجع سابق، الصفحة:68.

[19]-خالد ممدوح إبراهيم، إبرام العقد الالكتروني، دراسة مقارنة، مطبعة دار الفكر الجامعي-الاسكندرية، الطبعة الثانية 2011، الصفحة 255

[20]- أحمد البختي، استعمال الوسائل الالكترونية في المعملات التجارية، رسالة لنيل دبلوم الدراسات العليا المعمقة في القانون الخاص، كلية العلوم القانونية والاقتصادية والاجتماعية، جامعة محمد الخامس السويسي الرباط، السنة الجامعية 2003-2004 –الصفحة: 42.

[21]- زينب غريب، مرجع سابق، الصفحة:37.

وبالتالي في حالة سرقة البطاقة والرقم السري، فإنه ليس من السهل القيام بعملية التوقيع، وذلك لأن البرنامج المخصص يكتشف ذلك من خلال التحقق من التوقيع الذي يتم لأنه ليس من السهل القيام بنفس الحركات التي يقوم بها صاحب التوقيع الأصلي[22].

غير أنه هنا يطرح مشكل بخصوص إثبات العلاقة التوقيع والمحرر، حيث بإمكان المرسل إليه الاحتفاظ بنسخة من التوقيع، ثم يعيد وضعها على محرر إلكتروني أخر ويدعي أن واضعها هو صاحب التوقيع الفعلي[23]، غير أن هذه العيوب لا تنال من موثوقية هذا التوقيع حيث يعد عنصرا من عناصر دليل الإثبات، خاصة إذا توفرت الأجهزة وتم التأكد من سلامة التوقيع بالقلم الإلكتروني ونسبته للموقع الحقيقي.

ومن المشاكل التي تحد أيضا من إنتشار التوقيع بالقلم الالكتروني هو أنه لابد لإتمام هذا التوقيع من وجود حاسوب ذي موصفات خاصة، كإحتوائه حلى وحدة القلم الالكتروني والشاشة الحساسة، إضافة إلى أنه مكلف جدا[24]، كما أنه لابد من التحقق في كل مرة من صحة التوقيع، بالتالي لابد من وجود مقدم خدمة التصديق الالكتروني للتحقق مسبقا من شخصية الموقع لتسجيل عينات من التوقيع وتقديمها خدمة التقاط التوقيع والتحقق منه.

كل هذه الصور تدخل في إطار التوقيع الالكتروني المؤمن الذي أخذ به المشرع المغربي، بالرغم من كونه لم يتطرق لأي واحدة منها، وينضاف إلى هذه الصور نوع أخر من التوقيع الالكتروني ويتعلق الأمر بالتوقيع الالكتروني البسيط، الذي أخذت به الدول الأوروبية، وحجية هذا التوقيع معلقة على عدم إنكاره وضرورة تقديم دليل على موثوقيته.

الفقرة الثانية: وظائف التوقيع الإلكتروني

يلعب التوقيع التقليدي كعلامة خطية وشخصية دور مهم في عملية الاثبات، لكونه يقوم بتحديد شخصية الموقع، ومن ناحية أخرى يقوم بالتعبير عن إرادة الموقع في التزامه بمضمون الورقة وإقراره لها، وأمام هذا الدور الثلاثي الذي يلعبه التوقيع التقليدي، يطرح التساؤل حول الدور الذي يقوم به التوقيع الالكتروني، فهل يقوم بنفس وظائف السابقة الذكر أمم هناك وظائف أخرى خاصة به؟ وما مدى تحقيقه لهذه الوظائف خاصة عند اعتماده على تقنية التشفير والمصادقة الالكترونية؟

بالرجوع إلى قانون الأونسترال النموذجي بشأن التجارة الالكترونية لعام 1996 خاصة المادة 7 منه نجده يؤكد على أن التوقيع الالكتروني يجب أن يقوم بتعيين هوية الشخص الموقع، وتوفير ما يؤكد يقينا مشاركة ذلك الشخص بالذات في

---

[22]- لورنس محمد عبيدات، إثبات المحرر الالكتروني، مطبعة دار الثقافة – الطبعة الأولى 2005، الصفحة :148.

[23]- إدريس النوازلي، مرجع سابق، الصفحة: 68.

[24]- ماء العينين السعداني، مرجع سابق، الصفحة: 111.

فعل التوقيع، والربط بين ذلك الشخص ومضمون المستند، وهو نفس الأمر الذي أكدت عليه المادة 6 [25]من القانون رقم 53.05، كذلك الفصل 1-417[26] و2-417[27] و3-417 [28]من قانون الالتزامات والعقود.

وانطلاقا من الفصول أعلاه تتحدد وظائف التوقيع الالكتروني فيما يلي:

أولا: تهديد هوية الشخص الموقع

فمن المعلوم أن الوثيقة الالكترونية لا يمكن أن تتمتع بالقوة الإثباتية، إذا تعذر تحديد هوية شخصية لصاحبها، فالتعريف بالشخص الذي أبرم التصرف بطريقة الالكترونية هو من إحدى الوظائف الجوهرية للتوقيع الالكتروني[29].

فالتوقيع الالكتروني بصوره المختلفة له القدرة على تحديد هوية الشخص الموقع في حالة تدعيم هذه الصور بوسائل تحكم الثقة بها، للقيام بوظائفها على قدر يفوق ما تقوم به الصور التقليدية للتوقيع.

فالتوقيع الالكتروني العادي يقوم بهذا الدور، وذلك باتخاذه شكل حروف أو أرقام أو رموز أو أي إشارة تدل على شخصية الموقع وتمييزه عن غيره[30].

أما التوقيع الالكتروني المؤمن، وبالنظر إلى قدرته على الوثوق من شخصية صاحب التوقيع في كل مرة قد يستخدم فيها التوقيع أي صورة من صور التوقيع الالكتروني مؤمن، لاعتمادهم على تقنية التشفير[31] والمصادقة الالكترونية، فإنه له قدرة تامة على تحديد هوية الشخص الموقع.

---

[25] - تنص المادة 6 من القانون رقم 53.05 على أنه " يجب أن يستوفي التوقيع الإلكتروني المؤمن، المنصوص عليه في الفصل 3-417 من الظهير الشريف المعتبر بمثابة قانون الالتزامات والعقود، الشروط التالية:

- أن يكون خاصا بالموقع
- أن يتم إنشاؤه بوسائل يمكن للموقع الاحتفاظ بها تحت مراقبته الخاصة بصفة حصرية
- أن يضمن وجود ارتباط بالوثيقة المتصلة به بكيفية تؤدي إلى كشف أي تغيير لاحق أدخل عليها.

يجب أن يوضع التوقيع بواسطة آلية لإنشاء التوقيع الإلكتروني، تكون صلاحيتها مثبتة بشهادة للمطابق يتعين أن يشار إلى معطيات التحقق من التوقيع الإلكتروني المؤمن في الشهادة الإلكترونية المؤمنة المنصوص عليها في المادة 10 من هذا القانون

[26]- ينص الفصل 1-417 من قانون الالتزامات والعقود على أنه " تتمتع الوثيقة المحررة على دعامة إلكترونية بنفس قوة الإثبات التي تتمتع بها الوثيقة المحررة على الورق.تقبل الوثيقة المحررة بشكل إلكتروني للإثبات، شأنها في ذلك شأن الوثيقة المحررة على الورق، شريطة أن يكون بالإمكان التعرف، بصفة قانونية، على الشخص الذي صدرت عنه وأن تكون معدة ومحفوظة وفق شروط من شأنها ضمان تماميتها."

[27]- ينص الفصل 2-417 من قانون الالتزامات والعقود على أنه " يتيح التوقيع الضروري لإتمام وثيقة قانونية التعرف على الشخص الموقع ويعبر عن قبوله للالتزامات الناتجة عن الوثيقة المذكورة.تصبح الوثيقة رسمية إذا وضع التوقيع المذكور عليها أمام موظف عمومي له صلاحية التوثيق.
عندما يكون التوقيع إلكترونيا، يتعين استعمال وسيلة تعريف موثوق بها تضمن ارتباطه بالوثيقة المتصلة به."

[28]- ينص الفصل 3-417 من قانون الالتزامات والعقود على أنه " يفترض الوثوق في الوسيلة المستعملة في التوقيع الإلكتروني، عندما تتيح استخدام توقيع إلكتروني مؤمن إلى أن يثبت ما يخالف ذلك. يعتبر التوقيع الإلكتروني مؤمنا إذا تم إنشاؤه وكانت هوية الموقع مؤكدة وتمامية الوثيقة القانونية مضمونة، وفق النصوص التشريعية والتنظيمية المعمول بها في هذا المجال.
تتمتع كل وثيقة مذيلة بتوقيع إلكتروني مؤمن والمختومة زمنيا بنفس قوة الإثبات التي تتمتع بها الوثيقة المصادق على صحة توقيعها والمذيلة بتاريخ ثابت."

[29]- زينب غريب، مرجع سابق، الصفحة: 42-43.

[30]- مبارك الحسناوي، الإثبات في العقد الالكتروني، سلسلة الفقه القضاء التجاري، المنازعات التجارية بين المستجدات التشريعية والاجتهادات القضائية، منشورات مجلة العلوم القانونية، العدد الأول، الطبعة الأولى 2015 -الصفحة: 178.

[31]- تنص المادة 12 من القانون رقم 53.05 على أنه " تهدف وسائل التشفير على الخصوص إلى ضمان سلامة تبادل المعطيات القانونية بطريقة إلكترونية أو تخزينها أو هما معا، بكيفية تمكن من ضمان سريتها وصدقيتها ومراقبة تماميتها.
يراد بوسيلة التشفير كل عتاد أو برمجية أو هما معا، ينشأ أو يعدل من أجل تحويل معطيات سواء كانت عبارة عن معلومات أو إشارات أو رموز استنادا إلى اتفاقيات سرية أو من أجل إنجاز عملية عكسية لذلك بموجب اتفاقية سرية أو بدونها.
يراد بتقديم خدمة التشفير كل عملية تهدف إلى استخدام وسائل التشفير لحساب الغير."

ومن بين صور التوقيع الالكتروني المؤمن التي يمكنها تحقيق هذه الوظيفة نجد التوقيع الرقمي الذي له قدرة عالية على تحديد هوية الشخص الموقع لاعتماده على تقنية التشفير، إذ يتم تأكد من شخصية الموقع بشكل متكرر في كل مرة يتم فيها استخدام الرقم السري أو المفتاح الخاص[32].

والملاحظ التي يمكن تسجيلها من خلال المادة 8 من القانون رقم 53.05[33]، أن ألية الميكانزيم التي تتكلف بتحليل وترجمة الاوامر وتنفيذها في جهاز الحاسوب، هي التي توقع مكان الموقع بالاستعانة بالبرمجية، وهذا يمثل أصل المشكل في التوقيع الالكتروني ، حيث يمكن أن نتصور الصعوبات التي قد تصادفها المحكمة عندما ينفي موقع المفترض أي علم له بمحتوى وثيقة الالكترونية التي تحمل توقيعه، منكرا إعدادها أو إنشاءها، من غير رفض أو استبعاد تقرير الخبير الذي يؤكد أن التركيبة الحسابية للتشفير، تثبت أن المفتاح الخاص بالموقع هو الذي استعمل في التوقيع على الوثيقة، كما أن الغير لا يستطيع من جهته دحض ادعاء الشخص الذي نسب إليه هذا التوقيع[34].

خاصة وأن للقاضي الموضوع السلطة التقديرية في قبول ما يؤكد استخدام التوقيع وعدم منازعة الأطراف في صحته، أو برفض قبول هذا التوقيع لعدم اقتناعه به، حيث جاء في أحد قرارات محكمة النقض أن " التليكس يخضع كوسيلة من وسائل الإثبات في المادة التجارية لتقدير القاضي الموضوع ولو لم يكن موقعا..."[35]

وكحل لهذا الإشكال نرجع إلى المادة 9 من نفس القانون أعلاه التي نص على ضرورة التأكد من أن المعدات والاليات

" 1-أن تضمن، بوسائل تقنية وإجراءات ملائمة، أن معطيات إنشاء التوقيع الإلكتروني

أ) -لا يمكن إعدادها أكثر من مرة واحدة وتكون سريتها مضمونة

ب) -لا يمكن الوصول إليها عن طريق الاستنباط ويكون التوقيع الإلكتروني محميا من أي تزوير

ج) -أن يكون بالإمكان حمايتها من قبل الموقع بشكل كاف يحول دون أي استعمال من لدن الغير

2-أن تحول دون أي تغيير أو تبديل لمحتوى الوثيقة المراد توقيعها وألا تشكل عائقا يحول دون إلمام الموقع بالوثيقة قبل توقيعها إلماما تاما."

ثانيا: اثبات إرادة الموقع في التزامه بمضمون الورقة وإقراره لها

يعد التوقيع من وسائل التعبير عن الارادة التي بتطلبها القانون في الشخص لإنشاء تصرف قانوني سواء كان هذا التصرف عقدا أو إرادة منفردة والالتزام به.

وتتحقق وظيفة التعبير عن إرادة الموقع بمجرد قبوله للالتزام وتوقيعه بشكل الكتروني على البيانات التي تحتويها المحررات الالكترونية[36]، كمثال على ذلك قيام الشخص بإدخال الرقم السري أو مفتاح الترميز في التوقيع الرقمي بشكل إرادي على المحرر الالكتروني الخاص به، يعتبر موافقة على كامل مضمون العقد.

---

[32]- انتصار اليعكوبي، مرجع سابق، الصفحة: 34.

[33]- تنص المادة 8 من القانون رقم 53.05 على أنه "تتمثل آلية إنشاء التوقيع الإلكتروني في معدات أو برمجيات أو هما معا يكون الغرض منها توظيف معطيات إنشاء التوقيع الإلكتروني التي تتضمن العناصر المميزة الخاصة بالموقع، كمفتاح الشفرة الخاصة المستخدم من لدنه لإنشاء التوقيع الإلكتروني."

[34]- عزيز إطويان، حجية العقد الإلكتروني في الإثبات، مجلة الحقوق المغربية، العدد الحادي عشر، السنة السادسة، مطبعة الأمنية، دار الآفاق المغربية للنشر والتوزيع بالدار البيضاء، يونيو 2011، الصفحة: 108-109.

[35]- قرار عدد 531 بتاريخ 2009/04/08، ملف تجاري عدد 2006/1/3/614، مذكور عند عبد الرحيم بحار، القضاء التجاري والمنازعات التجارية، دراسة تأصيلية مقارنة، بدون مطبعة، الطبعة الأولى 2014، الصفحة: 117.

[36]- أحمد ادريوش، تأملات حول قانون التبادل الالكتروني للمعطيات القانونية، عناصر لمناقشة مدى تأثير القانون رقم 53.05 على قانون الالتزامات والعقود، مطبعة الأمنية الرباط، الطبعة الأولى 2009، الصفحة: 71.

وتبرز إرادة الموقع من خلال شروط التوقيع الالكتروني نفسه، لا سيم المؤمن منه والذي يؤكد مدى التلازم بين التوقيع وصاحبه، فإذا تحقق هذا الأمر فإن التوقيع يؤكد رضى الموقع بالمحرر الالكتروني الذي يحمل توقيعه[37].

ثالثا: إثبات سلامة العقد

بالإضافة إلى هذه الوظائف السابقة يحقق التوقيع الالكتروني وظائف أخرى يعجز التوقيع التقليدي عن القيام بها، ويتعلق الأمر بالتحقق من سلامة بيانات المحرر الالكتروني والتأكد من أن بياناته لم تحرف بعد أن تم توقيعه[38].

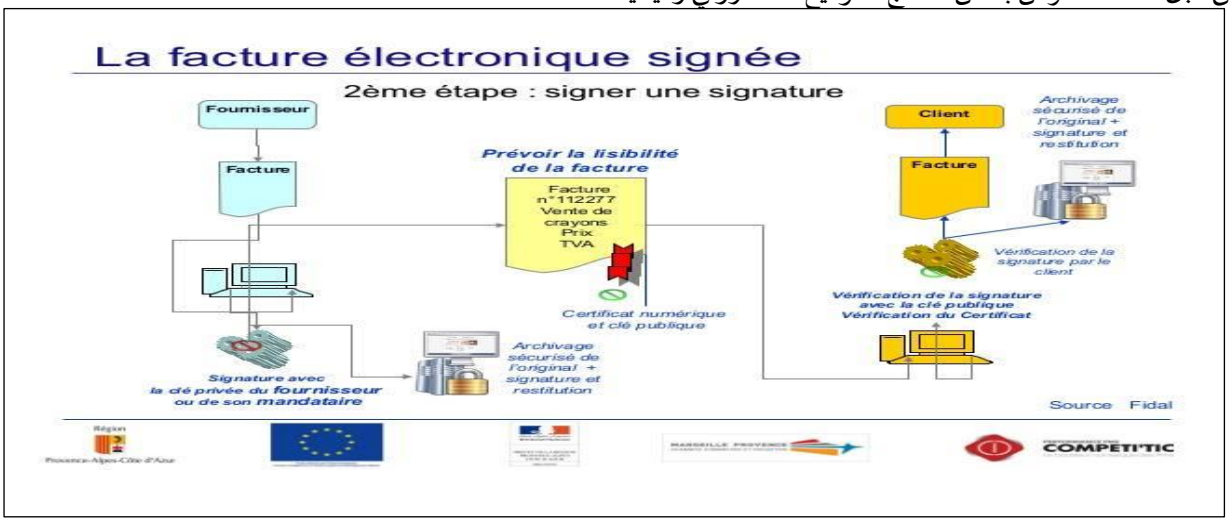
والملاحظة أن المشرع المغربي من خلال القانون رقم 53.05، وعلى عكس التشريعات الأخرى قد أعطى هذه الوظيفة للتوقيع الالكتروني المؤمن وليس للتوقيع الالكتروني العادي، وذلك لأن وظيفة الحفاظ على سلامة العقد لا تتحقق إلا باستخدام التوقيع الالكتروني المؤمن دون التوقيعات الأخرى لقيامه على تقنية التشفير.

ويجب على التوقيع الإلكتروني أن يحقق وظيفة الكشف عن أي تغيير لاحق ببيانات المحرر الالكتروني لكونه توقيعا متطور، فقد يتعرض للتغير أثناء عملية نقله إلى المرسل إليه، وهذا التغيير قد يكون سببه عطلا في الرسائل الفنية، أو سببه الغير أو المرسل إليه.

لتحقيق سلامة بيانات المحرر الالكتروني يتطلب هذا الأخير وظيفة إضافية عن وظائف التقليدية، يتمثل الأمر في كشف عن أي تغيير لاحق يمس ببيانات المحرر الالكتروني، أو ببيانات إنشائه عقب توقيعه، ويمكن كشف التغيير من خلال منظومة فحص التوقيع الالكتروني، فمن اللحظة التي يستقبل المرسل إليه المحرر الالكتروني يجب عليه أن يفحص بيانات إنشاء التوقيع الالكتروني وسلامة بيانات المحرر كذلك، ويتم هذا التحقق بالاعتماد على أليات أهمها تقنية التشفير وكذا هيئات المصادقة الالكترونية[39].

وكخلاصة يمكن الخروج بها هو أن التوقيع الالكتروني يؤدي نفس الوظائف التي يتطلبها القانون في التوقيع التقليدي، بل وأكثر من ذلك فالتوقيع الالكتروني يفوق التوقيع التقليدي، ويفضل عنه من خلال الأمن والسلامة التي يعطيها للعقد، باعتماده على تقنية التشفير والمصادقة، كل هذا يدفعنا إلى التساؤل حول حجية التوقيع الالكتروني في إثبات العقود الإلكترونية؟

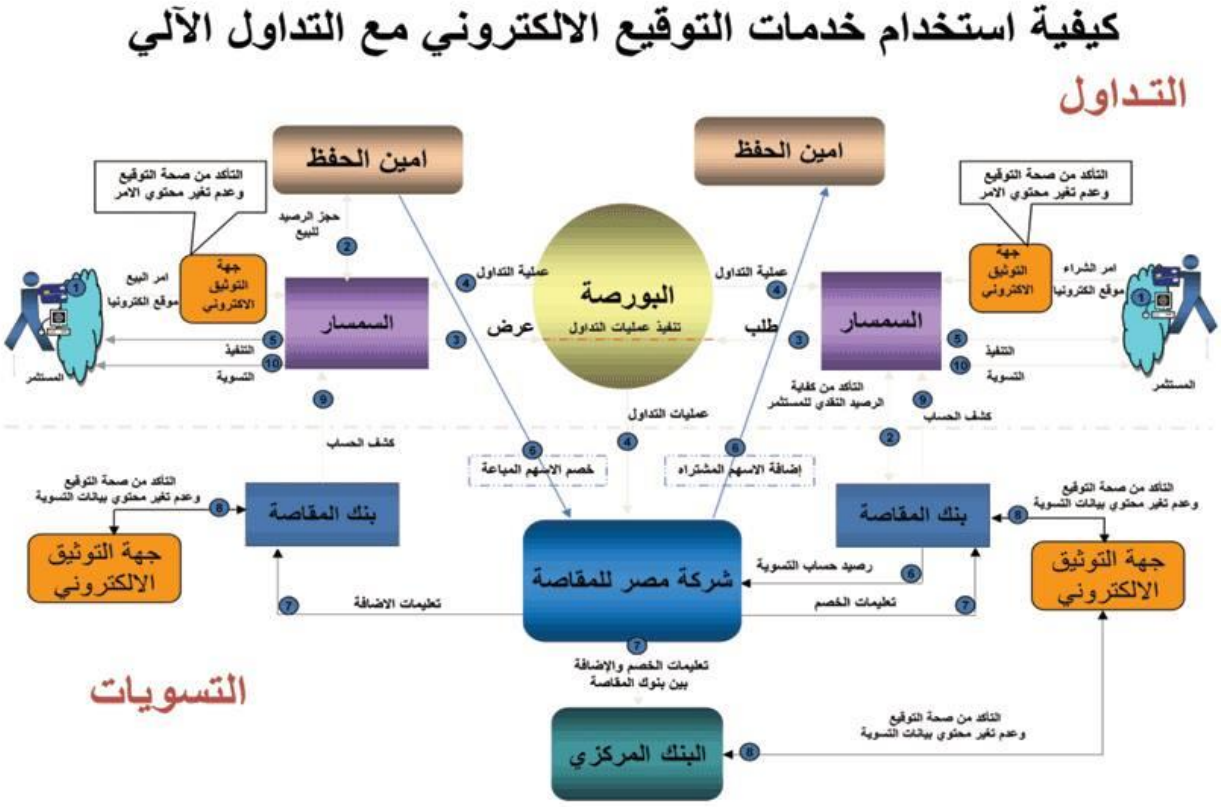
ولكن قبل ذلك سنعرض بعض نماذج التوقيع الالكتروني وكيفية استعماله



[37]- زروق يوسف، مرجع سابق، الصفحة:243.

[38]- عزيز إطويان، مرجع سابق، الصفحة: 110 – 111 -112.

[39]- زينب غريب، مرجع سابق، الصفحة:130.



♦ المطلب الثاني: حجية التوقيع الالكتروني في إثبات العقود الالكترونية

تعد الغاية الأساسية من التوقيع الالكتروني، إضفاء القوة الثبوتية للتصرف القانوني (المحرر الالكتروني) ، وهذه الغاية لا يمكن التوصل إليها إلا إذا حددنا العناصر المتدخلة في التوقيع الالكتروني والتي تظفي عليه القوة الثبوتية (الفقرة الثانية)، ولكن قبل ذلك لابد لنا أن نسلط الضوء على المحرر الالكتروني ومدى حجيته من خلال المعادلة بينه وبين المحرر الورقي (الفقرة الأولى).

الفقرة الأولى: المعادلة بين الدليل الورقي والدليل الالكتروني

يعتبر الدليل الكتابي من أهم أدلة الإثبات على الإطلاق في القانون المغربي، إذ يمتاز على غيره من الأدلة بإمكانية إعداده منذ نشوء الحق وقبل قيام النزاع، كما أن الدليل الكتابي يوفر لأطراف العقد عدة ضمانات أهمها أنه يضبط الحقوق القائمة بينهم سواء قبل النزاع أو بعده، إضافة إلى أن الكتابة أقل تعرضا لتأثير عوامل الزمن، ولعل هذا هو أساس تغليب جل التشريعات الوضعية الإثبات عن طريق الكتابة[40].

[40]- نور الدين الناصري، المعاملات والإثبات في مجال الاتصالات الحديثة، سلسلة الدراسات القانونية المعاصرة، العدد 12، مطبعة النجاح، الدار البيضاء، الطبعة الأولى، 2007، الصفحة 9

لكن التطور حمل إلى الكتابة مستندا جديدا، تجاوز الورق إلى الرقاقات والدعامات الالكترونية، التي صار بإمكانها الآن أن تشكل حملا لمختلف أشكال الكتابات على غرار الأوراق، بل هي أشد من الأوراق سعة وأدق استعمالا.

لذلك عمل المشرع المغربي من خلال قانون التبادل الالكتروني للمعطيات القانونية على التوسيع من وعاء الدليل الكتابي المنصوص عليه في الفصل 417 من قانون الالتزامات والعقود المغربي، حيث أدخل تعديلا على هذا الأخير وصارت الكتابة بمقتضاه شاملة-فضلا عن الثابت قانونا[41]-من خلال إضافة أية إشارات أو رموز أخرى ذات دلالة واضحة، كيفما كانت دعامتها وطريقة إرسالها.

فرغم إغفاله في إعطاء تعريف أو تحديد مفهوم للدليل الالكتروني أو المحرر الالكتروني، فإنه اكتفى بمنح شروط إصدار هذه المحررات وإجراءاتها الشكلية، وهو نفس النهج الذي سار عليه القانون المدني الفرنسي، بخلاف القانون التونسي وبعض التشريعات العربية، حيث عرفت المادة 2 من قانون الأونسترال النموذجي بشأن التوقيعات الإلكترونية لسنة 2001 المحرر الإلكتروني بأنه:" معلومات يتم إنشاؤها أو إرسالها أو استلامها أو تخزينها بوسائل الكترونية أو ضوئية أو بوسائل مشابهة، بما في ذلك على سبيل المثال لا الحصر، التبادل الالكتروني للبيانات أو البريد الإلكتروني أو البرق أو التلكس أو النسخ البرقي"[42].

ولكي يرقى الدليل الالكتروني أو المحرر الالكتروني للدليل الكتابي الورقي، قيده المشرع المغربي حسب الفصل 1-417من قانون الالتزامات والعقود -نفس صيغة الفصلين1-1316و3-1316من القانون المدني الفرنسي[43]-بشروط تتمثل في إمكانية التعرف القانوني على صاحبه، وأن يكون معدا ومحفوظا وفق شروط تضمن تماميته[44]، مما يمكن الأطراف الرجوع إليه في حالة نشوب خلاف فيما بينهم، وذلك من أجل تحصينه من أي تغيير يطرأ على محتواه، خاصة وأنه مكتوب على دعامة هشة عكس الدعامة الورقية التي من خصائصها الثبات والدوام عندما يتم حفظها بالعناية المطلوبة، وبالتالي فإن تخوف المتعاملين من اللجوء إلى التقنيات الحديثة للاتصال له ما يبرره، كما أن احتمال تزوير أو تحريف بيانات الوثائق المتبادلة الكترونيا، يطرح إشكالية مدى قدرة هذه التقنيات المستعملة لإرسالها وتلقيها، على اتقان أي تغيير يطالها؟

فجوهر المشكل إذن هو تقني بالدرجة الأولى يرتبط بنوع التكنولوجيا المستخدمة لصياغة الدليل الالكتروني وصيانته، ويعتمد على موثوقية النظام المعلوماتي المستعمل، لذلك ركز القانون رقم 05-53 على السلامة والأمان التقني، اللذان

41- مصطفى مالك، إبرام العقد بشكل إلكتروني، مجلة المحاكم المغربية العدد المزدوج 137-138 شتنبر-دجنبر 2012 الصفحة 118

42- وجاء في نص المادة 1/ب من قانون تنظيم التوقيع الالكتروني المصري أن المحرر الالكتروني:
"هو رسالة بيانات تتضمن معلومات تنشأ أو تدمج أو تخزن، أو ترسل أو تستقبل كليا أو جزئيا بوسيلة إلكترونية أو ضوئية أو بأية وسيلة أخرى مشابهة".
كما عرف المشرع الإماراتي في المادة 2 من قانون المعاملات والتجارة الالكترونية المحرر الالكتروني على أنه:
"سجل أو مستند يتم إنشاؤه أو تخزينه أو استخراجه أو إرساله أو إبلاغه أو استلامه بوسيلة إلكترونية على وسيط ملموس أو على أي وسيط الكتروني آخر يكون قابلا للاسترجاع بشكل يمكن فهمه".

43- يقابل الفقرة الأولى من الفصل 1-417 من قانون الالتزامات والعقود، الفصل 3-1316 من القانون المدني الفرنسي:
- Art 1316-3 du code civil français :
« L'écrit sur support électronique à la même force probante que l'écrit sur support papier ».
كما يقابل الفقرة الثانية من الفصل 1-417 من قانون الالتزامات والعقود، الفصل 1-1316 من القانون المدني الفرنسي:
- Art 1316-1 du code civil français :
« L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité ».

44- التمامية هي كل خاصية تضمن عدم تغيير المعطيات أو إتلافها، بشكل غير مسموح به، أثناء إنشائها أو حفظها أو نقلها.

ينبغي توفرهما في النظام المعلوماتي، سواء في مجال حفظ المعطيات القانونية أو عند تبادلها الكترونيا، هذا إلى جانب المعدات الالكترونية التي يجب أن تتوفر فيها مواصفات معينة للوثوق بها، وباختصار، إن فعالية الترسانة القانونية متوقفة على مدى توفر التقنيات الحديثة للإتصال على الأمان التقني[45].

إلا أن السؤال الذي يبقى مطروحا في هذا الأمر ماذا لو وقع تضارب أو نزاع بين المحرر الكتابي والمحرر الالكتروني؟ أو في حالة نزاع بين وثيقتين إلكترونيتين؟

إن المشرع المغربي بمجرد أن اعترف بالمساواة بين الوثيقتين، حسم التعايش بينهما لكن قد تطرأ صعوبات تتعلق باستخدامهما كوسيلة إثبات أمام القاضي في حالة تضارب بين الوثيقة الورقية والالكترونية، أو في حالة تضارب بين الوثيقتين الالكترونيتين معا، في هذا السياق نصت المادة 417 من قانون الالتزامات والعقود على أنه يجب التمسك بالمستند الأكثر مصداقية، فلا فرق في هذا المجال بين المحرر الورقي والمحرر الالكتروني، وإنما المعيار الوحيد هي عناصر المصداقية التي يبحث عنها القاضي بكل الوسائل، كما يمكن للأطراف أن يفصلوا مقدما هذه المسألة عن طريق الاتفاق من أجل تفضيل أحد المحررات عن الآخر، مثلا تفضيل التوقيع الالكتروني عن التوقيع اليدوي أو العكس[46].

الفقرة الثانية: القوة الثبوتية للتوقيع الإلكتروني في اثبات العقود الإلكترونية

بصدور القوانين الخاصة بالتجارة الالكترونية، تكفل المشرع المغربي بإعطاء التوقيع الالكتروني حجية إثبات، وذلك استجابة لمتطلبات التجارة، والحفاظ على استقرار المعاملات[47]، الأمر الذي يجعلنا نطرح تساؤلات هامة من قبيل مدى استيفاء التوقيع الالكتروني لشروط التوقيع العادي، حتى يمكن اعتباره حجة في الإثبات؟ ذلك أن التعاقد عن طريق الانترنت يواجه مشكلة قبول التوقيع الالكتروني في الاثبات، وبالتالي حجية المحرر الذي تم التوقيع عليه الكترونيا. فهل التوقيع الالكتروني قادر على تحديد شخصية الموقع أم لا؟ وما الذي يضمن للمستخدم أن ما وصله من معلومات جاءه من موقع موثوق به؟ أو أن هذا الموقع حقيقي وموجود على الشبكة؟ وبناء على هذه التساؤلات نستخلص اشكاليتين هامتين:

هل حجية التوقيع الالكتروني في الاثبات مطلقة أم مقيدة بشروط؟ وإذا كانت مقيدة فما مدى فعاليته عند توفر هذه الشروط؟

لو عدنا إلى ما نصت عليه المادة 3-417 من ظهير الالتزامات والعقود بموجب المادة4 من قانون رقم 05-53 "تتمتع كل وثيقة مذيلة بتوقيع الكتروني مؤمن، والمختومة زمنيا بنفس قوة الإثبات التي تتمتع بها الوثيقة المصادق على صحة توقيعها والمذيلة بتاريخ ثابت"، سنجد أن المشرع المغربي اعترف بالتوقيع الالكتروني المؤمن وهو التوقيع الذي يستوفي شروط سلامة التعاقد ليرتب آثاره القانونية المتوخاة، ذلك أن التوقيع المذكور يعتمد عليه في التعامل بخصوص التصرفات الالكترونية، وهو عبارة عن رقم أو كتابة ولا علاقة له بالبصمة أو الختم المعتمد في التعاقد التقليدي، ويرتبط ارتباطا عضويا

---

[45]- عزيز أطوبان، مرجع سابق، الصفحة 104

[46]- انتصار اليعقوبي، مرجع سابق، الصفحة 70

[47]- نور الدين الرحالي، التطبيقات العملية الحديثة في قضايا الاستهلاك، مطبعة النجاح الجديدة بالدار البيضاء، الطبعة الأولى 2014، الصفحة 71

بالتشفير[48]، ونفس شيء أقرت به محكمة النقض المغربية في غرفتها التجارية في ملف عدد 2012/1/3/894 والتي جاء فيها < لئن كان التوقيع هو المجسد لإرادة الملتزم ويتم في الحالات العادية بوضع علامة بخط يد الملتزم نفسه طبقا لأحكام الفصل 426 من قانون الالتزامات والعقود، فإن التوقيع الالكتروني لا يكون بنفس طريقة التوقيع التقليدي، بل إنه وبمقتضى الفصل 417 من نفس القانون يكون بكل ما يتيح التعرف على الشخص الموقع ويعبر عن قبوله للالتزامات الناتجة عن الوثيقة الالكترونية، ومن ثم لا يشترط توقيع هذه الوثيقة بيد الملتزم، ولا وضع خاتمة عليها.

مادامت المحكمة استندت فيما انتهت إليه إلى إقرار الطالبة الوارد بالرسالة الصادرة عنها المحددة لمبالغ العمولة المستحقة للمطلوبة، فإنها لم تكن في حاجة للبحث في تكييف العقد الرابط بين الطرفين>[49].

وتتلخص هذه الشروط في المادة 6 من القانون 53.05، وهي كالتالي:

- أن يكون خاصا بالموقع[50].

لكي يقوم التوقيع بوظيفته لابد أن يكون التوقيع علامة مميزة لشخصية الموقع عن غيره وتضمن تحديد هويته، ليؤكد سلطته في إبرام التصرف القانوني ورضاه بمضمونه، فحتى يتسنى للتوقيع القيام بأداء وظيفته يجب أن يكون دالا على شخصية الموقع، ونجد أن التوقيع الالكتروني بصوره المختلفة إذا تم إنشاؤه بصورة صحيحة، فإنه يعد من قبل العلامات المميزة والخاصة بالشخص وحده دون غيره، والذي يعني أن قيام أكثر من شخص باستعمال بعض أدوات إنشاء التوقيعات تملكها مؤسسة مثلا، فإن تلك الأداة يجب أن تكون قادرة على تحديد هوية مستعمل واحد تحديدا لا لبس فيه في سياق كل توقيع الكتروني على حده[51].

- أن ينشأ بوسائل يمكن للموقع الاحتفاظ بها تحت مراقبته الخاصة بصفة حصرية.

لقد حرص المشرع المغربي على تحديد وظيفة آلية انشاء التوقيع الالكتروني واعتبرها تتمثل في المعدات أو البرمجيات أو هما معا، ويكون الغرض منها توظيف معطيات إنشاء التوقيع الالكتروني التي تحتضن العناصر المميزة الخاصة بالموقع وذلك كمفتاح الشفرة الخاصة المستخدمة من طرف الموقع لإنشاء التوقيع الإلكتروني[52].

- أن يضمن وجود ارتباط بالوثيقة المتصلة به، بكيفية تؤدي إلى كشف كل تغيير ألحق عليها.

و في هذا الاطار جاء حكم قضائي فرنسي يؤكد ضرورة سيطرة الموقع على وسيلة التوقيع، حيث يعد أول حكم صدر في فرنسا بعد صدور قانون مارس2000، الخاص بالتوقيع الالكتروني، إذ أصدرت محكمة استئناف Besançon في 20 أكتوبر 2000 هذا الحكم أكد على ضرورة أن تكون وسائل التوقيع الالكتروني تحت سيطرة الموقع, وحده دون غيره ,وإلا لا يعتبر هذا التوقيع حجة على الموقع ولا على الغير.

---

[48]- المختار بن أحمد عطار، العقد الالكتروني، مطبعة النجاح الجديدة، الطبعة الاولى 2010، الصفحة 59

[49]- قرار عدد 250 الصادر بتاريخ 2013/06/06 في الملف رقم 2012/1/3/894 من الغرفة التجارية بمحكمة النقض منشور في الموقع الالكتروني تم الاطلاع عليه يوم 2016/11/24 على الساعة 23:00

https://www.mahkamaty.com

[50]- للتذكير فقد عرف المشرع المغربي الموقع في المادة 7 من القانون المذكور بأنه:

" هو الشخص الطبيعي الذي يعمل لحسابه الخاص أو لحساب الشخص الطبيعي أو المعنوي الذي يمثله والذي يستخدم آلية إنشاء التوقيع الالكتروني".

[51]- زينب غريب، مرجع سابق، الصفحة 45-46-47

[52]- المختار بن أحمد العطار، مرجع سابق، الصفحة 61

وتتلخص وقائع هذه القضية-وهي ما تعرف بقضية Sarl Chaalets Boisson C /Bernard G. أن محامي أحد الأشخاص (الموقع) احتج بالتوقيع الالكتروني لموكله أمام المحكمة، وقدم في صحيفة بيانات هذا التوقيع السرية، التي من المفترض أن الموقع هو الذي يعلمها وحده دون غيره، كما أن هذه البيانات كان يعرفها أيضا أشخاص آخرون يعملون في مكتب المحامي وقد رفضت المحكمة الحكم بصحة هذا التوقيع ,لأن دوره في اثبات شخصية الموقع أصبح مشكوكا فيه ,ولأن بيانات التوقيع خرجت من تحت يد الموقع إلى شخص آخر وهو محاميه ومعاونوه في مكتبه.

ومقتضى هذا الحكم أن التوقيع الالكتروني يكون له قيمة قانونية إذا كانت الوسائل التي يتم بها تقع تحت السيطرة المباشرة للموقع وحده دون غيره, كما يجب أن تكون هناك صلة بين التصرف المتضمن لهذا التوقيع, وأن يكون هذا التصرف صحيحا، وإن لم تتوفر هذه الشروط فلا ينتج التوقيع الالكتروني أثرا قانونيا, ولا يكون له أي حجية في الإثبات, لأنه لا يعبر عن هوية الموقع[53].

- أن يوضع بواسطة آلية للتوقيع الإلكتروني، تكون صلاحيتها مثبتة بشهادة للمطابقة[54].

ويجري سياق المادة 8 من القانون رقم 05-53 على أن آلية إنشاء التوقيع الالكتروني تتمثل في المعدات أو البرمجيات أو هما معا، ويكون الغرض منها توظيف معطيات إنشاء التوقيع الالكتروني التي تحتضن العناصر المميزة الخاصة بالموقع وذلك كمفتاح الشفرة الخاصة المستخدمة من طرف الموقع لإنشاء التوقيع الإلكتروني بالإضافة إلى شهادة المطابقة عندما تستجيب آلية إنشاء التوقيع الإلكتروني للمتطلبات التالية حسب المادة 9 من قانون رقم 05-53:

1- أن تضمن، بوسائل تقنية وإجراءات ملائمة، أن معطيات إنشاء التوقيع الإلكتروني:

أ) لا يمكن إعدادها أآثر من مرة واحدة وتكون سريتها مضمونة

ب) لا يمكن الوصول إليها عن طريق الاستنباط ويكون التوقيع الإلكتروني محميا من أي تزوير

ج) أن يكون بالإمكان حمايتها من قبل الموقع بشكل آاف يحول دون أي استعمال من لدن الغير

2-أن تحول دون أي تغيير أو تبديل لمحتوى الوثيقة المراد توقيعها وألا تشكل عائقا يحول دون إلمام الموقع بالوثيقة قبل توقيعها إلماما تاما.

- أن يشار في الشهادة الالكترونية المؤمنة إلى معطيات التحقق من التوقيع الالكتروني المؤمن.

ذلك أن التوقيع الالكتروني هو الذي يمنح الحياة للتصرف القانوني، وهناك علاقة قانونية قائمة ومرتبطة بينهما. وهذا من شأنه ان يساعد المرسل إليه الإيجاب من التعرف على شخصية الموجب ونوع التصرف القانوني ونطاقه بكيفية مستمرة

---

[53] -C.Cass, 2e civ.30 Avr.2003, SARL Boisson C/G : Juris-Data No.2003-018798
- محمد أشفيع، حجية التوقيع الالكتروني في الإثبات، من الموقع الالكتروني لكلية العلوم القانونية والاقتصادية والاجتماعية لأكادير تم الإطلاع عليه يوم 2016/11/21 على الساعة 23:10
http://www.fsjes-agadir.info/

[54]- يجري في سياق المادة 8 من القانون 05.53، على أن آليات إنشاء التوقيع الالكتروني، تتمثل في معدات أو برمجيات أو هما معا وغرضها هو توظيف معطيات إنشاء التوقيع الالكتروني التي تحتوي العناصر الفريدة الخاصة بالموقع كمفتاح الشفرة الخاصة المستخدم من الموقع بغرض إنشاء التوقيع الالكتروني. في هذا الصدد سوف نتحدث عن كيفية إنشاء التوقيع الالكتروني ومراحله، في إطار التصديق على التوقيع الالكتروني لاحقا.

تمتد إلى ما بعد ترتيب الآثار القانونية للتصرف القانوني الالكتروني، وجعله آمنا، فضلا عن حماية كلا من المتعاقدين، بحيث أن كل تغيير يلحق بالوثيقة الالكترونية يستطيع أي من المتعاقدين الوصول إليه[55].

نستنتج مما تقدم أن المشرع المغربي إتجه إلى المساواة بين التوقيع التقليدي والتوقيع الالكتروني ومنحه نفس درجة حجية الاثبات، غير أن هذه الحجية ليست مطلقة ولا تمنح لأي توقيع الكتروني أيا كانت مصداقيته ودرجة توثيقه، وإنما علقت الحجية الكاملة على توافر متطلبات وشروط معينة في هذا التوقيع تجعله توقيعا موثوقا به، وذلك لإضفاء قدرا من الأمن والثقة على المعاملة الالكترونية، ولا بد أن يتطابق التوقيع الالكتروني مع رمز التعريف الموجود في الشهادة الالكترونية التي تعتبر بمثابة الهوية الالكترونية للشخص، ولا تتم المعاملة إلا بعد التأكد من شخصية صاحب الشهادة، وبالتالي يكون من الصعب على من نسب إليه توقيع الكتروني أن ينكر صدوره عنه، ولكن المشكلة تثور فيما لو أقر الشخص بأن هذا التوقيع الالكتروني هو توقيعه، وأدعى في نفس الوقت أنه لم يقم بإجراء هذه المعاملة الموقعة بتوقيعه الالكتروني، كأن يدعي بأن رمز التعريف الخاص به قد سرق أو ضاع منه وتم استخدام الشهادة الالكترونية من قبل شخص آخر، فما هو الحل؟

بالرجوع إلى المادة(10/ب) من قانون المعاملات الالكترونية الأردني نلاحظ أنها نصت على أنه < يتم إثبات صحة التوقيع الإلكتروني ونسبته إلى صاحبه إذا توفرت طريقة لتحديد هويته والدلالة على موافقته على المعلومات الواردة في السجل الإلكتروني الذي يحمل توقيعه إذا كانت تلك الطريقة مما يعول عليها لهذه الغاية في ضوء الظروف المتعلقة بالمعاملة، بما في ذلك اتفاق الأطراف على استخدام تلك الطريقة>.

وأيضا قرار محكمة النقض الفرنسية في قضية Alptis التي تقر بأنها تعاقدت الكترونيا مع السيد X ، والذي قام هذا الأخير بنفي تعاقده ونفي أن التوقيع الالكتروني الذي تم هو توقيعه، رفضت محكمة النقض في قرارها الصادر في 6 أبريل 2016 في الاستئناف، قائلا: "ولكن في حين أن الحكم يذهب الى ان الطلب العضوية إلكترونيا تم إنشاءه والاحتفاظ به في ظروف تضمن سلامته، وأنه تم التعرف على التوقيع في عملية موثوقة ضانة للتوقيع الالكتروني و الفعل الذي تمسك به، وأن طلب العضوية في جلسة الاستماع تبين صدور هذه الوثيقة من قبل عقود منصة Contraleo على الانترنت، مما يتيح تحديد دقيق والتوثيق من الموقعين في 25 أيار 2011؛ وبالتالي زعم حدفها، فإن المحكمة محلية قد بررت قرارها [56]".

---

[55]-عبد الكريم عبدلاوي، التوقيع الالكتروني، من الموقع الالكتروني لمجلة منازعات الأعمال، تم الاطلاع عليه يوم 2016/11/17 على الساعة 21:30

http://frssiwa.blogspot.com/

[56] -La Cour de cassation, dans sa décision du 6 avril 2016, rejette le pourvoi en ces termes : "Mais attendu que le jugement retient que la demande d'adhésion sous forme électronique a été établie et conservée dans des conditions de nature à garantir son intégrité, que la signature a été identifiée par un procédé fiable garantissant le lien de la signature électronique avec l'acte auquel elle s'attache, et que la demande d'adhésion produite à l'audience porte mention de la délivrance de ce document par la plate-forme de contractualisation en ligne Contraleo, permettant une identification et une authentification précise des signataires en date du 25 mai 2011 ; qu'ayant ainsi effectué la recherche prétendument omise, la juridiction de proximité a légalement justifié sa décision

- Cour de cassation, civile, Chambre civile 1, 6 avril 2016, 15-10.732, Inédit
- https://www.legifrance.gouv.fr/ vu 24/11/2016 à 22:00

ومنه نستنتج أن التحقق من صحة التوقيع الالكتروني ونسبته إلى صاحبه يتم من خلال طريقة تحديد هوية الموقع على السجل الالكتروني والمعاملة الالكترونية في تلكك اللحظة، لمعرفة ما إذا كان هو صاحب التوقيع الأصلي، أم أنه شخص آخر يستخدم ذلك التوقيع دون علم صاحبه، وهذا الامر يتطلب إجراءات دقيقة وخبرة عالية في مجال المعاملات الالكترونية وهذه هي الطريقة التي لابد أن تكون مما يعول عليه لهذه الغاية حيث يشترط أن تكون دقيقة وحاسمة يمكن التعويل عليها في هذا المجال، لما لهذا الموضوع من حساسية كبيرة في مجال المعاملات الالكترونية[57].

[57]-محمد أطويف، مرجع سابق، الصفحة 88

المبحث الثاني: الآليات الحمائية للتوقيع الالكتروني في العقود الإلكترونية

إن التوقيع الإلكتروني ليس آداة للمصادقة فقط، بل وسيلة لتحقيق الأمان في التبادل التجاري الإلكتروني، وبث الثقة في نفوس المتعاملين فيه، لذلك فلا يمكن تحقيق حماية كافية عبر الحماية القانونية فحسب **(المطلب الثاني)**، بل كان لزاما تطويقه بآليات تقنية تنتصر لحماية المعطيات الشخصية **(المطلب الأول)**.

♦ المطلب الأول: الحماية التقنية للتوقيع الإلكتروني

تتمثل الحماية التقنية عبر آلية التشفير **(الفقرة الأولى)**، والشهادة الرقمية **(الفقرة الثانية)**.

الفقرة الأولى: تقنية التشفير

يعد التشفير من أنجع الوسائل الحمائية للتوقيع الإلكتروني، حيث لا يمكن أن ينشأ هذا الأخير وأن يتم التحقق منه إلا باستخدام التشفير. والتشفير فرع من علم الرياضيات التطبيقية، الذي يعني: "تحويل نص الرسائل إلى صيغ غير مفهومة، ثم بعد ذلك إعادتها إلى تصنيفها الأصلي". [58]

كما عرفه المشرع المغربي، بأنه كل عتاد أو برمجية أو هما معا، ينشأ أو يعدل من أجل تحويل معطيات سواء كانت عبارة عن معلومات أو إشارات أو رموز، استنادا إلى اتفاقيات سرية أو من اجل إنجاز عملية عكسية لذلك بموجب اتفاقية سرية أو بدونها.[59]

وعمليا، فالتشفير يتم باللجوء إلى وظيفة التجزئة، والتي تعني تجزئة النص وتحويله إلى بصمة (fingerprint)، بحيث كل تغيير في النص ينتج عنه تغيير في البصمة. هذا وتتم عملية التوقيع بتشفير تلك البصمة بواسطة مفتاح خاص من طرف الموقع، حيث يعمل هذا الأخير على إعادة رسالة البيانات إلى مصدرها مرفوقة بتوقيعه في ملف، بحيث لا يمكن لمصدرها إجراء أي تعديل لأنه لا يملك المفتاح الخاص، بيد أنه يمكن في المقابل فك شفرة رسالة البيانات من طرف أي شخص مهتم بقراءتها بواسطة مفتاح عام، لكن دون التمكن من إدخال أي تعديل عليها.[60] وتسمى هذه الطريقة بالتشفير اللامتماثل، وهو الأكثر شيوعا. وتقابلها طريقة أخرى تسمى بالتشفير المتماثل أو "شفرة قيصر"، وهو أقدم أنواع التشفير، حيث يستخدم فيه كل من المرسل والمستقبل مفتاحا واحدا، يتم إعداده بين طرفي العلاقة ليتم التشفير من خلاله وتحويل الرسالة إلى رموز وإشارات غير مفهومة، ومن ثم يتم فك التشفير بواسطة المفتاح نفسه المعد للتشفير.[61]

وعموما يمكن تبسيط عملية التشفير بالأشكال التالية:

1- التشفير اللامتماثل: Principe du chiffrage par bi- clef

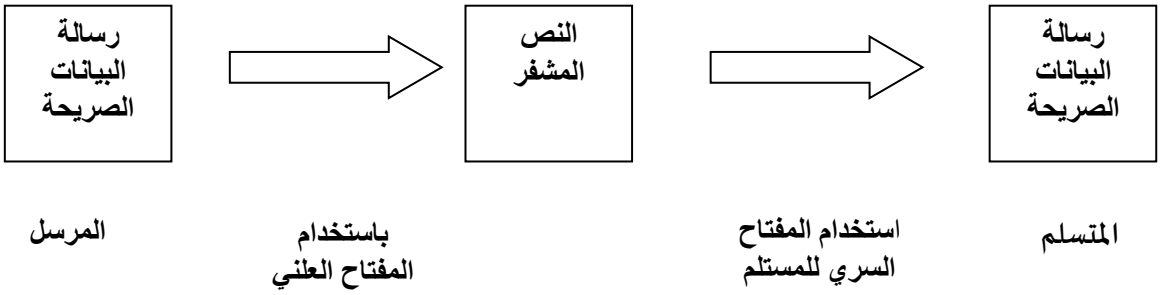
---

[58] -محمد اطويف، مرجع سابق صفحة 77.

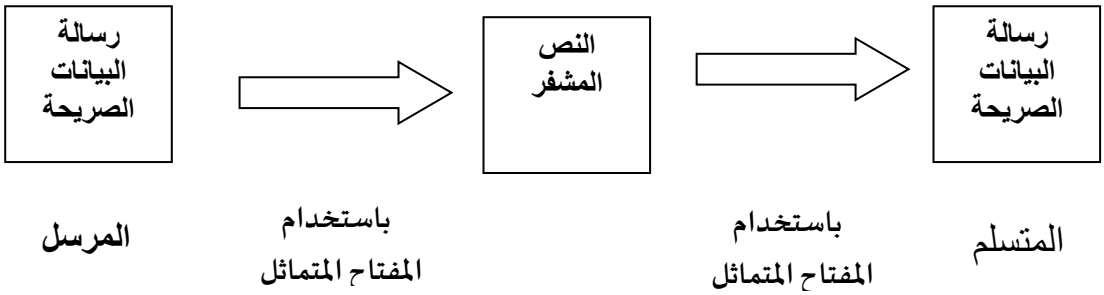
[59] -المادة 12 من قانون 53.05 المتعلق بالتبادل الإلكتروني للمعطيات القانونية.

[60] Charles CHEBLI, « signature et chiffrement », rapport de DEA (diplôme d'études approfondies), Université Saint-Joseph, Faculté d'ingénierie, BEYROUT- LIBAN, année universitaire 2002-2003 page 18.

[61]- محمد فواز- محمد المطالقة، "الوجيز في عقود التجارة الإلكترونية"، دار الثقافة، الطبعة الأولى 2008 صفحة 162، ورد عند زينب غريب، مرجع سابق الصفحة 77.



2- **شفرة قيصر : chiffrement de césar**



وتبقى تقنية التشفير أساس الحماية التقنية للتوقيع الإلكتروني، لكن هذه الحماية تبقى قاصرة دون التأكد من هوية الموقع ومطابقة توقيعه لمعطيات الشخصية عبر ما يسمى بالشهادات الرقمية او الإلكترونية.

الفقرة الثانية: الشهادات الرقمية

لا يمكن تطبيق التوقيع الإلكتروني نهائيا إلا في حالة وجود الشهادات الرقمية،[62] التي تصدر عن جهات التوثيق المرخص لها من قبل الجهات المسؤولة في كل دولة، لتشهد بأن التوقيع الإلكتروني صحيح، ويذهب بذلك لمن أصدره ويستوفي الشروط، وتمثل هذه الشهادات طرفا ثالثا بين المرسل والمستقبل ومن أمثلة هذه الجهات، شركة magenta corporation في الولايات المتحدة الأمريكية،[63] أما في فرنسا، فتخضع هذه الجهات لرقابة الوكالة الوطنية لحماية الأنظمة المعلوماتية، حيث تقوم هذه الجهات بالتأكد من هوية الشخص الذي ستسلم له هذه الشهادة ولتتمكن كذلك من تسجيل المفتاح العام. وتحديد هوية طالب الشهادة لا تعني بالضرورة اِسمه الحقيقي بل يمكن أن يكون اِسم المستخدم، ولا يؤثر ذلك على إثبات التوقيع أمام المحاكم. حيث وفي جميع الأحوال تطلب هذه الجهات الوثائق الرسمية المحددة لهوية الشخص،[64] وفي

---

[62] -عرف المشرع الفرنسي الشهادة الإلكترونية بأنها: "وثيقة إلكترونية تشهد بالتحقق من العلاقة التي تربط معطيات التوقيع الإلكتروني بالموقع".
- مرسوم رقم 272-2001 لـ 30 مارس 2001 المتعلق بتطبيق الفصل 4-1316 من القانون المدني الفرنسي والمتعلق بالتوقيع الإلكتروني والمنشور بموقع www.legiframe.gov.fr تاريخ الاطلاع 26 نونبر 2016 الساعة 04:00.

[63] -طلال حسن-الأرقم قاسم-محمد عبد المنعم- أحمد علي، "التوقيع الإلكتروني"، تقرير في مقرر أمن المعلومات والشبكات، جامعة أم درمان الإسلامية، كلية العلوم والثقافة، أم درمان، السودان الصفحة 11.

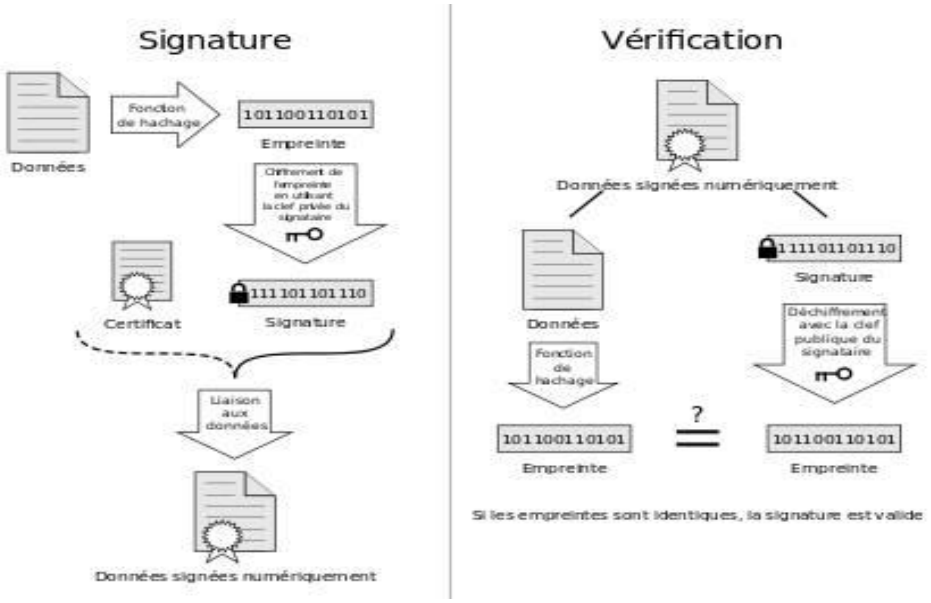
[64] Virgine ETIENNE .ancien référence. page 42

نفس السياق أكد المشرع المغربي على ضرورة استعمال وسيلة تعريف موثوق بها تضمن ارتباطه بالوثيقة المتصلة بالتوقيع الإلكتروني.[65]

أما في المغرب فقد كان يعمد بإصدار شهادة التوقيع الإلكتروني إلى الوكالة الوطنية لتقنين المواصلات (ANRT)، إلى غاية فبراير 2015،[66] حيث أصبحت العمليات المتعلقة بالتوقيع الإلكتروني والتشفير وتبادل المعطيات القانونية على شبكة الإنترنت في المغرب تحت سلطة إدارة الدفاع الوطني وبالضبط المديرية العامة لأمن نظم المعلومات، يتبعها بنك المغرب، ثم هيئات أخرى كـ Maroc télécommerce.[67]

وتأتي إناطة هذه المهمة بإدارة الدفاع الوطني – حسب السلطات-تماشيا مع انخراط المغرب في سياسة تقويم الأمن الوطني، خصوصا محاربة الإرهاب المعلوماتي والجريمة المنظمة.[68] لكننا نرى من جانبنا أن هذا المقتضى يشكل تهديدا لاستغلال المعطيات الشخصية لمستخدمي الإنترنت، وانتهاكا لحرمة حياتهم الشخصية، خصوصا في ظل عدم تفعيل القوانين المتعلقة بحماية حقوق مستخدمي الإنترنت بما في ذلك سرية المراسلات والحياة الشخصية.

ومهما يكن، فلا يمكن إنكار أهمية هذه الشواهد ودورها في تأمين التوقيع الإلكتروني، كآلية من الآليات التقنية التي تشكل وسائل الحماية القبلية له، لتفادي مجموعة من الجرائم التي قد تهدد سلامة هذا الأخير. ذلك فان التصدي لهذه الجرائم بكافة الوسائل القانونية، -كما سنرى في المطلب الثاني-لايمكن اعتباره حماية كافية، خصوصا وأنها حماية بعدية لا تطبق إلا بعد تضرر الموقع الكترونيا.



[65] -الفقرة الأخيرة من الفصل 2-417 من قانون رقم 05-53

[66] - إلى غاية صدور المرسوم رقم 881-13-2 الصادر بتاريخ 28 ربيع الأول 1436 (20 يناير 2015) المعدل والمتمم لظهير 518-08-2 الصادر في 25 جمادى الأولى 1430 (21 ماي 2009).

[67]- Omar RADI, « la certification électronique passe sous le contrôle de la défense nationale » medias 24, mercredi 14 mai 2014 page2/3 منشور في موقع www.medias24.com 21/30 الساعة 2016/11/25 تاريخ الاطلاع

[68]- « stratégie nationale en matière de cyber sécurité www.dagssi.gov.ma. - منشور بموقع تاريخ الاطلاع 25 نونبر2016 الساعة 00: 15.

♦ المطلب الثاني: الحماية القانونية للتوقيع الإلكتروني

تنضاف إلى الحماية السالف ذكرها، حماية قانونية أخرى للتوقيع الإلكتروني تتمثل في الحماية الجنائية وفق مقتضيات قانون 53.05 [69](الفقرة الأولى) وقانون 07.03[70] (الفقرة الثانية).

فنظرا لأهمية التدخل الجنائي في مجال المعاملات الإلكترونية، ودور ذلك في تكريس الثقة في التعامل بواسطة الوسائل التكنولوجية المستحدثة، وما يترتب عنه من تشجيع الاستثمار عبر التجارة الالكترونية والإقدام على إبرام العقود الالكترونية، فقد تدخل المشرع المغربي بمقتضيات زجرية من خلال القانونين السالف ذكرهما لإضفاء نوع من الحماية الجنائية للتوقيع الإلكتروني، عبر تحديده الأفعال الإجرامية المخالفة لهذين الأخيرين وعقوباتها من جهة.[71]

فماهي إذن أوجه الحماية الجنائية للتوقيع الإلكتروني المقررة في هذين القانونين؟ وهل هذه الحماية كافية لدرء جميع المخاطر التي تهدده؟

الفقرة الأولى: الحماية الجنائية للتوقيع الإلكتروني في قانون 53.05

قد يتعرض التوقيع الإلكتروني لعدد من الجرائم منها جريمة التشفير.

فماهي هذه الجريمة؟ وماهي عقوبتها؟

أولا: جريمة التشفير

قد تتعرض البيانات المشفرة ووسائل التشفير إلى اعتداء من قبل الجناة، وذلك عبر اختراقها عن طريق فك الشفرة أو تسريبها من قبل من له الحق الاحتفاظ بها، وتتجلى العناصر التكوينية لهذه الجريمة في الركن المادي ويتمثل في فك مفاتيح

---

[69]- الباب الثالث من القسم الثاني، المتعلق بالعقوبات والتدابير الوقائية ومعاينة المخالفات، المواد من 29 إلى 41.

[70]قانون رقم 07.03، الصادر بتنفيذه ظهير شريف رقم 1.03.197 بتاريخ 16من رمضان 1424(11 نوفمبر 2003)، بتتميم مجموعة القانون الجنائي في ما يتعلق بالجرائم المتعلقة بنظم المعالجة الآلية للمعطيات، منشور بالجريدة الرسمية عدد 5171 بتاريخ 27 شوال 1424 الموافق (22 دجنبر 2003)، صفحة: 4284

[71]ادريس النوازلي، مرجع سابق، الصفحة :117

التشفير التي تتعلق بالتوقيع الإلكتروني، ذلك أن فضها يعني كشف البرامج الخاصة بتشفير التوقيع الإلكتروني وذلك بنقل التوقيع من صورة مكتوبة إلى صورة رقمية. وأما الركن المعنوي فيتمثل في القصد الجنائي.[72]

ومن أجل ضمان سلامة تبادل المعطيات القانونية بطريقة إلكترونيا وضمان سريتها وصحتها، فرض المشرع المغربي حماية جنائية خاصة لوسائل التشفير من خلال المادة 32 [73]من قانون 53.05 التي تجرم استيراد أو توريد أو استغلال أو استعمال إحدى الوسائل أو خدمة من خدمات التشفير دون الإدلاء بالتصريح أو الحصول على الترخيص المنصوص عليهما في المادتين 13[74]و14[75]من القانون السالف الذكر، وعاقب مرتكبها بعقوبة حبسيه محددة في سنة وغرامة مالية قدرها 100.000 درهم. أما عقوبة السجن فقد نصت عليها المادة 33[76].ونظرا للضوابط التي تحكم عملية التشفير، فإن غالبية التشريعات أقرت عقوبات جنائية على هذه الجريمة منها التشريع التونسي في فصله48 [77]من قانون المبادلات والتجارة الإلكترونية.

ولتحقيق حماية جنائية أكثر للتوقيع الإلكتروني، عاقبت المادة 35 [78]من قانون رقم 53.05 كل استعمال غير قانوني للعناصر الشخصية لإنشاء التوقيع المتعلقة بتوقيع الغير، وحماية لحجية الشهادة الإلكترونية جرمت المادة 37 الاستمرار في استعمال الشهادة المذكورة بعد انتهاء صلاحيتها أو بعد إلغائها. وبالإضافة إلى تجريم الأفعال المرتكبة من طرف مقدمي خدمات المصادقة الإلكترونية وقد عاقب المشرع المغربي في صور التجريم هاته بعقوبات سالبة للحرية تتراوح بين شهر إلى خمس سنوات وأخرى مالية تتراوح بين 10000 درهم كحد أدنى و500000 درهم كحد أقصى.

وتجدر الإشارة إلى أن الغرامات السالف ذكرها ترفع إلى الضعف إذا كان مرتكب الجريمة شخصا معنويا، كما قد يتعرض لبعض العقوبات الإضافية.[79]

ويبدو أن المشرع المغربي، وبالنص على عقوبات مالية بقيمة مرتفعة، مقارنة مع الغرامات المنصوص عليها في القانون الجنائي العام والتي يحكم بها بالموازاة مع العقوبات الحبسية يعكس إرادته في إضفاء الحماية الجنائية الفعالة التي تؤمن

---

[72]مصطفى الفوركي، الحماية القانونية والتقنية للتجارة الإلكترونية، مقال منشور في موقع الالكتروني، تم الاطلاع عليه يوم 2016/11/26، على الساعة00:01

www. marocdroit.com

[73]تنص المادة32 على: "..كل من استورد أو صدر أو ورد أو استغل أو استعمل إحدى الوسائل أو خدمة من خدمات التشفير، دون الإدلاء بالتصريح أو الحصول على الترخيص المنصوص عليهما في المادتين 13و 14 أعلاه."

[74] تنص المادة 13 في فقرتها الأخيرة "...يجوز للحكومة أن تقرر نظاما مبسطا للتصريح أو الترخيص أو لإعفاء من التصريح أو من الترخيص بالنسبة لبعض أنواع وسائل أو خدمات التشفير أو بالنسبة لبعض فئات المستعملين."

[75] تنص المادة 14 على: «يختص مقدمو خدمات المصادقة الإلكترونية المعتمدون لهذا الغرض وفقا لأحكام المادة 21 من هذا القانون، بتوريد وسائل أو خدمات التشفير الخاضعة للترخيص، وإذا تعذر ذلك، تعين أن يكون الأشخاص الراغبون في تقديم خدمات التشفير الخاضعة للترخيص معتمدين لهذا الغرض من لدن الإدارة."

[76] تنص المادة 33على: "عندما يتم استعمال وسيلة تشفير حسب مدلول المادة 14 أعلاه لتمهيد أو ارتكاب جناية أو جنحة أو لتسهيل تمهيدها أو ارتكابها، يرفع الحد الأقصى للعقوبة السالبة للحرية المتعرض لها على النحو التالي:

-إلى السجن المؤبد إذا كان معاقبا على الجريمة ب 20 سنة من السجن

-إلى ثلاثين سنة من السجن إذا كان معاقبا على الجريمة ب 20 سنة من السجن

- إلى عشرين سنة من السجن إذا كان معاقبا على جريمة ب 15 سنة من السجن

- إلى خمس عشرة سنة من السجن إذا كان معاقبا على جريمة ب 10 سنوات من السجن

- إلى عشر سنوات من السجن إذا كان معاقبا على جريمة ب 5سنوات من السجن

-إلى الضعف إذا كان معاقبا على الجريمة ب 3 سنوات من الحبس على الأكثر.

[77]الفصل 48 ينص على: " يعاقب كل من استعمل بصفة غير مشروعة عناصر تشفير شخصية متعلقة بإمضاء غيره بالسجن لمدة تتراوح بين 6أشهر وعامين وبخطية تتراوح بين 1.000 و10.000 دينار أو بإحدى هاتين العقوبتين."

[78]تنص المادة 35 على: "يعاقب بالحبس من سنة إلى خمس سنوات وبغرامة من 10.000إلى 100.000 درهم كل من استعمل، بوجه غير قانوني، العناصر الشخصية لإنشاء التوقيع المتعلقة بتوقيع الغير."

[79]خالد عثماني، مكافحة الجريمة الإلكترونية في ضوء التشريع المغربي، مجلة العلوم الجنائية، العدد الأول 2014 صفحة :44و45.

الثقة في إبرام المعاملات التجارية بواسطة الوسائل التكنولوجية الحديثة وكذا في تضييق الخناق على الخروقات التي يمكن أن ترتكب في ميدان المعاملات التجارية الالكترونية، لأن زجر الأفعال الجرمية التي يسعى مرتكبوها إلى تحقيق الأرباح، لا يتم عن طريق العقوبات السالبة للحرية وحدها، بل لابد من معاملة مرتكبي تلك الأفعال بنقيض قصدهم، وذلك لن يأتي إلا بتغريمهم بأموال تعادل أو تفوق الأرباح الممكن تحقيقها. ومع ذلك تبقى الحماية المقررة غير كافية لأن الإشكال الذي يطرح هنا هو أن المجرم ليس إي شخص بل هو مجرم فائق الذكاء مما يجعل إثبات جرائمه الإلكترونية في منتهى الصعوبة.

الفقرة الثانية: الحماية الجنائية في ضوء القانون الجنائي المغربي

أصبحت الجريمة الإلكترونية تطرح إشكاليات خطيرة على الصعيدين الاقتصادي والقانوني، خصوصا وأن المغرب من أكثر الدول العربية تحررا فيما يتعلق باستخدام شبكة الإنترنيت.

ومن أهم النصوص التي أضيفت لمجموعة القانون الجنائي من أجل سد الفراغ التشريعي في مجال مكافحة الجريمة الإلكترونية، القانون المغربي المتعلق بالإخلال بسير نظم المعالجة الآلية للمعطيات. فنتساءل عن مدى حمايته؟

يواجه التوقيع الإلكتروني خطر القرصنة عبر اختراق النظم المعلوماتية والاعتداء على سريته وسلامته وذلك بسرقته أو تزويره أو تزييفه، فهذا النوع من الإجرام أصبح يشكل عائقا في وجه التجارة الإلكترونية[80]، لذا عمل المشرع المغربي من خلال هذا القانون على توفير حماية جنائية لنضم المعلوماتية عبر تجريمه لمجموعة من الأفعال وذلك في الفصول من 607/3 إلى 607/11 من مجموعة القانون الجنائي.

إسوة بالمشرع الفرنسي الذي تصدى للاختراق المعلوماتي في قانونه المتعلق بالإعلاميات الصادر سنة 1978، وكذلك بمقتضى القانون الصادر بتاريخ 1988 المتعلق بالغش المعلوماتي.[81]

فقد جرم قانون 07.03 في فصله 3-607[82] عملية الدخول عن طريق الاحتيال إلى نظام المعالجة الآلية للمعطيات متى توفر عنصر القصد، أي متى دخل الشخص إلى النظام بطريقة غير مشروعة، سواء تم ذلك لمجموع النظام أو لجزء منه، وسواء أتحققت النتيجة بالحذف أو تغيير المعطيات المدرجة في النظام، أم لم تتحقق، إذ الجريمة لا تتوقف على حصول النتيجة، فقد نص المشرع المغربي صراحة على أن المحاولة تعاقب بنفس عقوبة الجريمة التامة في الفصل 8-607 من القانون الجنائي .وقد عرف قضاؤنا المغربي نماذج من الإجرام المعلوماتي، نسوق على سبيل المثال القضية الجنحية المسجلة لدى المحكمة الابتدائية بخريبكة تحت عدد 04/358[83] حيث أدانت أحد التقنيين من أجل جنحة الدخول إلى نظام المعالجة الآلية للمعطيات نتج عنه حذف واضطراب في سيره، ذلك أن هذا الجاني أحدث موقعا له بالإنترنيت وبدأ يتراسل مع أشخاص ذاتية ومعنوية بفرنسا من خلال الدخول إلى مواقعهم بالإنترنيت وتسلم على ضوء ذلك طرودا بريدية بدون وجه حق كما ألحق ضررا بمواقع إحدى الشركات.

---

[80] عبد اللطيف بن موسى، الحماية الجنائية للمحرر الالكتروني من التزوير المعلوماتي، مجلة العلوم القانونية العدد الأول 2014، صفحة :91

[81] عبد الله الكرجي وصليحة حاجي، التعاقد الرقمي ونظم الحماية الإلكترونية، مطبعة الأمنية، الرباط، الطبعة الأول ى2015، صفحة: 154

[82] ينص الفصل 3-607 على: "يعاقب بالحبس من شهر إلى ثلاثة أشهر وبالغرامة من 2000 إلى 10000 درهم أو بإحدى هاتين العقوبتين فقط كل من دخل إلى مجموع أو بعض نظام المعالجة الآلية للمعطيات عن طريق الاحتيال".

[83] حكم جنحي تلبسي عدد 04/408 صدر بتاريخ 2004/02/18 عن ابتدائية خريبكة في الملف الجنحي عدد 04/358.مجلة العلوم الجنائية العدد الأول 2014، صفحة: 39

كما وضع المشرع المغربي نصا قانونيا يجرم فيه التزوير الالكتروني أو المعلوماتي، فقبل صدور قانون رقم 03-07 المتمم لمجموعة القانون الجنائي لم يكن من الممكن الحديث عن التزوير إلا في ضل كتابة تقليدية[84]، أما الآن فإن القضاء المغربي يملك آلية قانونية يمكن بوجبها متابعة الجاني الذي زور وثائق معلوماتية من خلال الفصل 7-607[85] من القانون السالف ذكره، حيث فرض عقوبات على تزوير وتزييف وثائق المعلوماتية، فكل ذلك يصب في إطار توفير حماية قانونية للمعاملات الإلكترونية.

وما يمكن تسجله من خلال ما ذكر، بأن السياسة الزجرية لا تكفي لوحدها لصد مد جرائم الالكترونية بصفة عامة وتوقيع الالكتروني بصفة خاصة، بل لابد من وضع سياسة وقائية سابقة، وتكثيف المجهودات على الصعيد الدولي من أجل التصدي لها، مع العمل على لم شتات النصوص الجنائية الخاصة بالمعاملات الإلكترونية في قانون واحد حتى يتمكن القاضي من الرجوع إليها عند وقوع جرائم الإلكترونية.

[84] انتصار اليعكوبي، مرجع سابق صفحة :79و80

[85] الفصل 7-607 ينص على: "دون الإخلال بالمقتضيات الجنائية الأشد، يعاقب بالحبس من سنة إلى خمس سنوات وبالغرامة من 10.000إلى 1.000.000 درهم كل من زور أو زيف وثائق المعلوميات أيا كان شكلها إذا كان من شأن التزوير أو التزييف إلحاق ضرر بالغير.
دون الإخلال بالمقتضيات الجنائية الأشد، تطبق نفس العقوبة على كل من استعمل وثائق المعلومات المشار إليها في الفقرة السابقة وهو يعلم أنها مزورة أو مزيفة."

خاتمة:

انطلاقا من دراستنا هذه خلصنا إلى أن التوقيع الالكتروني يقوم بذات الدور الذي يقوم به التوقيع التقليدي من حيث كونه محددا لشخصية صاحبه ومعبرا عن إرادته، إلا أنه إذا كان يماثل التوقيع القليدي في هذه الوظائف، فإنه لا يماثله في الشكل المطلوب قانونا، بحيث يقوم على استخدام تقنيات حديثة من حاسوب وإنترنيت وغيرها، مما أدى إلى اتخاذه عدة أشكال وصور، وذلك لتعدد طرق إصداره، كما أن درجة الأمن والموثوقية للتوقيع الالكتروني تختلف بإختلاف صوره. بالاضافة إلى إعتماده على تقنية التشفير عن طريق معادلات رياضية أو غريتمية، ليضمن له الأمن من خلال حفظه في حاسب الآلي بشكل مشفر يتم الرجوع إليه عند الحاجة من قبل مصدره.

كما لاحظنا من خلال دراستنا أن المشرع المغربي منح التوقيع الالكتروني الذي تم توثيقه وفقا إجراءات التوثيق المحددة أثرا قانونيا في الإثبات، بحيث تكون له حجية التوقيع العادي عن طريق إلزام صاحبه، وصلاحيته في الإثبات نظرا لقيامه على تقنية التشقير والمصادقة الالكترونية. وهكذا فالمعملات الالكترونية لا تدخل حيز التنفيذ إلا بتوقيعها من طرف المتعاقد، حيث إن هذا التوقيع هو الذي يضفي على هذا النوع من الصفقات الإلكترونية صفة الإثبات، وكذلك تحديد شخصية وهوية الموقع.

ونعطي في الأخير بعض التوصيات حتى نتمكن من مواكبة المستجدات المتعلقة بالتجارة الإلكترونية، وهي كالآتي:

* العمل على خلق محاكم متخصصة في مجال التجارة الإلكترونية، وعقد دورات تدريبية في هذا المجال لمواكبة التطور العالمي في موضوع التجارة الإلكترونية.

* تشديد الجزاءات الجنائية على الجرائم المتعلقة بنظم المعلومات، وخصوصا جريمة السرقة والتزوير والتشفير والتي يتم ارتكابها بواسطة الحاسوب، مما تؤثر سلبا على التجارة الإلكترونية.

*إنشاء مكتب توثيق إلكتروني يقوم بتوثيق المعاملات الإلكترونية بغية إعطاء الثقة والأمان في مجال التجارة الإلكترونية، وهذا ما سيؤدي إلى رعاية وحماية مصالح المتعاملين بهذا النوع من التجارة، سواء أكان تاجرا ام مستهلكا.

لائحة المراجع:

❖ المؤلفات:

العامة:

- أحمد ادريوش، تأملات حول قانون التبادل الالكتروني للمعطيات القانونية، عناصر لمناقشة مدى تأثير القانون رقم 53.05 على قانون الالتزامات والعقود، مطبعة الأمنية الرباط، الطبعة الأولى 2009
- إدريس النوازلي، حماية عقود التجارية الإلكترونية في القانون المغربي، دراسة مقارنة، المطبعة والوراقة الوطنية، الطبعة الأولى 2010
- المختار بن أحمد عطار، العقد الالكتروني، مطبعة النجاح الجديدة، الطبعة الاولى 2010
- خالد ممدوح إبراهيم، إبرام العقد الالكتروني، دراسة مقارنة، مطبعة دار الفكر الجامعي-الاسكندرية، الطبعة الثانية 2011
- عبد الرحيم بحار، القضاء التجاري والمنازعات التجارية، دراسة تأصيلية مقارنة، بدون مطبعة، الطبعة الأولى 2014
- عبد الله الكرجي وصليحة حاجي، التعاقد الرقمي ونظم الحماية الإلكترونية، مطبعة الأمنية، الرباط، الطبعة الأول ى2015
- ماجد محمد سليمان أبا الخيل، العقد الاكتروني، مكتبة الرشد،المملكة العربية السعودية، الطبعة الأولى 2009
- لورنس محمد عبيدات، إثبات المحرر الالكتروني، مطبعة دار الثقافة – الطبعة الأولى 2005
- نورالدين الناصري، المعاملات والإثبات في مجال الاتصالات الحديثة، سلسلة الدراسات القانونية المعاصرة، العدد 12، مطبعة النجاح، الدار البيضاء، الطبعة الأولى، 2007
- نور الدين الرحالي، التطبيقات العملية الحديثة في قضايا الاستهلاك، مطبعة النجاح الجديدة بالدار البيضاء، الطبعة الأولى 2014

الخاصة:

- مبارك الحسناوي، الإثبات في العقد الالكتروني، سلسلة الفقه القضاء التجاري، المنازعات التجارية بين المستجدات التشريعية والاجتهادات القضائية، منشورات مجلة العلوم القانونية، العدد الأول، الطبعة الأولى 2015

❖ **الأطروحات والرسائل:**

الأطروحات:

- أحمد البختي، استعمال الوسائل الالكترونية في المعملات التجارية، رسالة لنيل دبلوم الدراسات العليا المعمقة في القانون الخاص، كلية العلوم القانونية والاقتصادية والاجتماعية، جامعة محمد الخامس السويسي الرباط، السنة الجامعية 2003-2004
- زروق يوسف، حجية وسائل الإثبات الحديثة، رسالة لنيل شهادة دكتوراه في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبوبكر بلقايد تلمسان، السنة الجامعية 2012 -2013

الرسائل :

- انتصار اليعكوبي، مدى حجية المحررات لإلكترونية في الإثيات -دراسة مقارنة-بحث لنيل دبلوم الماستر في القانون الخاص، تخصص المدني والأعمال، السنة الجامعية 2010-2011
- طارق عبد الرحمان ناجي كميل، التعاقد عبر الأنترنيت وأثاره، دراسة مقارنة، بحث لنيل دبلوم الدراسات العليا في لقانون الخاص، كلية العلوم القانونية والاقتصادية والاجتماعية، جامعة محمد الخامس أكدال، السنة الجامعية 2003-2004
- زينب غريب، إشكالية التوقيع الالكتروني وحجيته في الإثبات، رسالة لنيل دبلوم الماستر في القانون الخاص، من كلية العلوم القانونية والاقتصادية والاجتماعية، جامعة محمدد الخامس السويسي الرباط، السنة الجامعية 2009-2010
- virginie ETIENNE »le développement de la signature électronique », master 2, recherche droit des affaires, université PARIS 13 NORD, année universitaire 2010 – 2011

❖ **المجلات والتقارير**

- خالد عثماني، مكافحة الجريمة الإلكترونية في ضوء التشريع المغربي، مجلة العلوم الجنائية، العدد الأول 2014
- عزيز إطويان، حجية العقد الإلكتروني في الإثبات، مجلة الحقوق المغربية، مطبعة الأمنية، العدد الحادي عشر2011
- ماء العينين السعداني، الإطار القانوني للمصادقة على التعاملات الالكترونية، مجلة قانون وأعمال، المطبعة والوراقة الوطنية، العدد الثاني دجنبر 2011
- محمد أطويف، إشكالية إثبات عقد التجارة الإلكترونية، مجلة الحقوق، العدد 15، مطبعة المعارف الجديدة، الرباط السنة 8، يونيو 2013-يناير 2014
- محمد برادة غزيول، قراءة في القانون المتعلق بالتبادل الالكتروني للمعطيات القانونية، مجلة المعيار، العدد 39، يونيو 2008،
- مصطفى مالك، إبرام العقد بشكل إلكتروني، مجلة المحاكم المغربية العدد المزدوج 137-138 شتنبر-دجنبر 2012
- مجلة العلوم الجنائية العدد الأول 2014

- طلال حسن-الأرقم قاسم-محمد عبد المنعم- أحمد علي، "التوقيع الإلكتروني"، تقرير في مقرر أمن المعلومات والشبكات، جامعة أم درمان الإسلامية، كلية العلوم والثقافة، أم درمان، السودان

❖ **المواقع الالكترونية:**

- https://www.mahkamaty.com
- http://www.fsjes-agadir.info/
- http://frssiwa.blogspot.com/
- https://www.legifrance.gouv.fr/
- www.medias24.com
- www.dagssi.gov.ma
- www. marocdroit.com

الفهرس: