جامعة مولود معمري – تيزي وزو
كلية الحقوق والعلوم السياسية
قسم القانون- نظام (ل.م.د)

النظام القانوني للتوقيع الالكتروني في القانون الجزائري

مذكرة لنيل شهادة ماستر في القانون

تخصص : قانون الأعمال

من إعداد الطالبتين :

- براهيمي فريدة
- بوخاري نسيمة

تحت إشراف الأستاذ:

لملوم كريم

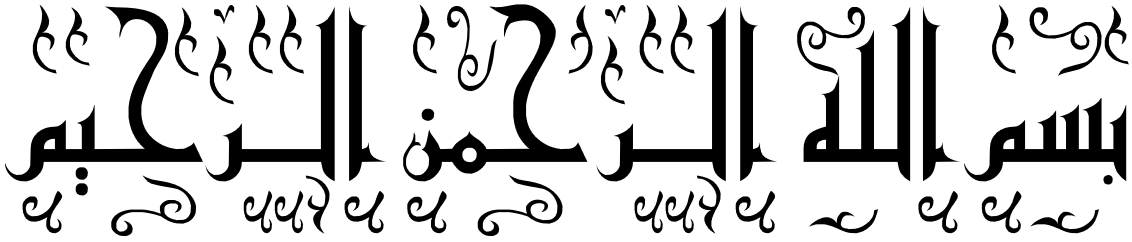
لجنة المناقشة:

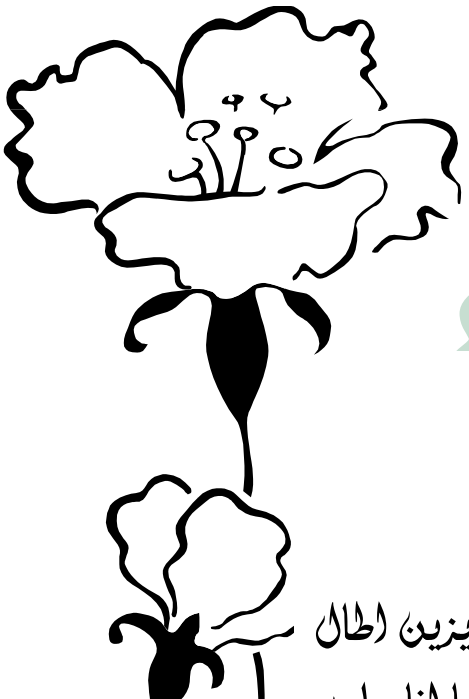
د-نسير رفيق ، أستاذ محاضر(ب) ، جامعة مولود معمري، تيزي وزو..... رئيسا

– لملوم كريم ، أستاذ محاضر (أ) ، جامعة مولود معمري، تيزي وزو .....مشرفا و مقررا

– لالوش راضية ، أستاذة مساعدة (أ) ، جامعة مولود معمري، تيزي وزو..... ممتحنة

تاريخ المناقشة: 26-09-2017


بسم الله الرحمن الرحيم



إهداء

اهدي ثمرة جهدي المتواضعة الى ابي و امي العزيزين اطال الله في عمرهما اللذان لو لاهما لما وصلت الى ما انا عليه اليوم.

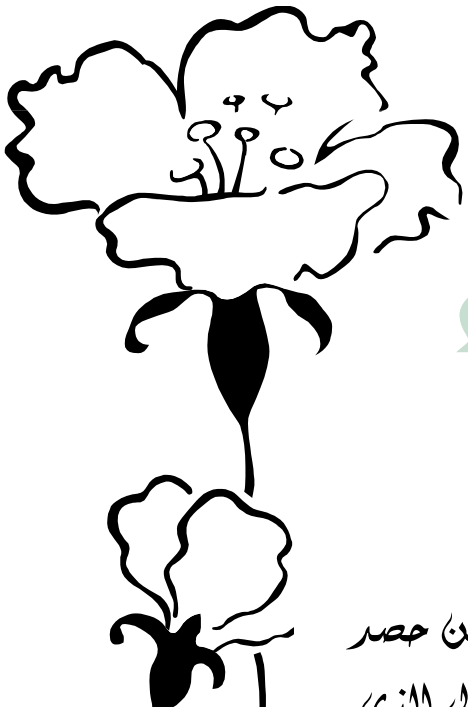
الى روح جدي و جدتي و خالي الاعزاء غمرهم الله برحمته و اسكنهم فسيح جناته .

الى اخواي العزيزين انوار و مخلوف و اختاي مليزة و سميرة و زوجيهما و اولادهما و الى صديقتي الحميمة فريدة.

اهديه ايضا الى كل من ساهم من قريب او بعيد في مساعدتي في اعداد هذه المذكرة خاصة صديقاتي :

حسينة،روزة،حياة،صارة،مليسا،ياسمين،سعرة.

نسيمة



إهداء

الى اغلى ما في الوجود وسندي في الحياة ،الى من حصد الاشواك عن دربي ليمهد لي طريق العلم ،الى الذي وهبني كل رعايته واهتمامه،الى رمز القوة الذي افنى عمره لاجلنا ابي الغالي اطال الله في عمرك و اوامك لنا سندا .

الى التي اهدتني نور الحياة ،الى القلب الناصع وبهجة الحياة ،الى اعذب كلمة رددها لساني امي الحبيبة اطال الله في عمرها .

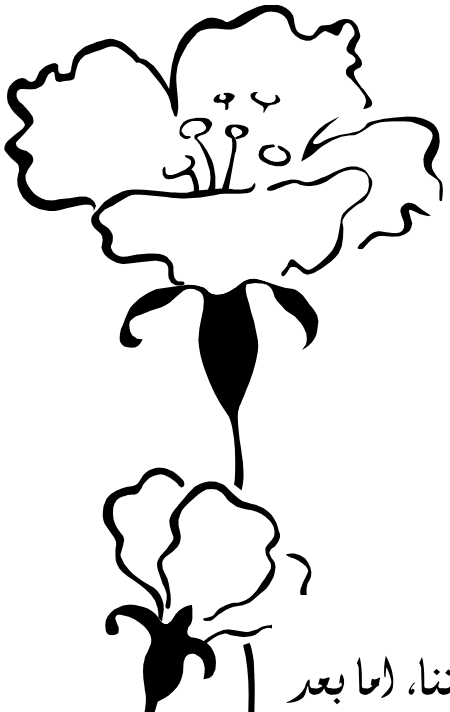
الى روح جدي الطاهرة راجية من الله ان يسكنه الجنة .

الى جدتايا العزيزتين اطال الله في عمرهما .

الى القلوب الرفيقة اخواتي وبالاخص الصغيرتين ايمان و انابيس.

الى جميع الاصدقاء و خاصة نسيمة،امينة،سهيلة.

فريدة.



شكر و عرفان

نشكر الله سبحانه و تعالى الذي وفقنا في دراستنا، اما بعد
نتوجه بالشكر الجزيل الى استاذنا المشرف المدوم كريم
الذي لم يبخل علينا بتوجيهاته و نصائحه منذ بداية بحثنا
هذا الى ان الكتمل جزاه الله عنا كل خير و اداه
لطلابه و للعلم .
بوخاري نسيمة و براهيمي فريدة

نسيمة +فريدة

قائمة أهم المختصرات :

أولا– باللغة العربية:

ص: صفحة.

ص.ص: من الصفحة إلى الصفحة.

د.ط: دون طبعة.

ق.م.ج: القانون المدني الجزائري.

ق.ا.م: قانون الإثبات المصري .

م.ا: المشرع الأردني.

ق.ت.ج: القانون التجاري الجزائري.

م.خ.ت.ا: مقدم خدمات التصديق الالكتروني.

ق.ع.ج: قانون العقوبات الجزائري.

ق.ع.ف: قانون العقوبات الفرنسي.

ج. ر : جريدة رسمية.

ثانيا– باللغة الفرنسية:

Art : Article.
http : protocole de transfère de fichier.
Op . Cit : référence précitée.
P : Page.
pp : De la page n°...àla page n°…

مقدمة:

نجم عن ثورة الاتصالات و التطور التقني الكبير في استخدام الحاسب الآلي و شبكات الانترنيت تحول كبير جدا في مجالات الحياة وارتبط ذلك بظهور مفهوم جديد ألا وهو التعامل بين الأفراد عن طريق استخدام الانترنيت الذي يعتبر أهم مظاهر العولمة كونه يقضي على مختلف العقبات لان البيئة الالكترونية تتمتع بخصائص تمكنها من التأثير على القواعد و القوانين التقليدية.

و لعل من أبرز المجالات التي شهدت ثورة الانترنيت على نحو ملحوظ هو مجال النشاط التجاري الذي يحتاج إلى الثقة في التعامل و السرعة و الدقة في إنجاز المعاملات التجارية وقد نتج في الواقع العملي عن هذا النوع الجديد من التجارة طرق ووسائل حديثة في التعاملات الالكترونية أهمها إبرام العقود على دعامات غير ورقية مما تسبب في ظهور بعض المشكلات العملية من المستحيل تكييفها مع هذه العقود الجديدة، ولمواكبة هذه التطورات تم البحث عن بديل للتوقيع التقليدي يكون قادرا على التناسب و هذه التصرفات الالكترونية و بالفعل تم التوصل إلى وسيلة بديلة ذات طبيعة إلكترونية لها أشكال مختلفة يمكن أن تحقق الوظائف التي يقدمها التوقيع التقليدي، كما أنه يزيل المخاطر الناجمة عن عدم تحقق اللقاء المباشر بين المتعاقدين الذي بدوره يجعل كلا من المتعاقدين يتأكد من هوية المتعاقد الأخر ويطمئن في التعامل معه على أساس من الأمان و الموثوقية .

فالتوقيع الإلكتروني هو وسيلة مثلى تمكن من تحديد هوية الأشخاص المتعاقدين وتحديد المواقع الالكترونية وكذا حماية الخصوصيات، فالتوقيع الالكتروني بدوره يقابل التوقيع التقليدي المستخدم في الواقع المادي حيث يتفق كل منهما بالدور الوظيفي الذي يقوم به ألا وهو تحقيق الموثوقية في التعامل من خلال تحديد هوية المتعاملين و التعبير عن إرادتهم بالإلتزام بمضمون المحررّ الذي تم التوقيع عليه إلا أن مفهوم التوقيع الإلكتروني

مفهوم جديد في عالم التجارة الإلكترونية التي إزداد استخدامها بشكل ملحوظ، وأصبحت ضرورة ملحة لمواكبة التطور التقني المتسارع و ترسيخ العمل بالأساليب الحديثة و المتطورة لتحقيق النتائج المرجوة في القطاع الاقتصادي و توفير الجهد و الوقت في آن واحد.

أمام ظهور ما يسمى بالمحررات الالكترونية التي تعتمد على الكتابة الالكترونية أصبحت هناك ضرورة ألزمها التطور التكنولوجي لإدخال مثل هذه الوسائل في النظام القانوني للدولة و الاعتراف بها كوسيلة لإبرام التصرفات القانونية والاستناد عليها كأدلة إثبات وفي إطار

ذلك انطلقت حملات تشريعية في العديد من الدول استهدفت إستيعاب هذه الوسائل الحديثة و مرجعيتها الأولية كانت قوانين الأونسترال النموذجي للتجارة الإلكترونية بالاضافة الى القانون النموذجي للتوقيع الإلكتروني حيث أصدرت لجنة القانون التجاري الدولي التابعة لمنظمة الأمم المتحدة قانون الأونيسترال النموذجي (uncitral) ودعت الدول إلى تنظيم قوانينها الداخلية لهذه التقنيات المستحدثة و ضمن هذا التوجيه سارت العديد من التشريعات في أوروبا وأمريكا وشرق آسيا محاولة بذلك ضبط ومعالجة المسائل القانونية التي أثارتها هذه الوسائل، ومن بينها قبول المحررات الإلكترونية كأدلة كتابية في الإثبات و اقرار حجيتها القانونية والعمل بها بين الدول وعدم إصدار قوانين تتعارض معها.

في هذا الإطار أصدرت بعض الدول قوانين مستقلة تنظم هذا النوع الحديث من المحررات فيما ذهبت أخرى إلى إدخال تعديل على قوانينها المتعلقة بالإثبات وهو ما انتهجه المشرع الجزائري كغيره من التشريعات المقارنة أين ذهب إلى الاعتراف بالكتابة الالكترونية والتوقيع الالكتروني في تعديله الأخير للتقنين المدني وتتحدث عنها وبصفة حصرية المادة 323 مكرر وما بعدها في المادة 327 من ت.م.ج بعد تعديلها بموجب القانون 05-10

المعدل والمتمم للقانون المدني[1] وعند هذا الحد توقف المشرع أين حدد القيمة القانونية للمحررات الإلكترونية بعد ما أعطاها الحجية والقوة الثبوتية الكاملة مثلها مثل الأدلة الكتابية العادية على خلاف معظم التشريعات المقارنة التي أصدرت فيها قوانين خاصة كالتشريع الفرنسي المغربي و الأردني و الخليجي.

وحتى يكون لمثل هذه المحررات الحجية الكاملة في الإثبات وإمكانية مساواتها للمحررات التقليدية يجب توافر جملة من الشروط منها ما تم النص عليه صراحة بموجب القانون ومنها ما تفرضه الطبيعة الإلكترونية للمحرر فجاء نص المادة 323 مكرر 1 من القانون 05-10 مانحة للكتابة في الشكل الإلكتروني نفس الحجية المقررة للدليل الكتابي العادي لكن بشروط إمكانية التأكد من هوية الشخص الذي أصدرها وأن تكون معدة ومحفوظة في طرق تضمن سلامتها.

إزاء هذه التحولات الكبيرة التي عرفتها التجارة نتيجة استخدام المتعاملين الاقتصاديين المتزايد للانترنيت و الاعتماد على هذه الأخيرة في معاملاتهم التجارية أعطت اغلب التشريعات بما فيها المشرع الجزائري أهمية بالغة في وضع سياسة شاملة وناجحة لهدف حماية المتعاملين عبر شبكات الانترنيت، وذلك من خلال ضرورة وضع اكبر قدر من الحماية و الأمان للتوقيع الالكتروني عن طريق وضع حد لمرتكبي الجرائم الالكترونية وخاصة تلك المتصلة بالتوقيع الالكتروني وذلك بوضع مجموعة من العقوبات من طرف السلطات المختصة تطبق على المجرم المعلوماتي لوضع حد لمثل هذه الجرائم.

و من بين الأسباب التي دفعتنا لاختيار هذا الموضوع التطور السريع لعالم التكنولوجيا و الاتصال ومدى تأثيره على التجارة و منحها مفهوم جديد عن طريق استبدال التوقيع التقليدي بالتوقيع الالكتروني لمنح المعاملات بين التجار نوع من السرعة و الدقة والموثوقية

1-القانون رقم 05-10 ،مؤرخ في 2005/06/20 يعدل و يتمم الامر رقم 58/75 ، المؤرخ في 10 سبتمبر 1975، المتضمن القانون المدني ، ج ر عدد 44، الصادرة في 26 جوان 2005.

بالإضافة إلى ذلك كيف بادرت الجزائر على غرار باقي الدول إلى تعزيز نظامها القانوني في سبيل التصدي للجريمة المعلوماتية بالسعي إلى وضع تشريعات تحد قدر الإمكان من حالات ارتكابها و من هنا تبرز أهمية الموضوع.

بناءا على ما سبق توصلنا إلى طرح الإشكالية التالية: ***كيف نظم المشرع الجزائري التوقيع الالكتروني؟***

وبناءا على ذلك قمنا بتقسيم موضوع بحثنا إلى فصلين، **(الفصل الأول)** التوقيع بمفهوميه التقليدي و الحديث،**(الفصل الثاني)** وسائل حماية التوقيع الالكتروني.

الفصل الأول

التوقيع بمفهوميه التقليدي والحديث

يعد التوقيع وسيلة لإثبات موافقة الموقع على المعلومات الواردة في مستند ما صدر عنه، فقد نشأ منذ أن بدأت الشعوب تتواصل عبر التجارة وبدأ الإنسان يبرم العقود، لكنه ظهر بشكله المادي عبر وضع رسم أو شكل معين على قطعة خزف أو جلد أو مخطوطة ورقية، ففي العصور الرومانية كان التوقيع عبارة عن رمز مرسوم أو خاتم مطبوع على شمع باسم مالك الختم، لكن التحول العميق للمجتمع أدى إلى تطور التوقيع بشكل تدريجي حتى وصل إلى شكله الحالي، فالتوقيع يعمل على نقل المحررات من مرحلة الإعداد إلى مرحلة الإنجاز وإعطائها صفة الأصل في نظر القانون، كما أنه يلعب دورا جوهريا،واساسيا في اضفاء القوة

الثبوتية على المحررات، وينسب المحرر إلى الشخص الذي وقعه ولو لم يكن مكتوبا بخطه، كما أنه يعبر عن إرادته في الالتزام بذلك المحرر، حيث يعتبر التوقيع ظاهرة اجتماعية وضرورية يحميها القانون، ومع ذلك فلا تزال هذه الظاهرة يكتنفها الغموض في بعض جوانبها، ولعل ذلك يرجع في جزء كبير الى غياب فكرة واضحة ومحددة للتوقيع التقليدي تشريعيا وقضائيا وفقهيا، ومع ظهور وسائل الاتصالات الحديثة، أصبح النظر إلى التوقيع التقليدي على أنه اجراء غير ملائم للإثبات ولإرتباط التوقيع بالكتابة باعتبارها دليلا للإثبات،وكما هو معروف أن الكتابة لا تعد دليلا كاملا في الإثبات إلا إذا كانت موقعة، وعليه فغياب التوقيع يفقد الدليل الكتابي حجيته في الإثبات،ولان الواقع العملي قد اتجه الى ادخال طرق ووسائل حديثة في التعامل لا تتفق مع فكرة التوقيع بمفهومه التقليدي وإزاء انتشار نظم المعالجة الالكترونية للمعلومات التي بدأت تغزو الشركات والإدارات والبنوك،

اعتمادا على هذه الآلات، وأنه لا مجال للإجراءات اليدوية في ظلها، أصبح التوقيع التقليدي عقبة من المستحيل تكييفها مع النظم الحديثة للإدارة والمحاسبة، وقد تم الاتجاه نحو بديل للتوقيع التقليدي ألا و هو التوقيع بمفهومه الحديث،أي التوقيع الالكتروني، استجابة لمتطلبات التعامل الحديث وخاصة التعاملات التجارية عبر الانترنيت حيث أن التوقيع الالكتروني جاء في سياق الصيرورة العلمية للثورة التقنية،إذ نجده غير لابس لثوب التوقيع العادي الذي يعتبر الوسيلة المعروفة والشائعة الاستعمال كأداة للتفريد، ونظرا للأهمية البالغة في إثبات المعاملات الالكترونية عرف اهتمام وافر وكبير من قبل المشرعين والفقهاء على حد سواء.

فما هو المقصود بكلا التوقيعين؟ وما هي شروط ووظائف كل منهما؟ هذا ما سنحاول الإجابة عليه من خلال المبحثين الآتيين:

المبحث الأول

التوقيــع التقليـدي

يعتبر التوقيع تعبيرا عن رضا الملتزم، فهو المظهر الخارجي للإرادة ومن هنا اكتسى أهميته، إذ يعتبر الرضا شرطا جوهريا في حصول العقد، فالتوقيع أهم عنصر في المحرر أو الورقة العرفية وهو الذي ينسب الورقة إلى من يراد الاحتجاج عليه بها، فالمستند الموقع بخط اليد يعبر عن رضا صاحبه ونيته في التعاقد فبدون التوقيع لا يوجد سوى مشروع ورقة أو مجرد بداية حجة.

يقصد بالتوقيع في اللغة القانونية ذلك الشرط الوحيد اللازم لصحة الدليل الكتابي، حيث تعتبر تلك العملية اليدوية التي تعطي دلالة معبرة بشكل واضح على الموافقة بما جاء بالمحرر من بنود، والمؤكدة على شخصية صاحبها حيث تفيد صدور المحرر من الموقع شخصيا، فالتوقيع يعد الشرط الأساسي للدليل الكتابي سواء بالنسبة للورقة الرسمية أو الورقة العرفية، فهذا التوقيع علامة شخصية يمكن عن طريقها تمييز هوية الموقع أو شخصيته والذي يوقع بخط يده، فهو عادة يوضع مستقلا على محتوى المحرر حرصا على وضوحه إذ يوجد عقب آخر سطر في أي مستند، وفي حالة تعدد الأوراق في المستند الواحد، فإنها تحمل توقيعا على كل ورقة حتى يمكن القول بنسبة هذا المحرر لمن وقع عليه، ففي هذا المبحث سنتطرق إلى تعريف التوقيع التقليدي وشروطه، صوره ووظائفه من خلال المطلبين التاليين:

المطلب الأول

مفهوم التوقيع

يتسع مفهوم التوقيع ليشمل كل علاقة من شأنها أن ترتبط ارتباطا وثيقا بالشخص الذي تصدر عنه، فقد يكون عبارة عن كلمة معينة تحدد اسم هذا الشخص أو لقبه أو كلمة أخرى يختارها بنفسه،و قد يكون عبارة عن حرف أو عدة أحرف، كما يمكن أن يتخذ رمزا معينا أو رقما معينا، وقد يكون عبارة عن بصمة الأصبع أو ختم خاص بصاحب الحق يستخدمه في معاملاته، والتوقيع يعبر عن صاحبه بطريقة ما ومن ثم يمكن لمن يصدر عنه التوقيع أن يختار الطريقة التي سيفرغ توقيعه من خلالها على أن تحدد هويته بشكل واضح.

فما هو تعريف التوقيع التقليدي وما هي الشروط أو العناصر التي يجب أن تتوفر فيه لكي يكون صحيحا؟

الفرع الأول

تعريف التوقيع

التوقيع كلمة اشتقت من الفعل الثلاثي (وقع)، ووقع العقد، أو الصك كتب في أسفله اسمه إمضاءه، أو إقرارا به.

والتوقيع لغة معناه: ما يعلقه الرئيس على كتاب أو طلب برأيه فيه، وتوقيع العقد أو الصك ونحوه أن يكتب الكاتب اسمه في ذيله إمضاءً له أو إقراراً به[1].

1- إياد محمد عارف عطا سده، مدى حجية المحررات الالكترونية في الإثبات، دراسة مقارنة، أطروحة لاستكمال متطلبات درجة الماجستير في القانون الخاص بكلية الدراسات العليا، جامعة النجاح الوطنية، نابلس، فلسطين، 2009، ص 49.

أما التوقيع اصطلاحا: يستخدم بمعنين الأول، هو عملية التوقيع ذاتها، أي واقعة وضع الإمضاء أو أي إشارة أخرى على محرر يحتوي على معلومات معينة، والثاني: هو علامة أو إشارة تسمح بتمييز شخص الموقع[1].

أولا: التعريف القانوني للتوقيع:

على الرغم من أهمية التوقيع التقليدي بوصفه يثبت حجية الورقة في الإثبات كونه شرط جوهري في المحرر العرفي، ورغم الدور المهم الذي يلعبه في الحياة اليومية وخاصة الحياة الاقتصادية، إلا أن مشرعي مختلف الدول لم يعطوا تعريف محدد له، بل أشار معظمهم إلى تحديد أشكاله التي تتمثل في: الإمضاء، البصمة والختم، كما اكتفت بعض التشريعات في تعريفه بالنص عليه من خلال تبيان وظائفه ومن بين تلك التشريعات نذكر التقنين المدني الجزائري في مادته 327 بنصها: "يعتبر العقد العرفي صادرا ممن وقعه ما لم ينكر صراحة ما هو منسوب إليه من خط أو إمضاء. أما ورثته أو خلفه فلا يطلب منهم الإنكار، ويكفي أن يحلفوا يمينا بأنهم لا يعلمون أن الخط أو الإمضاء هو لمن تلقوا منه هذا الحق". يضاف إليها نص المادة 165 من قانون الإجراءات المدنية والإدارية الجديد[2].

نجد كذلك المشرع المغربي لم يأت بتعريف محدد للتوقيع، لكنه حصر التوقيع في الإمضاء باليد حيث جاء في الفصل 426 من ق ل ع على أنه: "يسوغ أن تكون الورقة العرفية مكتوبة بيد غير الشخص الملتزم بها بشرط أن تكون موقعة منه. ويلزم أن يكون

1- إياد محمد عارف عطا سده، المرجع السابق ص ص 51 52 .

2- أ. عجابي إلياس، "**الطبيعة القانونية للتوقيع الالكتروني**"، جامعة محمد بوضياف، المسيلة، مقال منشور على الموقع: www.asjp.cerist.dz

التوقيع بيد الملتزم نفسه وأن يرد في أسفل الورقة ولا يقوم الطابع أو الخاتم مقام التوقيع ويعتبر وجوده كعدمه"[1].

كما عرفه القانون المدني مقاطعة كبيك الكندية في المادة 2827 التي تنص على أن: "التوقيع يتمثل في قيام الشخص بوضع اسمه أو أية علامة أو إشارة أخرى تميزه شخصيا ويستعملها بصورة معتادة على محرر بقصد التعبير عن رضاه"[2].

غير أن القانون الفرنسي الصادر في 16 يوليو 1966 والخاص بالأوراق التجارية، قد أجاز أن يكون التوقيع باليد، أو بأية وسيلة أخرى، كما أنه في المعاملات التجارية، حيث يسود مبدأ حرية الإثبات يمكن التوقيع بالإمضاء أو الختم أو بصمة الأصابع.

لقد سلك المشرع التونسي نهج المشرع الفرنسي وقصر التوقيع على الإمضاء فقط، ولم يعط أية قيمة للتوقيع عن طريق بصمة اليد أو بصمة الختم[3].

أما بالنسبة لقانون الإثبات المصري رقم 25 لسنة 1968 في المادة العاشرة منه الفقرة الثانية نص على أن: "فإذا لم تكسب هذه المحررات صفة رسمية فلا يكون لها إلا قيمة المحررات العرفية متى كان ذوي الشأن قد وقعوها بإمضاءاتهم أو أختامهم أو بصمات أصابعهم". يتضح من هذا النص أن المشرع المصري لم يتعرض لتعريف التوقيع المطلوب

1- زينب غريب، إشكالية التوقيع الالكتروني وحجيته في الإثبات، رسالة لنيل شهادة الماستر قانون خاص، جامعة محمد الخامس السويسي، الرباط، 2009 – 2010، ص 13.

2- عمر خالد زريقات، عقد البيع عبر الأنترنت، دار الحامد للنشر والتوزيع، عمان، 2007، ص 243.

3- زينب غريب ،المرجع السابق، ص 22.

في قانون الإثبات، إنما اكتفى فقط بذكر الصورة المختلفة التي يعتد بها كصور لهذا التوقيع، وهي الإمضاء أو الختم أو بصمة الأصبع[1].

بالتمعن في هذه المادة، نلاحظ أن المشرع أراد الاكتفاء بإحدى هذه الطرق لكي يثبت صحة ما هو منسوب للموقع، وعلى اعتبار التوقيع مصطلح يشمل كل من الاسم كاملا أو مختصرا، كما يشمل كل إشارة أو اصطلاح خطي يختاره الشخص لنفسه بمحض إرادته للتعبير عن صدور المحرر منه والالتزام بما ورد في مضمون هذا المحرر أما الختم فهو وسيلة ميكانيكية تستخدم لطبع توقيع الشخص، ولا يشترط أن يكون اسم الشخص هو المطبوع، بل يجوز الأخذ بأي اختصار قد اعتاد عليه الشخص، أما بصمة الأصبع فهي الأثر الذي يتركه اصبع الشخص على المحرر نتيجة طبعه بلون ظاهر، مما يكون نقوشا لا يمكن أن تتشابه لدى اثنين من البشر[2].

ثانيا: التعريف الفقهي للتوقيع:

أمام غياب مفهوم واضح ومحدد للتوقيع من جانب المشرع، حاول الفقه والقضاء ذكر عناصره، وإن كان بصورة غير مباشرة دون وضع تصور عام له.

فوفقا لقاموس روبير الفرنسي يمكن تعريف التوقيع بأنه: "علامة شخصية يضعها الموقع باسمه (شكل خاص وثابت) ليؤكد صحة مضمون الورقة وصدق ما كتب بها، وإقراره بتحمل المسؤولية عنه"[3].

1- كريم لملوم، الإثبات في معاملات التجارة الالكترونية بين التشريعات الوطنية و الدولية، مذكرة لنيل درجة الماجستير في القانون فرع قانون التعاون الدولي، كلية الحقوق ، جامعة مولود معمري تيزي وزو ، 2011 ص 103.

2- عمر خالد زريقات، المرجع السابق، ص 244.

3- كريم لملوم، المرجع السابق ص 102.

كما يعرف الأستاذ Christophe Devys التوقيع: "بأنه كل علامة توضع على سند تميز هوية وشخصية الموقع وتكشف عن إرادته بقبول التزامه بمضمون هذا المستند وإقراره له"، كما ذهب Gerve Groze إلى أن إصطلاح التوقيع يستعمل بمعنيين، الأول: أنه عبارة عن علامة أو إشارة تسمح بتمييز الشخص الموقع، والثاني: هو فعل أو عمل التوقيع ذاته، بمعنى وضع التوقيع على مستند يحتوي على معلومات معينة، ويقال في المفهوم التقليدي أن التوقيع هو الكتابة المخطوطة باليد والمستند الموقع هو المحرر، ويعد المعنى الأول المعنى المقصود بالتوقيع في نطاق الإثبات، وبناءً على ذلك فإن التوقيع ينصرف إلى العلامة الخاصة والمميزة التي يضعها صاحبها (الموقع) بأية وسيلة على مستند[1].

كما قام أحد الفقهاء بتعريف التوقيع وقال بأنه: "العلامة الخطية التي يضعها شخص على وثيقة مكتوبة، يعبر بها عن وجوده المادي في التصرف، أو تأييده لمضمون الوثيقة التي صدرت عنه[2]، وقام فقيه آخر في فرنسا بتعريف التوقيع على أنه: "كل علامة مكتوبة بخط اليد مميزة وشخصية تساعد على تحديد ذاتية مؤلفها دون شك وتترجم إرادته في قبول هذا التصرف"[3].

ومن هنا يتضح لنا جليا أن التعريف جد ضيق حتى يستوعب التوقيع من حيث الشكل، فقد اقتصر فقط على التوقيع الكتابي مستبعدا التوقيع بالختم أو ببصمة الأصبع رغم شموله على وظائف التوقيع والمتمثلة في تحديد هوية الموقع، والتعبير عن إرادته في قبول التصرف القانوني.

1- زينب غريب، المرجع السابق، ص 14.

2- إبراهيم عرسان أبو الهيجاء، القانون الواجب التطبيق على عقود التجارة الالكترونية، رسالة دكتوراه، جامعة الدول العربية، القاهرة، 2004، ص 77.

3- زينب غريب، المرجع السابق، ص 14 .

كما عرفت موسوعة Larousse لسنة 2002 التوقيع بأنه: "اسم أو علامة شخصية توضع أسفل المحرر أو النص، تعين هوية الموقع الذي يلتزم بتنفيذ ما ورد في العقد"[1].

يمكن تعريف التوقيع بصورة عامة، بأنه علامة شخصية مؤلفة من اسم الموقع أو لقبه أو الاثنين معا، أو قد يكون حرفا أو عدة حروف أو أي رمز يمكنه أن يعبر من خلاله عن التزامه بمضمون المستند الكتابي الذي وقع عليه مهما اختلفت الوسائل المستخدمة من أجل ذلك، يتبين من هذا التعريف أن التوقيع يفرغ بالشكل الذي يختاره الموقع لتحديد هويته بأية وسيلة كانت، وصولا إلى التوقيع الالكتروني الذي فرضه التعامل الجديد في العالم الالكتروني، كما يوضح هذا التعريف الغاية الرئيسية من التوقيع المتمثلة في التعبير عن التزام الموقع بمضون الورقة الموقعة[2].

أما بالنسبة للقضاء فقد كان إلى جانب الفقهاء الذين اكتفوا بوضع عناصر التوقيع دون وضع تعريف شامل أو محدد له وقد عرفته محكمة النقض الفرنسية بأن:" التوقيع التقليدي شهادة بخط اليد تكشف عن رضا الموقع بهذا التصرف وتمكن من التحقق من إسناد التوقيع لصاحب الوثيقة"[3].

1- كريم لملوم، المرجع السابق، ص 104.

2- حنان مليكة، النظام القانوني للتوقيع الالكتروني في ضوء قانون التوقيع الالكتروني السوري رقم 4 الصادر بتاريخ 2009/02/25، دراسة قانونية مقارنة، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 26، العدد الثاني، 2010، ص ص 552 – 553.

3- أ. عبد العزيز سمية، التوقيع الالكتروني وسيلة حديثة للإثبات، دراسة مقارنة، مجلة علمية تصدر عن جامعة آكلي محند أولحاج، قسم العلوم القانونية، البويرة، الجزائر، العدد 17، 2014.

ونفس التوجه عكس قرار صادر عن محكمة باريس، الذي حدد التوقيع الصحيح في: "كل علامة مميزة شخصية وخطية، وتسمح بتفريد الشخص الموقع بدون أي شك، وتعكس الإرادة الواضحة لهذا الأخير في إبرام التصرف"[1].

أما محكمة النقض المصرية فقد عرفت الإمضاء الخطي وهو أحد أشكال التوقيع التقليدي بأنه: "الكتابة المخطوطة بيد من تصدر منه".

تكمن أهمية التوقيع في المكانة المتميزة التي يحتلها فيما يتعلق بالاعتراف بالحجية للورقة العرفية واجتماع القضاء على اعتباره الشرط الوحيد والجوهري لصحة هذه الورقة، واعتباره دليلا كاملا في الإثبات[2].

الفرع الثاني

شروط التوقيع التقليدي

أولا:التوقيع علامة شخصية خطية مميزة للشخص الموقع:

يشترط في التوقيع أن يحقق الدلالة على شخصية صاحبه ويميز هويته وذلك من خلال النظر في اعتياد الشخص التعامل به كتوقيع يتميز به عن غيره من الناس بشكل يقطع الشك ويقرب إلى اليقين بأن هذا إشارة إلى فلان ولذلك يشترط أن يتم التوقيع بخط يد من ينسب إليه المحرر، فلا يجوز أن يكون بخط سواه ولو كان موكلا عنه، لأنه الوكيل يكون له أن يوقع باسمه هو بصفته وكيلا لا باسم الموكل، وحسب تعبير محكمة النقض المصرية فالتوقيع أو الإمضاء هو الكتابة المخطوطة بيد من تصدر عنه[3].

1- زينب غريب، المرجع السابق، ص 15.

2- إياد محمد عارف عطا سده، المرجع السابق، ص 52.

3- كريم لملوم، المرجع السابق، ص 105.

يشترط كذلك في التوقيع أن يكون محددا لشخصية الموقع (فالتوقيع علامة شخصية يمكن من خلالها تمييز هوية الموقع وهو كما يقول الأستاذ Saoatier (ترجمة لكلام أو لفظ تميز شفاهة شخصية الموقع)، ولهذا يتجه فريق من الفقهاء إلى القول بأن التوقيع يجب أن يكون بالاسم واللقب كاملين بحيث لا يكفي التوقيع المختصر أو بالأحرف الأولى من الاسم واللقب، فالعلامة الرمزية أو الأحرف الأولى تؤكد بدرجة كافية إقرار الموقع للورقة والتزامه بمضمونها، وإن كان هناك اتجاه آخر يرى بأنه لا يلتزم أن يكون التوقيع بالاسم الكامل، وإنما يكفي التوقيع المختصر، ما دام قد ثبت أن هذا التوقيع هو توقيع الموقع.

لا يلزم أن يكون التوقيع بالاسم المقيد في شهادة الميلاد بل يكفي أن يكون باسم الشهرة، أو الاسم الذي اعتاد الشخص التوقيع به، والمهم أن يكون التوقيع أو التواقيع التي يشتمل عليها المحرر، يمكن معها الجزم بأنها صادرة حقيقة من منشئه، كذلك لا يلزم أن يكون التوقيع الخطي مباشرا، وإنما يجوز أن يتم باستخدام الكربون للتوقيع في نفس الوقت على عدة نسخ من المحرر، فيعتبر كل منها أصلا لا مجرد صورة من المحرر، ولقد قضت محكمة النقض المصرية بأن المحرر الموقع عليه بإمضاء الكربون يكون في حقيقة الأمر محررا قائما بذاته، له حجيته في الإثبات وفقا لنص المادة 14 من قانون الإثبات المصري.

بالرجوع لأحكام القضاء الفرنسي، نجدها تقبل التوقيع باسم مستعار أو بلقب ديني أو بالاسم الأول دون اللقب العائلي، أو بالأحرف الأولى من الاسم، كذلك الحال بالنسبة لاستخدام علامة غير مقروءة ما دامت تمكن من نسبتها إلى شخص معين[1].

يكون التوقيع أيضا بإمضاء الشخص بنفسه، كما يكون كذلك بالختم أو ببصمة الأصبع، فقد اعتبر المشرعان المصري والكويتي التوقيع أيضا هو الإمضاء بالختم أو

1- لملوم كريم، المرجع السابق، ص 106.

البصمة، أما المشرع الفرنسي فقد اعترف فقط بتوقيع الخاتم، وهو وسيلة ميكانيكية غير الكتابة، يتم التعامل بها في مجال التوقيع على الأوراق التجارية، فقد أجازت المادتين 110 و117 من قانون التجارة الفرنسي بعد تعديلهما بالقانون رقم 166/380 الصادر في 16 جوان 1996، أن يوقع صاحب الكمبيالة باليد أو بأي وسيلة أخرى، ولكنه لم يعترف بالختم على عكس المشرعان المصري والكويتي اللذان اعتبراه توقيعا، فقد رفضه المرسوم الفرنسي الصادر سنة 1967 ولم يعترف به، ثم تبعه القضاء بحجة أنه لا يسمح بالتعيين الدقيق لشخص الموقع، ومعنى ذلك أنه فيما عدا الاستثناءات المقررة بنصوص صريحة يبقى الأصل العام في فرنسا قائما، وهو أن التوقيع يجب أن يكون مكتوبا باليد، وأي توقيع آخر أي كانت وسيلته لا يظهر على الورقة الموقعة ليست له حجية في الإثبات، وتكون الورقة الموقعة حينئذ كالورقة غير الموقعة نهائيا.

على العموم لا يشترط بالنسبة للتوقيع ببصمة الختم أية شروط سوى أن تكون البصمة واضحة ومقروءة، ويستوي أن تكون بصمة بصحة الختم قد وضعها صاحب الختم بنفسه أو قام غيره بوضعها برضاه[1].

ثانيا: أن يكون التوقيع مقروءًا ثابتاً ومستمراً ومرتبطاً بالمحرر الكتابي:

يعد التوقيع شكلا من أشكال الكتابة لذا فهو يخضع لنفس الشروط التي تخضع لها الكتابة، لتقدير مدى صحتها[2]، ونجد أن المشرع الفرنسي والجزائري قد ربطا إمكانية الاحتجاج بالكتابة بتوافر شروط نستنتجها من خلال استقراء المادتين 1316 و1/1316، من القانون المدني الفرنسي والمادة 323 مكرر و323 مكرر1 من الق.م.ج والتي هي:

1- محمد السعيد رشدي، التعاقد بوسائل الاتصال الحديثة و مدى حجيتها في الاثبات ، منشاة المعارف، الاسكندرية2007،، ص ص 187 – 188.

2- إياد محمد عارف عطا سدة، المرجع السابق، ص 57.

- أن تكون الكتابة أو التوقيع ذات معنى واضح ومفهوم حتى يعتد بالمحرر يجب أن يكون مقروءً وواضحاً بشكل مباشر.
- أن تتمتع الكتابة أو التوقيع بالاستمرارية والثبات[1].

وهو لن يكون كذلك إلا إذا تم تحرير العقد بشكل يسمح بالرجوع إليه طوال الفترة الكافية لاستمراره كوسيلة إثبات، حيث أن التكوين المادي للمستند يجب أن لا يتأثر بسهولة بالعوامل الطبيعية، إلا ما كان مما يتأثر بعوامل التربة والرطوبة أو يتميز بقدرة عالية من الحساسية تعرضها للتلف المباشر، ونظرا لحرص الأفراد على وضوح التوقيع، فقد جرى العمل على أن يكون التوقيع مستقلا على مستوى السند، غير متداخل فيه أو مختلط به، ولذلك يوضع التوقيع عادة في نهاية الكتابة، لكن المهم من الناحية القانونية أن يكون التوقيع ثابتا وواضحا ومتميزا سواء وضع في نهاية الكتابة أو أعلى الورقة.

إلى جانب ما سبق من شروط يتعين في التوقيع أن يرتبط بالمحرر الالكتروني، وأن يتصل به بشكل مباشر ويتحقق هذا الاتصال ما بين المحرر بشكل يستحيل فصله على الورق، إلا باتلاف المحرر والراجع لطبيعة كل منهما، فالمواد التي تتم بها الكتابة تتكون من مواد كيميائية قابلة للاتصال بشكل وثيق بالورق بمجرد أن تجف وهو ما لا نجده في التوقيع الالكتروني[2].

يتميز التوقيع التقليدي بمجموعة من الخصائص نذكر منها: أنه يتم عبر وسيط مادي ملموس ومحسوس وهو في الغالب وسيط ورقي[3]، وأنه لا يوجد مدة معينة لصلاحيته، وأن

1- عبد اللطيف بركات، الإثبات الالكتروني في المعاملات الإدارية، مذكرة مكملة من مقتضيات شهادة الماستر في الحقوق، جامعة محمد خيضر، بسكرة، 2012 – 2013، ص 16.

2- إياد محمد عارف عطا سده، المرجع السابق، ص ص 57 – 58.

3- مجلة المدرسة الوطنية للإدارة، المجلد 13، العدد 2، 2003، العدد 26.

التوقيع يتطلب الوجود المادي للشخص الموقع، كما يتميز بوحدة التوقيع بمعنى أنه لكل شخص توقيعا خاصا به، فالتوقيع يكون على دعامة ورقية والتي تضمن عدم إمكانية تجزئة محتوى المحرر عن التوقيع لأن هذا الاخير يجعل من المحرر أصلا، كما أنه يتميز بعدم إمكانية تزوير محتوى الموقع بدون وجود آثار مرئية على المحرر[1].

المطلب الثاني

صور ووظائف التوقيع التقليدي

يتضح لنا مما سبق ذكره، أن التوقيع هو الشرط الوحيد والجوهري لصحة الورقة العرفية، فإذا لم يوضع على الورقة لا تكون لها حجية في الإثبات، ذلك أن الورقة العرفية إنما تستمد حجيتها من التوقيع وحده، والورقة العرفية غير الموقعة لا تصلح حتى مبدأ ثبوت بالكتابة إلا إذا كانت مكتوبة بخط المدين، والتوقيع له صور وأشكال فإما أن يكون بالختم أو ببصمة الأصبع أو بالإمضاء، كما أن للتوقيع وظيفتين أساسيتين يتمثلان في تحديد هوية الموقع وتمييزه عن غيره، والتعبير عن إرادة الموقع في إقراره بالمحرر والالتزام بما ورد فيه[2].

الفرع الأول

صور التوقيع التقليدي

أولا: التوقيع بالختم:

يعتبر الختم من أهم علامات الإثبات، فهو دليل على صحة المكتوب، وجد منذ عصر الدولة القديمة في المشرق فقد كان منقوشا عليه الأسماء ويغمس في مداد الطين،

1- د. هالة جمال الدين محمد محمود، أحكام الإثبات في عقود التجارة الالكترونية، دار النهضة العربية، ش عبد الخالق ثروت، القاهرة، 2013، ص ص 328 – 329.

2- إياد محمد عارف عطا سده، المرجع السابق، ص 53.

ويكون صنع الخاتم من الشمع، ومع مرور الوقت اصبح يصب في قوالب مصنوعة من مواد عديدة منها الفخار والمعادن والأخشاب، كما تعددت أشكاله فمنها الهندسي والمستطيل والمثلث والمربع والدائري، وفي عهد الرسول صلى الله عليه وسلم اتخذ خاتما من فضة نقش عليه محمد رسول الله في ثلاثة أسطر واستخدمه أبو بكر وعمر وعثمان ثم سقط من عثمان فتفرق فصنع غيره، وكان لكل خليفة من الخلفاء الراشدين خاتمه الخاص للطبع على الرسائل، وكان لهذه الأختام قيمة بالغة، ولما كان الخاتم يعطي الصفة الرسمية للمكتوب فقد قامت الدولة الأموية والعباسية بإلحاق أختام على المكاييل الإسلامية للتعامل بها في الأسواق، وقد اتخذ معاوية منه ديوانا سمي ديوان الختم وعين له وزيرا سمي (مهردار) معناه حامل الخاتم، وقد أكدت الوثائق على أن استخدام الختم في توثيق المحررات لم يقتصر على من لا يعرفون الكتابة والقراءة فقط، إنما الناس بمختلف تقاليدهم وطوائفهم استخدموا الختم، فقضاة المحاكم المصرية كانت لهم أختامهم الشخصية للتوقيع على السجلات والوثائق[1]، ولذلك جاء في القانون الخاص الصادر في عام 1926 المتعلق بالمحاكم المصرية على ما يلي: "إن جميع السندات الشرعية وصورها التي تكتب على الأوراق المدموغة وصور الأحكام تختم بخاتم رئيس المحكمة الذاتي، بما يقيد تسجيلها"، ولهذا فالختم وسيلة ميكانيكية لطبع توقيع الشخص، ولا يشترط بالتوقيع سوى أن يكون واضحا ومقروءا، فإن كان غير ذلك فلا يعتد به.

كما تنص المادة 144 من تقنين أصول المحاكمات المدنية اللبناني على أن الشخص الذي لا يعرف أن يوقع بإمضائه يستبدل الإمضاء بوضع طابع أصبعه، والتوقيع بالختم يكون من خلال صاحبه أو حضوره، وطبيعي أن التوقيع بالختم أمر لا يخلو من خطر السرقة أو الضياع أو الفقد، ولذلك نصت المادة 14 من ق.ا.م على أنه: "يعتبر المحرر

1- إياد محمد عارف عطا سده، المرجع السابق، ص ص 53 – 54.

صادر ممن وقعه ما لم ينكر صاحبه الإمضاء أو الختم[1]، ونرى أن القانون الفرنسي لا يجيز التوقيع إلا بخط اليد، إلا أنه رخص التوقيع بالختم وذلك في حالات استثنائية مثل الأوراق التجارية[2].

ثانيا: التوقيع ببصمة الأصبع:

بصمة الأصبع عبارة عن الأثر الذي يتركه اصبع الشخص على الورق بعد طلائه بمداد ملون، حيث وفق ما جرت عليه العامة يضع الشخص إبهامه الأيسر بمداد السائل ومن ثم يضع اصبعه على الورقة وفي الأغلب في أسفل السند، والاعتماد على البصمة أمر اقتضاه وجود الأمية حيث لا يجوز لمن لا يجيد الكتابة والقراءة التوقيع ببصمة الأصبع، بالإضافة لذلك يجب شهادة شاهدين على البصمة وهذا ما أكدته المادة 2/221 من قانون التجارة الأردني بقولها: "ويجب أن يشهد شاهدان على صاحب الختم أو البصمة بأنه وقع أمامها وعلما بما وقع عليه"، وبما أن التوقيع من البيانات الإلزامية الواردة في المادة 228 من قانون التجارة، فإن وجود بصمة إبهام المشتكي عليه على الشيك الخالي من أحد البيانات الإلزامية يعتبر سندا عاديا وليس شكليا ولا عقاب على هذا السند في حال عدم صرفه[3].

بالرغم من أن المشرعين اعتمدوا التوقيع ببصمة الأصبع والتوقيع بالختم كإحدى اشكال التوقيع المعمول به قانونا إلا أن هناك جانبا من الفقه انتقدهما لما لهما من أخطار كتعرضهما للسرقة أو ضياعهما، أو تقليدهما، ومع أن لكلا الشكلين مخاطر، إلا أن التوقيع

1- إيناس الخالدي، "**حجية التوقيع الالكتروني في الإثبات**"، دراسة التعاملات الالكترونية السعودي، كلية الدراسات القضائية والأنظمة، جامعة أم القرى، السعودية، مقال منشور على موقع: www.qu.edu.sa

2- د. عباس العبودي، التعاقد عن طريق وسائل الاتصال الفوري وحجيتها في الإثبات المدني، دار الثقافة للنشر والتوزيع، الأردن، ص 26.

3- إيناس الخالدي، المرجع السابق.

بالختم أكثر خطورة من التوقيع ببصمة الأصبع، ونظرا لاستحالة التشابه ما بين بصمات الأفراد وانفصال الختم عن شخصية صاحبه، أثبت العلم أن التوقيع ببصمة الأصبع أكثر ضمانا من التوقيع بالختم، وقد اقترح هذا الجانب من الفقه في حالة الاستمرار بالعمل بهذين الشكلين وضع الضمانات التي تقلل من النتائج السلبية المفاجئة، ويجوز إثبات واقعة التوقيع بالختم أو ببصمة اليد (الأصبع) على المحرر بطرق الإثبات جميعا[1].

ثالثا: التوقيع بالإمضاء:

الإمضاء هو مجموعة من الخطوط اتخذت شكلا لا يمد بأي صلة إلى الشكل المعتاد للكتابة، بل اتخذ شكلا هندسيا مميزا ويشترط في الإمضاء أن يحدد شخصية صاحبه وأن يصدر عنه لا عن غيره، وأن يكون بأي قلم كان ويكون غالبا في نهاية السند ليعبر عن موافقة الموقع بما ذكر في المحرر[2]، فعندما يضع الشخص توقيعه على السند إنما يعبر عن إرادته في الالتزام بمضمون المحرر وإقراره له، ذلك أن واقعة إلصاق التوقيع بالورقة هي التي تضع للتوقيع أثره، كما أن اشتمال الورقة على توقيع صاحب التعهد هو الذي يجعل لها قيمة قانونية، ولذلك في حالة التوقيع بكتابة الاسم الشخصي أي الإمضاء، فإن الاسم يظهر هنا كما لو كان أداة وضعتها الجماعة تحت تصرف الشخص ليضع إرادته على كتابة معينة، ويتحمل مسؤولية ما ورد بها وليحول بذلك هذه الكتابة المادية إلى تصرف قانوني، كما أن التوقيع بالإمضاء إذا لم يطعن فيه أو لم ينكره صاحبه هو دليل على الحضور الجسدي لصاحبه، ولهذا يستلزم الأمر إذا ضرورة وجود رابطة قوية بين التوقيع والالتزامات المضمنة في الورقة العرفية، بحيث يكون صاحبه على بينة من أمره عالما بمضمون الورقة، قاصداً

1- د. عيسى غسان ربضي، المرجع السابق، ص 35.

2- حابت آمال، التجارة الالكترونية في الجزائر، رسالة لنيل شهادة الدكتوراه في العلوم، تخصص قانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2015، ص ص 106 – 107.

إلى إجازة ما ورد بها، وإلزام نفسه بكل ما ينشأ عنها من تعهدات فإذا انتفت هذه الرابطة فقدت الورقة حجيتها ولم تعد تصلح دليلا للإثبات[1].

الفرع الثاني

وظائف التوقيع التقليدي

تتمثل وظيفة التوقيع القانونية في منح المحرر القوة الثبوتية، وهذه الاخيرة لا يمكن تحقيقها إلا إذا قام التوقيع بوظائفه الموضوعية والتي تنحصر في عنصرين هما تحديد هوية الشخص الموقع والتعبير عن إرادته بالالتزام بمحتويات المحرر باعتبار أن الموقع يعبر عن إرادة صاحبه، لذلك يتوجب أن يصدر من شخص كامل الأهلية، ولا تعتبر الكتابة دليلا كاملا في الإثبات إلا إذا كانت موقعة، فالتوقيع هو العنصر الثاني من عناصر الدليل الكتابي المعد أصلا للإثبات، وبدون التوقيع يفقد الدليل الكتابي حجيته، وبذلك فإن التوقيع هو الذي ينسب الورقة إلى من وقعها حتى ولو كتبت بخط غيره[2].

أولا: تحديد هوية الشخص الموقع

يحقق التوقيع هذه الوظيفة مهما كان شكله، وبالعودة للنصوص القانونية، نجد نص المادة الثانية من قانون البيانات الأردني لسنة 1952 أقرت هذه الوظيفة بنصها: "من أحتج عليه بسند عادي وكان لا يريد أن يعترف به، وجب عليه أن ينكر صراحة ما هو منسوب إليه من خط أو توقيع أو ختم أو بصمة أصبع، وإلا فهو حجة عليه"، فعبارة ما هو منسوب إليه أشارت بوضوح الى ان طريقة التوقيع تدل على الشخص الموقع وتحدد هويته، ففي

1- اياد محمد عارف عطا سده ،المرجع السابق ،ص 55 .

2- كريم لملوم ، المرجع السابق ، ص 108.

الإمضاءات فإن كل شخص يختار إمضاء معين يصبح معرفا له، وبالتالي يصبح محدد الهوية[1].

كذلك الحال مع الختم، فالشخص عندما يختار ختما معينا، فإنه يحدد هوية ذلك الشخص نظرا لكونه علامة مميزة للشخص، وغالبا يحتوي على اسمه وبعض البيانات الخاصة به، كذلك البصمة، نجد إنها قادرة على تحديد هوية صاحبها بسبب عدم وجود مجال التشابه بين البصمات، لذلك أقرتها القوانين كوسيلة للتوقيع، إذ إنه عندما يقوم نزاع بشأن صحتها ونسبتها لشخص ما، فإن علم البصمات يستطيع تحديد عائدية البصمة للشخص الموقع من عدمه، وبالتالي تحديد هوية الشخص الموقع[2].

ثانيا: التعبير عن الإرادة بالالتزام بالتصرف في مضمون السند

التوقيع يشكل أداة صحة، بمعنى أنه يعطي التصرف القانوني قوة وقيمة أكبر،فان التوقيع بالإمضاء والذي يستخدم الاسم، هو المتعارف عليه في القانون الفرنسي، يضاف إليه التوقيع بالختم وببصمة الأصبع في كل من القانون المصري والكويتي، مع التحفظ على ما لهاذين النوعين من التوقيعات من معايير وشروط، ما يعطي ضمانا على كون صاحبه أو الموقع ملتزم ومقر بمضمون العقد ، بالتالي فالتوقيع يعطي التصرف القانوني قيمة وقوة أكبر، لذلك فلابد من أن يعبر التوقيع عن إرادة الموقع في الالتزام بالتصرف القانوني، فبالنسبة للإمضاء نجد أن إمضاء الشخص على سند ما، يعني أنه اطلع عليه وعلم بما فيه،

1- علاء محمد نصيرات، حجية التوقيع الالكتروني في الإثبات (دراسة مقارنة)، دار الثقافة للنشر و التوزيع، الأردن، 2005، ص 67.

2- كريم لملوم، المرجع السابق، ص ص 108 – 109.

بالتالي فهو موافق على ما جاء فيه ومقرا به، وهو من أفضل الوسائل لذلك إذ جاء جاء مطابقا للأوضاع القانونية المطلوبة في الإمضاء[1].

يأخذ القضاء بعين الاعتبار ما تعرف عليه الأشخاص في توقيعاتهم للتدليل على توافر نية التوقيع لدى الموقع، فمثلا عندما يستخدم أحد الأشخاص الاسم المستعار، يعتبر القضاة بأن لديه نية التوقيع، وبالتالي يتم الرجوع إلى عادات الأشخاص المعنيين بالأمر للوصول إلى توافر نية التوقيع من عدمه، ونية التوقيع يمكن أيضا إثباتها بالاستعانة بعناصر داخلية للتصرف لا تكون ضمن عناصر التوقيع، فمن المتعارف عليه أن مكان التوقيع يكون في آخر التصرف، وبالتالي فوضعه في مكان آخر يثير الشكوك حول مدى توافر الرغبة في التوقيع لدى الموقع من عدمه.

نجد كذلك من ضمن العناصر التي يمكن الاستعانة بها، الوقت الذي يوضع فيه التوقيع، أي التوقيع على بياض، وهو التوقيع الذي يوضع على ورقة بيضاء وتتم الكتابة عليها بعد ذلك وهو توقيع صحيح وله قيمة ويحتج به في مواجهة الموقع[1]

أما البصمة وإن كانت تحدد هوية الموقع، إلا أنها أثارت شكوكا وجدلا حول مدى تعبيرها عن إرادة الموقع، مما ادى بالبعض إلى رفض اعتبارها كوسيلة للتوقيع، لكن انتشار الأمية جعل بعض الدول تأخذ بها كوسيلة توقيع على اعتبار أنها قادرة على التعبير عن إرادة الموقع بالموافقة على مضمون السند، ومن الأفضل إحاطة هذه الوسيلة بضمانات معينة حتى تؤدي وظيفتها بصورة فعالة، فمثلا المشرع العراقي اشترط وجوب حضور شاهدين يوقعان على السند، أو حضور موظف مختص يصادق على السند، كذلك فعل المشرع الأردني في مجال التوقيع على الأوراق التجارية بواسطة البصمة.

2- علاء محمد نصيرات، المرجع السابق، ص 71.

أما الختم فيمكن القول فيه ما قيل في البصمة من حيث التشكيك في قدرته على التعبير عن إرادة الموقع، لكن يمكن القول بأن الختم والبصمة يدلان على إرادة الموقع بالموافقة على مضمون السند إذا ما روعي في ذلك إجراءات وشروط معينة، ويبقى للقاضي دور في استخلاص نية التوقيع من عدمه، وذلك بالاستعانة بعناصر داخلية في التصرف، تدخل ضمن عناصر التوقيع مثل مكان التوقيع وورقته وغيره، وعليه إذا ما تم التوقيع صحيحا فإنه يعطي للسند القوة القانونية، ويحوله لتصرف قانوني ملزم لأطرافه الموقعين[1].

1- عايض راشد عايض المرئ، مدى حجية الوسائل التكنولوجية الحديثة في اثبات العقود التجارية، رسالة دكتوراه، جامعة القاهرة، مصر، 1998، ص 87

المبحث الثاني

ماهية التوقيع الالكتروني

يكتسي التوقيع الالكتروني أهمية بالغة في إثبات المعاملات الالكترونية لذلك عرف اهتمام وافر من قبل المشرعين والفقهاء على حد سواء، ولهذا فقد تم البحث عن بديل للتوقيع التقليدي يكون قادرا على التناسب مع مميزات العقد الالكتروني فنتج التوقيع الالكتروني واعترف به بشكل قانوني مع تطور التكنولوجيا الحديثة وانتشارها عبر العالم. وبدأت الخطوات العلمية في تعميم استخدامه ليكون أداة من أدوات التعاملات المستقبلية بين الناس حيث أنها تسهل على مستخدمي شبكة الانترنت أعمالهم ومهامهم، وقد حظي قطاع الأعمال الالكترونية بدعم كبير ودفعة قوية من قبل الحكومات من خلال وضع قرارات وتشريعات هامة خاصة بالتوقيع الالكتروني لإضفاء الشرعية والصفة القانونية عليها، لتكون كالتوقيع التقليدي تماما في التعاملات المالية والتجارية سواء كان من خلال النصوص التشريعية الخاصة بالتجارة الالكترونية أو بعض مشاريع القوانين الخاصة بالتجارة الالكترونية أو الخاصة بالتوقيع الالكتروني، فالتوقيع الالكتروني هو عبارة عن ملف رقمي صغير (شهادة رقمية) تصدر عن إحدى الهيئات المتخصصة والمستقلة والمعترف بها من الحكومة تماما، مثل جهة تصديق وإصدار التواقيع أو أي جهة يتم اعتمادها من طرف الحكومة، فيتم تخزين اسم صاحب التوقيع مفتاحين عما: المفتاح العام والمفتاح الخاص، ويعتبر المفتاح الخاص هو التوقيع الالكتروني الذي يميز صاحبه عن غيره، أما المفتاح العام فيتم نشره في الدليل ليكون متاحا للكافة ليتمكنوا من التأكد من صحة التوقيع وأنه عائد لصاحبه، و في هذا المبحث سوف نتطرق إلى مفهوم التوقيع الالكتروني وصوره (المطلب الاول)،مدى تحقيق التوقيع الالكتروني لوظائف التوقيع التقليدي وشروطه(المطلب الثاني).

المطلب الأول

مفهوم التوقيع الالكتروني و صوره

لإتمام إبرام العقد الالكتروني بين طرفي العلاقة العقدية، وليكون لهذا التصرف قيمة قانونية في إتمام التعاقد والآثار المترتبة عليه ولإثباته كان من الضروري أن يتم التوقيع عليه ممن صدر عنه، ليكسب هذا العقد درجة عالية من الإلزام لطرفي العلاقة، فإن استخدام العقد الالكتروني المبرم عبر الأنترنيت وحلوله محل العقد التقليدي، يتطلب إيجاد بديل للتوقيع التقليدي الذي يتبلور من خلال عدة أشكال نص عليها المشرع، فقد تكون إمضاء أو بصمة أو ختم إلا أن التطور أدى إلى البحث عن طرق ووسائل حديثة في التعامل بين طرفي العقد الالكتروني، إلا أن هذا الاخير لا يتفق مع فكرة التوقيع التقليدي الذي من المتوقع أن لا يجد مجالا له في ظل النظام الالكتروني الحديث، ذلك النظام الذي بدأت كافة المؤسسات العامة والخاصة والحكومية باستخدامه وإدخاله في أنظمة العمل لديها والاستغناء عن الإجراءات التقليدية التي أصبحت إحدى المعيقات التي تواجه تطور عصر المعلوماتية واستخدام الانترنت.

وهذا ما سنتناوله في هذا المطلب حيث سنقسمه إلى فرعين: الفرع الأول (تعريف التوقيع الالكتروني) ، الفرع الثاني (صور التوقيع الالكتروني).

الفرع الأول

تعريف التوقيع الالكتروني

تختلف التعاريف التي أطلقت على التوقيع الالكتروني، باختلاف النظرة إليه، فالبعض يعرفه بناءً على الرسائل التي يتم بها، أو يحسب الوظيفة أو الدور الذي يؤديه التوقيع، أو بناءً على التطبيقات العملية للتوقيع ويقصد بالتوقيع الالكتروني الرمز المصدري أو الرقم السري الذي يتم إدخاله في جهاز الحاسب عن طريق وسائل الإدخال، ليتم من خلاله إنجاز بعض المعاملات باتباع إجراءات محددة متفق عليها بين أطراف الالتزام وضمن الحدود التي تم الاتفاق عليها بين طرفي العلاقة القانونية[1].

كما عرف أيضا بأنه: "مجموعة من الإجراءات التقنية التي تسمح بتحديد شخصية من تصدر عنه هذه الإجراءات وقبوله بمضمون التصرف الذي يصدر التوقيع من أجله"[2].

وعرف التوقيع الالكتروني أيضا على أنه مصطلح نشأ نتيجة ازدهار التجارة الالكترونية والحاجة إلى تحديد هوية كل طرف من الأطراف عبر وسائل الاتصال، ومعرفة ما إذا كان قد انصرفت إرادة كل طرف إلى الموافقة على مضمون المحرر، ولذلك فإن الأمر يتطلب البحث في مدى تحقيق التوقيع الالكتروني لوظائف التوقيع التقليدي، إذ أن هذه المسألة يتوقف عليها مدى الاعتراف القانوني بالتوقيع الالكتروني إن كان سيحقق تلك الوظائف أو عدم الاعتراف به إن عجز عن ذلك[3].

1- محمد فواز المطالقة، الوجيز في عقود التجارة الالكترونية، التوقيع الالكتروني، أركانه، إثباته، القانون الواجب التطبيق (حماية التشفير)، جامعة البلقان التطبيقية، دار الثقافة للنشر والتوزيع، 2006، ص ص 132 – 133.

2- محمد فواز المطالقة، المرجع السابق، ص 173.

3- د هالة جمال الدين محمد محمود، المرجع السابق، ص ص 329 – 330.

ولقد عرف التوقيع الالكتروني مشروع قانون المبادلات والتجارة الالكترونية الفلسطيني في المادة الأولى بأنه: "بيانات في شكل الكتروني مدرجة في رسالة بيانات أو مضافة إليها أو مرتبطة بها منطقيا، يجوز أن تستخدم لتحديد شخصية الموقع بالنسبة إلى رسالة البيانات"، وهذا النص موافق لنص المادة 2 من قانون الأونيستيرال النموذجي.

أيضا عرف الم.ا في قانون المعاملات الالكترونية التوقيع الالكتروني في المادة الثانية منه بأنه: "البيانات التي تتخذ هيئة حروف أو أرقام أو رموز أو إشارات أو غيرها وتكون مدرجة بشكل الكتروني أو رقمي أو ضوئي أو أي وسيلة أخرى مماثلة في رسالة معلومات أو مضافة اليها أو مرتبطة بها ولها طابع يسمح بتحديد هوية الشخص الذي وقعها ويميزه عن غيره من أجل توقيعه وبغرض الموافقة على مضمونه".

أما المشرع المصري قد عرفه في المادة الاولى من قانون تنظيم التوقيع الالكتروني بأنه: "ما يوضع على محرر الكتروني ويتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها ويكون له طابع منفرد يسمح بتحديد الشخص الموقع ويميزه عن غيره"، أما قانون المعاملات في إمارة دبي فقد عرفه من خلال نص المادة الثانية: "توقيع مكون من حروف أو أرقام أو رموز أو صوت أو نظام معالجة ذي شكل الكتروني وملحق مرتبط الكترونيا برسالة الكترونية ومعهود بنية توثيق أو اعتماد تلك الرسالة"[1].

لقد منح قانون الاونيستيرال النموذجي بشأن التجارة الالكترونية رسائل البيانات الالكترونية حجية في الإثبات، كما اعترف بالتوقيع الالكتروني وسوى بينه وبين التوقيع التقليدي غير أنه عند الاطلاع على مواد قانون الأمم المتحدة النموذجي بشأن التجارة الالكترونية، نجد أنه لم يعرف التوقيع الالكتروني واكتفى في مادته السابعة بالإشارة للشروط الواجب توافرها في التوقيع، حيث نصت الفقرة الأولى منها على أنه: "عندما يشترط القانون

1- إياد محمد عارف عطا سده، المرجع السابق، ص ص 59 – 60.

وجود توقيع من شخص يستوفي ذلك الشرط بالنسبة إلى رسالة البيانات إذا استخدمت طريقة لتعيين هوية ذلك الشخص والتدليل على موافقتة على المعلومات الواردة في رسالة البيانات كانت تلك الطريقة جديدة 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].

ولقد أجرى المشرع الجزائري تعديلا في مواد الإثبات من القانون المدني بما يتلاءم مع تقنيات الاتصال الحديثة والتوقيع الالكتروني بالقانون رقم 10/05 المؤرخ في 20 جويلية 2005، لكنه لم يضع تعريفا للتوقيع الالكتروني على الرغم من أنه لم ينكر التعامل به، فبالرجوع إلى نص المادة 327 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 أنه: "يعتبر الإثبات بالكتابة في الشكل الالكتروني كالإثبات بالكتابة على الورق بشرط إمكانية التأكد من هوية الشخص الذي أصدرها وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها وهذه الشروط هي إمكانية التأكد من هوية الشخص الموقع وأن تكون منظومة إنشاء التوقيع الالكتروني محفوظة في ظروف تضمن سلامته".

وقد جاء في نص المادة 2/323 كما يلي: "يعتد بالتوقيع الالكتروني وفقا للشروط المذكورة في المادة 323 مكرر1"، أما عن تعريف التوقيع، فإن القانون الجزائري ميز بين التوقيع المؤمن وذلك بموجب المادة 3 من المرسوم التنفيذي 162/07[2]، التي جاء فيها أن "التوقيع الالكتروني هو أسلوب عمل يستجيب للشروط المحددة في المادتين 323 مكرر

1- لالوش راضية، أمن التوقيع الالكتروني، مذكرة لنيل شهادة الماجستير في القانون، فرع القانون الدولي للاعمال، كلية الحقوق و العلوم السياسية،2012 ،ص 24.

2- لالوش راضية ، المرجع السابق، ص 25. انظر كذلك المرسوم التنفيذي رقم 07-162 مؤرخ في 30 ماي 2007 يعدل و يتمم المرسوم التنفيذي رقم 01-123 و المتعلق بالنظام المطبق على كل نوع من انواع الشبكات بما فيها اللاسلكية الكهربائية ،ج ر رقم 37 .صادر في 07-06-2007.

و323 مكرر1 حيث أنه اعتبر التوقيع الالكتروني المؤمن هو توقيع الكتروني 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 الالكتروني استكمالا باعترافه بحجية الكتابة في الشكل الالكتروني في المادة 323 مكرر 1 وذلك تماشيا مع إفرازات التطور التكنولوجي الذي أدخل وسائل حديثة في إبرام العقود والتوقيع عليها الكترونيا إلا أنه يؤخذ على المشرع الجزائري عدم إصدار نص قانوني أو مرسوم يبين كيفية تنظيم هذا التوقيع الالكتروني ويحدد إطاره العام ويوضح مفاهيمه القانونية، على غرار التشريعات المقارنة، لذلك على الجزائر أن تضعه حيز التنفيذ وذلك قصد إعطاء الدفع للمبادلات الالكترونية والتجارة الالكترونية بأكملها تطوير التجارة الخارجية لأي بلد[1].

الفرع الثاني

صور التوقيع الالكتروني

من دراستنا للتوقيع الالكتروني ومحاولة إيجاد تعريف مانع جامع له من خلال التطرق لبعض التعريفات التي نصت عليها التشريعات الخاصة بالتجارة الالكترونية العربية وقانون الأونيسترال النموذجي، حاولنا التوصل من الآراء السابقة لاستخلاص بعض الشروط الواجب توافرها في التوقيع لإضفاء نوع من الحجية عليه، لأنه من أهم وسائل إبرام العقود وحمايتها

1- لالوش راضية، المرجع السابق، ص ص 25 – 26.

من أي اعتداء يمكن أن يمارس على هذه التصرفات المبرمة عبر الأنترنت فتم اعتماده في المعاملات اليومية سواء كانت تجارية أو مدنية[1].

لقد بيننا في الفرع الأول الخاص بتعريف التوقيع الالكتروني أن أغلب التشريعات لم تحدد نوعا معينا من التوقيع، ولم تحدد على سبيل الحصر ماهية هذه التواقيع التي يكون لها حجية في الإثبات على أن من ذكر بعضا من هذه الأنواع ذكرها على سبيل المثال لا الحصر تاركا المجال مفتوحا كي يتسع هذا التعريف لما يستجد من تطورات تكنولوجية قد تفرز أشكالا وصورا جديدة من التواقيع الالكترونية فكما أن التوقيع التقليدي متعدد الأشكال والصور إذ يتخذ شكل الإمضاء أو الختم أو بصمة الأصبع، فإن التوقيع الالكتروني أيضا لا يتخذ شكلا واحدا وإنما أفرز التقدم التكنولوجي العديد من الصور والأشكال لهذا التوقيع والتي يمكن أن تؤدي المهمة نفسها التي يؤديها التوقيع العادي لا بل قد تتفوق عليه في العديد من الجوانب، لهذا فقد عرفت في وقتنا الحاضر العديد من الصور للتوقيع الالكتروني[2]، نتناولها فيما يلي:

أولا: التوقيع بالقلم الالكتروني

التوقيع بالقلم الالكتروني يتم إجراؤه من خلال الاستعانة ببرامج خاصة يتم إعدادها لتتناسب والقلم الالكتروني من خلال الربط بجهاز الحاسب الآلي، ليتم قراءة البيانات التي تعرض على القلم ومن خلال الحركات التي يتم القيام بها أثناء تحريكه على الشاشة ليتم رسم أو إنشاء الشكل الذي يظهر التوقيع من خلاله.

1- محمد فواز المطالقة، المرجع السابق، ص 179.

2- د. علي أبو مارية، التوقيع الالكتروني ومدى قوته في الإثبات "دراسة مقارنة"، مجلة جامعة الخليل للبحوث، كلية الحقوق، قسم القانون الخاص، جامعة فلسطين الأهلية، بيت لحم، المجلد 5 ،العدد 2، سنة 2010، ص 111.

هذا الأمر يقوم بأداء وظيفتين هما: القيام بالتقاط إمضاء العميل الذي يتم كتابته بقلم الكتروني ضوئي حساس في المكان المخصص لذلك على شاشة الحاسب أو أي مكان مخصص له، بعد أن يتم إدخال الرقم السري الخاص به من خلال بطاقة تحتوي على بيانات خاصة بصاحبها، فيتم إدخال البطاقة التي تحتوي على بيانات كاملة عن مركز هذا العميل، كما يتم من خلال استخدام القلم الالكتروني التحقق من صحة توقيع العميل وبيان إلى من يعود هذا التوقيع من خلال مقارنته مع التوقيع الأصلي للعميل المحفوظ والمودع لدى جهة الإيداع أو على الموقع الالكتروني الخاص أو على القرص الصلب لجهاز الحاسب الآلي[1].

وتتم هذه العملية (Op-pen) عن طريق نقل التوقيع المحرر بخط اليد عن طريق التصوير بالماسح الضوئي (Scanner) ثم تخزينه في جهاز الحاسوب، ولقد توصلوا إلى أن هذه الطريقة بشكل عام تخلو من أدنى درجات الأمان الواجب تحقيقها في التوقيع في الشكل الالكتروني، بحيث باستطاعة المرسل إليه في هذه العملية الاحتفاظ بنسخة من صورة التوقيع التي وصلته على أحد المحررات، ثم يقوم بإعادة رصدها على أية وثيقة محررة عبر وسيط الكتروني ويدعي أن واضعها هو صاحب التوقيع الفعلي[2].

ثانيا: التوقيع الرقمي

جاءت فكرة التوقيع الرقمي من فكرة الرموز السرية والمفاتيح غير المتماثلة، فهذا التوقيع يعتمد على المعادلات الرياضية المعقدة من الناحية الفنية، وتم إيجاد هذا النوع

1- د. محمد فواز المطالقة، المرجع السابق، ص ص 179 – 180. وللمزيد من المعلومات حول التوقيع بالقلم الالكتروني راجع لالوش راضية المرجع السابق، ص ص 44 – 45.

2- بشار محمود دودين، الإطار القانوني للعقد المبرم عبر شبكة الانترنت وفقا لقانون المعاملات الالكترونية وبالتأصيل مع النظرية العامة للعقد في القانون المدني، رسالة ماجستير، دار الثقافة للنشر والتوزيع، د ط، سنة 2006، ص ص 249 – 250.

كطريقة من طرق الأمان التي يسعى إليها المتعاقدان عند إبرام العقود أو إجراء أي تصرف عبر الانترنت.

فهذه الصورة يتم استخدامها لتحديد هوية طرفي العقد، تتضمن عدم إمكانية تدخل أي من الطرفين أو أي شخص آخر في مضمون التوقيع وشكله، محققا بذلك كافة الشروط التي يتطلبها المشرع ويتم استخدام هذا النوع في أغلب المعاملات الالكترونية وبالذات في المعاملات البنكية من خلال استخدام بطاقات الائتمان التي تتضمن رقما سريا خاصا بالعميل، فالرقم السري يكون خاصا بالعميل صاحب التوقيع ولا يكون من حق أي شخص التعرف عليه، لأنه خاص بالعميل بالذات ولا يمكن لأي شخص آخر معرفة هذا الرقم ، وفي حالة التعامل مع هذا النوع من خلال نظامي (Ofline)، (Online) أي الخطين المباشر وغير المباشر المربوطين على شبكة الانترنت ففي النظام الأول يتم التسجيل على شريط ممغنط وفي حال الانتهاء من إدخال الرقم يتم السماح للمستخدم بإتمام العملية التي يرغب بها، وفي حالات انتهاء ساعات العمل يتم إتمام التصرف، أما النوع الثاني فيتم إجراء العملية بشكل مباشر وفوري مع الانتهاء من إدخال البيانات فإن العملية التي تكون قد تمت بشكل كامل، يتم ذلك في أغلب البطاقات الذكية التي يتم حفظ كافة العمليات التي تتم بذاكرتها[1]، التي يتطلبها المشرع في المحررات الالكترونية لكي تصلح لأن تكون دليلا كاملا في الإثبات، مع ضرورة الإشارة إلى أنه يتوجب إيجاد أو خلق جهات متخصصة رسمية كانت أو خاصة تشرف عليها الدولة بحيث تقوم على تسجيل التوقيع الرقمي وإصدار شهادات تدل على صحته لكي يتم تحقيق جميع الآثار القانونية المرجوة منه وبشكل يعترف به القانون[2].

1- د. محمد فواز المطالقة، المرجع السابق، ص ص 180 – 181. ، ص ص 50 – 51.

2- بشار محمود دودين، المرجع السابق، ص 255.

ثالثا: التوقيع باستخدام الحواس الذاتية (التوقيع البيومتري)

تعتمد هذه الصورة على العلامات المميزة لكل شخص كالبصمة بواسطة الأصبع أو بصمة شبكة العين أو نبرة الصوت أو الحمض النووي (DNA) وغيرها من الخصائص الذاتية للإنسان، وتتم هذه العملية عبر استقبال جهاز الحاسب الآلي وكاميرا وجهاز لقراءة البصمة، من أجل تمييز هوية المستخدم ثم تخزين العلامة المميزة للشخص في جهاز الكمبيوتر بطريقة مشفرة في ذاكرة الحاسب عند الرغبة في إجراء أي عملية لاحقة لا يسمح للشخص بالدخول في هذا النظام إلا إذا تطابقت المعلومات الخاصة بالشخص مع ما هو مسجل ومشفر داخل جهاز الكمبيوتر حيث قامت شركة (Litonic) بإدخال نظام توقيع يعتمد على الخصائص البيولوجية للإنسان بتاريخ 2000/08/14 فوفقا لهذا النظام عندما يقوم شخص بتوقيع مستند الكتروني يتم التحقق من هويته من خلال تلك الخصائص المميزة له[1]، لكن تلك الآلية مازالت في مرحلة الاختبار الأولى، لأن استعمالها يصطدم بعدة عقبات منها:

1- احتمال تغيير بعض خصائص الإنسان بفعل الظروف، كتآكل بصمات الأصابع عبر الزمن، أو بفعل بعض المهن اليدوية، أو تأثير التوتر على نبرة الصوت، أو بتشابه أشكال أوجه التوائم.

2-أيضا يؤخذ على هذا النوع من التوقيع أن صورته يتم وضعها على القرص الصلب للحاسوب، ومن ثم يمكن مهاجمتها أو نسخها بواسطة الطرق المستخدمة في القرصنة الالكترونية.

1- إياد محمد عارف عطا سده، المرجع السابق ص 75.

3-كذلك لا يمكن استخدام هذه التقنية في جميع الحسابات المتوفرة لاختلاف نظم التشغيل والتخزين.

4-كما يحتاج هذا النوع من التوقيع لاستثمارات ضخمة لكي يتمكن مستعملوا الشبكة الالكترونية من استخدام الخواص الذاتية للشخص الموقع في التوقيع الالكتروني، وهذا ما حد من انتشاره إلى درجة كبيرة، واقتصر استخدام هذه التقنيات حاليا على أجهزة الأمن والمخابرات كوسيلة للتحقق من الشخصية وتحديد استخدام المرخص لها[1].

5-يرى البعض أن هذه الصورة من التوقيع من الممكن أن تزور عن طريق ارتداء عدسات لاصقة يتم تصميمها بالكمبيوتر بحيث تطابق رسمة قرصية العين للشخص المراد انتحال شخصيته، كذلك فإن بصمة الصوت من الممكن تسجيلها ثم إعادة التسجيل بعد ذلك والدخول للنظام وكذلك بصمة الأصبع من الممكن وضع مادة بلاستيكية أو مطاطة مطابقة تماما لبصمة أصابع الشخص صاحب التوقيع[1].

رابعا: التوقيع بواسطة الرقم السري المقترن بالبطاقة الممغنطة

تعتبر هذه الصورة الأكثر انتشارا في المعاملات الالكترونية، خاصة المعاملات البنكية حيث درجت البنوك على إصدار بطاقات ذكية، بطاقات بلاستيكية، مصحوبة برقم سري يتمثل في أرقام أو حروف أو رموز تمنحها لعملائها لاستخدامها في سحب وإيداع النقود أو لسداد ثمن السلع والخدمات، وتتم عملية سحب النقود أو إيداعها أو عملية الدفع الالكتروني من خلال جهاز آلي تؤمنه البنوك للعملاء كجهاز الصراف الآلي (ATM) أو جهاز الدفع الالكتروني الموجود في المحلات التجارية، أي المحلات التي تقبل الدفع بهذه البطاقة بموجب اتفاق مع الجهة المصدرة لها.

1- إياد محمد عارف عطا سده، المرجع السابق، ص ص 76 – 77.

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

- إدخال البطاقة التي تحتوي على البيانات الخاصة بالعميل بالوضع الصحيح على فتحة خاصة في جهاز الصراف الآلي (ATM).
- إدخال الرقم السري المخصص له الذي يعد بمثابة التوقيع وذلك بكتابته بواسطة لوحة المفاتيح الموجودة على الجهاز الآلي، فإذا كان الرقم صحيحا فإن 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[1].

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 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 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.

يوجد نظامين تعمل عليهما أجهزة الصرف الآلية (ATM) الأول يعرف بنظام الدفع غير المباشر (Off.line)،في حالة استخدام هذا النظام، يقوم جهاز التاجر بتسجيل العملية التي أنجزها العميل على شريط مغناطيسي ولا يتغير موقفه المالي كما هو حتى يتم نقل هذه

1- لالوش راضية، المرجع السابق، ص ص 40 – 41.

الشرائح المغناطيسية إلى الجهة المصدرة للبطاقة البنكية حسب المدة الزمنية المتفق عليها يومين أو أسبوعين ليقوم موظف البنك في النهاية بتوقيف هذه العملية عن طريق تسجيلها في الحاسب المركزي التابع للجهة مصدرة البطاقة.

يعرف النظام الثاني بنظام الدفع المباشر (On.line) وهو يقوم فورا وبمجرد انتهاء العميل من العملية بتحديد موقفه المالي.

يتميز هذا الشكل أو هذه الصورة من التوقيع الالكتروني بالإضافة إلى سهولته وبساطته، بقدر كبير من الآمان والثقة، كما أنه يتميز بقدرته على تحديد هوية الشخص الموقع، فاتباع العميل الإجراءات التي ذكرناها سابقا، يؤكد أن من قام بالعملية المصرفية هو الشخص صاحب الرقم السري[1].

1- لالوش راضية، المرجع السابق، ص ص 41 – 42.

المطلب الثاني

مدى تحقيق التوقيع الالكتروني لوظائف التوقيع وشروطه

ان الاعتراف بالتوقيع الالكتروني مقرون بتحقيقه لوظائف التوقيع المعروفة والمتمثلة في تحديد هوية الشخص الموقع والتعبير عن إرادته، وقصد التحقق من ذلك لابد من التحقق من قدرة التوقيع الالكتروني على تحقيق شروط التوقيع.

فبعد أن رأينا أن التوقيع الالكتروني هو شكل جديد من أشكال التوقيع المعروفة، كالتوقيع الخطي بالإمضاء أو بالختم أو بالبصمة فإن التوقيع الالكتروني يجب أن يتمتع بشروط التوقيع التقليدي.

الفرع الأول

مدى توفر شروط التوقيع في التوقيع الالكتروني

أولا: أن يكون علامة مميزة للشخص الموقع

يمكن اعتبار التوقيع الالكتروني من قبيل العلامات المميزة للشخص وحده دون غيره فالتوقيع البيومتري القائم على الخصائص الذاتية للشخص، أو التوقيع بالرقم السري أو بالقلم الالكتروني أو التوقيع الرقمي، كلها علامات مميزة ومحددة للشخص الموقع[1].

فالتوقيع البيومتري يقوم على أساس الخواص الذاتية للشخص التي يتميز بها عن غيره، كذلك الرقم السري لا يمكن أن يشابه شخصا بنفس الرقم السري داخل النظام الواحد، فهو يميز كل شخص عن غيره، فلا يستطيع أحد استخدام الرقم السري لشخص آخر ولا يمكنه

1- كريم لملوم، المرجع السابق. ص142.

أن يعرفه بأية طريقة إلا بإهمال من صاحبه، كذلك التوقيع بالقلم الالكتروني، فإننا نجده مثل الإمضاء العادي له قدرته على تمييز الشخص الموقع عن غيره، ويتمتع بقدر من الحماية، فلا يمكن إنجازه إلا إذا طابق التوقيع المخزن في ذاكرة الحاسوب أما بالنسبة للتوقيع الرقمي فهو كالرقم السري خاص بصاحبه ويستطيع أن يميزه عن غيره فهو يقوم على مفتاحين عام وخاص، المفتاح الخاص لا يعلمه إلا الشخص الموقع، وعند استخدام هذا التوقيع يستطيع الشخص الذي يصله التوقيع أن يتحقق من صحته بواسطة سلطات الإشهار التي تؤكد صحة التوقيع وعليه فإن لكل شخص توقيع رقمي مميز له[1].

ثانيا اتصال التوقيع بالسند

يجب أن يكون التوقيع الالكتروني متصلا بالمحرر الالكتروني حتى يمكن أن يثبت إقرار الموقع بمضمون السند، هذا يكون أساسا بالاعتماد على التقنيات المستخدمة ومدى كفاءتها في تأمين مضمون المحرر المدون الكترونيا، وبالتالي تأمين ارتباطه بشكل لا يقبل الانفصال عن التوقيع ومن أهم هذه التقنيات، تقنية التوقيع الرقمي، الذي يتمتع بنوع من الأمان يجعله يرتبط بالمحرر على نحو لا يمكن فصله ولا يمكن لأحد غير صاحب المحرر المدون على هذا النحو التدخل بتعديل مضمونه.

ثالثا: أن يكون التوقيع واضحا ومستمرا

يعد التوقيع شكلا من أشكال الكتابة، بالتالي يخضع للشروط المقررة للكتابة من حيث إمكانية الاطلاع عليه وقراءته بشكل مباشر أو باستخدام الآلة، فيجب أن يتم تحريره بشكل يتيح الرجوع إليه لاحقا، وهي شروط يمكن تحققها في التوقيع الالكتروني كونه يحمل بيانات مختلفة يمكن قراءتها باستخدام الكمبيوتر، الذي يحتوي على برامج لها القدرة على ترجمة لغة

1- كريم لملوم، المرجع السابق، ص ص 144 – 145.

الآلة التي تتكون من توافق وتبادل بين الأرقام إلى لغة مقروءة للإنسان، أما الاستمرارية فهناك نوع من الشك نظرا للطبيعة المادية والكيميائية للحوامل الالكترونية التي تتميز بالحساسية التي تجعلها دائما عرضة للتلف السريع إلا أن هذه المشكلة قد تم التغلب عليها بالاعتماد على وسائط أكثر جودة ولها القدرة الكافية على حفظ البيانات لمدة تفوق مدة حياة الورق[1].

الفرع الثاني

أهم وظائف التوقيع الالكتروني وخصائصه

أولا: وظائف التوقيع الالكتروني

كما هو الحال بالنسبة للتوقيع التقليدي تجمعت التشريعات والفقه على أن التوقيع الالكتروني حتى يحوز على القوة الثبوتية، فلابد ومن خلال التعريفات السابقة له من أن يحقق وظيفتين تتمثل أولهما:

1. تحديد هوية الموقع على المحرر والتعريف بشخصيته:

حيث أنه كما هو الوضع فالتوقيع التقليدي، منبثق عن الشخص الموقع ويعتبر امتدادا لهذه الشخصية لدرجة يصعب معها انفصال أحدهما عن الآخر أو حتى صدوره من غيره فيما لو استوفى ما تتطلبه التشريعات من شروط.

2. التعبير عن إرادة الموقع وقبوله بموضوع المحرر ومضمونه:

1- كريم لملوم، المرجع السابق، ص 145.

التوقيع إذا ما وضع على المحرر ولم يثبت الموقع أنه أرغم عليه أو ادعى تزويره، كما لو قام شخص آخر باستخدامه، فإنه يكون معبرا عن إرادة من صدر عنه، وبالتالي يكون حجة كاملة في الإثبات، ويذهب البعض الآخر إلى أن هناك وظيفة ثالثة يقوم بها التوقيع الالكتروني وتتمثل في الحفاظ على مضمون السند وسلامته أي سلامة ما يحتويه من معلومات عن طريق ما يتخذه من شكل جديد في البيئة الرقمية، وبذلك فإن التوقيع الالكتروني لابد من أن يحقق الوظائف التالية[1]:

أ- الدلالة على هوية الموقع

تعد من أولى أهم وظائف التوقيع لأنها تدل على هوية الشخص الموقع وهذه الوظيفة أشارت إليها المادة 16/1 من قانون البيانات الفلسطيني والتي جاء فيها ما يلي: "يعتبر السند العرفي حجة على من وقعه ما لم ينكر ما هو منسوب إليه من خط أو إمضاء أو ختم أو بصمة عند اطلاعه عليه، ويعتبر سكوته إقرارا بصحة ما نسب إليه"[2]، فهذا النص يوضح أن التوقيع المعتمد لابد من أن يحدد بوضوح شخصية الموقع بغض النظر عن الشكل الذي يتخذه ذلك التوقيع، سواء تم بالإمضاء أو بالختم أو بالبصمة فجعل السند العرفي حجة على موقعه ما دام هذا الشخص لم ينازع في صحته وسكوته اعتبره المشرع إقرارا بصحة ما نسب إليه من توقيع، وبالنظر إلى التوقيع الالكتروني، فإننا نجده يحقق هذه الوظيفة إذا ما روعيت فيه وسائل وإجراءات موثوق بها يتم اعتمادها، وتتمثل في عدد من الأنظمة المختلفة تمثل أنواع التوقيعات الالكترونية، كالتوقيع بالبصمة الالكترونية أو بالقلم الالكتروني أو باستخدام

1- د. علي أبو مارية، المرجع السابق، الصفحة الالكترونية للمجلة http://www.hebron.edu/journal/ ، ص ص 113- 114.

2 - المرجع نفسه، ص 114.

نظام التشفير بأشكاله، فهذه الوسائل المختلفة تمكن من التعرف على هوية أطراف المعاملة التي أوجدوها من خلال الربط بين هوياتهم والنصوص والرسائل التي يتبادلونها.

كما أكدت على هذه الوظيفة للتوقيع الالكتروني أغلب تشريعات التجارة الالكترونية، وخاصة منها من تطرقت إلى تعريفه بصورة مباشرة، حيث اعتبرت هذه الوظيفة أساسا لابد من توافره في التوقيع حتى تكون له قوة ثبوتية، لكن هذه الوظيفة تختلف اختلافا كليا عما هي عملية في التوقيع العادي الذي يعتمد اعتمادا تاما على الإثبات الجسدي لتحديد هوية الموقع فلابد من تقديم وثائق صادرة عن سلطة رسمية، ولا يتم اللجوء إلى ثباته إلا في حالة حصول نزاع بين أطراف العلاقة التعاقدية وإقامة الدليل على الوجود الفعلي للعقد والموافقة على مضمونه.

هذه الوظيفة أيضا تتعلق بالتوقيع بالخصائص الذاتية لأن هذه الأخيرة تميز الشخص عن غيره من الأشخاص، وبالتالي هذه الوظيفة تتحقق أيضا في التوقيع بالقلم السري، لأن هذا الرقم لا يعرفه سوى صاحبه فلا فرصة أمامه لإنكار استخدامه للبطاقة المقترنة بالرقم السري الذي لا يمكن أن يشابه رقما آخر ولا يعرفه سواه، وأيضا تتوافر هذه الوظيفة في التوقيع بالقلم الالكتروني الذي لا يمكن استخدامه إلا من قبل صاحبه، لأن هذا النظام لا يمكن أن يعمل إلا إذا تطابق التوقيع مع ما هو محفوظ في ذاكرة الحاسب الآلي[1].

ب- التعبير عن إرادة الموقع في الموافقة على مضمون السند

يفترض القانون أن مجرد وضع الشخص توقيعه على مستند هو إقرار منه على ما ورد في هذا السند وهو بذلك يعبر بالتوقيع على موافقته عليه، إلا إذا أنكر ما هو منسوب إليه ودون ذلك فالتوقيع إقرار صريح بالموافقة على مضمون السند.

1- د. علي أبو مارية، المرجع السابق، ص ص 105 – 130.

لم يحصر التعبير عن الإرادة في وسيلة معينة، بل أن المشرع فتح المجال أمام أية وسيلة تكون قادرة على التعبير عن الإرادة، وبسبب التطور العلمي والتكنولوجي أصبح التعبير عن الإرادة يتم بأشكال توافق هذا التطور.

إن التوقيع الالكتروني قادر على التعبير عن الإرادة بدرجة أكثر من التوقيع التقليدي ذلك أن بعض أشكال التوقيع التقليدي كالختم والبصمة تدل على الشخص صاحبها لكنها لا تعبر دائما عن إرادته وإقراره بمضمون السند لأنها قابلة للتزوير، وبالتالي لا تحقق هذا الدول على أكمل وجه بعكس التوقيع الالكتروني، ففي التوقيع البيومتري الموقع لا يضع توقيعه، خاصة في مجال الصراف الآلي أو الانترنت إلا عند لدخول الى نظام الصراف الآلي والقيام بالعملية المطلوبة وهو بذلك يعبر عن إرادته، كذلك التوقيع بالرقم السري فالشخص يقوم بنفس الأمر فهو عند إدخال الرقم السري لإتمام المعاملة يعبر عن رضاه بإجراءها دون شك أو ريب في ذلك ولا يمكن لأحد أن يعبر عن إرادته عوضا عنه أو بإرغامه على ذلك.

أما التوقيع الرقمي المبني على المفتاحين العام والخاص، فقد استحدث أصلا لتوثيق مضمون الإرادة عبر الشبكات المفتوحة لمواجهة الاختراقات و القرصنة التي تؤدي لتحريف مضمون الرسالة، لهذا يستخدم نظام تأمين الشبكات والمعاملات والتحقق من صحة مضمون الرسالة الحاملة لإرادة الأطراف وهي أفضل وسيلة للتوقيع تضمن سلامة التعبير عن الإرادة وحمايتها[1].

1- كريم لملوم، المرجع السابق، ص ص 147 – 148.

ج –التوقيع يدل على حضور صاحب التوقيع

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

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

نلخص مما سبق أن التوقيع الالكتروني أمكن أن يؤدي نفس الوظائف التي يتطلبها القانون من التوقيع التقليدي وهو ذات الدور الذي يقوم به التوقيع الكتابي، لذا لم يذهب الفقه إلى اعتبار الرقم السري أو تلك الشفرة السرية كالتوقيع دليلا على الحقيقة، بل ذهب إلى أكثر من ذلك حيث يرى أن التوقيع الالكتروني يفوق التوقيع الكتابي[1].

1– لالوش راضية، المرجع السابق، ص ص 34 – 35.

ثانيا: أهم الخصائص التي يتميز بها التوقيع الالكتروني

يمكن استخلاص خصائص التوقيع الالكتروني كالتالي:

1. أنه يتكون من عناصر منفردة، وسمات ذاتية خاصة بالموقع تتخذ شكل حروف أو أرقام، أو رموز، أو إشارات، أو نبرات صوت، أو غيرها.
2. إنه يحقق درجة عالية من الأمان في تحديد هوية صاحبه، حيث أنه لا يمكن الادعاء بسهولة بتزويره كما يحدث في التوقيع التقليدي عند وجود طرف ثالث هو الموثق.
3. أنه يوضع على محرر الكتروني، ويتصل به عبر رسالة الكترونية.
4. أنه لا يتيح معرفة موقعه من مجرد رؤيته، فهو ليس علامة على صاحبه ولكنه وسيلة لتحديد الهوية.

لذلك يرى جانب من الفقهاء أن التوقيع الالكتروني لا يمكن أن يكون له حجية إلا إذا كان خاليا من كل معنى واضح، فصاحبه هو فقط الذي يعرفه، ولذلك فهو لا يمكن أن يكون صورة من توقيع الشخص أخذت بواسطة الماسح الضوئي وذلك لإمكان تزويرها[1].

فالتوقيع الالكتروني وعلى عكس التوقيع في الشكل الكتابي لا يقتصر على الإمضاء أو بصمة الأصابع، بل يشمل صورا لا تقع تحت حصر منها صور أو حروف أو أرقام أو رموز أو إشارات أو حتى أصوات كما سبق وذكرنا أعلاه، كل ذلك بشرط أن

1- د. هالة جمال الدين محمد محمود، المرجع السابق، ص ص 331 – 332.

يكون لها طابع فردي، يسمح بتمييز شخص صاحب التوقيع، وتحديد هويته وإظهار رغبته في إقرار العمل القانوني والرضا بمضمونه[1].

ان التوقيع الالكتروني يتميز بأنه لا يتم عبر وسيط مادي أي دعامة ورقية، حيث تذيل به الكتابة كما هو الحال بالنسبة للتوقيع الكتابي، وإنما يتم كليا أو جزئيا عبر وسيط الكتروني من خلال أجهزة الحاسب الآلي، وعبر الانترنت، بحيث يكون في إمكان أطراف العقد الاتصال ببعضهم البعض، والاطلاع على وثائق التعاقد، والتفاوض بشأن شروطه، وأخيرا إبرام العقود وإفراغها في محررات الكترونية، ثم بعد ذلك التوقيع عليها الكترونيا.

لزوم تدخل طرف ثالث الذي يقوم بدور الوسيط بين أطراف التصرف القانوني، حيث استلزمت ضرورة الأمن القانوني وجوب استخدام تقنية آمنة في التوقيع الالكتروني، تسمح بالتعرف على شخصية الموقع وتضمن سلامة المحرر الالكتروني من العبث والتحريف وهو ما استلزم إدخال طرف ثالث يضمن توثيق التوقيع، ويعمل عند الحاجة، على تحديد هوية صاحبه.

وقد عهد بهذه المهمة في الدول التي نظمت التوقيع لما يعرف بمقدمي خدمات التصديق والترسيم، وهي عبارة عن أشخاص طبيعية أو اعتبارية ترخص لها السلطات المختصة باعتماد التوقيع الالكتروني.

وقد انتهت هذه الجهات إلى استعمال تقنيات متطورة بقصد تلاقي أي قصور في أنظمة تأمين استخدامات شبكة الانترنت في التجارة الالكترونية والملفات الشخصية

1- الاستعجال الإداري في أحكام القضاء الإداري الجزائري، التوقيع الالكتروني واقع وآفاق التجارة الالكترونية، مجلة المدرسة الوطنية للإدارة، المجلد 13، العدد 2-2003، العدد 26، ص 57.

والحكومية، والمعاملات المصرفية، والعمل على منع عمليات الاحتيال الالكتروني، وإيجاد نظام أمن وسلامة يضمن الحفاظ على الحقوق، ويقلل الخسائر الناجمة عن عمليات الاختراق والقرصنة واللصوصية الالكترونية، وبوجه عام فإن رجال الصناعة اهتدوا إلى أهمية وخطر التوقيع الالكتروني فاكتشفوا لهذا الغرض عدة أساليب تعتمد في مجملها على الخصائص الفيزيائية والطبيعية السلوكية للأفراد نذكر منها: البصمة الشخصية، التوقيع الشخصي التعرف عن طريق مسح العين البشرية، والتعرف على الصورة الظلية[1].و مما سبق تحليله اعلاه يمكن ان نتوصل الى استخلاص اهمية التوقيع الالكتروني كفرع ثالث من المطلب الثاني.

الفرع الثالث

أهمية التوقيع الالكتروني

يعتبر التوقيع من المبادئ الأساسية في الإثبات وشرطا مهما لتوثيق أي مستند سواء في المراسلات العادية أو الالكترونية على اختلاف أنواعها ووسائطها داخل المؤسسة أو المراسلات التي تتم بين المؤسسات داخل الدولة أو خارجها وهذا بدوره يتماشى مع مقتضيات التجارة الالكترونية، وفيه استجابة وتيسير لمعاملات التجار الذين يرغبون في إقامة علاقات تعاقدية عبر الانترنت ومن هنا تكمن مقاصد المشرع من حيث أهمية التوقيع الالكتروني في مدى السرية والضمان الذي يتمتع به، وعليه فإنه يمكن الاستفادة من استخداماته في شتى المجالات الآتية[1].

1 اياد محمد عارف عطا سدة ،المرجع السابق ، ص 68.

أولا: توفير عامل الوقت والجهد الثمنين للمواطن والموظف

في هذه الحالة لن يضطر المواطن إلى أن يذهب بسيارته أو باستخدام وسائل النقل الأخرى إلى الدوائر الحكومية والانتظار طويلا كما هو الحال في معظم الدول النامية بخلاف الدول المتقدمة[21]، حيث أنه بالكاد ترى أشخاصا يتابعون وينهون معاملاتهم إلا بأضيق الحالات، وهو ظهور الشخص إن لزم في مسألة شخصية، وبذلك نرى أن التوقيع الالكتروني يسمح بعقد الصفقات عن بعد ودون حضور المتعاقدين.

ثانيا: يمكن الاعتماد عليه كليا ضمن الإجراءات القانونية والقضائية

في المنازعات بين الأشخاص والشركات الخاصة أو المؤسسات والهيئات الحكومية، وهنا يكون لقناعة القاضي دور كبير حيث يتم التعويل على الثقة في الجهاز الذي من خلاله تم إجراء التوقيع الالكتروني، ويقيم هذه الإجراءات ومدى قوة إجراءات السرية والتخزين والإرسال والحفظ وغيرها وكفاءة القائمين على هذه الإجراءات، ومدى تقدم التكنولوجيا كل هذه الاعتبارات ينظرها ويحكم في ضوئها مدى جدارة التوقيع الالكتروني في أن يتم الاعتماد عليه من عدمه.

ثالثا: يساهم التوقيع في فتح قناة اتصال جديدة بين المواطن والجهات الحكومية يمكن من خلالها النفاذ إلى مستويات الإدارة العليا لزيادة الشفافية في الأعمال الحكومية، وبالتالي يعد عامل وأداة مهمة لنجاح فكرة الحكومة الالكترونية.

رابعا: أن التوسع في استخدام التوقيع الالكتروني يرفع كفاءة العمل الإداري ويساعد على الارتقاء بمستوى أداء الخدمات الحكومية بما يتفق مع متطلبات ومستجدات العصر

1- إياد محمد عارف عطا سده، المرجع السابق، ص 69.

الحديث وبالتالي يؤدي هذا النمط إلى التحقيق من نمط البيروقراطية التي توفر زيادة النشاطات والمعاملات بكافة صورها.

خامسا: بما أن التوقيع الالكتروني يتم استخدامه في جميع المستندات ونماذج الطلبات، فإن ذلك يساعد على توفير الهوية الرقمية لكل مواطن وهذا يساهم في خلق وعي فكري للمواطن وتطوير التعامل بالانترنت مما يؤثر على التجارة الالكترونية، فنرى الكثيرين من الأشخاص الأذكياء الذين يملكون شركات ضخمة حققت الكثير من الأرباح دون أن يكون لها مقر بحجم الشركات الكبيرة، ومن هنا تكمن أهمية التوقيع الالكتروني في أنه يوفر الضمان من خلال استخدام عمليات البيع والشراء في المعاملات التجارية الالكترونية المختلفة كالبيع وغيرها من العقود والتصرفات القانونية التجارية الأخرى والاستيراد وباقي التعاقدات، وحجز تذاكر السفر والفنادق والمعاملات المصرفية بكل أنواعها، والتي تتم في شكل محرر الكتروني موقع توقيعا الكترونيا، وغير ذلك من المزايا الأخرى التي تؤدي بدورها إلى التوفير في جميع إجراءات إرسال البيانات إلى المواطن والحصول على معلومات منه (التوفير في الورق، الطلبات، الطباعة ...الخ) [1].

1- إياد محمد عارف عطا سده، المرجع السابق، ص. ص 69 – 70.

الفصل الثاني:

وسائل حماية التوقيع الالكتروني

الكتابة سواء كانت إلكترونية أو على دعامة مادية لا يمكن اعتبارها دليلا كاملا في الإثبات إلاّ إذا كانت موقعة، فالتوقيع يعتبر العنصر الثاني من عناصر الدليل المعد أصلا للإثبات وهو شرط أساسي لصحة أية وثيقة ورقية كانت أو إلكترونية ولهذا كان إلزاميا وضع مجموعة من القواعد تكفل قبوله وتضمن حجيته القانونية في الإثبات وهذا ما جعل معظم التّشريعات تنظم الإثبات للتوقيع الإلكتروني وتعطي له بعدًا قانونيًا يعادل بقوته الحجية المقررة للتوقيع اليدوي(التقليدي) ويساويه، وذلك طبعًا حسب ما تقتضيه التجارة الإلكترونية.

– من أجل حماية عقود التجارة الإلكترونية من مخاطر القرصنة زاد الطلب على أنظمة التشفير، وهذه الحماية تتم عادة عن طريق استخدام برامج خاصة لهذه الانتهاكات. ومن أجل مواجهة الأخطار التي قد يتعرض لها المتعاقدين عبر شبكة الانترنت، كإفشاء الأسرار مثلا تم اللجوء إلى استخدام تقنية التشفير كوسيلة فعالة لحماية وسلامة سرية المعلومات المرسلة بين المتعاقدين عبر شبكة الانترنت وإيجاد ضمانات كفيلة بإرساء الأمن القانوني من قبل جهات محايدة تسمى جهات التصديق الإلكتروني.

– يرتبط التوقيع الإلكتروني ارتباطا وثيقا بتوثيق التّصرفات القانونية الإلكترونية وتحديد كلا من هوية المرسل والمستقبل والتأكد من صحة البيانات كوسيلة مدنية لحماية معاملات التجارة الإلكترونية. لهذا كان من الضروري وجود حماية جنائية لمعاقبة أي شخص يقوم بالاعتداء على التوقيع الإلكتروني لأن هذا الأخير يعتبر بمثابة اعتداء على التّجارة الإلكترونية ككل.

ولبيان أهمية هذه النقاط سوق تتطرق إلى دراسة موضوع الاعتراف التشريعي بحجية التوقيع الإلكتروني(**المبحث الأول**) ثم نتناول موضوع تأمين التوقيع الإلكتروني(**المبحث الثاني**)

المبحث الأول

الاعتراف التشريعي بحجية التوقيع الإلكتروني

– يكمن مدى قبول المحررات الإلكترونية أو التوقيع الإلكتروني كدليل لإثبات الحق المدعى به في حالة ما إذا استوفت هذه المحررات الإلكترونية جميع شروط صحتها وذلك طبعا عن طريق توفير أكبر درجة من الأمان والحماية بهدف عدم التلاعب أو العبث بمضمونها. وهذا ما جعل أغلب التشريعات العالمية لا تقر بحجية الإثبات المكتوب دون توقيع، وبالتالي فإن الطابع الخاص والمعقد لشبكة الانترنت جعل الأفراد يسلكون الطريق الإتفاقي للاحتجاج بطريقة أخرى غير التوقيع الخطي المعروف لدى الفقه التقليدي لسد القصور التشريعي مستعينين بطبيعة القواعد القانونية المكمّلة المتعلقة بالإثبات لعدم تعلقها بالنظام العام حتى يضفوا حجية على آليات التوقيع الإلكتروني وكذلك الاستفادة من المواد التجارية وبالخصوص التي جاء فيها المفهوم الواسع لمبدأ الإثبات بالإضافة إلى ذلك الاستعانة بحرية الإثبات المقيدة في القانون المدني كنص المادة 333 من القانون المدني الجزائري، بالتالي سوف نقسم هذا المبحث إلى مطلبين الاعتراف التشريعي بالتواقيع الإلكترونية في التشريعات الدولية والتشريع الجزائري (المطلب الأول)، المعادلة القانونية بين التّوقيع الإلكتروني والتوقيع اليدوي (المطلب الثاني) حيث انقسم الفقه إلى اتجاه معارض واتجاه آخر مؤيد حول الوصف القانوني الذي يجب منحه للتوقيع الإلكتروني.

المطلب الأول

الاعتراف التشريعي بحجية التوقيع الإلكتروني في التشريعات الدولية والتشريع الجزائري

– نظرًا لأهمية وحساسية التوقيع الإلكتروني واعتباره كدليل للإثبات فإنه كان محل اهتمام سواء بالنسبة للتشريعات الدولية ونفس الشيء بالنسبة للتشريع الجزائري هذا ما جعل الحجية القانونية للتوقيع الإلكتروني تتمتع باهمية بالغة في الإثبات الإلكتروني، وبالتالي في حماية حقوق المتعاملين عبر الوسائط الإلكترونية. و يتضح بأنه لا يمكن الاعتداد بالكتابة سواء كانت كتابة تقليدية على دعامة مادية أو كتبت في الشكل الإلكتروني دليلا كاملا في الإثبات إلا إذا كانت موقعة، فالتوقيع يعتبر العنصر الثاني من الدليل المعد أصلا للإثبات ويعتبر كشرط أساسي لصحة الوثيقة سواء كانت ورقية أو إلكترونية ولذلك لكي يكون الإثبات الإلكتروني تاما لابد من توفر التوقيع الإلكتروني كون هذا الأخير يحدد هوية الشخص ويعبرعن قبوله لكافة الالتزامات الواردة في المحرّر الإلكتروني، لذا كان إلزاميا وضع القواعد التي تكفل قبوله وتضمن حجيته وقوته القانونية في الإثبات، ولهذا السبب رصدت التشريعات التي نظمت الإثبات للتوقيع الإلكتروني واعطت له بعدا قانونيا يعادل بقوته الحجية المقرّرة للتوقيع التقليدي وذلك بما يتفق مع مقتضيات التجارة الإلكترونية لذلك سوق نتناول الحجية القانونية للتوقيع الإلكتروني في التشريعات الدولية في الفرع الأول، الحجية القانونية للتوقيع الإلكتروني في القانون الجزائري في الفرع الثاني.

الفرع الأول

الاعتراف التشريعي بحجية التوقيع الإلكتروني في التشريعات الدولية

لقد تبنت معظم التشريعات الدولية مبدأ التكافئ بين المحررات الإلكترونية والورقية وسنحاول من خلال هذا الفرع التعرف على بعض الاتجاهات وموقف التشريعات في التعامل مع المحررات الالكترونية باعتبارها نوع حديث في أدلة الإثباتات تفرض نفسها على الدول .

أولا: الحجية القانونية للتوقيع الإلكتروني وفقا لتوجيهات الإتحاد الأوروبي (1999/93).

– يتوجب على الدول الأعضاء في الإتحاد الأوربي مراعاة التأثير القانوني للتوقيع الإلكتروني وقبوله كحجية في الإثبات، وهذا ما جاء به نص المادة 5 **الفقرة 2** من التوجيهات الأوروبية المتعلقة بالتوقيع الإلكتروني، وحسب هذه المادة التي لا يمكن أن يرفض التوقيع الإلكتروني لأحد الأسباب التالية:

– لأن التوقيع قد قدّم في شكل إلكتروني

– لأنه لم يوضع على شهادة معتمدة ومسلمة من أحد مقدمي خدمات التصديق على الشهادات المعتمدة

– لأنه لم ينشأ بأمر لإنشاء هذا التوقيع[1].

ولتحليل هذه الفقرة يتطلب الاشارة الى أمرين مهمين وهما:

[1] Art 5/2 de la directive 1999/93/CE du parlement européen du conseil du 13 décembre 1999.

1- منحت الفقرة الأولى من المادة السالفة الذكر نفس الحجية القانونية الممنوحة للتوقيع الخطي للتوقيع الإلكتروني المقدم، أي الذي تم التصديق عليه واعتماده.

2- لم تستخدم الفقرة الثانية من نفس المادة مصطلح التوقيع الإلكتروني المقدم وبناءًا عليه يمكن تطبيق هذه المادة على التوقيع الإلكتروني البسيط قبل اعتماده من قبل مقدمي خدمات التصديق المعتمدين لدى الدولة وهذا يعني أنه يتعين قبول هذا النوع من التوقيع كدليل إثبات ولكن يجب أن ناخذ في الحسبان أنه عند حدوث ازدواجية في هذه الحالة بين توقيعين إلكترونيين أحدهما بسيط والآخر مقدّم تكون الأولوية لهذا الأخير كونه يتمتع بعناصر أمان يمكن أن تمنحه هذه الأولوية.

- لقد أضفت توجيهات الإتحاد الأوربي على المحررات الإلكترونية نفس الحجية القانونية في الإثبات الممنوحة للتوقيع التقليدي كما تبنى مفهوما واسعا للتوقيع الإلكتروني يشمل جميع صور التوقيع الإلكتروني، والتي من شأنها تحديد صاحب التوقيع وتمييزه عند استخدام تقنيات الاتصال الحديثة[1].

كما كرّس في هذا الشأن المشرع الفرنسي قرينة صحة التوقيع الإلكتروني في المادة (1316-4) إذ بعد أن عرف التوقيع الإلكتروني بأنه ما ينتج من استخدام إجراء آمن يكفل تحديد هوية الشخص الموقع، وتضمن أنه متصل تماما بالتصرف الذي يحمل توقيعه المرتبط به، وبالتالي هذا الإجراء الآمن طالما أنه جرى وفقا لشروط معيّنة يعد مفترضا، وطالما أن هذه الشروط ترتبط بطابع تقني فلقد ترك تحديدها لمجلس الدولة ولقد صدر مرسوم من مجلس الدولة الفرنسي **رقم 272 في 30 مارس 2001** ومرسوما معدل ومكملا له برقم

[1] - كريم لملوم ، المرجع السابق ، ص ص 149-150.

535 في 18 أفريل 2002، وقد حدد هذا الأخير القرينة التي افترضها المشرع بالمادة(**1316-4**) حيث جاء في المادة الثانية منه توافر قرينة بسيطة على صحة التوقيع الإلكتروني متى توفرت شروط عددتها المادة المذكورة تتمثل في أن يكون الإجراء المستخدم في التوقيع الإلكتروني آمنا وأن يتم استحداث هذا الاخير بفضل أجهزة آمنة في انشاء التوقيعات، وأن يستند التحقق من التوقيع إلى شهادة معتمدة تصدرها الجهة المختصة[1].

ثانيا: الحجية القانونية للتوقيع الإلكتروني وفقا لقانون الأونيسترال النموذجي

– كان الهدف الوحيد من وضع قانون الأونسترال النموذجي من قبل لجنة الأمم المتحدة للقانون التجاري الدولي هو أن يكون هذا القانون أداة فعالة لتطوير تشريعاتها الداخلية وفقا للتطورات التكنولوجية الحديثة وظهور التجارة الإلكترونية إضافة إلى مساعدة مستخدمي هذه الوسائل الحديثة والباحثين في هذا المجال ومساعدة الدول التي لا تزال تستخدم الأساليب التقليدية لحفظ المعلومات وتدارك المساوئ الناجمة عن قصور التشريعات الوطنية في التعامل مع هذه الأساليب الحديثة في مجال التعاقد وكل المعاملات المدنية والتجارية كما أنه يساعد في تفسير بعض الاتفاقيات الدولية التي قد تترتب عنها مشاكل قد تعرقل استخدام هذه التقنيات التكنولوجية في مجال الاتفاقيات التي تشترط وجوب الكتابة الورقية[2].

– لقد ورد في البند الأول من المادة السادسة من قانون "الأونسترال" النموذجي الخاص بالتوقيعات الإلكترونية لسنة 2001 بأنه:

[1] لالوش راضية ، المرجع السابق ، ص ص 78-79 . لمزيد من المعلومات أنظر محمد محروك ، المرجع السابق ص ص 25-27.

[2] هدار عبد الكريم ، مبدأ الثبوت بالكتابة في ظل ظهور المحررات الإلكترونية، جامعة الجزائر، كلية الحقوق، بن عكنون، 2013-2014، ص ص 35-36.

« حينما يشترط وجود توقيع من شخص، يعد ذلك الاشتراط ضروريا بالنسبة إلى رسالة البيانات إذا استخدم توقيع إلكتروني يعول عليه بالقدر المناسب للغرض الذي أنشئت أو ابلغت من أجله الرسالة مع مراعاة كل الظروف، بما في ذلك أي اتفاق ذي صلة». كما جاء في البند الثالث من نفس المادة افتراض مفاده أن المحررات الإلكترونية يصبح موثوقا بها، ومن ثم يمكن الاعتماد على التوقيع الإلكتروني متى كانت الأداة التي استخدمت في انشائه تخص الموقع دون غيره، وكانت لحضة إجراء تحت سيطرته، بالتالي يمكن اكتشاف أي تحريف يطرأ على التوقيع الإلكتروني بعد صدوره.

– وقد نصت المادة السابعة من القانون النموذجي للتجارة الإلكترونية على الاعتراف بحجية التوقيع الإلكتروني بشرط أن يكون التوقيع دالاً على هوية الشخص الموقع[1].

– إذن كما سبق وذكرنا أعلاه فقانون الأونسترال النموذجي لشأن التجارة الإلكترونية يعتبر من المنطلقات الأولى التي تأكد جميعها على ضرورة الاحتواء التشريعي لتنظيم الإثبات بالسندات الإلكترونية وعدم ترك المسألة للاجتهاد وهذا ما عرضته الجمعية العامة للأمم المتحدة كما سبق وذكرنا أعلاه بتاريخ 1996/12/16 يؤكد هذا القانون أنّ: **« الجمعية العامة للأمم المتحدة إذ تلاحظ أن عددا متزايدا من المعاملات في التجارة الدولية يتم عن طريق التبادل الإلكتروني للبيانات، وتشير الى التوصية التي اعتمدتها اللجنة، وذلك بغية تأمين الضمان القانوني في سياق استخدام التجهيز الآلي للبيانات واقتناعا منها بأن وضع قانون نموذجي يسيراستخدام التجارة الإلكترونية ويكون مقبولا لدى الدول ذات الأنظمة القانونية والاجتماعية والاقتصادية المختلفة ويمكن أن يساهم على نمو هام في تنمية علاقات اقتصادية دولية منسجمة وإذ تؤمن أن اعتماد اللجنة للقانون النموذجي بشأن التجارة الإلكترونية سيساعد على نحو هام جميع الدول في تعزيز تشريعاتها التي تنظم بدائل للأشكال الورقية، وتوصي بأن تولي جميع الدول اعتبارها لهذا القانون عندما تقوم**

[1] زينب غريب ،المرجع السابق ، ص 111 .

بسن قوانينها أو تعديلها» كما جاء في المادة التاسعة(9) الفقرة 2 من هذا القانون: **« يعطى للمعلومات التي تكون على شكل رسالة بيانات ما تستحقه من حجية في الإثبات»**، كما تضمنت أيضا في المادة 17 بشكل صريح إرساء مبدأ حجية استخدام تبادل البيانات إلكترونيا في إبرام عقود التجارة الإلكترونية وقبولها في الإثبات.

ونصت المادة الخامسة(5) من نفس القانون على مبدأ عدم التفريق بين الوثائق الورقية والإلكترونية، فقد قام في نصوص أخرى بتعريف كل من الكتابة والتوقيع تعريفاً موسعاً وأعطى في المادة السادسة(6) الفقرة الأولى مفهوما واسعا للكتابة حتى لا يكون التعريف عائقا في وجه ما قد تسفر عنه التكنولوجيا الحديثة[1].

– ولقد صدر كذلك عن هذه اللجنة، قانون نموذجي خاص بالتوقيعات سنة 2001 بهدف تعريف التوقيع الإلكتروني، وإعطائه الحجية القانونية الكاملة لمسايرة مستجدات التجارة الإلكترونية، كما تبنت قواعد موحدة للتوقيع الإلكتروني .

– رغم أن قانون الأونسترال النموذجي بشأن التجارة الإلكترونية ساوى بين السندات الإلكترونية والورقية، إلاّ أنه لم يشترط توفر كل شروط المحررات التقليدية في المحررات الإلكترونية، لكن رغم ذلك نص على شروط أخرى مثل وجوب استنساخ وقراءة رسالة البيانات وأن تكون في المتناول بحيث يمكن العودة إليها عند الحاجة مع عدم قابليتها للتحريف وهذا وفقا لنص المادة السادسة من هذا القانون[2]. وتجدر الإشارة إلى أنه يجب مراعاة بعض قواعأخرى لا تتوفر في السندات التقليدية ترمي إلى إضفاء الثقة في التعامل بها ومن أهم هذه القواعد نذكر

[1] طمين سهيلة، الشكلية في عقود التجارة الإلكترونية ،رسالة لنيل شهادة الماجيستر في القانون، فرع القانون الدولي للأعمال، كلية الحقوق، مدرسة الدكتوراه للقانون الأساسي والعلوم السياسية، 2011 ص 101. لمزيد من العلومات حول قانون الأونيسترال النموذجي بشأن التوقيع الإلكتروني ،راجع كذلك أسامة بن غانم العبيدي ،المرجع السابق ،ص 172.

[2] طمين سهيلة، المرجع السابق، ص 102.

ما جاء في المادتين 13 و14 من القانون النموذجي حول إسناد رسائل البيانات والإقرار باستلامها ونذكر منها:

– تعتبر رسالة البيانات صادرة عن المنشئ المرسل وبالتالي يعد ملزما بها متى ثبت أنه هو من أرسلها أو من شخص له صلاحية التصريف نيابة عنه، أو حتى من نظام معلوماتي مبرمج من طرفه أو من ينوب عنه للعمل تلقائيا.

- يحق للمرسل إليه أن يعتبر رسالة البيانات صادرة عن المنشئ إذا:

- قام المرسل إليه بتطبيق سليم من أجل التأكد أنّ رسالة البيانات قد صدرت عن المنشئ أو سبق أن وافق عليها المنشئ لهذا الغرض.

- كانت رسالة البيانات كما تسلّمها المرسل إليه ناتجة عن تصرفات شخص بحكم علاقته بالمنشئ أو بأي وكيل لهذا الاخير من الوصول إلى طريقة يستخدمها المنشئ لإثبات أن رسالة البيانات صادرة فعلا عنه[1].

فالمرسل في حالة ما إذا لم يستلم إشعارًا من المنشئ يفيد أن رسالة البيانات لم تصدر عنه لا يمكنه التمسك بصدور رسالة البيانات[2].

تعتبر كل رسالة بيانات يتسلمها المرسل إليه رسالة بيانات مستقلة، ويكون للمرسل إليه التصرف على أساس هذا الافتراض، حيث يمكن اعتبارها نسخة ثانية من رسالة البيانات من المرسل إليه و يمكن لهذا الاخير التصرف على أساس هذا الافتراض ومع ذلك يمكن اعتبارها نسخة ثانية من رسالة البيانات الأخرى إذا عرف المرسل إليه ذلك ، أو كان عليه أن يعرف إذا بذل العناية المعقولة أو استخدم أي إجراء متفق عليه يفهم منه أن رسالة البيانات كانت نسخة ثانية.

[1] أنظر المواد 3/2/1/13 من قانون الأونيسترال النموذجي.

[2] أنظر المادة 4/13 من قانون الأونيسترال النموذجي.

يعتد بشكل الإقرار باستلام رسالة البيانات من المرسل إليه باتفاق الطّرفين، فإن لم يتفقا جاز أن يتم الإقرار بأي بلاغ من جانب المرسل إليه او بأي وسيلة آلية أو غيرها، أو بأي سلوك من جانب المرسل إليه يفيد استلام رسالة البيانات[1].

ومن كل ما سبق تحليله أعلاه ومن خلال نصوص المواد التي سبق وذكرناها يمكننا القول بأن قانون الأونسترال النموذجي بشأن التجارة الإلكترونية الذي اعتمدته لجنة القانون التجاري الدولي قد اعترف بحجية التوقيع الإلكتروني كدليل كامل في الإثبات.

الفرع الثاني

حجية التوقيع الإلكتروني في التشريع الجزائري

لقد جاء المشرع الجزائري خاصة في السنوات الأخيرة بمعاملات إلكترونية حديثة إلى جانب المعاملات التقليدية المعروفة سابقا في القانون الخاص الجزائري **بموجب القانون رقم 10/05 المؤرخ في 20-06-2005 المعدّل والمتمم للأمر رقم 58/75** المتضمن القانون المدني وذلك بإدراج مواد جديدة تتعلق بالإثبات بالتوقيع الإلكتروني، واعتباره كالإثبات بالتوقيع التقليدي لذلك سوف يتبين في هذا الفرع موقف المشرع الجزائري من حجية التوقيع الإلكتروني وذلك من خلال تبنيه لمبدأ التكافؤ بين المحررات في تعديلاته الأخيرة للقانون المدني والقانون التجاري وبعض القوانين الخاصة.

[1] طمين سهيلة ،المرجع السابق ، ص 103. وأنظر المادة 14 من قانون الأونيسترال النموذجي.

أولا: قواعد الإثبات بالتوقيع الإلكتروني في التشريع الجزائري

سنقوم بدراسة القانون المدني(قبل تعديل القانون المدني لسنة 2005، وبعد التعديل الذي تم بموجب القانون 10/05 لسنة 2005 المعدّل والمتمم للقانون المدني الجزائري)[1]. ومن خلاله سوف نحاول التعرف على القواعد العامة للإثبات في التشريع الجزائري كما سنتطرق لذلك أيضًا في القانون التجاري حيث انتقل المشرع من النظام الورقي في الإثبات إلى النظام الإلكتروني.

1- الاعتراف بالتوقيع الإلكتروني في القانون المدني الجزائري

أ- قبل تعديل القانون المدني الجزائري:

يمكن أن نستخلص قواعد الإثبات في القانون الجزائري بصفة عامة كغيره من القوانين في نوعين من نظام الإثبات، الأول هو نظام إثبات مقيد في القانون المدني والمعاملات المدنية والثاني وهو النظام الحرّ في القانون التجاري والمعاملات التجارية وسنبين كل نظام كما يلي:

- الإثبات المقيد في المواد المدنية:

لدينا القانون العام الذي هو مجموعة من القواعد القانونية التي تنظم علاقة الدولة بغيرها من الدول وهذا ما يعرف بالقانون الدولي العام أو ما ينظم علاقة الدولة بمؤسساتها الإدارية أو علاقة الدولة بالأفراد أما القانون الخاص فهو مجموعة القواعد القانونية التي تنظم علاقة الأفراد فيما بينهم ليس لديهم السلطة ولا السيادة، وبالتالي فالقانون المدني يعتبر الشريعة العامة لفروع القانون الخاص، بحيث يعتبر المرجع والأصل فيما لا ينص فيه في فروع القانون الخاص الأخرى ، وقد سبق لنا العلم أن العقود من حيث الإبرام تنقسم إلى عقود رضائية تبرم بمجرد

[1] الأمر رقم 75-58 ل26 سبتمبر1975 المتضمن القانون المدني المعدّل والمتمم.

رضى الطرفين دون الحاجة إلى صبها في قالب رسمي، ولدينا أيضًا ما يسمى بالعقود الشكلية التي يتطلب انعقادها إفراغها في قالب رسمي وهذه الشكلية تكون للانعقاد و تعتبر ركن من أركان العقد وعند تخلفها يترتب بطلان العقد، وقد تكون الشكلية فقط لإثبات ،ويقصد بالشكلية كتابة العقد وأنها قد تكون عرفية أو رسمية وتنص المادة 333 من القانون المدني الجزائري[1]، على التصرفات القانونية المدنية أنّ الغالب فيها هو الكتابة فيما زاد التصرف عن 1000 دج.

والمادة 324 مكرر[2]، من ق.م.ج تنص على: **« زيادة العقود التي يأمر القانون بإخضاعها إلى شكل رسمي يجب تحت طائلة البطلان تحرير العقود التي تتضمن نقل ملكية العقار أو حقوق عقارية أو محلات تجارية أو صناعية أو كل عنصر من عناصرها... ».**

- الإثبات الحر في المواد التجارية:

يعتبر المبدأ في المادة التجارية هو حرية الإثبات عكس المادة المدنية التي يعتبر الأصل فيها تقييد الإثبات، وحرية الإثبات في المواد التجارية تعني التخلي عن كثير من القيود المتعلقة بالإثبات المدني.

الأصل في الفقه والتشريع الحديثين هو حرية الإثبات في المواد التجارية مهما كان المبلغ المراد إثباته على عكس المعاملات المدنية التي يجب فيها تقديم دليل كتابي في إثبات ما يتجاوز مبلغا معينا ينص عليه القانون.

من خلال دراستنا لمفهوم التوقيع التقليدي والتوقيع الإلكتروني تبين لنا أنّ القواعد

[1] أنظر المادة 324 للقانون88-14 ل 3ماي 1988المعدل و المتمم للأمر 75-58 ل26 سبتمبر 1975 المتضمن القانون المدني الجزائري.

[2] أنظر القانون رقم 88-14 السابق الذكر.

التقليدية للإثبات لا يمكنها استيعاب الوسائل الحديثة في التعامل خصوصا أنّ الكتابة الإلكترونية تعتمد على دعامات إلكترونية ، فإن التصرف القانوني يتم على مستوى الحاسوب وبالتالي يخضع لارادة المبرمج مما يجعل المعلومات التي تم تخزينها من صنع مستعمل الحاسوب أي صادرة منه شخصيا فيرى القانون انه لا يجوز الاحتجاج بها كدليل الإثبات.

ومن هنا جاءت الحتمية إلى تعديل قواعد الإثبات في التشريع الجزائري مواكبًا للتطور التكنولوجي كما هو الحال في معظم التشريعات المقارنة نظرا لكون القواعد التقليدية في ظل القانون المدني القديم لا تملك قوّة ثبوتية تحتم على المشرع الجزائري التدخل لإعطائها قوّة ثبوتية بموجب نصوص قانونية.

ب- الإثبات في ظل تعديل القانون المدني الجزائري لموجب القانون رقم 10/05:

على غرار باقي التشريعات اعتمد المشرع الجزائري في تعديله لأحكام التقنين المدني على المبادئ التي جاء بها القانون النموذجي بشأن التجارة الإلكترونية.

جاء في نص المادة **323 مكرّر 1** مايلي: **« يعتبر الإثبات بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة على الورق بشرط إمكانية التأكيد من هوية الشخص الذي أصدرها وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها»** كما جاء أيضا في نص المادة **327** [1].

« يعتد بالتوقيع الإلكتروني وفق الشروط المذكورة في المادة 323 مكرر 1 أعلاه».

بعد ما قام المشرع الجزائري بهذا التعديل الجديد أصبح للكتابة في الشكل الإلكتروني مكانا ضمن قواعد الإثبات في التقنين المدني الجزائري طبقا لنص المادة **323 مكرر** ق.م.ج

[1] هدار عبد الكريم،المرجع السابق،ص 79.

الكتابة في الشكل الإلكتروني ذات التسلسل في الأوصاف أو الأرقام أو أية رموز أو علامات ذات معنى مفهوم مهما كانت الوسيلة الإلكترونية المستعملة ومهما كانت طرق إرسالها.

– نستنتج من خلال دراستنا لهذه النصوص الجديدة أن المشرع الجزائري اعترف بالتوقيع الإلكتروني وأعطاه نفس حجية التوقيع التقليدي وبناءا على ذلك أخذ المشرع بمبدأ تكافئ المحررات الإلكترونية والورقية الذي جاء به قانون الأونسترال النموذجي للتجارة الإلكترونية.

2- الاعتراف التشريعي بالتوقيع الإلكتروني في القانون التجاري الجزائري

يعتبر القانون 03-15 المتضمن الموافقة في الأمر 03-11 المتعلق بالنقد والقرض أول قانون جزائري تضمن التعامل الإلكتروني الحديث في القطاع المصرفي، ويتضح ذلك من خلال المادة 69 التي نصت على: **« تعتبر وسائل الدّفع كل الأدوات التي تمكن كل شخص من تحويل أموال مهما يكون السند أو الأسلوب التقني المستعمل»**. وكذلك الأمر 05-06 المؤرخ بتاريخ 23 أوت 2005 المتعلق بمكافحة التهريب في المادة 03 إستعمل صراحة مصطلح **« وسائل الدّفع الإلكتروني »** حيث اعتبرها المشرع الجزائري من بين التدابير والإجراءات الوقائية لمكافحة التهريب[1].

القانون رقم 05-02 المؤرخ في 06 فيفري 2005 أضاف فقرة ثالثة للمادة **414** في وفاء السفتجة على**« يمكن أن يتم التقديم أيضا بأية وسيلة تبادل إلكترونية محددة في التشريع والتنظيم المعمول بهما »** وتم إضافة نفس الفقرة إلى المادة **502 بمناسبة تقديم الشك للوفاء** و بموجب القانون 05-02 المؤرخ ب **06 فيفري 2005** أضاف المشرع

[1]- هدار عبد الكريم، المرجع السابق، ص 80.

الجزائري باب رابع إلى الكتاب الرابع من التقنين التجاري والمعني بالسندات التجارية الفصل الثالث منه يتضمن بطاقات السحب والدّفع **المادة 543 مكرر 23**[1]

المطلب الثاني

التعادل الوظيفي بين التوقيع التقليدي والتوقيع الإلكتروني

نص المشرع في المادة 327 فقرة 2 على أنه:" يعتد بالتوقيع الالكتروني وفقا للشروط المذكورة في المادة 323 مكرر 1 أعلاه "، ويكون المشرع قد سوى في الحجية بين التوقيع التقليدي والتوقيع الالكتروني، وهو ما يسمى بالتعادل الوظيفي بين التوقيع التقليدي والتوقيع الالكتروني، أي أن هذا الأخير يمكن أن يقوم بذات الوظائف التي يقوم بها التوقيع الخطي من حيث تحديد هوية الشخص الموقع وإقراره بمضمون التعادل الذي استخدم هذا التوقيع في إنجازه،وفي نفس الوقت أحال المشرع على الشروط المنصوص عليها في المادة 323 مكرر 1 للاعتداد بهذا التوقيع وهي: إمكانية التأكد من هوية الشخص الذي اصدره، وأن يكون التوقيع معدا ومحفوظا في ظروف تضمن سلامته.

كما سبقت الإشارة إليه أعلاه فإنه يصعب تحقيق هذين الشرطين إلاّ بوجود جهات وسيطة تصادق على صحة هذا التوقيع، وضمان أن صدوره كان من الشخص المنسوب إليه وتأكيد أنه لم يحدث أي تحريف أو تعديل فيه.

[1]– هدار عبد الكريم، المرجع السابق ، ص 81 .انظر طمين سهيلة، المرجع السابق ، ص ص 61 – 62 . راجع كذلك حابت امال ، المرجع السابق، ص ص 93– 94.

الفرع الأول

مدى تحقيق التوقيع الإلكتروني لشروط التوقيع

التوقيع الإلكتروني هو شكل من أشكال التوقيع ظهر بسبب استخدام الوسائط الإلكترونية في تنفيذ المعاملات الإلكترونية وليحل محل الشكل التقليدي للتوقيع، وترك أمر تنظيم هذه التواقيع للتشريعات المختلفة، ولعل أغلبيتها تضع شروطًا للاعتداد بالتوقيع الإلكتروني، فما مدى تمتع التوقيع الإلكتروني بالشروط التي تتطلب في التوقيع[1]؟

أولا: أن يكون التوقيع علامة مميزة للشخص

لكي يصدر عن أي شخص توقيع لابد أن يتبلور على شكل مادي، هذا الشكل هو التوقيع الذي يكون مميزا لشخص الموقع عن غيره ومحددا لهويته[2]، حتى يقوم التوقيع بوظائفه، وإذا كان كل من الإمضاء والختم وبصمة الأصبع علامات مميزة للشخص دون غيره فهل التوقيع الإلكتروني يحقق هذا الشرط؟

يعد التوقيع الإلكتروني من قبيل العلامات المميزة للموقع وحده دون غيره، فالتوقيع البيومتري القائم على الخصائص الذاتية أو بالرقم السري بكل مجالاته أو بالقلم الإلكتروني أو التوقيع الرقمي، كلها تتضمن علامات تميز الشخص عن غيره، فالتوقيع البيومتري يقوم على الخصائص الذاتية للشخص الذي يتميز بها عن غيره ، كذلك الرقم السري فلا يمكن أن يتشابه اثنان بنفس الرقم السري داخل النظام الواحد فهو يميز كل شخص عن غيره فلا يستطيع أحد

[1] حابت آمال، المرجع السابق، ص 109.

[2] محمد فواز المطالقة، المرجع السابق، ص 176.

استخدام الرقم السري لشخص آخر ولا يمكنه أن يعرفه بأي طريقة إلاّ بإهمال صاحبه في حفظه.

كذلك التوقيع بالقلم الإلكتروني فهو مثل الإمضاء العادي في قدرته على تمييز الشخص عن غيره، ويتمتع بقدر من الحماية فلا يمكن إنجازه إلاّ إذا طابق التوقيع بالقلم الإلكتروني الإمضاء المخزن في الكمبيوتر، أما بالنسبة للتوقيع الرقمي فهو يقوم على مفتاحين عام وخاص، وهذا الاخير لا يعلمه إلاّ الشخص الموقع، وعند استخدام هذا التوقيع يستطيع الشخص الذي يصله أن يتحقق منه بواسطة سلطات الاشهار التي تاكد صحة التوقيع ،و عليه فلكل شخص توقيع رقمي خاص به.

ثانيا: أن يكون التوقيع واضحا ومستمرا

يعد التوقيع شكلا من أشكال الكتابة وبالتالي يخضع للشروط التي تخضع لها الكتابة من حيث إمكان الإطلاع عليه وقراءته بشكل مباشر أو عن طريق استخدام الحاسب ويجب أن يتم تحريره بشكل يسمح بالرجوع إليه خلال فترة معينة[1]، فهل يحقق التوقيع الإلكتروني هذا الشرط؟

يمكننا القول أن التوقيع الإلكتروني يستطيع تحقيق هذا الشرط إذ أن التوقيع يترك بيانات مختلفة يمكن قراءتها من خلال إيصال المعلومات في الحاسب الآلي الذي سيتم تغذيته ببرامج لها القدرة على ترجمة لغة الآلة التي تتكون من توافق وتبادل بين رقم واحد وصفر إلى لغة مقروءة للإنسان.

بالنسبة للاستمرارية فربما كان هناك شك بسبب التكوين المادي والكميائي للشرائح الممغنطة وأقراص التسجيل المستخدمة في الحاسوب الذي يتميز بقدر من الحساسية مما

[1] حابت آمال، المرجع السابق، ص 109.

يعرضها للتلف السريع عند اختلاف قوة التيار الكهربائي، إلاّ ان أمكن التغلب عليه باستخدام أجهزة و وسائط أكثر قدرة وبالتالي يمكن الاحتفاظ بالبيانات لمدة طويلة قد تفوق الورق العادي الذي قد يتآكل بفعل الرطوبة أو الحشرات لسوء التخزين[1].

ثالثا: اتصال التوقيع بالسند

لكي يقوم التوقيع الإلكتروني بوظيفته المتمثلة في إقرار الموقع بما ورد بمحتوى السند فلا بد أن يرتبط التوقيع ارتباطا وثيقا بالسند[2]، أي اتصالا ماديا ومباشرا فإلى أي مدى يتحقق هذا الشرط في التوقيع الإلكتروني؟

يتعلق هذا الأمر أساسا بكفاءة التقنيات المستخدمة في تأمين مضمون المحرر المدون إلكترونيا، وبالتالي تأمين ارتباطه بشكل لا يقبل الانفصال عن التوقيع، ومن أهم هذه التقنيات نذكر تقنية التوقيع الرقمي الذي يعتمد على مفتاحين عام وخاص ولا يستطيع أحد أن يطلع على مضمون المحرر إلاّ الشخص الذي يملك المفتاح ، فهو يحوّل التوقيع إلى معادلة رياضية لا يمكن فهمها ولا حتى قراءتها إلاّ بالمفتاح الخاص من خلال تقنيات فنية، وبناءا على ذلك فإن المحرر يرتبط بالتوقيع على نحو لا يمكن فصله ولا يمكن لأحد غير صاحب المحرر المدون من التدخل في تعديل مضمونه[3].

[1] حابت آمال، المرجع السابق، ص 110.

[2] محمد فواز المطالقة، المرجع السابق، ص 177.

[3] حابت امال، المرجع السابق، ص111.

الفرع الثالث

مدى تحقيق التوقيع الإلكتروني لوظائف التوقيع التقليدي

لعل المساواة بين التوقيع العادي والتوقيع الإلكتروني، تكون من خلال تحقيق هذا الأخير لوظائف التوقيع التقليدي ، الذي يؤدي دورًا وظيفيا مزدوجا، فمن ناحية يحدد هوية الموقع ويميزه عن غيره ومن ناحية أخرى يعبر عن إرادة الموقع وإقراره بمضمون المحرر والالتزام بما ورد فيه ولكن بالنظر إلى التوقيع الإلكتروني فهو ينشا على وسيط إلكتروني على عكس التوقيع التقليدي الذي ينشأ على وسيط مادي، مع انفصال التوقيع الإلكتروني عن شخص الموقع، ثم تداوله عبر شبكة الاتصالات المفتوحة، فإن جميع هذه المعطيات قد تثير الشك حول مصداقيته في ضمان ارتباطه بالمحرر حتى يمكن التحقق من سلامة مضمونه أثناء التعامل[1].

أوّلا: فعالية التوقيع الإلكتروني في تحديد هوية صاحبه

إنّ الحديث عن المعادلة بين التوقيع التقليدي والتوقيع الإلكتروني تستدعي الحديث عن تحقيق هذا الأخير لوظائف التوقيع بصفة عامة إذ أن تحديد هوية الشخص الموقع تعتبر من أولى وظائف التوقيع، هذا التحديد الذي يسهل توفره في حالة التوقيع في الشكل الكتابي لحضور أطراف العقد عند صياغته وبالتالي التوقيع عليه، أما بالنسبة للتوقيع الإلكتروني فإن وظيفة تحديد هوية الشخص الموقع تدعو إلى الشك في قيمته نظرا لكون التوقيع الإلكتروني منفصلا عن شخصية صاحبه، حيث نجد المشرع المغربي قد اعتبر التوقيع الإلكتروني مماثل للتوقيع اليدوي من خلال القانون 53.05 في كونه يحدد نفس الوظائف المبتغاة من التوقيع فإذن يمكن القول بأن التوقيع الإلكتروني قادر على تحديد هوية الشخص الموقع وهذا يتضح لنا

[1] أنظر الفقرة الرابعة من المادة 13/6 قانون مدني فرنسي.

من خلال صوره التي ذكرناها سابقا، فالتوقيع بالرقم السري (التوقيع الكودي) قادر على تحديد هوية الموقع، فمثلا بالنسبة لبطاقات السحب، فالجهازلا يستجيب لطلب السحب بمجرد إدخال بطاقة السحب ولكن بعد إدخال صاحب البطاقة للرقم السري هذا الرقم ، والذي يحصل عليه بطريقة سرية، تجعله قادرًا على القيام بوظيفة تحديد هوية الشخص الموقع، أما بالنسبة للتوقيع البيومتري فهو يقوم مثلاً على أساس استخدام الصفات والمميزات الجسمانية والخصائص الطبيعية و الفيزيائية التي يختلف بها الفرد عن الآخر مما يجعلها قادرة على تحديد هوية الشخص الموقع تحديدا قد يفوق قدرة التوقيع العادي.

ولعل الغاية من تحقيق التوقيع الإلكتروني لوظيفة التوقيع التقليدي والمتمثلة في تحديد هوية الشخص الموقع تمكن في نسب الوثيقة للشخص الموقع وبالتالي تحمل مسؤوليته تجاهها[1].

ثانيا: اتصال التوقيع بالمحرر الإلكتروني

لكي يتمكن التوقيع الخطي من أداء وظيفته في إثبات إقرار الموقع بمضمون المحرر يتوجب أن يكون هذا التوقيع متصلا اتصالا ماديًا ومباشرا بالمحرر المكتوب، لأن واقعة كتابة التوقيع على المحرر نفسه هي التي تعطي التوقيع أثره، وأن استخدام الورق في كتابة المحررات المعدة للإثبات يتحقق معه اتصال التوقيع بالمحرر اتصالا ماديا وكيميائيا على نحو لا يمكن فصل إحداهما عن الآخر إلا بإتلاف المحرر أو بإحداث تعديل في التركيب الكيميائي لاحبار أو مادة الأوراق المستخدمة وفي هذه الحالة يسهل اكتشاف ذلك سواء من خلال المناظرة أو الاستعانة بالخبرة الفنية بالخصوص[2].

[1] محمد محروك، المرجع السابق.

[2] حابت آمال المرجع السابق، ص 113.

أما بالنسبة للتوقيع الإلكتروني، نظرا للطبيعة المادية التي تتميز بها المحررات الإلكترونية، فإن الرابطة بينهما هي رابطة منطقية ترتبط بكفاءة التقنيات المستخدمة في إنشاء التوقيع وتأمين الثقة فيه وكذا تأمين ارتباطه بشكل لا يقبل الانفصال عن المحرر، وبالتالي وجب البحث عن وسيلة تقنية موثوق بها يتحقق بها اتصاله بتلك البيانات، فمثلا التوقيع الرقمي المعتمد على التشفير، وخاصة المفتاح اللامتماثل يؤدي دورا بالغ الأهمية في توفير الارتباط المنطقي بين التوقيع والمحرر على نحو لا يمكن فصل هذه الرابطة و لا يمكن لأحد تعديل مضمون المحرر غير صاحبه لأنه محصن ضد القرصنة ومقاومة الانتهاكات من خلال المفتاح الخاص المعتمد من أحد مقدمي خدمات التصديق الإلكتروني المرخص له بذلك[1].

ثالثا: التحقق من سلامة مضمون المحرر

التحقق من سلامة مضمون المحرر هي وظيفة ثالثة للتوقيع حيث تتأكد هذه الوظيفة من خلال ما تقدمه الدعامة الورقية من ضمانات كعدم قابلية تحريف مضمون المحرر، لأن كل كشط أو تزوير يترك أثره على الحامل الورقي.

وبالتالي يمكن اكتشافه بسهولة سواء من خلال الاستعانة بأهل الخبرة الفنية إذا كان التزوير متقنا أو عن طريق المناظرة. كما يكفل المحرر الورقي عدم المساس بمضمونه الموقع لعدم قابلية انفصال المحرر عن الدعامة مما يحول دون التنصل من الالتزامات الواردة بهذا المضمون، حيث لا يجوز أن يتم انفصال الرابطة بينهما إلا في الحالات التي يسمح بها القانون كما في حالة إنكار الشخص لتوقيعه.

أما بالنسبة للوسيط الإلكتروني وبالمقارنة بالضمانات التي تقدمها الدعامة الورقية فإن الأمر يختلف، ففيما يتعلق بالتوقيعات الإلكترونية كفالة توفير الأمان ينصب على الالتزامات

[1] حابت آمال المرجع السابق ، ص 114.

والبيانات الواردة بمضمون المحرر عبر الشبكة المفتوحة للاتصالات وليس للدعامة الإلكترونية ذات الطابع اللامادي، ويعود ذلك لانفصال الدعامة عن مضمون المحرر[1].

المبحث الثاني

أمن التوقيع الإلكتروني

بتطوّر وسائل الاتصالات الحديثة وتقنية المعلومات أصبحت المعملات الإلكترونية في المجال الاقتصادي تتم عن بعد في بيئة إلكترونية افتراضية بوساطة طرف ثالث مستقل ومؤتمن به، كما أن الحاجة إلى تنظيم مبادلات التجارة الإلكترونية دفعت بمختلف الدول والمنظمات الدولية والجهوية إلى إصدار تشريعات وتنظيمات قانونية خاصة بالمعاملات الإلكترونية، بهدف وضع مخططات تقديم خدمات تصديق إلكتروني وفقا لمستويات أمنية معينة تسمح للدولة المعنية بإتباع نموذج تصديق موثوق به في إطار مرافق المفاتيح العمومية ونظرا لوجود مخاطر تتعرض لها المعاملات الإلكترونية التي يقوم بها المتعاملون في مجال التوقيع الإلكتروني ولردع هذه المخاطر أصبح من الضروري إيجاد تقنيات وآليات للتقليل من المخاطر التي تعاني منها المؤسسات والمستهلكين في الوقت الذي تتم فيه معاملة التجارة الإلكترونية فظهر ما يسمى بالتشفير فهو أفضل تقنية لحماية البيانات والمعلومات المرسلة عبر الشبكات المفتوحة من أي تعديل أو تغيير غير مرغوب فيه ولذلك تأتي تقنيات التشفير في مقدمة الوسائل والأدوات المبتكرة في مجال توفير الأمن وسلامة وسرية المعلومات والمعاملات والصفقات المتبادلة عبر شبكة الانترنت، ومع تزايد العمليات التجارية الإلكترونية على المستوى العالمي والمحلي والتطور الكبير في الوسائل التقنية المستعملة لحماية التجارة الإلكترونية، كان من الإلزامي توفير الحماية التشريعية والقانونية لهذا النوع من التجارة. فالقاعدة العامة تنص

[1] حابت آمال المرجع نفسه، ص 115.

على أن 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 إن تم تزويره، كونه مصلحة يرى المشرع أنها جديرة بالحماية التشريعية، وبالتالي ينص على حمايتها بتجريم الاعتداء عليها وهذا ما سنحاول توضيحه من خلال مطلبين . الحماية الوقائية للتوقيع الإلكتروني (المطلب الأول) و جرائم الاعتداء على التوقيع الإلكتروني (المطلب الثاني).

المطلب الأول

الحماية الوقائية للتوقيع الإلكتروني

تمتع التوقيع الإلكتروني بالحجية القانونية يستلزم إجراءات إنشاء ورقابة موثوقة، وذلك باعتماد الطرف الثالث الموثوق الذي يلعب دور ضامن لصحة التوقيع الإلكتروني، هذا الطرف يكون بدوره خاضع لرقابة الدولة ويتحمل المسؤولية عن أي إخلال بمهامه، مما يوفر جوا من الأمان لدى الأطراف في المعاملات الإلكترونية.

الفرع الأول

التوثيق الإلكتروني

أوجب المشرع على أي شخص يجري تصرفا من خلال شبكة الانترنت أن يقوم بتوثيقه للحفاظ على حقوق المتعاملين من خلال شبكة الانترنت من أي اعتداء أو غش يمكن أن

يمارس من الغير مما استوجب ذلك القيام بالبحث عن طريقة يتم إدراج كافة المحررات الإلكترونية بها ليتم إصدار محررات ذات قيمة قانونية والبعد عن الاعتداء على حقوق الغير[1].

أولا: جهة التوثيق الإلكتروني

للتحقق من صحة التوقيع فلا بد من وجود جهة موثوق بها لربط شخص أو كيان بعينه بالتوقيع، ويتم ذلك باستخدام طرف ثالث محايد يسمى مقدم خدمات التصديق أو مورد خدمات التصديق أو جهة التوثيق[2].

1- تعريف جهات التوثيق الإلكتروني:

جهات التوثيق الإلكتروني أو الغير الموثق هي جهات معينة من قبل سلطات الدولة أو من قبل الأفراد، أو من جهات خاصة أخرى لغاية تأمين المعاملات الإلكترونية والتعامل بالتوقيع الإلكتروني بحيث تعمل على إنشائه وإصدار شهادات تثبت صحته وتقوم بحفظها[3].

ونجد المشرع الجزائري بعد اعترافه بالكتابة والتوقيع الإلكتروني في الإثبات على إثر تعديله لأحكام التنفيذ المدني، قام بإصدار قانون رقم 15-04 مؤرخ في 01 فيفري 2015 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين[4]، الذي تطرق من خلال المادة 4/02 منه إلى منظومة أمن إحداث التوقيع الإلكتروني، المتمثلة في أي جهاز أو برنامج

[1] د محمد فواز المطالقة، المرجع السابق، ص 209.

[2] خالد ممدوح إبراهيم، إبرام العقد الإلكتروني، دراسة مقارنة، دار الفكر الجامعي، 30 ش سوتير الإزاريطة الإسكندرية، 2006، ص 195.

[3] حمودي ناصر، النظام القانوني لعقد البيع الدولي المبرم عبر الأنترنت، رسالة لنيل شهادة الدكتوراه في القانون، كلية الحقوق، جامعة مولود معمري، تيزي وزو، 2009، ص 305.

[4] -قانون رقم 15-04 مؤرخ في 1 فيفري 2015 يحدد القواعد العامة المتعلقة بالتوقيع و التصديق الالكترونين .ج ر عدد 06 الصادر في 10 فيفري 2015

معلوماتي معدّ لتطبيق بيانات إنشاء التوقيع الإلكتروني الفريدة ، كالرموز أو مفاتيح التشفير الخاصة التي يستعملها الموقع في إحداث توقيعيه الإلكتروني، والتي يجب ان تضمن وفقا للمادة 11 من نفس القانون سرية وأحادية البيانات المستخدمة في إحداث التوقيع الإلكتروني مع عدم اكتشافها عن طريق عملية الاستنتاج، وأن لا تغير من البيانات التي ستوقع أو تمنع من عرضها للموقع قبل عملية التوقيع عليها، وأن تمكّن الموقع من حماية توقيعه بطريقة مؤمنة.

أما منظومة فحص التوقيع الإلكتروني الموثوق بها وفقا للمادتين 13و6/02 من نفس القانون، تتمثل في أي جهاز أو برنامج معلوماتي معد لتطبيق بيانات التحقق من التوقيع الإلكتروني، كالرموز أو مفاتيح التشفير العمومية التي يجب أن تضمن تحديد هوية الموقع ومطابقة بيانات إحداث التوقيع الإلكتروني لبيانات فصحه بوضوح، مع كشف أي تغيير أو تعديل في محتوى البيانات الإلكترونية بطريقة مؤمنة، كما يجب على الطرف المعول التأكد من مصداقية البيانات الواردة في شهادة التصديق الإلكتروني الموصوفة.

انطلاقا من ذلك ميز المشرع الجزائري بين التوقيعات الإلكترونية وفقا لمستويات أمان معينة، فالتوقيع الإلكتروني البسيط(Signature électronique simple) وفقا للمادة 02 منه يحتوي على بيانات إلكترونية مرفقه أو مرتبطة منطقيا بالبيانات الإلكترونية الأخرى لاستعمالها كوسيلة توثيق، بينما التوقيع الإلكتروني الموصوف(Signature électronique qualifiée) وفقا للمادة 07 من نفس القانون يعني التوقيع الإلكتروني المؤمن الذي تم إحداثه على أساس شهادة تصديق إلكتروني موصوفة، بموجب آلية أمن إنشاء التوقيعات الإلكترونية الموصوفة

تحت سيطرة الموقع لوحده، بوساطة جهة توثيق إلكتروني مرخص لها من طرف الجهات الرسمية لمزاولة نشاطها[1].

بالأضافة إلى ذلك ميز المشرع الجزائري بموجب المادة 11/02-12 من نفس القانون بين نوعين من سلطات التصديق الإلكتروني بحسب القطاع(الخاص أو العام) الذي تمارس فيه خدمات التصديق، ف (م.خ.ت إ) يقصد به كل شخص طبيعي أو معنوي يقوم بمنح شهادات تصديق إلكتروني موصوفة، وقد يقدم خدمات أخرى في مجال التصديق الإلكتروني أما« الطرف الثالث الموثوق» يتمثل في هيئة شخص معنوي يقوم بمنح شهادات تصديق إلكتروني موصوفة، وقد يقدم خدمات أخرى متعلقة بالتصديق الإلكتروني لفائدة المتدخلين في الفرع الحكومي، كالمؤسسات والإدارات العمومية والهيئات العمومية المحددة في التشريع المعمول به والمؤسسات الوطنية المستقلة وسلطات الضبط، والمتدخلون في المبادلات ما بين البنوك، وكذا كل شخص أو كيان ينتمي إلى الفرع الحكومي بحكم طبيعته أو مهامه[2].

ولقد عرفت المادة الثانية من التوجيه الأوربي رقم 93 لسنة 1999 هذه الجهات بأنها شخص قانوني طبيعي أو اعتباري يقوم بتقديم شهادات إلكترونية للجمهور أو يقدم له خدمات مرتبطة بالتوقيعات الإلكترونية[3].

ومن النصوص التشريعية التي تضمنت كذلك أعمال هذه السلطة المادة 12 هـ من قانون اليونيسترال النموذجي بشأن التوقيعات الإلكترونية لعام 2001 حيث عرفت مقدم خدمة

1 دحماني سمير، التوثيق في المعاملات الإلكترونية دراسة مقارنة، مذكرة لنيل شهادة الماجستير في القانون، فرع قانون دولي للأعمال، جامعة مولود معمري، تيزي وزو، كلية الحقوق والعلوم السياسية، 2015، ص 34.

2 المرجع نفسه، 35.

3 إبراهيم الدسوقي أبو الليل، الحجج القانونية للتعاملات الإلكترونية، مجلس النشر العلمي، الكويت، 2003، ص 180.

التصديق بأنه يعني شخص يصدر الشهادات ويجوز أن يقدم خدمات أخرى ذات صلة بالتوقيعات الإلكترونية[1].

أما قانون التوقيع الإلكتروني المصري فقد جاء خاليا من ثمة تعريف لجهة التوثيق الإلكتروني، وإن كان خطر مزاولة نشاط إصدار شهادات التصديق الإلكتروني إلا بعد الحصول على ترخيص بذلك من الهيئة المختصة وهي هيئة تنمية صناعة تكنولوجيا المعلومات وفقا للقواعد والإجراءات والضمانات التي تحددها اللائحة التنفيذية(م 19)، كما وضع عقوبة جنائية في حالة مخالفة ذلك (م 23).

وقد خصص قانون التوقيع الإلكتروني هيئة تنمية صناعة تكنولوجيا المعلومات وحدها وعلى سبيل الاستئثار، سلطة إصدار وتجديد التراخيص اللازمة لمزاولة أنشطة خدمات التوقيع الإلكتروني(المادة 4/أ)، والترخيص بمزاولة نشاط إصدار شهادات التصديق الإلكتروني (المادة 19)، وتقوم الهيئة بمباشرة تلك الأنشطة من خلال مجلس إدارتها باعتباره هو السلطة المسؤولة عن شؤونها وتصريف أمورها وله في سبيل ذلك وضع نظم وقواعد التوقيع الإلكتروني والمعاملات الإلكترونية، ووضع القواعد الفنية والإدارية والمالية الخاصة بإصدار تراخيص مزاولة نشاط خدمات التوقيع الإلكتروني(المادة9). وعلى الرغم من تنظيم قانون التوقيع الإلكتروني المصري لنشاط جهات التوثيق والتصديق الإلكتروني إلاّ أنه لم يجعل هذا التوثيق إلزاميا على أطراف المعاملة الإلكترونية وإنما ترك لهم حرية اللجوء إليه[2].

أما في القانون التونسي رقم 83 لسنة 2000م بشأن المبادلات والتجارة الإلكترونية استخدم المشرع التونسي مصطلح" مزود خدمات المصادقة الإلكترونية بالنسبة للجهة المختصة

[1] حمودي ناصر، المرجع السابق، ص 306.

[2] د خالد ممدوح إبراهيم، المرجع السابق، ص ص 196-197.

بإصدار شهادات التصديق الإلكتروني، 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[1].

2- مهام جهات التوثيق الإلكتروني:

يمكن تلخيص المهام التي يقوم بها مزود خدمات التصديق فيما يلي:

أ- تحديد هوية المتعاملين في التعاملات الالكترونية وتحديد أهليتهم القانونية للتقاعد والتعامل والتحقق من مضمون هذا التعامل وسلامته وكذا جديته وبعده عن الغش والاحتيال.

ب- تعقب المواقع التجارية على شبكة الانترنت للتحري عنها وعن جديتها ومصداقيتها، وإذا تبين لها عدم أمن أحد هذه المواقع فإنها تقوم بتوجيه رسالة تحذيرية إلى المتعاملين معها توضح فيها عدم مصداقية هذه المواقع.

ج- تقوم بإصدار التوقيع الإلكتروني(الرقمي) وشهادة توثيق هذا التوقيع التي تشهد بمقتضاها على صحته ونسبتيه إلى من صدر عنه.

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

إن السلطة التي تمنح الترخيص بإصدار هذه الشهادات- شهادات التوثيق الإلكتروني هي سلطة واحدة لكن مصدري هذه الشهادات قد يتعددون وذلك بقيام الشركات التي تعمل في مجال

[1] لالوش راضية، المرجع السابق، ص 107.

خدمة الانترنت بوضع برامج إحداث التوقيعات الإلكترونية، ثم منح الشهادات بصحة هذه التوقيعات[1].

ولأننا بصدد دراسة موضوع الإثبات، ولأن هدف التوقيع الإلكتروني في مجال التجارة الإلكترونية هو بالدرجة الأولى تأمين المبادلات الإلكترونية من خلال التأكيد من شخصية الموقع، والتأكد من سلامة وتكامل محتوى الرسالة، مما يضفي جو من الأمان والثقة في المبادلات، ويكون ذلك عن طريق اعتماد تقنيات التشفير التي تخص المعاملات الإلكترونية من الاختراقات والتلاعبات، وذلك من خلال سماحها للمتعاملين الذين لا يتعارفون ويتعاملون عبر الشبكات الإلكترونية من التعرف على بعضهم، ذلك أن هذه التقنية هي تقنية التشفير تحمي الرسالة الإلكترونية وكذلك التوقيع الإلكتروني لاعتمادها على تقنيات فائقة لتحديد شخصية المتعامل، بالإضافة إلى هذا تقوم جهات التوثيق الإلكتروني بتزويد المتعاقدين في مجال التجارة الإلكترونية بشهادات التوثيق الإلكتروني[2].

3- مسؤولية جهات التوثيق الإلكتروني

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 على صحة البيانات التي صدق عليها، وعن نسبة التوقيع لصاحبه في تاريخ تسليم شهادة لمن يتسلمها[3]، تقوم هذه المسؤولية

---

[1] عبد الفتاح بيومي حجازي، حماية المستهلك عبر شبكة الانترنت، دار الفكر الجامعي، الإسكندرية، 2006، ص 103.

[2] حمودي ناصر، المرجع السابق، ص 311.

[3] سعيد السيد قنديل، التوقيع الإلكتروني، ماهيته، صوره، حجيته في الإثبات بين التداول والاقتباس، دار الجامعة الجديدة الإسكندرية، 2006 ص 92.انظر كذلك : Patrick Thiefry : l'émergence d'un droit européenne du commerce électronique, revue trimestrielle du droit européenne, p 672.

طبقا للمادة1/8 من التوجيه الأوربي المتعلق بالتوقيع الإلكتروني، و تقريبا من ذلك المادة 8 من القانون النموذجي للجنة القانون التجاري الدولي التابعة للأمم المتحدة[1]،إلاّ أنه يجوز لمقدم خدمات التصديق إثبات عدم وجود أي خطأ من جهة، وأنه قام بواجبه كما ينبغي من حفظ لسرية البيانات الشخصية الخاصة بعمله وصحة البيانات المدونة على الشهادة التي يصدرها ونسبتها لصاحبها، ولا ريب في أن عبء الإثبات الذي يقع على عاتق مقدم خدمة التصديق هو امر 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 مسؤولا 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، وإلا فإنه يكون هو المسؤول عن صحتها، إلا أن مقدم خدمة التصديق الإلكتروني يكون مسؤولا في حالة نسيانه تسجيل إلغاء الشهادة او في حالة وجود إهمال من جانبه يؤدي إلى إلحاق ضرر بالغير[2].

كي يضمن مقدم خدمة التصديق صحة البيانات الواردة في الشهادة له عند إصدارها أن يطلب من طالبها كل ما يفيد وثائق تأكد هويته، والتي لا يتحمل مسؤولية تزويرها من قبل مقدمها[3]، كما أنه يجب على الغير أن يتأكد من صلاحية شهادة التصديق من حيث مدتها وما

[1] حمودي ناصر، المرجع السابق، ص 319.

[2] سمير حامد عبد العزيز الجمال، النقادات عبر تقنيات الاتصال الحديثة، دراسة مقارنة، دار النهضة العربية، 2006، ص 346.

[3] سعيد السيد قنديل، المرجع السابق، ص 95.

لحقها من تعديل أو إلغاء والغرض من استخدامها ، وذلك بالرجوع إلى السجل الإلكتروني الذي ينشره مقدم خدمة التصديق عبر الانترنت[1].

نظرا لأهمية شهادة التصديق الإلكتروني، وخطورة المعلومات التي تتضمنها والتي يعول عليها الغير لدى إتمام تعاملاتهم، فإن دور جهات التصديق الإلكتروني 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 الإلكتروني، فإنه كان لزاما تحديد المسؤوليات في حالة حدوث إخلال بالالتزامات المناطة بجهات التوثيق الإلكتروني، حيث بقدر المسؤولية التي تتحملها هاته الجهات تكون الثقة التي تؤمنها لدى المتعاملين[2].

ثانيـــا- شهادة التوثيق الإلكتروني:

تقوم جهات التوثيق الإلكتروني بتزويد المتعاقدين في مجال التجارة الإلكترونية بشهادات التوثيق الإلكتروني، وهي تلك الشهادات التي تثبت نسبة التوقيع الإلكتروني إلى الشخص مصدره استنادا إلى إجراءات توثيق معتمدة[3]، وتقدم هذه الشهادات الدليل على أن صاحب الشهادة هو الشخص صاحب المفتاح العام، وشهد بأن التوقيع الإلكتروني هو توقيع صحيح ينسب لمن أصدره، ويستوفي الشروط والضوابط المطلوبة فيه باعتباره دليل إثبات يعول عليه.

إضافة إلى تقديم مجموعة من المعلومات عن هوية الشخص الموقع وعن سلطة التصديق التي أصدرتها، و المفتاح العام وتاريخ إصداره وانتهاء صلاحية الشهادة، وحدود مسؤولية

[1] سمير حامد عبد العزيز الجمال، المرجع السابق ، ص 346.

[2] إبراهيم الدسوقي أبو الليل، الجوانب القانونية للتعاملات الإلكترونية، المرجع السابق، ص 188.

[3] حمودي ناصر، المرجع السابق، ص 311.

مصدرها، ومعلومات أخرى بحسب مستوى الشهادة والغرض من إصدارها وحجم الصفقات التي يستخدم فيها المفتاح[1].

إن الغرض من شهادة التوثيق الإلكترونية هو تأكيد أن التوقيع الإلكتروني أو الرسالة الإلكترونية بصفة عامة صادرة ممن نسبت إليه، وأن توقيعه صحيح، كما تؤكد الشهادة أن

البيانات الموقع عليها بيانات صحيحة صادرة عن الموقع، ولم يتم التلاعب فيها، ولم يطرأ عليها اي تبديل سواء بالحذف أو بالإضافة أو التغيير فهذه البيانات تصبح موثقة ولا يمكن إنكارها.

ويمكن التحقق من المعلومات السابقة عن طريق استخدام المفتاح العام لمن صدرت عنه الشهادة الإلكترونية، والذي يكون مذكورا في الشهادة نفسها نظرا لارتباطها بين هذا المفتاح العام والمفتاح العام والمفتاح الخاص لصاحب الشهادة ويجب في شهادة التصديق الإلكتروني أن تستجيب لمقتضيات السلامة والوثوق بها، ويتم ذلك باستخدام أنظمة معلوماتية متطورة تحقق الأمن وتخلق الثقة لدى من يتعامل معولاً على هذه الشهادة[2].

في الواقع فإن هناك مستويات عدّة لشهادة التوثيق التي تصدرها سلطات التصديق تبعا لنوع الوثائق الثبوتية المعتمدة للتأكد من الشخصية فوفقا لشركة(Belsing) وهي إحدى شركات سلطات التصديق العالمية فإن هناك ثلاثة مستويات من شهادات التصديق:

المستوى الأول(الأدنى) يتطلب إصداره من المشترك، أن يقدم عنوانا إلكترونيا صالحا للاستعمال ليتم إصدار شهادة مجانية تستعمل في معاملات ذات قيم مالية منخفضة في حين

[1] إبراهيم الدسوقي أبو الليل، المرجع السابق ص 183. كذلك: عمر حسن المومني، التوقيع الإلكتروني وقانون التجارة الإلكترونية ، الطبعة الأولى، دار وائل للنشر، الأردن ، 2003، ص 64.

[2] إبراهيم الدسوقي ابو الليل، المرجع السابق، ص 184.

أن المستوى الثاني(الأعلى) يتطلب من المشترك الحضور أمام سلطة تسجيل محلية وبحوزته وثائق الثبوتية قبل إصدار شهادة توثيق له يمكن استعمالها في معاملات مالية ضخمة.

كما أن شهادات التوثيق قد تختلف أيضا من حيث وظيفة كل منها. فهناك شهادات تعرف فقط بشخصية المشترك دون تقديم بيانات أخرى، وشهادات تصدر لكي تستعمل في تعامل واحد فقط وشهادات أخرى تستعمل من قبل أشخاص مخولين للتوقيع على شركة أو هيئة معينة[1]، وإضافة إلى شهادة توثيق التوقيع، هناك شهادات أخرى تتنوع بحسب الهدف منها ومن أمثلة ذلك:

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

2- شهادة الإذن Authoringing certificate : وبمقتضاها يتم تقديم معلومات إضافية عن صاحبها، مثل عمله ومؤهلاته والترخيصات التي يملكها.

3- شهادة البيان Attesting certificate : والتي تفيد في بيان صحة واقعة معينة أو حدث ما وقت وقوعه[2].

وغالبا ما تصدر الشهادة لفترة محدودة، و بمجرد انتهاء مدتها فإنها تصبح غير قابلة للاستعمال. حيث يتم غالبا رفضها تلقائيا من قبل برمجيات المستقبل، ولهذا فإن سلطات التصديق غالبا ما تقوم بإعداد ونشر قائمة بالشهادات الصالحة للاستعمال وأخرى للشهادات التي تنتهي فترة استعمالها وتصبح غير صالحة للاستعمال لأسباب أخرى. كما يمكن أن يتم

[1] عمر حسن المومني، المرجع السابق، ص 65.

[2] إبراهيم الدسوقي أبو الليل، المرجع السابق، ص 186.

إبطال مفعول الشهادة بالسيطرة على مفتاحه الخاص أو يتم كشفه، حيث يقع على عاتقه في مثل هذه الحالة إبلاغ سلطة التصديق أو الجهة المزودة بالتوقيع الرقمي وذلك حتى يتم إلغاؤه ونشر و إعلان ذلك إلكترونيا من خلال سلطة التصديق تحت طائلة تحمل الطرف المقصر المسؤولية اتجاه أي متعامل حسن النية يستند إلى شهادة التصديق التي يتم إلغاؤها.

الفرع الثاني

التّشفير كوسيلة لحماية التّوقيع الإلكتروني

أولا: مفهوم التّشفير

يعرف التّشفير بأنه: « كلّ العمليات التي تؤدي بفضل بروتوكولات سرّية إلى تحويل معلومات أو إشارات مفهومة(مقروءة) أو القيام بالعكس وذلك باستخدام برامج مصممة لهذه الغاية» ويعرف أيضا بأنه آلية يتم بمقتضاها ترجمة معلومة مفهومة إلى معلومة غير مفهومة عبر تطبيق بروتوكولات سرية قابلة للإنعكاس، أي يمكن إرجاعها إلى حالتها الأصلية[1].

بالتالي فلقد إنفرد المشرع التونسي في نصوصه عن باقي التشريعات العربية الخاصة بالتجارة الإلكترونية بتعريف التشفير، كذلك الحال بالنسبة إلى مشروع قانون التجارة الإلكترونية المصري، فعرفه المشرع التونسي على النحو التالي (التشفير عبارة عن استعمال رموز وإشارات غير متداولة تصبح بمقتضاها المعلومات المرغوب تحريرها أو إرسالها غير قابلة للفهم من قبل الغير أو استعمال رموز وإشارات لا يمكن وصول المعلومة بدونها» كما عرّفه مشروع قانون

[1] كريم لملوم، المرجع السابق ص 167.أنظر كذلك:
Bensoussan Alaine, signature électronique et preuve: evolution on révolution, pp49-50.

التجارة الإلكترونية المصري بأنه: « تغير في شكل البيانات عن طريق تحويلها إلى رموز أو إشارات لحماية هذه البيانات من إطلاع الغير عليها أو تعديلها أو تغييرها[1].

ومن خلال التعريف السابق نجد أنّ التشفير يعتمد على عمليات رياضية يتم بها تحويل النص المراد إرساله إلى رموز وإشارات لا يمكن فهم محتواها إلاّ بواسطة فك الشفرة وتحويل الرموز والإشارات إلى نصوص مقروءة ومفهومة باستخدام مفاتيح التشفير العامة والخاصة فهذه العملية لا تتم إلاّ إذا كان مستقبل الرّسالة يملك مفتاح التشفير الذي يحول الإشارات والرّموز إلى النّص الأصلي[2].

ثانيا-أنواع التّشفير: ينقسم التّشفير إلى نوعين هما: التشفير بالمفتاح المماثل والتشفير بالمفتاح غير المماثل، المزدوج وسف نتناول هاذين النّوعين على النحو التالي:

1-التّشفير بالمفتاح المماثل: يسمى أيضا بالنظام السيمتري، ويتمثل هذا النوع من التّشفير باستخدام كل من المرسل والمستقبل نفس المفتاح السّري للتّشفير، 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 التّشفير، حيث يحرّر المرسل الرّسالة ثم يقوم بتشفيرها بالمفتاح المماثل، وذلك بتحويل الرّسالة من صورتها المقروءة والمفهومة إلى رسالة رقمية غير مقروءة تتخذ أشكالاً ورموزا وعلامات غير مفهومة ، ثم يقوم بإرسال الرّسالة وكذلك المفتاح المماثل الذي شفّر به بيانات المحرر الإلكتروني إلى المرسل إليه، ليتمكن هذا الأخير من فك شفرة هذه الرّسالة وإعادتها إلى حالتها الأصلية.

---

[1] محمد فواز المطالقة، المرجع السابق ص 159.

[2] أسامة بن غانم العبيدي، "**حجية التوقيع الإلكتروني في الإثبات**"، المجلة العربية للدّراسات الأمنية والتدريب، المجلد 28-العدد56 ص 158/157.أنظر كذلك: Bensoussa Alaine, op cit, p-p 50-51

تتميز هذه الطريقة بالسرعة والسهولة في إجراء التشفير، حيث لا تحتاج إلى حساب آلي ذو تقنية متطورة أو وقت طويل في فك التشفير. ما يعاب عليها هو عملية تبادل المفتاح المماثل بين المرسل والمرسل إليه، فعملية التبادل تشكل خطورة على بيانات المحرر الإلكتروني المرسلة، لعدم توفر الأمان والثقة في هذا النوع من التشفير وهو ما أدى إلى تراجع إستخدامه.

هذا ما أوجب اللجوء إلى وسيلة اتصال آمنة يتم من خلالها إبلاغ المرسل إليه مفتاح فك التشفير لذلك فإن التعامل بالنظام السيمتري (التشفير بمفتاح المتماثل)، مقصور على الأشخاص التي تربطهم علاقة تعارف مسبقة وأيضا هذا النظام فعال في الشبكات المختلفة كشبكات الانترانيت وشبكات الاكسترانيت.

وبالتالي فإن التشفير المماثل (Syptolegie Symetrique) فقد استخدم هذا النوع من التشفير في البداية لتشفير التوقيع الإلكتروني الرقمي وفيه يستخدم كل من مصدر الرسالة والمرسل إليه نفس مفتاح التشفير لفك رموزها كما سبق وذكرت أعلاه، وقبل إرسال الرسائل المشفرة يتم إرسال مفتاح التشفير إلى المرسل إليه بطريقة آمنة ليستطيع فك الشفرة ولكنه في الحقيقة غير آمن لأن الشخص المرسل والمستقبل يمتد كان المفتاح نفسه[1].

2- التشفير غير المماثل:

هذا النوع من التشفير يقوم على وجود مفتاحين هما مفتاح عام(Cle publique) معروف ومتاح للجميع يتم استخدامه في عملية التشفيرو مفتاح خاص(Clé priver) غير معروف لأي شخص إلا الشخص مرسل الرسالة. وهو النظام المعروف"بالسيمتري" فالمفتاح العام يتميز عن المفتاح الخاص كونه معروفا ومتاحا إلكترونيا لطرفين أو أكثر غير أن هذا التمايز الذي يخص المفتاح العام لا يفصله عن المفتاح الخاص، لأنهما مترابطان في عملهما، ويكمل كل

[1] هالة جمال الدين محمد محمود، المرجع السابق، ص 345.

منهما الآخر. فإذا استعمل المفتاح الخاص لتشفير الرسالة فلا يمكن فك التشفير إلاّ بالمفتاح العام كما أنه لو عرف أحد المفتاحين فلا يمكن معرفة المفتاح الآخر حسابيا[1].

ولقد تم البحث عن هذا النوع من التشفير نظرا لعدم نجاح النوع السابق ويؤدي الغاية المرجوة منه على أفضل وجه، وتم التوصل إلى هذا النوع الجديد ألا وهو التشفير المتماثل المذكور أعلاه لحل مشكلة التوقيع الغير الأمن للمفاتيح في التشفير المتماثل.فتم الاستغناء عن نوع واحد من المفاتيح وعوضا عنه تم استخدام مفتاحين في التشفير اللا متماثل تربط بينهما علاقة رياضية متينة، ويطلق على نظام التشفير الذي يستخدم المفاتيح العامة بنظام(RSA) وبالرغم من هذا النظام أفضل وأكثر أمنا من نظام(DES) إلاّ أنه يحتاج إلى وقت أكثر في القيام بعملية التشفير أو فكّها. إذ أن عملية التشفير وفك التشفير يجب أن تتزامن في الغالب كما أن نظام(RSA) لا يتمتع بدرجة عالية من الأمن فمن المتوقع أن تتم عملية الاختراق. إذ أنّ اختراقه أمر ممكن إذ توفر ما يلزم من ذلك من وقت ومال ولمحاولة الحد من الاختراقات التي تحدث تم تطوير نظام يسمى نظام(PGP) [2]. وبالإضافة إلى هذين النوعين المذكورين سابقا سنحاول بيان أنواع أخرى للتشفير بدرجة من التفصيل وبالذات من الناحية الفنية وذلك على النحو التالي:

3- **الخصوصية المتميزة (PGP):** تعدّ هذه الطريقة من أجود الطرق المستخدمة في تشفير البيانات كما ذكرنا سابقا. ومن أكثر الطرق المستخدمة في تشفير البيانات، ذلك لأن هذه الطريقة أكثر أمانا وتمكن من مواجهة أي اعتداء على البيانات المشفرة ليتم فك الشفرة الخاصة وتحويلها إلى بيانات مقروءة، لأنه يتوفر .... ذو مستوى عالي من الخبرة قائمون على إدارة

[1] براهيم سليمان عبد الله، التجارة الإلكترونية أمن المعلومات، مقال منشور على البريد الإلكتروني:
www.kau.edu.sa/iabdullah.

[2] محمد فواز المطالقة، المرجع السابق ص 165.

ممتازة ومرنة، بالإضافة إلى توافر العديد من المعادلات الخوارزمية ذو مستوى عالي وتستخدم في التشفير، وهذه العوامل هي التي أكسبت هذه الطريقة الشهرة العالمية فأصبحت من أشهر أساليب تشفير البيانات المستخدمة في الرسائل الإلكترونية، لتوفير الأمن للبيانات المرسلة والمتداولة من خلال شبكة الانترنت.

ويتم استخدام مفتاح التشفير مزدوج الوظيفة بحيث يقوم هذا المفتاح بتشفير النص ومن ثم يتم فك الشفرة وتحويل النص المشفّر إلى الوضع الذي كان عليه من خلال استخدام نفس المفتاح الذي تم التشفير به، ويطلق على هذا المفتاح تسمية(Cryptosystems) وهذا المفتاح من المفاتيح التقليدية المستخدمة في التشفير، وأهم ما يميز هذا البرنامج أنه يستخدم في التشفير مفتاحا بطول(128 bit).

يحقق هذا التصرف الغاية من أجلها تم التوصل إلى هذه الأساليب المستخدمة في حماية التعاملات أو المعاملات التي تبرم من خلال شبكة الانترنت وإبرام معاملات إلكترونية آمنة فمن الضروري أن يتقيد المستخدم لهذه الأساليب ببعض الشروط التي منها ما يتوجب توافره لضمان الأمن والسرية وعدم تمكن الغير من اكتشاف ومعرفة المفتاح السري الذي يتم التشفير به[1].

4- **تشفير القرص الصلب:** لم يقتصر التشفير على البيانات فقط بل وصل الأمر إلى القيام بتشفير القرص الصلب لجهاز الحاسب الآلي، فالقيام بعملية تشفير القرص الصلب تتم بالبساطة والسهولة، وتحقق أمانا أكثر من أية عملية تشفير أخرى، فاستخدام هذه الطريقة يوفر أكبر قدر ممكن من الأمن والحماية لمستخدمي الشبكة من خلال عدم إتاحة القرصنة للغيرللقيام باقتحام البيانات المتوافرة على أجهزة الحاسب الآلي والإطلاع عليها والاعتداء على خصوصية

[1] فواز المطالقة، المرجع السابق، ص 167.

طرفي العلاقة الذين قاما بتشفير البيانات المتبادلة بينهما بهذه الطريقة السهلة الاستخدام ولا تحتاج متخصص في البرمجة ليقوم بعملية التشفير فيتم التشفير من خلال القيام بحجز مساحة معينة من القرص الصلب المتوافر على جهاز الحاسب، ومن ثم عمل قرص افتراضي منفصل عن القرص الأصلي، يتم إدراج كافة البيانات الضرورية بالمستخدم،بحيث لا يتمكن الغير من الدخول إلى القرص الافتراضي والإطلاع على البيانات التي يحتويها هذا القرص[1].

5-**التشفير المزدوج:** هذا النوع من التشفير هو عبارة عن نظام مختلط بين النظامين السابقين **(التشفير المماثل، التشفير غير المماثل)** وفيه يتم تشفير الرسالة بمفتاح خاص، ثم تشفير المفتاح الخاص بمفتاح عام وإرسال كل من الرسالة المشفّرة والمفتاح الخاص المشفر إلى المرسل إليه، ويجب عدم الخلط بين التوقيع الإلكتروني وتشفير الرسالة الإلكترونية فإذا كان كلاهما يقوم على عملية حسابية يتم من خلالها تشفير مضمون التوقيع والرسالة لكنهما يختلفان لأن تشفير الرسالة يشملها بأكملها في حين أن التشفير في التوقيع الإلكتروني يقتصر على التوقيع دون بقية الرسالة بحيث يمكن أن يربط التوقيع برسالة غير مشفرة[2].

ثالثا: مستويات التشفير

توجد عدّة مستويات للتشفير فقد يكون على مستوى الإرسال أو على مستوى التنقل أو التصفح، كما قد يكون على مستوى التطبيق أو التقنية، وأخيرا التشفير على مستوى الملفات، وسوف نقوم بدراسة هذه المستويات على النحو التالي:

1- **التشفير على مستوى الإرسال:** يتم في هذا المستوى تشفير جميع المعلومات والبيانات بين نقطة الإرسال ونقطة الاستقبال، ويتم عن طريق الشبكات الافتراضية الخاصة، وهي شبكات

[1] د محمد فواز المطالقة، المرجع السابق، ص ص 168-169.

[2] هالة جمال الدين محمد محمود، المرجع السابق، ص 346.

جزئية من شبكة الانترنت، تقوم فيه إحدى المشروعات بتخصصه(خدمتها عن طريق إحاطته بالاحتياط التأمينية المطلوبة لإرسال واستقبال المعلومات من خلاله بشكل آمن أي تبادل المعلومات بشكل آمن على شبكة الانترنت، ويتم عن طريق تشفير جميع البيانات والمعلومات من نقطة الإرسال إلى نقطة الاستقبال[1].

2- التشفير على مستوى التّصفح والتنقل: وفقا لهذا المستوى يتم تشفير جميع الاتصالات بين نوافذ الشبكة أو أحد برامج التصفح وأحد مقار المعلومات أو المواقع الموجودة عليها، ممّا يؤدي إلى حماية البيانات أثناء انتقالها، وقد أعلنت شركة(Netscape) أحد البروتوكولات الأمنية عام 1995 وهو بروتوكول(Secureso chat layer) والمعروف اختصارا:SSL وتمكن مهمة أو وظيفة هذا البروتوكول في تشفير جميع الاتصالات على النحو المذكور سابقا. الأمر الذي يقلل من فرصة نسخ أو وصول البيانات إلى أي شخص غير مرغوب فيه وقصر وصولها للمستقبل النهائي، مما قد يعطي هذا الأمر شكلا من أشكال الثقة والأمان للعملاء، لأن المعلومات والبيانات الخاصة بهم فيها أرقام بطاقة الإئتمان لتكون متاحة سوى للتاجر أو المنشأة أو المؤسسة المراد التعامل معها عن طريق هذه الشبكة دون غيرها، وبالتالي عندما يرغب أحد المستهلكين بشراء سلعة على مستوى الانترنت، يقوم بالدخول على الموقع الخاص بالمؤسسة المراد التعامل معها(website) وبعد اختيار الشيء المراد شراءه يدخل إلى الطريق الآمن لإتمام عملية الشراء، مما يؤدي إلى انتقال الموقع على المقر او الخادم الأمن sewre) (serverعندها يتم تشفير جميع قنوات الاتصال والإرسال بين نافذة شبكة المعلومات ومقر المعلومات ويتغير بداية اسم مقر المعلومات من HTTP إلى HTTP[2] بروتوكول SSL قد بدأ عمله أثناء إتمام الصفقة التجارية، وبمجرّد وصول تلك البيانات إلى مقر المعلومات يتم حل

[1] لالوش راضية، المرجع السابق، ص ص 99-100.

الشفرة بواسطة برنامج خاص لاستخراج أمر الشراء. ويعتبر هذا البروتوكول الأكثر انتشارا واستخداما[1].

3- **التشفير على مستوى التطبيق والتنفيذ:** يتمثل في نظام التأمين الخاص بالمعاملات الإلكترونية SET. ويتم فيه تشفير طلب الشراء وعملية الدفع عبر شبكة online. ويعتبر هذا النظام من أهم البروتوكولات المتعلقة بالنواحي التي ظهرت في مجال منظومة التجارة الدولية.
يتطلب العمل بنظامset فتح حساب بنكي لكل من البائع والمشتري بأحد البنوك المستخدمة له واستخدام المشتري لأحد برامج التصفح. نوافذ شبكة المعلومات المدعم بنظامset واستخدام البائع لمقر معلومات Server هو أيضا بدوره يدعم هذا النظام.

عندما يقوم المشتري بفتح حساب في البنك يقوم هذا الأخير بإرسال كل من شهادة خاصة بالمشتري ومفتاحين للتشفير إحداهما 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 كل واحد منهما بملف من ملفات الحساب الآلي. وأثناء الصفقة التجارية يتم تبادل ملفات الشهادات بين البائع والمشتري وذلك يتم بصورة مشفرة بحيث لا يستطيع أي شخص آخر الإطلاع عليها، وبعد تأكد كلا من التاجر والمشتري من هوية الآخر، يتبادل الشهادات المشفرّة وحل شفرتها، وبالتالي تأتي الخطوة الأخيرة المتمثلة في عملية الدفع مقابل السلعة أو الخدمة المراد شرائها، ويتم ذلك عن طريق المشتري لبطاقة الإئتمان الخاصة به، وبالتالي لا يستطيع حل الشفرة إلاّ البنك الضامن لكل من البائع والمشتري. ويتوجب على البائع أن يتأكد من أن طلب الشراء الذي قام بإستقباله هو نفس الطلب الذي تم إرساله من قبل المشتري عن طريق بصمة خاصة يحملها طلب الشراء، وبعد ذلك يقوم البائع بإرسال نسخة من طلب الشراء والبيانات الخاصة بإجراءات عملية الدفع إلى البنك، حيث ينتظر

[1] لالوش راضية، المرجع السابق، ص 100.

اعتماد البنك للصفقة بعد التأكد من هوية البائع وصحة الرسالة، وكذلك التأكد من رصيد المشتري الذي يسمع بإتمام الصفقة وهكذا يسمح للبائع بإتمام الصفقة على هذا الأساس[1] ويستطيع البائع أن يقوم بإرسال ما هو مطلوب شرائه إلى المشتري سواء كان عبر شبكة المعلوماتonline أو عن طريق إرساله بالطرق التقليدية التي تعتمد على التنقل أو الشحن[2].

4- **التشفير على مستوى الملفات:** وفقا للبرنامج التأميني الذي وضعه فليب زمرمان philp zimmerman لحماية الرسائل الإلكترونية عام 1995 والذي يطلق عليه اختصارpgp، يتم التشفير هنا على مستوى الرسائل الإلكترونية والملفات التي يتم تداولها فيتم تشفير البيانات التي تحتويها الرسائل باستخدام الأسلوب العام clé publique. ويتميز هذا البرنامج بسهولة استخدامه وفي نفس الوقت صعوبة الهجوم عليه.

يعتمد(pgp)-(pretty good privacy) في حل الشفرة الخاصة بالرسالة المشفرة به على استخدام المفتاح الملائم لحل الشفرة. وهكذا فإن أية تجربة لأي مفتاح آخر غير المفتاح المطلوب لحل الشفرة يعتبرمن المهام المستحيلة التي لا يمكن أن تنجح[3].

رابعا: ضوابط التشفير: تتمثل ضوابط التشفير فيما يلي:

1- إباحة تشفير البيانات والمعلومات التي يتم كتابتها أو التعامل فيها باستخدام الوسائل الإلكترونية: نجد على سبيل المثال وليس الحصر أن القانون التونسي الخاص بالمبادلات والتجارة الإلكترونية تعامل معه بشكل مباشر من خلال نصوص خاصة، حيث أن غالبية التشريعات المقارنة وضعت قواعد ونصوص قانونية تتعامل مع تشفير البيانات والمعلومات

[1] لالوش راضية، المرجع السابق ، ص 100.
[2] المرجع نفسه، ص. ص 101- 102.
[3] المرجع نفسه، ص 103.

وأصدرت تلك الدّول قوانين خاصة بالتجارة الإلكترونية لتتعامل بالتشفير، فقد أحاز استخدامه في المراسلات الإلكترونية وفي المعاملات الإلكترونية عبر شبكة الانترنت.

كما أكد قانون المبادلات والتجارة الالكترونية التونسي أهمية حماية البيانات المشفرة والعناصر المستخدمة في عملة التشفير وفكها من أي اعتداء عليها سواء تم ذلك لاستخدام التشفير في ارتكاب جرائم احتيالية أو سرقة مفاتيح التشفير التي تفك النص المشفر وترجعه إلى النص الأصلي باستخدام مفاتيح التشفير الخاصة[1].

وقد عالجت التشريعات العربية الخاصة بالتجارة الإلكترونية عملية التشفير بطريقة غير مباشرة، كما تطرقنا سابقا من خلال التوقيع الإلكتروني وذلك باستثناء المشرع التونسي الذي تعامل مع عملية التشفير بشكل مباشر من خلال نصوص خاصة به منعا لاختلاف التفسيرات والاجتهادات الفقهية بشأنها.

2- **الحفاظ على سرية البيانات والمعلومات المشفرّة:** يتطلب ذلك الاعتراف بحق أصحابها في سرية تلك البيانات والمعلومات وتجريم الاعتداء عليها. فقد اعتبر مشروع قانون التجارة الإلكترونية المصري أنّ الاعتداء على البيانات المرسلة بين طرفي العقد عبر شبكة الانترنت هو اعتداء على خصوصية وسرية البيانات والمعلومات المرسلة من طرفي العلاقة، لأن تلك البيانات والمعلومات تتميز بالخصوصية والسرية وتعبر عن إرادة الطرفين بالقيام بتصرف قانوني وإطلاع الغير على هذه البيانات والمعلومات يمكن أن يؤدي إلى إلحاق الضرر بطرفي العلاقة والاعتداء على خصوصيتهم بمعرفة البيانات التي تم كشفها بعد فك التشفير[2].

[1] مد حت عبد الحليم رمضان. الحماية الجنائية للتجارة الإلكترونية ، دار النهضة العربية، القاهرة، 2001، ص 31، أنظر أيضا لورنس محمد عبيدات، إثبات المحرر الإلكتروني، دار الثقافة للنشر والتوزيع ، عمان 2002، ص 132.

[2] لورنس محمد عبيدات، المرجع السابق ص 136.

وقد وضع المشرع المصري رضوما في قوانين التجارة الإلكترونية تعاقب كل من يقوم بانتهاك سرية البيانات المشفرة وإفشائها، سواء كان ذلك بشكل مباشر أو عن طريق النص على أن اي اعتداء يقع على التجارة الإلكترونية يعد مخالفا لأحكام القوانين وبالتالي يعاقب العقوبة المقررة[1].

3- **اعتبار استخدام التشفير وسيلة يعتد بها قانونا: في تحرير البيانات والمعلومات من قبل الجهة المختصة،** كأثر لإقرار المشرع للنص المشفر وحجيتة في إثبات التصرّفات القانونية، فإنه يعتبر من المحررات الإلكترونية، حيث يمكن تحويل الإشارات والرموز إلى نصوص مقروءة ومفهومة تكون بمثابة حجة على من قام بمخالفة الاتفاق المبرم بين الطرفين[2].

خامسا: طرق التشفير:

يتم التشفير من خلال استعمال المفاتيح الخاصة في عملية تشفير الرسالة و فك تشفيرها، ويكمن ذلك في إعادة النص إلى ما كان عليه في السابق فيتم الاستعانة بمفتاحين مختلفين مرتبطين بشكل حسابي لإنشاء التوقيع الإلكتروني، وتحويل المعلومات والبيانات ثم القيام بتثبيتها مرّة أخرى بنظام التشفير غير المماثل ولا يستطيع أي شخص آخر ولو كان يعرف مفتاح الشفق العام اكتشاف المفتاح الخاص بالموقع واستخدامه في التعرف على مستوى الرّسالة، والمفتاح الخاص يكون معروفا لدى جهة واحدة فقط أو شخص واحد وهو المرسل، ويستخدم لتشفير الرّسالة وفك شفرتها أما بالنسبة للمفتاح العام فبالعادة يكون معروفا لدى أكثر من جهة أو شخص.

[1] د أسامة بن غانم العبيدي، المرجع السابق ص 160.

[2] عبد الفتاح الحجاري، النظام القانوني لحماية التجارة الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2002 ص 250.

يمكن ان تنجم مجموعة من الأضرار تعود على صاحب الشّفرة أو قد تضر بالغير في حالة اذا ما قام أحد ما بإنشاء البيانات والمعلومات الموجودة بالشفرة وقام بنشرها بعد القيام بفكها. في هذه الحالة يتوجب على الهيئات المختصة بتسليط عقوبة على من يقوم بفك الشفرة وإفشاء المعلومات المشفرة نظرا للأضرار التي تنجم عن هذا الفعل[1].

المطلب الثاني:

الجرائم المتعلقة بالتوقيع الالكتروني

أصبح التوقيع الإلكتروني إحدى وسائل الحماية المدنية للمعاملات المتعلقة بالتجارة الإلكترونية، 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 لتطوّر التقنية، حتى تظل الفرصة سامحة لهم لارتكاب جرائمهم، فتولدت جرائم مستحدثة تحدث في البيئة الإلكترونية، أو ترتكب بوسائل إلكترونية تسمى الجريمة المعلوماتية.

الفرع الأول:

صور جرائم التوقيع الإلكتروني

تعرف الجريمة عموما في نطاق القانون الجنائي أنها فعل غير مشروع صادر عن إرادة جنائية يقرر له القانون عقوبة أو تدبيرًا احترازيا.

[1] عبد الفاتح الحجازي، المرجع السابق ص 250.

أولا: الجريمة المعلوماتية:"هي كل فعل ضار يأتيه المواطن عبر استعماله لوسائط إلكترونية مثل الحواسيب أجهزة الموبايل، شبكات الاتصالات الهاتفية، شبكات الانترنت أو الاستخدامات غير القانونية للبيانات الحاسوبية أو الإلكترونية عموما، فتطور الانترنت وزيادة عدد المستخدمين لها في العالم جعل منها وسطا ملائما للتخطيط وتنفيذ الجرائم بعيدا عن أعين الجهات الأمنية[1].

إن الجريمة المعلوماتية تستهدف في جوهرها المعلومات بمفهومها الواسع، من بيانات ومعلومات وبرامج تطبيقية، حيث تقوم هذه الجريمة على اعتبارين مهمين أو لهما أن تكون المعلوماتية وسيلة للغش والتحاليل والاعتداء والثاني ان تكون المعلوماتية نفسها محلا للاعتداء.

يعرف المشرع الجزائري الجريمة المعلوماتية في المادة 2 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بأنها: "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحدّدة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام به الاتصالات الإلكترونية.

من هذه التعاريف يمكن أن نستخلص أن الجريمة المعلوماتية هي التي يكون موضوعها النظام المعلوماتي، أي البيانات نفسها التي تتداول عبر قنوات الاتصال، مما يعرض التوقيع الإلكتروني لخطر التزوير والغش وعرضه للعديد من الجرائم التي سيتم التطرق إليها فيما يلي[2]:

ثانيا: جريمة تزوير التوقيع الإلكتروني:

[1] لالوش راضية، المرجع السابق، ص 133. أنظر كذلك سوير سفيان، جرائم المعلوماتية، مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2010-2011، ص ص 9-10.
[2] لالوش راضية، المرجع نفسه، ص 135.

يتمثل الركن المادي لهذه الجريمة في تزوير التوقيع الإلكتروني بتغيير الحقيقة في التوقيع الإلكتروني بطريقة الاصطناع أو التعديل أو التحويل، وبأي طريق على نحو يضر بالغير ومن أشهر الوسائل التي يمكن الاعتماد عليها في تزوير التوقيع الإلكتروني استخدام برامج حاسوبية وأنظمة معلوماتية خاصة بذلك، يتم تصميمها على غرار البرامج والأنظمة المشروعة أو محاولة البعض كسر الشفرة والوصول إلى الأرقام الخاصة بالتوقيع الإلكتروني، والقيام بنسخها[1].

يجب الإشارة إلى أن جريمة تزوير التوقيع الإلكتروني من الجرائم التي تقع على مضمون التجارة الإلكترونية ذاتها، وليس على البيانات الخاصة بها.

الركن المعنوي في جريمة التزوير لا بد من وجود قصد جنائي يتأسس به، و وجود إرادة تنصرف إلى ارتكاب الفعل إضافة إلى هذا العنصر لا بد من توافر قصد خاص يتمثل في اتجاه نية الجاني إلى استعمال المحرر فيما زوّر من أجله، فعنصرا الركن المعنوي في جريمة التزوير هما: إرادة الفعل ونية استعمال المحرر المزوّر[2].

ثالثا:جريمة الاعتداء على بيانات التشفير:

يوفر المشرع الفرنسي حماية جنائية للنظام المعلوماتي ومحتوياته في المواد 323/1-323/7 من قانون العقوبات، وباعتبار التوقيع الإلكتروني نظام معلوماتي فيعاقب بالدخول أو البقاء غير المشروع على قاعدة بيانات التوقيع الإلكتروني والاعتداء على سلامته[3].

---

[1] صالح شنين، الحماية الجنائية للتجارة الإلكترونية (دراسة مقارنة)، رسالة لنيل شهادة الدكتوراه في القانون الخاص، كلية الحقوق، جامعة ابو بكر بلقايد، تلمسان 2012، 2013، ص 178.

[2] حفصي عباس، جرائم التزوير الالكترونية(دراسة مقارنة) أطروحة لنيل شهادة دكتوراه في العلوم الإسلامية تخصص شريعة وقانون، جامعة وهران 1 أحمد بن بلة، كلية العلوم الإنسانية والعلوم الإسلامية، وهران 2014-2015 ص 105، أنظر كذلك سمية مزغيس، جرائم المساس بالأنظمة المعلوماتية، مذكرة لنيل شهادة الماستر في الحقوق تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، 2013-2014، ص 50.

[3] صالح شنين، المرجع السابق، ص 180.

نقصد بقاعدة البيانات التي تتعلق بالتوقيع الإلكتروني تلك البيانات المخزنة داخل الحاسب الآلي أو قرص منفصل، مثل البيانات المتعلقة بإسم صاحب التوقيع ومهنته و كافة بياناته الشخصية وكل المعلومات المتعلقة بذلك التوقيع والتي يفترض سريتها، فالتلاعب بهذه البيانات سواء بتعديلها، أو إلغائها أو مجرد الدخول غير المشرع في نظم وقواعد معالجة البيانات يعتبر جريمة إلكترونية[1].

يتمثل الركن المادي في هذه الجريمة في قيام الجاني بالاتصال بنظام البيانات والمعلومات المتعلقة بالتوقيع، حيث أن الجاني ليس له حق في الاتصال بهذين النظامين المتعلقين بالتوقيع الإلكتروني أما الركن المعنوي فيها هو القصد الجنائي العام بعنصريه العلم والإرادة، وذلك بأن يعلم الجاني بحقيقة سلوكه الإجرامي.

نص المشرع الجزائري على هذه الجريمة في المادة 394 ق ع ج الفقرة الأولى حيث يجب لقيام الجريمة اشتمالها على: فعل الدخول إلى النظام المعلوماتي، وفعل البقاء ويقصد بهذا الأخير التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام اي الدخول غير المشروع الى حاسب الي بقصد ارتكاب أو تسهيل ارتكاب جريمة سواء بواسطته أو بواسطة شخص آخر[2].

رابعا:جريمة فض تشفير الكتروني :

لقيام هذه الجريمة يتطلب توافر ركنين مادي ومعنوي الركن المادي يتمثل في اختراق التشفير المتعلق بالإمضاء الإلكتروني وبالتالي كل من استعمل عناصر تشفير غيره بصفة غير مشروعة بشكل اختراق لنظام التشفير يجعله عرضة للمتابعة الجزائية أما الركن المعنوي في

[1] لالوش راضية، المرجع السابق، ص 154.

[2] المرجع نفسه، ص 155.

قيامها هو القصد الجنائي العام بعنصريه العلم والإرادة وبالتالي يجب أن يعلم الجاني أن ذلك الفصل محظورا وفقا للقانون ومع ذلك تتصرف إرادته إلى فعل الاعتداء على البيانات المشفّرة[1].

وهذه الجريمة من جرائم السلوك المجرد لا يتطلب فيها تحقق نتيجة إجرامية بل تقوم بمجرد فض شفرة التوقيع الإلكتروني دون حصول ضرر المجني عليه.

وما يلاحظ أنه بالنظر للصيغة الفنية لهذه الجرائم فقد حرص المشرع أن تكون معاينتها من قبل أشخاص مختصين حتى تتم الإحاطة بهذه الجرائم المعقدة، لكن دون أن يمنع ذلك من إمكانية معاينة أعوان الضابطة العدلية لمثل هذه المخالفات.

خامسا:جريمة منع أو حيازة برامج لإعداد وتوقيع إلكتروني مزور

يتمثل الركن المادي لهذه الجريمة في صور عديدة هي: صناعة نظام معلوماتي برامج لإعداد توقيع الكتروني، حيازة النظام، والبرنامج وذلك بغرض إعداد توقيع الكتروني دون موافقة صاحبه، الفاعل قد يقوم بصناعة البرامج أو النظام المعلوماتي، بمعنى خلقه من العدم أي يتم تصميمه حسب مواصفات فنية وتقنية معينة بنفس الأدوات التي يعد بها البرامج أو النظام المشروع لهدف التوصل في النهاية إلى عمل ذلك التوقيع الالكتروني، اما الوسيلة التي يستخدمها الجاني مجموعة من الأجهزة والأدوات التي يختلس بها معلومات عن توقيعات قائمة بالفعل ليحصل على نسخة منها دون موافقة صاحبها، أو عمل برنامج معلوماتي جديد غير النظام القائم وذلك حتى يساعده في تحقيق غرضه الإجرامي غير المشروع.

أما الحيازة المعاقب عليها في هذا الغرض، فهي حيازة البرنامج أو النظام المعلوماتي القادر على عمل توقيع الكتروني رغما عن إرادة صاحب الشأن، والغرض أن حيازة الجاني للبرنامج المعلوماتي غير المشروعة، أي مالكا له أو مستأجرا أو مستعيرا من آخر حيث الزم المشرع المصري الحصول على الترخيص من الجهات المختصة، وقد خول مركز المعلومات

[1] صالح شنين، المرجع السابق، ص 184.

ودعم القرار بمجلس الوزراء منح الترخيص للجهات أو الأشخاص الراغبة في إعداد هذه البرامج أو صناعتها أو استردادها وإلا عدّت الحيازة للبرنامج أو النظام المعلوماتي غير مشروعة[1].

الفرع الثاني

العقوبات المقررة على جرائم التوقيع الإلكتروني

على غرار باقي التشريعات العربية والغربية، أصدر المشرع الجزائري نصوصا قانونية بموجب قانون العقوبات الجزائري 04-15 تحت عنوان جرائم المساس بأنظمة المعالجة الآلية للمعطيات والاستعمال للإعلام الآلي من خلاله جرّم كل أنواع الاعتداءات التي تستهدف الدخول الغير مشروع لأنظمة المعلوماتية، تغيير أو إتلاف المعطيات[2]، وفي هذا الصدد نص تقنين العقوبات على التزوير الخاص بالمحررات الالكترونية الذي يعتبر من اكبر واخطر الجرائم المتصلة بالتوقيع الالكتروني بالإضافة إلى الجرائم الأخرى المذكورة أعلاه، وقد نص عليه تقنين العقوبات في القسم الثالث، الرابع والخامس من الفصل السابع من الباب الأول من الكتاب الثالث منه في المواد من 124 إلى 229 التي تشترط المحرر في جريمة التزوير إلا انه لم يتخذ موقفا لتوسيع مفهوم المحرر من اجل إدماج المستندات المعلوماتية ضمن المحررات محل جريمة التزوير[3].

إذن فالمشرع الجزائري تبنى مثله من المشرع الفرنسي الحماية الجنائية للبرنامج من خلال تعديله الأخير للقانون 04-15 بهدف حماية النظام ككل، إلا انه لم يتعرض إلى الجرائم التي نص عليها المشرع الفرنسي، وان كانت على قدر من الأهمية كجريمة تزوير المستندات

[1] لالوش راضية، المرجع السابق، ص 152.

[2] المرجع نفسه، ص 167.

[3] حابت آمال، المرجع السابق، ص 401. أنظر كذلك مزغيش سمية، المرجع السابق ص ص 57-59.

المعلوماتية التي سبق ذكرها، رغم تداركه من خلال ق ع، الفراغ القانوني في مجال الإجرام المعلوماتي كما سبق القول و ذلك بتجريم الاعتداءات الواردة على الأنظمة المعلوماتية . إلا أنّ المشرع الجزائري أغفل تجريم الاعتداءات الواردة على منتجات الإعلام الآلي وتحديدا الخاصة بالتزوير المعلوماتي . بحيث نص على تزوير المحررات بمعزل عن جريمة استعمالها و جعل كل منها مستقلة عن الأخرى. حيث نص على استعمال الأوراق العمومية أو الرسمية في المادة 218 من ق ع و استعمل الأوراق العرفية أو التجارية أو المصرفية في المادة 221 و تطرق إلى الأوراق أو الوثائق الإدارية والشهادات في المواد من 222إلى 228 من ق.ع.ج ولم يتعرض إلى جريمة استعمال المستندات المعلوماتية المزورة. بخلاف المشرع الفرنسي الذي نص على جريمة التزوير وأورد لها نصا خاصا في المادة 6/462 ق.ع.ف

« كل من استخدم بتبصر– المستندات المعلوماتية المنصوص عليها في المادة 5/462 فإنه سيعاقب بالسجن من سنة إلى 5 سنوات و بغرامة من 20000فرنك إلى 200000 فرنك أو بإحدى هاتين العقوبتين ».

لسد الفراغ القانوني الذي عرفه المجال المعلوماتي بصدور قانون رقم 04–15 أصدر المشرع قانون مكافحة الجرائم المعلوماتية تحت عنوان "القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها" قانون رقم 09–04[1].

تم اقتراح على المشرع الجزائري إضافة نص إلى باب التزوير في المحررات يتناول فيه التزوير المعلوماتي على النحو التالي « كل تغيير للحقيقة بطريق الغش في مكتوب أو في أي دعامة أخرى تحتوي تعبيرا عن الفكر.

[1] لالوش راضية، المرجع السابق، ص ص 168–169. يمكن مراجعة أيضا المواد من 222 إلى 228 ق–ع–ج المذكورة أعلاه وأنظر أيضا القانون 09–04 السالف الذكر.

وبصفة عامة فإن المشرع الجزائري نص على مجموعة العقوبات التي يجب أن تطبق على الشخص الطبيعي كلما قام بارتكاب جريمة معلوماتية منها المتعلقة بالتوقيع الإلكتروني وهذه العقوبات تتمثل في:

1- **العقوبات الأصلية:** استخلصها من النصوص المتعلقة بالجرائم الماسة بالأنظمة المعلوماتية وهي كالتالي:

أ- **الدخول أو البقاء بالغش:** العقوبة المقررة هي من 03 أشهر إلى سنة ومن50،000دج إلى 100،000دج جريمة بسيطة.

ب- الدخول والبقاء بالغش: تضاعف العقوبة في حالة ترتب عنها تغيير أو حذف لمعطيات منظومة معلوماتية مما يشكل ظرف مشدد تكون العقوبة بالحبس من 06 أشهر إلى سنتين وغرامة من 500،000دج إلى 4000000دج [1].

ج-الاعتداء ألعمدي على المعطيات: طبقا لتقنين العقوبات فالعقوبة هي الحبس من ستة أشهر إلى ثلاثة سنوات وغرامة من 500000 إلى 2000000دج أمّا العقوبة المقررة لاستخدام المعطيات في إفشاء أو حيازة أو نشر أو استعمال المعلومات المتحصل عليها من إحدى الجرائم الماسة بالأنظمة المعلوماتية هي الحبس لشهرين إلى ثلاثة سنوات وغرامة مالية من 1000000دج إلى 5000000دج[2].

2- العقوبة التكميلية: نص عليها المشرع الجزائري في قانون العقوبات وتتمثل فيما يلي:

[1] أنظر نص المادة 394 مكرر/1 من ت.ع.

[2] أنظر نص المادة 394 مكرر/2 من ق-ع ولمزيد من التفاصيل راجع كذلك صالح شتين المرجع السابق ص 73.

المصادرة: تشمل الأجهزة والبرامج والوسائل المستخدمة في ارتكاب الجريمة من الجرائم الماسة بالأنظمة المعلوماتية.

إغلاق المواقع: التي تكون محلا لجريمة من الجرائم الماسة بالأنظمة المعلوماتية.

إغلاق المحل أو مكان الاستغلال: تطبق في حال ارتكاب الجريمة بعلم مالك المحل أو مكان الاستغلال كإغلاق مقهى الكتروني[1].

[1] راجع نص المادة 394 مكرر/6 من تقنين العقوبات الجزائري.

ولمزيد من المعلومات حول العقوبات التي قررها المشرع الجزائري فيما تخص الجريمة المعلوماتية يمكن مراجعة دردور نسيم. جرائم المعلوماتية على ضوء القانون الجزائري والمقارن. مذكرة لنيل شهادة الماجيستر .شعبة القانون الجنائي.كلية الحقوق جامعة منتوري(قسنطينة) سنة 2012.2013 ص ص 55-59.

خاتمة:

التوقيع التقليدي عبارة عن توقيع يشمل عدّة أشكال تناولها الفقه والقضاء تتمثل في الختم أو بصمة الأصبع أو الإمضاء وبالتالي بذكر هذه الأشكال لم يعط للتوقيع التقليدي تعريفا محددا، بالإضافة إلى الأشكال المذكورة أعلاه فللتوقيع التقليدي مجموعة من الوظائف تتمثل في منح المحرر القوة الثبوتية عن طريق تحديد هوية الشخص الموقع والتعبير عن الإرادة بالالتزام بالتصرف في مضمون السند.

كون التوقيع التقليدي يعتبر إحدى المعيقات التي تواجه تطور عصر المعلوماتية واستخدام الإنترنيت تم اللجوء إلى التوقيع الإلكتروني كون هذا الأخير واقعة مستحدثة فرضتها مقتضيات التجارة الإلكترونية فلقد صدرت تشريعات دولية ووطنية نظمت أحكام التوقيع الإلكتروني وبينت ماهيته واعترفت به ومن بينها قانون الأونيسترال النموذجي لعام 2001 بشأن التوقيعات الإلكترونية بالإضافة إلى ذلك أحكام التوجيه الأوروبي رقم 93 لسنة1999، كما نجد العديد من التشريعات الوطنية اعترفت بالتوقيع الإلكتروني وأضفت عليه حجية قانونية مساوية لحجية التوقيع التقليدي في الإثبات فالتوقيع الإلكتروني عبارة عن مجموعة من الحروف اوالأرقام أو رموز أو أصوات بحيث يعبر عن رضا الأطراف المتعاقدة ويحدد هوية الشخص موقعه كما يرتبط بمضمون المحرّر.

للتوقيع الإلكتروني مجموعة من الصور أو الأشكال والمتمثلة في التوقيع بالقلم الإلكتروني، التوقيع الرقمي، التوقيع بالرقم السري المقترن بالبطاقة الممغنطة، التوقيع البيومتري الذي يعتمد على الخواص الفيزيائية والطبيعية للإنسان.

خاتمة:

فيما يخص الاعتراف التشريعي بحجية التوقيع الإلكتروني لا بد أن يتمتع هذا الأخير بذات الحجية المقررة للتوقيع التقليدي وذلك من خلال توافر الشروط القانونية والضوابط التقنية التي تجعل منه توقيعا موثوقا ومنحته قوة في الإثبات تعادل قوة التوقيع التقليدي وقد تناول المشرع الجزائري هذه الحجية في ظل تعديل القانون المدني 05-10 وفي القانون التجاري الجزائري 03-15 في ظل الموافقة للقانون 03-15 المتعلق بالنقد والقرض.

من أجل حماية التوقيع الإلكتروني وتأمينه عمد المشرعين إيجاد بعض الوسائل المتمثلة في التوثيق(التصديق) بالإضافة إلى التشفير ولهذا الأخير نوعين أساسيين : التشفير المماثل والتشفير غير المماثل وبالتالي لديه مستويات مختلفة.

ولقد وجدت هذه الوسائل لحماية التوقيع الإلكتروني خاصة من الجرائم المتصلة بالتوقيع الإلكتروني أو ما يعرف بالجريمة المعلوماتية التي تعتبر من أخطر الجرائم التي واجهها العالم خاصة مع تطور عصر التكنولوجيا ومن هذه الجرائم لدينا جريمة التزوير الإلكتروني جريمة الاعتداء على بيانات التوقيع الإلكتروني، جريمة حيازة برنامج لإعداد توقيع الكتروني مزور، وبالتالي حاول المشرع الجزائري وضع مجموعة من العقوبات وجب تطبيقها على المجرم المعلوماتي.

قائمة المراجع:

أولا- باللغة العربية:

I- الكتب:

1- **إبراهيم الدسوقي أبو الليل**، الحجج القانونية للتعاملات الإلكترونية، مجلس النشر العلمي، الكويت، 2003 .

2- **بشار محمود دودين**، الإطار القانوني للعقد المبرم عبر شبكة الانترنت وفقا لقانون المعاملات الالكترونية وبالتأصيل مع النظرية العامة للعقد في القانون المدني، رسالة ماجستير، دار الثقافة للنشر والتوزيع، د ط، سنة 2006.

3- **خالد ممدوح إبراهيم**، إبرام العقد الإلكتروني، دراسة مقارنة، الطبعة الأولى، دار الفكر الجامعي، 30 شارع سوتير الإزاريطة الإسكندرية، 2006.

5- **سعيد السيد قنديل**، التوقيع الإلكتروني، ماهيته، صوره، حجيته في الإثبات بين التداول والاقتباس، دار الجامعة الجديدة الإسكندرية، 2006.

6- **عباس العبودي**، التعاقد عن طريق وسائل الاتصال الفوري وحجيتها في الإثبات المدني، دار الثقافة للنشر والتوزيع، الأردن.

7- **عبد الفتاح الحجاري**، النظام القانوني لحماية التجارة الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2002 .

8- **عبد الفتاح بيومي حجازي**، حماية المستهلك عبر شبكة الانترنت، دار الفكر الجامعي، الإسكندرية، 2006.

9- **علاء محمد نصيرات**، حجية التوقيع الالكتروني في الإثبات (دراسة مقارنة)، دار الثقافة للنشر و التوزيع، الأردن، 2005.

10- **عمر خالد زريقات**، عقد البيع عبر الأنترنت، دار الحامد للنشر والتوزيع، عمان، 2007.

11- **محمد السعيد رشدي**، التعاقد بوسائل الاتصال الحديثة و مدى حجيتها في الاثبات ، منشاة المعارف، الاسكندرية2007 .

12- **محمد فواز المطالقة**، الوجيز في عقود التجارة الالكترونية، التوقيع الالكتروني، أركانه، إثباته، القانون الواجب التطبيق (حماية التشفير)، جامعة البلقان التطبيقية، دار الثقافة للنشر والتوزيع، 2006.

13- **مدحت عبد الحليم رمضان**، الحماية الجنائية للتجارة الإلكترونية ، دار النهضة العربية، القاهرة، 2001

14-**لورنس محمد عبيدات**، إثبات المحرر الإلكتروني، دار الثقافة للنشر والتوزيع ، عمان 2002.

II - الرسائل و المذكرات الجامعية:

1- **إبراهيم عرسان أبو الهيجاء**، القانون الواجب التطبيق على عقود التجارة الالكترونية، رسالة دكتوراه، جامعة الدول العربية، القاهرة، 2004 .

2- **حابت آمال**، التجارة الالكترونية في الجزائر، رسالة لنيل شهادة الدكتوراه في العلوم، تخصص قانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2015.

3- **حفصي عباس**، جرائم التزوير الالكترونية(دراسة مقارنة) أطروحة لنيل شهادة دكتوراه في العلوم الإسلامية تخصص شريعة وقانون، جامعة وهران 1 أحمد بن بلة، كلية العلوم الإنسانية والعلوم الإسلامية، وهران 2014-2015.

4- **صالح شنين**، الحماية الجنائية للتجارة الإلكترونية (دراسة مقارنة)، رسالة لنيل شهادة الدكتوراه في القانون الخاص، كلية الحقوق، جامعة ابو بكر بلقايد، تلمسان 2012، 2013.

5- **إياد محمد عارف عطا سده**، مدى حجية المحررات الالكترونية في الإثبات، دراسة مقارنة، أطروحة لاستكمال متطلبات درجة الماجستير في القانون الخاص بكلية الدراسات العليا، جامعة النجاح الوطنية، نابلس، فلسطين، 2009.

6- **دحماني سمير**، التوثيق في المعاملات الإلكترونية دراسة مقارنة، مذكرة لنيل شهادة الماجستير في القانون، فرع قانون دولي للأعمال،

جامعة مولود معمري، تيزي وزو، كلية الحقوق والعلوم السياسية، 2015.

7- **طمين سهيلة**، الشكلية في عقود التجارة الإلكترونية ،رسالة لنيل شهادة الماجيستر في القانون، فرع القانون الدولي للأعمال، كلية الحقوق، مدرسة الدكتوراه للقانون الأساسي والعلوم السياسية، 2011 .

8- **سوير سفيان**، جرائم المعلوماتية، مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2010-2011 .

9- **كريم لملوم**، الإثبات في معاملات التجارة الالكترونية بين التشريعات الوطنية و الدولية، مذكرة لنيل درجة الماجستير في القانون فرع قانون التعاون الدولي، كلية الحقوق ، جامعة مولود معمري تيزي وزو ، 2011 .

10- **لالوش راضية**، أمن التوقيع الالكتروني، مذكرة لنيل شهادة الماجستير في القانون، فرع القانون الدولي للاعمال، كلية الحقوق و العلوم السياسية، جامعة مولود معمري تيزي وزو، سنة 2012 .

11- **هدار عبد الكريم** ، مبدأ الثبوت بالكتابة في ظل ظهور المحررات الإلكترونية، جامعة الجزائر، كلية الحقوق، بن عكنون، 2013-2014.

12- **زينب غريب**، إشكالية التوقيع الالكتروني وحجيته في الإثبات، رسالة لنيل شهادة الماستر قانون خاص، جامعة محمد الخامس السويسي، الرباط، 2009 – 2010.

13- **عبد اللطيف بركات**، الإثبات الالكتروني في المعاملات الإدارية، مذكرة مكملة من مقتضيات شهادة الماستر في الحقوق، جامعة محمد خيضر، بسكرة، 2012 – 2013 .

14- **سمية مزغيش**، جرائم المساس بالأنظمة المعلوماتية، مذكرة لنيل شهادة الماستر في الحقوق تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، 2013 -2014.

III- المقالات:

1- **حنان مليكة**، النظام القانوني للتوقيع الالكتروني في ضوء قانون التوقيع الالكتروني السوري رقم 4 الصادر بتاريخ 2009/02/25، دراسة قانونية مقارنة، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 26، العدد الثاني، 2010 .

2- **إيناس الخالدي**، حجية التوقيع الالكتروني في الإثبات، دراسة التعاملات الالكترونية السعودي، كلية الدراسات القضائية والأنظمة، جامعة أم القرى، السعودية، مقال منشور على موقع:
www.qu.edu.sa

3- **براهيم سليمان عبد الله**، التجارة الإلكترونية أمن المعلومات، مقال منشور على البريد الإلكتروني:
www.kau.edu.sa/iabdullah.

4- **عجابي إلياس**، الطبيعة القانونية للتوقيع الالكتروني، جامعة محمد بوضياف، المسيلة، مقال منشور على الموقع:

www.asjp.cerist.dz

IV- المجلات:

1- مجلة المدرسة الوطنية للإدارة، المجلد 13، العدد 2، 2003، العدد 26.

2- عبد العزيز سمية، التوقيع الالكتروني وسيلة حديثة للإثبات، دراسة مقارنة، مجلة علمية تصدر عن جامعة آكلي محند أولحاج، قسم العلوم القانونية، البويرة، الجزائر، العدد 17، 2014.

35- علي أبو مارية، التوقيع الالكتروني ومدى قوته في الإثبات "دراسة مقارنة"، مجلة جامعة الخليل للبحوث، كلية الحقوق، قسم القانون الخاص، جامعة فلسطين الأهلية، بيت لحم، المجلد 5 ،العدد 2، سنة 2010.

6- الاستعجال الإداري في أحكام القضاء الإداري الجزائري، التوقيع الالكتروني واقع وآفاق التجارة الالكترونية، مجلة المدرسة الوطنية للإدارة، المجلد 13، العدد 2- 2003، العدد 26.

V- النصوص القانونية:

1- القانون رقم 15/04، مؤرخ في 10 نوفمبر 2004. يعدل و يتمم الأمر رقم 156/66،المؤرخ في 08 جوان 1966 و المتضمن قانون العقوبات ،ج ر.عدد 71.صادر في 2004/11/10.

2- القانون رقم 10/05، مؤرخ في 2005/06/20، يعدل و يتمم الأمر رقم58/75،المؤرخ في 26 سبتمبر1975، المتضمن القانون المدني ،ج ر عدد 44،الصادرة في 26 جوان 2005.

3- قانون رقم 14-04 مؤرخ في 01 فيفري 2014 يحدد القواعد العامة المتعلقة بالتوقيع و التصديق الالكترونيين .

4- قانون رقم 09-04 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنلوجيا الاعلام والاتصال و مكافحتها،ج ر عدد 47.صادرة بتاريخ 16 أوت 2009.

5- قانون رقم 15-04 مؤرخ في 2015/02/01 يحدد القواعد العامة المتعلقة بالتوقيع و التصديق الالكترونيين ،ج. ر، عدد 06، الصادر في 10 فيفري **2015**.

- النصوص التنظيمية:

- مرسوم تنفيذي رقم **162/07** مؤرخ في 30 ماي 2007 يعدل يتمم المرسوم التنفيذي رقم 123/01 و المتعلق بالنظام المطبق على كل نوع من انواع الشبكات بما فيها اللاسلكية الكهربائية ، ج ر رقم37 صادر في 2007/06/07.

- القوانين النموذجية:

1- قانون اليونيسترال النموذجي بشان التجارة الالكترونية لسنة 1996، صادر في جلسة رقم 85 للجمعية العامة للامم المتحدة بتاريخ 1996/12/16،متوفر عبر الموقع:

http/www.uncitral.org/pdf/arabic….

2- قانون اليونيسترال النموذجي بشان التوقيعات الالكترونية صادر في جلسة رقم 85 للجمعية العامة للامم المتحدة بتاريخ 2001/12/12 ، متوفر عبر الموقع:

http//daccess-ods.un.org/tmp/7958533.html

- قوانين أخرى:

1-القانون التونسي رقم 85 لسنة 2000 بشان المبادلات و التجارة الالكترونية ، متوفر عبر الموقع:

http// :arabgov.com/news/news.asp.

2-التوجيه رقم 93/1999 و الصادر بتاريخ 13-12-1999 بشان التوقيع الالكتروني متوفر عبر الموقع :

http://eur-lex.europa,eu/lex uriserv/…

ثانيا - باللغة الفرنسية:

-Ouvrages :

1-Benssoussan Alain ,internet, aspects juridique ,revue et augmentée ,2éme Edition Hermès, Paris,1998.

2-Thieffry Patrick ,Commerce électronique : droit international et européen, litec, Paris,2002.

الفهرس:	
مقدمة:	01
الفصل الأول: **التوقيع بمفهوميه التقليدي والحديث**	05
المبحث الأول: التوقيع التقليدي	07
المطلب الأول: مفهوم التوقيع التقليدي	08
الفرع الأول: تعريف التوقيع	08
أولا: التعريف القانوني للتوقيع	09
ثانيا: التعريف الفقهي للتوقيع	11
الفرع الثاني:شروط التوقيع التقليدي(العناصر)	14
أولا: أن يكون التوقيع علامة خطية وشخصية	14
ثانيا:أن يكون التوقيع مقروءا وثابتا مستمرا ومرتبطا بالمحرر الكتابي	16
المطلب الثاني: صور ووظائف التوقيع التقليدي	**18**
الفرع الأول: صور وأشكال التوقيع التقليدي	18
أولا: التوقيع بالختم	18
ثانيا: التوقيع ببصمة الأصبع	20
ثالثا:التوقيع بالإمضاء	21
الفرع الثاني: وظائف التوقيع التقليدي	22
أولاّ: تحديد هوية الشخص الموقع	22
ثانيا: التعبير عن الإرادة بالالتزام بالتصرف في مضمون السند	23
المبحث الثاني: التوقيع الإلكتروني	**26**

المطلب الأول: مفهوم التوقيع الإلكتروني	27
الفرع الأول: تعريف التوقيع الإلكتروني	28
الفرع الثاني: صور التوقيع الإلكتروني	31
أولاّ: التوقيع بالقلم الإلكتروني	32
ثانيا: التوقيع الرقمي	33
ثالثا: التوقيع باستخدام الحواس الذاتية(التوقيع البيومتري)	35
رابعا: التوقيع بواسطة الرقم السري المقترن بالبطاقة الممغنطة	36
المطلب الثاني: مدى تحقيق التوقيع الإلكتروني لوظائف التوقيع التقليدي وشروطه	39
الفرع الأول: مدى توفر شروط التوقيع التقليدي في التوقيع الإلكتروني	39
أولا: أن يكون علامة مميزة للشخص الموقع	39
ثانيا: اتصال التوقيع بالسند	40
ثالثا: أن يكون التوقيع واضحا ومتميزا	40
الفرع الثاني: أهم وظائف التوقيع الإلكتروني وخصائصه	41
أولا: وظائف التوقيع الإلكتروني	41
1-تحديد هوية الموقع على المحرر والتعريف بشخصيته	41
2- التعبير عن إرادة الموقع وقبوله لموضوع المحرر ومضمونه	41
أ- الدّلالة على هوية الموقع	42
ب- التعبير على إرادة الموقع في الموافقة على مضمون السند	43
ج- التوقيع يدل على حضور صاحب التوقيع	45
ثانيا: أهم الخصائص التي يتميز بها التوقيع الإلكتروني	46
الفرع الثاني: أهمية التوقيع الإلكتروني	48

أولا: توفير عامل الوقت والجهد الثمينين للمواطن والموظف	49
ثانيا: يمكن الاعتماد عليه كليا ضمن الإجراءات القانونية و القضائية	49
ثالثا:يساهم الموقع في منح قناة اتصال جديدة بين المواطن والجهات الحكومية	49
رابعا: التوقيع في استخدام التوقيع الالكتروني يرفع كفاءة العمل الإداري	49
الفصل الثاني: **وسائل حماية التوقيع الإلكتروني**	51
المبحث الأول: الاعتراف الشريعي بحجية التوقيع الإلكتروني	**52**
المطلب الأول: الاعتراف التشريعي بحجية التوقيع الإلكتروني في التشريعات المقارنة والتشريع الجزائري	**53**
الفرع الأول: الاعتراف التشريعي بحجية التوقيع الإلكتروني في التشريعات المقارنة	54
أولا: الحجية القانونية للتوقيع الإلكتروني وفقا لتوجيهات الإتحاد الأوربي	54
ثانيا: الحجية القانونية للتوقيع الإلكتروني وفقا لقانون الاونيسترال النموذجي	56
الفرع الثاني: حجية التوقيع الإلكتروني في التشريع الجزائري	60
أولا: قواعد الإثبات بالتوقيع الالكتروني في التشريع الجزائري	61
1- الاعتراف التشريعي بالتوقيع الإلكتروني في القانون المدني الجزائري	61
2- الاعتراف التشريعي بالتوقيع الإلكتروني في القانون التجاري الجزائري	64
المطلب الثاني: التعادل الوظيفي بين التوقيع التقليدي والتوقيع الإلكتروني	**65**
الفرع الأول: مدى تحقيق التوقيع الإلكتروني لشروط التوقيع التقليدي	66
أولا: أن يكون التوقيع علامة مميزة للشخص	66
ثانيا: أن يكون التوقيع واضحا ومستمرا	67
ثالثا: اتصال التوقيع بالسند	68

الفرع الثاني: مدى تحقيق التوقيع الإلكتروني لوظائف التوقيع التقليدي	69
أولا: فعالية التوقيع الإلكتروني في تحديد هوية صاحبه	69
ثانيا: اتصال التوقيع بالمحرر الإلكتروني	70
ثالثا: التحقق من سلامة مضمون المحرر	71
المبحث الثاني: امن التوقيع الإلكتروني	**72**
المطلب الأول: الحماية الوقائية للتوقيع الإلكتروني	**73**
الفرع الأول: التوثيق الإلكتروني	73
أولا: جهة التوثيق الإلكتروني	74
1- تعريف جهة التوثيق الإلكتروني	74
2- مهام جهات التوثيق الإلكتروني	78
3- مسؤولية جهات التوثيق الإلكتروني	79
ثانيا: شهادة التوثيق الإلكتروني	81
1- شهادة Digital time stamp	83
2- شهادة الإذن Authoring certaficate	83
3- شهادة البيانAttesting certaficate	83
الفرع الثاني: التشفير كوسيلة لحماية التوقيع الالكتروني	84
أولا: مفهوم التشفير	84
ثانيا: أنواع التشفير	85
1- التشفير بالمفتاح المماثل	85
2- التشفير غير المماثل	86
3- الخصوصية المتميزة(PGP)	87
4- تشفير القرص الصلب	88

5- التشفير المزدوج	89
ثالثا: مستويات التشفير	89
1-التشفير على مستوى الإرسال	98
2- التشفير على مستوى التصفح أو التنقل	90
3- التشفير على مستوى التطبيق أو التنفيذ	91
4- التشفير على مستوى الملفات	92
رابعا: ضوابط التشفير	92
1-إباحة تشفير البيانات والمعلومات التي يتم كتابتها أو التعامل فيها باستخدام الوسائل الإلكترونية	92
2-الحفاظ على سرية البيانات والمعلومات المشفرة	93
3- اعتبار استخدام التشفير وسيلة يعتد بها قانونا	94
خامسا: طرق التشفير	94
المطلب الثاني: الجرائم المتعلقة بالتوقيع الإلكتروني	95
الفرع الأول: صور جرائم التوقيع الإلكتروني	95
أولا: الجريمة المعلوماتية	96
ثانيا: جريمة تزوير التوقيع الإلكتروني	96
ثالثا: جريمة الاعتداء على بيانات التوقيع الإلكتروني	97
رابعا: جريمة فض تشفير إمضاء الإلكتروني	98
خامسا: جريمة منح أو حيازة برنامج لإعداد توقيع الإلكتروني مزوّر	99
الفرع الثاني: العقوبات المقررة على جرائم التوقيع الإلكتروني	100
خاتمة:	104
قائمة المراجع:	106

الفهرس:	115