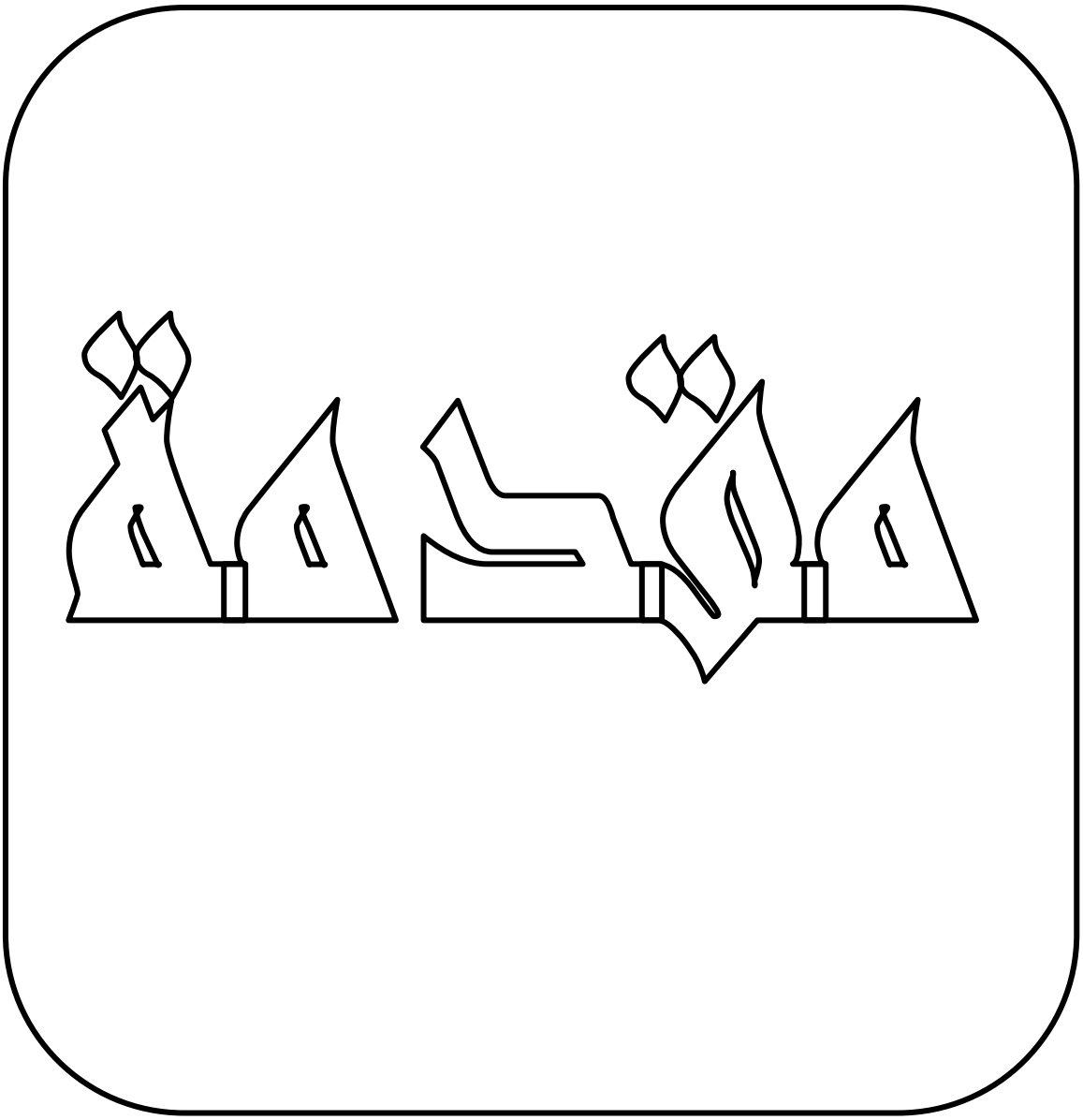


إنّ التطور التكنولوجي الذي نعيشه الآن والذي يطلق عليه عصر المعلومات والبيانات، أدّى إلى ظهور وسائل وأساليب جديدة في إبرام العقود، لم تكن معروفة منذ سنوات قليلة، وهذه الوسائل في تطور دائم ومستمر وسريع، ومع تطور تقنيات وأساليب إبرام التصرفات القانونية كان من الضروري إيجاد وسيلة تقرّ بهذه التصرّفات قوة ثبوتية لجعلها من الأدلّة المقبولة أمام القضاء، خاصة مع تعذّر استخدام التوقيع التقليدي في بعض التصرّفات، لذلك بحث المهتمون (قانونيّين وتقنيين) عن وسيلة بديلة أخرى تقوم بهذه المهمة وتوصّلوا إلى وسيلة إلكترونية لها أشكال مختلفة يمكن أن تحقّق الخصائص التي يقدّمها التوقيع التقليدي سمّيت ب**التوقيع الإلكتروني**.

والذي تكمن أهمّيته في زيادة مستوى الأمن والخصوصية في التعاملات، نظرا لقدرة هذه التقنية على حفظ سريّة المعلومات والرسائل المرسلة وعدم قدرة أيّ شخص آخر على الإطّلاع أو تعديل أو تحريف الرسالة، كما يمكنها أن تحدّد شخصية وهوية المرسل والمستقبل إلكترونيا للتأكّد من مصداقية الشخصية ممّا يسمح بكشف التحايل أو التلاعب.

ولقد أدركت الجزائر منذ أزيد من عشرية أهمية التحكم في تكنولوجيا الإعلام والإتصال، نظرا لعلاقة هذه الأخيرة بنجاح مسار التنمية المستدامة، وبغية التوصّل إلى تحقيق أهداف التنمية أضحى التوجه صوب استعمال التكنولوجيات في جميع الميادين ضرورة من أجل تمكين كلّ المواطنين والمؤسّسات من هذه الخدمات بدون تمييز.

وهذا ما كرّسه المشرع الجزائري من خلال تعديل قواعد الإثبات القانون رقم 10-05 المؤرخ في 20 جوان 2005 المعدّل والمتمم للقانون المدني، حيث اعتبر الإثبات بالشكل الإلكتروني كالإثبات بالكتابة بتوافر شروط معيّنة.

ومؤخرا صدر القانون رقم 04-15 المؤرخ في 01 فيفري 2015 يحدّد القواعد المتعلّقة بالتوقيع والتصديق الإلكترونيين قصد التكفّل بالمتطلبات القانونية والتنظيمية

والتقنيات التي ستسمح بإحداث جو من الثقة المواتية لتعميم وتطوير المبادلات الإلكترونية وترسيخ المبادئ العامة المتعلقة بنشاطي التوقيع والتصديق الإلكترونيين في الجزائر، يسمح بتعميم وتطوير التبادلات الإلكترونية بين المستعملين في مجالي التجارة الإلكترونية، والذي يسهم في النهاية في تحقيق التنمية الاقتصادية. كما يسمح الإطار القانوني لعدّة قطاعات، من بينها الإدارة الإلكترونية من أجل ضمان تسيير أفضل للهيئات والمؤسّسات وتسهيل الحياة اليومية للمواطنين والفاعلين الاجتماعيين والاقتصاديين.

وعليه يأتي هذا الموضوع من أجل إنجاح تطبيق العمل بهذا القانون في المجتمع من خلال زيادة الوعي الاجتماعي به، أي أن تكون لكلّ فئاته فكرة في مجال التعامل الإلكتروني بالنظر إلى قلّة وعي وثقة المجتمع به وخاصة المصارف والتجار وأبناء المجتمع بشكل عام في التعاملات الإلكترونية بدل من أن تكون تعاملاتهم ورقية تقليدية وذلك من أجل اللحاق بركب المجتمعات المتقدّمة التي سبقتنا في هذا المجال.

وانطلاقا ممّا سبق فإنّ هذا الموضوع يسعى للإجابة على الإشكالية التالية: **إلى أيّ مدى تكيف القانون الجديد الذي يحدّد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين مع التطور التكنولوجي الحاصل في إبرام العقود؟ وهل يوفر متطلبات الثقة والأمن بهذه الوسائل الحديثة؟**

وللإجابة عن الإشكالية المطروحة تمّ تقسيم هذا البحث إلى فصلين، تناول الفصل الأوّل **(التوقيع الإلكتروني)**، فيما عالج الفصل الثاني **(التصديق الإلكتروني)**.

وقد تمّ اعتماد المنهج التحليلي الذي يتلاءم مع دراستنا لما يتوفر عليه من مزايا، حيث بواسطته نستطيع القيام بعملية تحليل ودراسة أفكار النصوص القانونية، وفهم فحواها وإدراك نقائصها ومزاياها، بالإضافة إلى المنهج الوصفي الذي بواسطته نقدّم سلطة

واضحة المعالم على الموضوع وتبيان صفاته وخصائصه، بالإضافة إلى المنهج المقارن يعتبر ضروريا في دراستنا، على اعتبار القيام بعرض ومقارنة بعض النصوص القانونية المنظمة لهذا الموضوع لبعض تشريعات العديد من الدول.

ومن الصعوبات التي واجهت هذه الدراسة ندرة المراجع التي تناولت الموضوع من الناحية القانونية وخاصة المراجع الجزائرية منها، لأنّ غالبية المراجع عالجت موضوع التوقيع الإلكتروني باعتباره شرطا أساسيا لإضفاء الحجية على التوقيع الإلكتروني ومساواته والتوقيع التقليدي، كما أنّ غالبية هذه المراجع اعتمدت في معالجة الموضوع على سرد النصوص القانونية دون تحليل أو مناقشة.

وآمل أن أكون في هذا الجهد المتواضع قد وفّقت في دراسة الموضوع خاصة وأنّ موضوع **التصديق والتوقيع الإلكترونيين** موضوعا حديثا بالنسبة للجزائر لأنّه قيد الإنجاز.

الفصل الأول

التعريف الإلكتروني

إنّ التطور التكنولوجي الذي نعيشه الآن، والذي يطلق عليه عصر المعلومات والبيانات، أدّى إلى ظهور وسائل وأساليب جديدة في إبرام العقود، لم تكن معروفة منذ سنوات قليلة، وهذه الوسائل في تطور دائم ومستمر وسريع، ولما كان القانون مرآة الواقع كان لابدّ من المشرع الجزائري والتشريعات المقارنة من إصدار تشريعات مستحدثة، لتعالج ما استجدّ من وسائل وأساليب وطرق لإبرام العقود، ومع تطور تقنيات وأساليب إبرام التصرفات القانونية كان من الضروري إيجاد وسيلة تقرّ بهذه التصرفات قوة ثبوتية لجعلها من الأدلّة المقبولة أمام القضاء، خاصة مع تعذّر استخدام التوقيع التقليدي في مثل هذه التصرفات لذلك بحث المهتمون عن وسيلة بديلة أخرى تقوم بهذه المهمة، وتوصلوا إلى وسيلة إلكترونية لها أشكال مختلفة يمكن أن تحقق الخصائص التي يقدّمها التوقيع التقليدي سميّت **بالتوقيع الإلكتروني**.

ونظرا لأهمية عنصر التوقيع الإلكتروني في إثبات المعاملات الإلكترونية، ارتأينا بحث هذا العنصر من جوانب مختلفة وهذا من خلال معرفة **الإطار العام للتوقيع الإلكتروني** وذلك في المبحث الأوّل، **شروط ووظائف التوقيع الإلكتروني** في المبحث الثاني، **وحجية التوقيع الإلكتروني في الإثبات** في المبحث الثالث، و**آليات حماية التوقيع الإلكتروني** في المبحث الرابع.

المبحث الأوّل: الإطار العام للتوقيع الإلكتروني.

يعتبر التوقيع الإلكتروني من الأمور الجديدة على الأشخاص، إذ لم يكن في الحسبان أن يحدث يوما ويكون هناك توقيع غير التوقيع المألوف، فمع التطور المذهل الذي أحدث الإنترنت والتجارة الإلكترونية وعقد الصفقات الضخمة عبر الإنترنت نشأ هذا النمط من التوقيع بين أشخاص لا يرتبطون بعلاقة قانونية مسبقة، وقد لا يتم بينهم اتفاقات لحسم ما يثور بينهم من نزاعات، ومن هنا فقد نشطت الجهود الدولية والإقليمية لبحث السبل الكفيلة بتوفير الأمن والثقة لهذا التوقيع وهما من أهم الأسس التي تقوم عليها التجارة[1]، وهذا ما سيتم تناوله في هذا المبحث، حيث سنتناول في المطلب الأوّل **تعريف التوقيع الإلكتروني**، المطلب الثاني **خصائص التوقيع الإلكتروني**.

المطلب الأوّل: تعريف التوقيع الإلكتروني وأهميّته.

لقد عمدت أغلب التشريعات المقارنة التي نظمت التوقيع الإلكتروني أو التجارة الإلكترونية، إلى تعريف التوقيع الإلكتروني وإزالة الغموض عن هذا المصطلح القانوني الحديث.

وهذا ما سيتم تناوله في **الفرع الأوّل** (التعريف الفقهي للتوقيع الإلكتروني) **والفرع الثاني** (التعريف التشريعي).

الفرع الأوّل: التعريف الفقهي للتوقيع الإلكتروني.

يعرّف بعض الفقه **التوقيع الإلكتروني** بأنّه: "عبارة عن حروف أو أرقام أو رموز أو إشارات لها طابع منفرد تسمح بتحديد شخص صاحب التوقيع وتمييزه عن غيره، وهو الوسيلة

[1]. إيناس الخالدي، **حجية التوقيع الإلكتروني في الإثبات. دراسة في نظام التعاملات الإلكترونية السعودي**، جامعة القصيم، العربية السعودية، ص 11.

الضرورية للمعاملات الإلكترونية في إبرامها وتنفيذها، والمحافظة على سريّة المعلومات والرسائل".[1]

وعرّفه البعض الآخر بأنّه: "مجموعة من الإجراءات والوسائل التي يتبع استخدامها عن طريق الرموز أو الأرقام وكذا إخراج رسالة إلكترونية تتضمن علامة مميزة من صاحب الرسالة المنقولة إلكترونيا يجري تشفيرها واستخدام زوج من المفاتيح واحد معلن والآخر خاص بصاحب الرسالة".[2]

وعرّفه آخرون بأنّه: "بيان أو معلومة تتصل بمنظومة بيانات أخرى، أو تحويل منظومة بيانات إلى شفرة أو كود والذي يسمح للمرسل إليه بإثبات مصدرها والإستيثاق من سلامة مضمونها وتأمينها ضدّ أيّ تعديل أو تحريف".[3]

الفرع الثاني: تعريف التشريعات المقارنة للتوقيع الإلكتروني.

أوّلا: القانون الأونيسترال[4]:

لقد عّف قانون الأونيسترال النموذجي بشأن التوقيعات الإلكترونية لسنة 2001 في مادّته الثانية التوقيع الإلكتروني بأنّه: "بيانات في شكل إلكتروني مدرجة في رسالة بيانات أو مضافة إليها أو مرتبطة بها منطقيا، يجوز أن تستخدم لتعين هوية الموقع على المعلومات الواردة في رسالة البيانات".

---

[1]. محمد أمين الروماي، **النظام القانوني للتوقيع الإكتروني**، دار الفكر الجامعي، الطبعة الأولى، 2006، ص 13.

[2]. عيسى غسان ربضي، **القواعد الخاصة بالتوقيع الإلكتروني**، دار الثقافة للنشر والتوزيع، الطبعة الأولى، 2009، ص 15-16.

[3]. بشار محمود دودين، **الإطار القانوني للعقد المبرم عبر شبكة الإنترنت**، دار الثقافة للنشر والتوزيع، الطبعة الثانية، 2010، ص 245.

[4]. قانون الأونيسترال النموذجي بشأن التوقيعات الإلكترونية الصادر بتاريخ 10-01-2001.

ثانيا: التوجيه الأوروبي[1]:

أورد التوجيه الأوروبي بشأن التوقيعات الإلكترونية في نصوصه نوعين من التوقيع الإلكتروني:

* **النوع الأوّل:** يعرف بالتوقيع الإلكتروني العادي، وهذا التوقيع حسب نص المادة الثانية من التوجيه يعرف بأنّه: "معلومة تأخذ شكلا إلكترونيا تقترن أو ترتبط بشكل منطقي ببيانات أخرى إلكترونية، والذي يشكل أساس منهج التوثيق".

* أمّا**النوع الثاني:** فهو التوقيع الإلكتروني المتقدّم، وهو توقيع يرتبط بالنص الموقع، ولكي يتّصف التوقيع الإلكتروني، بأنّه توقيع متقدّم، يجب أن تتوفر فيه الشروط التالية:

1- أن يرتبط وبشكل منفرد بصاحب التوقيع؛

2- أن يتيح كشف هوية صاحب التوقيع؛

3- أن ينشأ من خلال وسائل موضوعة تحت رقابة صاحب التوقيع؛

4- أن يرتبط بالبيانات التي وضع عليها التوقيع إلى درجة أنّ أيّ تعديل لحق البيانات يمكن كشفه.

ثالثا: القانون المصري[2]:

حسب المادة 01/ج من القانون رقم 15 لسنة 2004 الخاص بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة التكنولوجيا، فإنّه يقصد بالتوقيع الإلكتروني: "كلّ ما يوضع على محرّر إلكتروني ويتّخذ شكلا أو حرفا أو رموزا أو إشارات أو غيرها، ويكون له طابع منفرد يسمح بتحديد الشخص الموقع ويميّزه عن غيره".

---

[1]. التوجيه الأوروبي رقم 39/1999 بشأن الإطار المشترك للتواقيع الإلكترونية الصادر بتاريخ 13-12-1999.

[2]. القانون المصري رقم 15 لسنة 2003 الخاص بتنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية الصناعة التكنولوجية الصادر بتاريخ 22-04-2004.

رابعا: القانون المغربي[1]:

بخلاف التشريعات السابقة، فإنّ المشرع المغربي لم يقم بتعريف التوقيع الإلكتروني وإنّما اكتفى بتحديد شروط صحّته، وذلك من خلال المادة السادسة من القانون رقم 05-53 الصادر في 30 نوفمبر 2007.

خامسا: القانون الجزائري[2]:

حسب نص المادة 02 من القانون رقم 15-04 الذي يحدّد القواعد العامة المتعلّقة بالتوقيع والتصديق الإلكترونيين، فإنّه يقصد بالتوقيع الإلكتروني: "بيانات في شكل إلكتروني، مرفقة أو مرتبطة منطقيا ببيانات إلكترونية أخرى، تستعمل كوسيلة توثيق". وبالتالي فالمشرع الجزائري أدرج التوقيع الإلكتروني للمرّة الأولى من خلال القانون رقم 05-10 المؤرخ في 20 جوان 2005 المعدّل والمتمم للقانون المدني الذي تم من خلاله الإعتراف بالكتابة الإلكترونية كوسيلة إثبات وذلك بإضافة المادتين 323 مكرّر و332 مكرّر 01.

الفرع الثالث: أهمية التوقيع الإلكتروني.

يعتبر التوقيع من المبادئ الأساسية في الإثبات وشرطا مهما لتوثيق أيّ مستند سواء في المراسلات العادية أو الإلكترونية على اختلاف أنواعها ووسائطها في داخل المؤسّسة أو المراسلات التي تتمّ بين المؤسّسات في داخل الدولة أو خارجها، وهذا بدوره يتماشى مع مقتضيات التجارة الإلكترونية وتيسير لمعاملات التجار الذين يرغبون في إقامة علاقات

[1]. ظهير شريف رقم 129-07-01 صادر في 30 نوفمبر 2007، متعلّق بتنفيذ القانون رقم 05-53 المتعلّق بالتبادل الإلكتروني للمعطيات القانونية المنشورة بالجريدة الرسمية عدد 5584 بتاريخ 25 ذو القعدة 1428 الموافق لـ 06-12-2007، ص 3879-3888.

[2]. قانون رقم 15-04 مؤرخ في 11 ربيع الثاني عام 1436 الموافق لأوّل فبراير 2015، يحدّد القواعد العامة المتعلّقة بالتوقيع والتصديق الإلكترونيين.

تعاقدية عبر الإنترنت، ومن هنا تكمن مقاصد المشرع من حيث أهمية التوقيع الإلكتروني في مدى السريّة والضمان الذي يتمتع به، وعليه فإنّه يمكن الإستفادة من استخداماته في شتى المجالات الآتية:

أوّلا: توفير عامل الوقت والجهد الثمين للمواطن والموظف، وهذه الحالة لن يضطر المواطن إلى أن يذهب بسيارته أو باستخدام وسائل النقل الأخرى إلى الدوائر الحكومية والإنتظار طويلا كما هو الحال في معظم الدول النامية، بخلاف الدول المتقدمة، حيث أنّه بالكاد أن ترى أشخاصا يتابعون وينهون معاملاتهم إلاّ بأضيق الحالات، وهو ظهور الشخص إن لزم في مسألة شخصية، وبذلك نرى أنّ التوقيع الإلكتروني يسمح بعقد الصفقات عن بعد ودون حضور المتعاقدين.

ثانيا: يمكن الإعتماد عليه كليا ضمن الإجراءات القانونية والقضائية في المنازعات بين الأشخاص والشركات الخاصة أو المؤسّسات والهيئات الحكومية، وهنا يكون لقناعة القاضي دور كبير حيث يتم التعويل على الثقة في الجهاز الذي من خلاله تمّ إجراء السرية والتخزين والإرسال والحفظ وغيرها، وكفاءة القائمين على هذه الإجراءات، ومدى تقدّم التكنولوجيا، كل هذه الإعتبارات ينظرها ويحكمها مدى جدارة التوقيع الإلكتروني في أن يتم الإعتماد عليه من عدمه.[1]

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 يعدّ عاملا وأداة مهمة لنجاح فكرة الحكومة الإلكترونية.

[1]. عبد الحميد ثروت، **التوقيع الإلكتروني (ماهيته، مخاطره وكيفية مواجهتها، مدى حجيته في الإثبات)**، دار الجامعة الجديدة، سنة 2007، ص 20.

رابعا: إنّ التوسع في استخدام التوقيع الإلكتروني يرفع كفاءة العمل الإداري ويساعد على الإرتقاء بمستوى أداء الخدمات الحكومية بما يتّفق مع متطلبات ومستجدّات العصر الحديث، وبالتالي يؤدّي هذا النمط إلى التخفيف من نمط البيروقراطية التي تؤخر زيادة النشاطات والمعاملات بكافة صورها.

خامسا: وبما أنّ التوقيع الإلكتروني يتم استخدامه في جميع المستندات ونماذج الطلبات، فإنّ ذلك يساعد على توفير الهوية الرقمية لكل مواطن وهذا يساهم في خلق وعي فكري لدى المواطن وتطوير التعامل بالإنترنت ممّا يؤثر على التجارة الإلكترونية فترى الكثير من الأشخاص الأذكياء الذين يملكون شركات ضخمة حققت الكثير من الأرباح من دون أن يكون لها مقرّ بحجم الشركات الكبيرة، ومن هنا تكمن أهمية التوقيع الرقمي في أنّه يوفر الضمان من خلال استخدام عمليات البيع والشراء من المعاملات التجارية الإلكترونية المختلفة كالبيع والشراء وغيرها من العقود والتصرفات القانونية والتجارية الأخرى والإستيراد والتصدير وباقي التعاقدات، وحجز تذاكر السفر والفنادق والمعاملات المصرفية بكل أنواعها، والتي تتم في شكل محرّر إلكتروني موقع توقيعا إلكترونيا، وغير ذلك من المزايا الأخرى التي تؤدّي بدورها إلى التوفير في جميع إجراءات إرسال البيانات إلى المواطن والحصول على معلومات منه التوفير في الورق، الطلبات، الطباعة...إلخ.[1]

المطلب الثاني: خصائص التوقيع الإلكتروني وصوره.

إنّ إصدار المشرع الجزائري للقانون رقم 15-04 المتعلّق بالتوقيع والتصديق الإلكترونيين، يجعلنا نتساءل عن خصائص هذا التوقيع باعتباره مصطلحا جديدا، وهو ما سنحاول دراسته من خلال **الفرع الأوّل** (الخصائص)، وسنخصص **الفرع الثاني** (صور التوقيع الإلكتروني).

[1]. إيناس الخالدي، المرجع السابق، ص 23.

الفرع الأوّل: خصائص التوقيع الإلكتروني.

يتميز التوقيع الإلكتروني بعدّة خصائص أهمها ما يلي:

1- التوقيع الإلكتروني يتمّ عبر وسائل إلكترونية وعن طريق جهاز الحاسوب الآلي والإنترنت أو على كسيت أو أسطوانة[1]، حيث أصبح بإمكان أطراف العقد والتفاوض بشأن شروطه وكيفية إبرامه وإفراغه في محرّرات إلكترونية أو خيرا إجراء التوقيع الإلكتروني عليه[2]، عكس التوقيع التقليدي الذي يوضع على دعامة مادية هي في الغالب دعامة ورقية، في هذه الحالة تديّل الكتابة بالتوقيع فتتحول الدعامة بعد ذلك إلى مستند صالح للإثبات.

2- لم يشترط في التوقيع الإلكتروني صورة معيّنة حيث أنّه يمكن أن يأتي على شكل حرف أو رمز أو رقم أو إشارة أو حتى صوت، المهم فيه أن يكون ذو طابع منفرد يسمح بتمييز شخص صاحب التوقيع وتحديد هويته وإظهار رغبته في إقرار العمل القانوني والرضا بمضمونه[3] بخلاف التوقيع التقليدي الذي يقتصر على الإمضاء بخط اليد وقد يضاف إليه الختم وقد يضاف إليه الختم وبصمة الأصابع.[4]

3- إذا كان التوقيع التقليدي عبارة عن رسم يقوم به الشخص أي أنّه فنّ وليس علم، وبالتالي فإنّه يسهل تزويره أو تقليده فإنّ **التوقيع الإلكتروني** علما وليس فنّا، وبالتالي يصعب تزويره[5]، حيث أنّ الوظيفة الرئيسية للتوقيع الإلكتروني هي الإستيثاق من مضمون المحرّر الإلكتروني وتأمينه من التعديل بالإضافة أو الحذف، وذلك عن طريق ربط المحرّر الإلكتروني والتوقيع الإلكتروني بحيث يقتضي إجراء أي تعديل لاحق إيقاع توقيع إلكتروني

---

[1]. عباس العبودي، **تحديّات الإثبات بالسندات الإلكترونية ومتطلبات النظام القانوني لتجاوزها**، منشورات الحلبي الحقوقية، الطبعة الأولى، 2010، ص 149.
[2]. بشار محمود دودين، المرجع السابق، ص 247.
[3]. عباس العبودي، المرجع السابق، ص 149.
[4]. عيسى غسان ربضي، المرجع السابق، ص 32 وما بعدها.
[5]. الناصري نور الدين، **المعاملات الإلكترونية في ضوء القانون الإقتصادي**، العدد الثاني، يناير، 2009، مطبوعات الهلال، وجدة، ص 139.

جديد. كما أنّ التوقيع بالشكل الإلكتروني يقوم أيضا بمنح المستند الإلكتروني صفة المحرّر الإلكتروني، وبالتالي يجعل منه دليلا معدا مسبقا للإثبات له نفس منزلة الدليل الكتابي الذي يتم إعداده مسبقا قبل أن يثور النزاع بين الأطراف.[1]

الفرع الثاني: صور التوقيع الإلكتروني.

تتعدّد صور التوقيع الإلكتروني بحسب الطريقة التي يتم بها هذا التوقيع، كما أنّ هذه الصور تختلف فيما بينها من حيث درجة الثقة ومستوى ما تقدّمه من ضمان، وذلك بحسب الإجراءات المتّبعة في إصدارها وتأمينها والتقنيات التي تتّبعها، وسنتطرّق في هذا الفرع لأهم صور التوقيع الإلكتروني.

1- التوقيع بالقلم الإلكتروني:

ويتمّ هذا التوقيع عن طريق قلم إلكتروني حسابي، يمكن عن طريقه الكتابة على شاشة الحاسوب الآلي، وذلك باستخدام برنامج معيّن[2]، ويقوم هذا النوع من التوقيعات بأداء وظيفتين هما:

- إلتقاط إمضاء العميل الذي يتمّ كتابته بقلم إلكتروني حساس في مرجع مخصص لذلك على شاشة الحاسب أو أيّ مكان يخصص له، بعد أن يكون العميل أدخل رقمه السرّي الخاص من

خلال بطاقة تحتوي على بيانات خاصة به.

- أمّا الوظيفة الثانية التي تقوم بها فهي التحقق من صحة توقيع العميل بمقارنته مع التوقيع الأصلي المخزن على الموقع الإلكتروني أو على جهاز الحاسوب، وذلك لبيان لمن يعود هذا التوقيع، معتمدا في ذلك على مجموعة من الخصائص البيولوجية للتوقيع ومنها:

[1]. بشار محمود دودين، المرجع السابق، ص 248.
[2]. عباس العبودي، المرجع السابق، ص 157.

البيانات المتعلّقة بموقع القلم على اللوحة، وتسارع مراحل كتابة التوقيع، السرعة الكلّية للكتابة، إتجاهات الكتابة بإحداثيات سلبية وإيجابية.[1]

2- التوقيع البيومتري:

يقصد بالتوقيع البيومتري التحقّق من الشخصية عن طريق الخواص الطبيعية والفيزيائية والسلوكية الحيوية، فلكلّ إنسان صفات وسمات خاصة به تميّزه عن غيره من البشر، ومن ذلك بصمة الإصبع ومسح قرينة العين وبصمة الشفاه والتوقيع الشخصي، ونبرة الصوت، وبصمة الأسنان، وبصمة صنوان الأذن، ووجه الشخص ذاته.[2]

ويتم استخدام هذا الأسلوب من التوقيع عن طريق أخذ صورة دقيقة للشكل وتخزينها بصورة مشفرة داخل الحاسوب الآلي في نظام حفظ الذاكرة، وذلك بهدف توفير الإستخدام القانوني فقط للأشخاص المصرح لهم بذلك، وبالتالي منع أي استخدام غير قانوني أو غير مرخص به لأيّ معلومات أو بيانات سرية أو شخصية موجودة في نظم المعلومات الخاصة بإحدى الجهات، ولما كانت الخواص الذاتية المميزة لكل شخص كمسح قرينة العين أو بصمة الشفاه، تختلف عن تلك التي تميزّ غيره من الأشخاص، فإنّ النتيجة المترتّبة عن ذلك تقضي بأنّ التوضيح البيومتري يعتبر وسيلة موثوق بها لتمييز الشخص وتحديد هويته نظرا لإرتباط الخصائص الذاتية به، الأمر الذي يسمح باستخدامها في إقرار التصرفات القانونية التي تبرم عبر وسيط إلكتروني.[3]

---

[1]. لورنس محمد عبيدات، **إثبات المحرّر الإلكتروني**، دار الثقافة للنشر والتوزيع، الطبعة الأولى، 2009، ص 130.
[2]. محمد أمين الرومي، **النظام القانوني للتوقيع الإلكتروني**، دار الفكر الجامعي، الطبعة الأولى، 2006، ص 37.
[3]. عباس العبودي، المرجع السابق، ص 156.

3- التوقيع ا لكودي (البطاقات الممغنطة):

هذه الصورة من أكثر الصور شيوعا في حياتنا العملية حيث تقوم البنوك بإصدار بطاقات إئتمان[1] والتي تستخدم في السحب النقدي من خلال بطاقات الصرف الآلي والتي تخوّل حاملها إمكانية سحب مبالغ نقدية من حسابه بحدّ متّفق عليه بينه وبين البنك مصدر البطاقة، إضافة إلى ما تقوم به هذه البطاقات من سداد ثمن بعض السلع والخدمات من خلال أجهزة مخصصة لذلك، وما تقوم به البطاقة على رقم سرّي لا يعرفه إلاّ صاحبها، والذي يخوّله الدخول إلى حسابه وإجراء العمليات التي يريدها.

وفي حالة إتمام العملية من خلال الصراف الآلي بصورة صحيحة وحصول العميل في عملية السحب مثلا المبلغ الذي أراده فإنّه يحصل على شريط ورقي يثبت فيه المبلغ الذي تم سحبه والتاريخ والساعة والمبلغ المسحوب والرصيد المتبقي، حيث حلت هذه الإجراءات جميعها محل التوقيع التقليدي لما يتميز به من الأمان والثقة وتمييز صاحب البطاقة الذي يحمل الرقم.[2]

[1]. محمد أمين الرومي، المرجع السابق، ص 31 وما بعدها.
[2]. لورنس محمد عبيدات، المرجع السابق، ص 149.

المبحث الثاني: شروط ووظائف التوقيع الإلكتروني.

بعد أن تعرفنا على مفهوم **التوقيع الإلكتروني** عند استعراضنا لتعريفه من قبل المشرع الجزائري في القانون المتعلّق بالتوقيع والتصديق الإلكترونيين، ودوره في حل المشكلات القانونية التي بدأت تفرض نفسها بقوة في مجال انتشار العقود الإلكترونية عن طريق إضفاء نوع من الثقة والحماية للمتعاقدين، يمكن استنتاج الشروط اللازم توافرها في التوقيع الإلكتروني من حيث وظيفته في الإثبات حيث يلعب دورا مهما في تحديد شخصية الموقع وتميزه عن غيره، كما يجب أن يعير عن إرادة صاحب التوقيع وهذا ما سنقوم بتوضيحه في (المطلب الأوّل) **شروط التوقيع الإلكتروني** وفي (المطلب الثاني) **وظائف التوقيع الإلكتروني.**[1]

المطلب الأوّل: شروط التوقيع الإلكتروني.

يشترط لتحقيق التوقيع الإلكتروني الوظائف التي وضع من أجلها أن تتوفر فيه مجموعة من الشروط وهي كالآتي:

الفرع الأوّل:أن يكون متميزا ومرتبطا بصاحبه.[2]

يجب أن يكون التوقيع الإلكتروني علامة مميزة لشخصية الموقع، فالتوقيع بالخصائص الذاتية للشخص[1]، وكذا التوقيع بالقلم الإلكتروني أو التوقيع الرقمي وغيرها،

[1]. إيناس الخالدي، المرجع السابق، ص 23.
[2]. قد نص المشرع المغربي عن هذا الشرط في المادة 06 من القانون رقم 05-53 المتعلق بالتبادل الإلكتروني للمعطيات الإلكترونية.

تتضمن علامات مميزة لشخص عن غيره، والذي يعني أنّ قيام أكثر من شخص باستعمال بعض أدوات إنشاء التوقيعات تمتلكها مؤسّسة مثلا، فإنّ تلك الأداة يجب أن تكون قادرة على تحديد هوية مستعمل واحد تحديدا لا لبس فيه في سياق كلّ توقيع إلكتروني على حدى.[2]

الفرع الثاني: أن يسمح بتعريف هوية الموقع.

يتطلب هذا الشرط أن يكون التوقيع الإلكتروني قادرا على التعريف بشخصية الموقع، فالتوقيع بالرقم السرّي مثلا قادر على تحديد هوية الموقع، لأنّ الرقم السرّي لا يعرفه إلاّ صاحبه بحيث لا يستطيع أن ينكر الموقع استخدامه للبطاقة المقترنة برقمه السرّي الذي لا يشابه رقما آخر ولا يعرفه إلاّ هو، والحال كذلك في التوقيع الرقمي إذ يمكّن من تحديد هوية الشخص الموقع، إضافة إلى الإستعانة بسلطات التصديق ونفس الشيء بالنسبة للتوقيع الإلكتروني بالقلم الإلكتروني حيث لا يمكن استخدامه إلاّ من قبل الشخص الموقع وحده، لأنّ هذا النظام لا يعمل إلاّ إذا تطابق مع ما هو مخزن في ذاكرة الكمبيوتر.[3]

وتحديد هوية مبرم العقد أمر ضروري خاصة في مجال الوفاء بالإلتزامات العقدية ليتم تحديد أهلية صاحب التوقيع فلا يتصور أن يتم منح شخص عديم الأهلية أو ناقصا توقيعا إلكترونيا، لأنّ هذا الأمر يبني عليه إلتزامات كثيرة، بحيث يتوجب على صاحب التوقيع الإلكتروني أن يكون كامل الأهلية للقيام بها، حتى تتمكن جهة إصدار التوقيع الإلكتروني من منح التوقيع لهذا الشخص.[4]

---

[1]. نضال سليم برهم، **أحكام عقود التجارة الإلكترونية**، دار الثقافة للنشر والتوزيع، الطبعة الأولى، 2009، ص 130.

[2]. لورنس محمد عبيدات، المرجع السابق، ص 130.

[3]. نضال سليم برهم، المرجع السابق، ص 231.

[4]. لورنس محمد عبيدات، المرجع السابق، ص 130.

الفرع الثالث: سيطرة صاحب التوقيع على منظومة التوقيع.

إنّ هذا الشرط يتطلب أن يكون صاحب التوقيع الإلكتروني منفردا به، بحيث لا يستطيع أيّ شخص معرفة فك رموز التوقيع الخاص به أو الدخول عليه سواء عند استعماله لهذا التوقيع أو عند إنشاءه.[1]

الفرع الرابع: إرتباط التوقيع الإلكتروني بالمحرّر إرتباطا وثيقا.

لابدّ أن يكون التوقيع متّصلا إتصالا ماديا ومباشرا بالمحرّر الإلكتروني حتى يكون دليلا على إقرار الموقع على ما ورد في المحرّر، وعند النظر إلى التوقيع الرقمي مثلا والذي يعتمد على مفتاحين عام وخاص، بحيث لا يستطيع أحد أن يطّلع على مضمون المحرّر إلاّ الشخص الذي يمتلك المفتاح الخاص، وبالتالي فإنّ المحرّر يرتبط بالتوقيع على نحو لا يمكن فصله أو التعديل فيه إلاّ من صاحب المحرّر نفسه.

المطلب الثاني: وظائف التوقيع الإلكتروني.

يتحدّد دور التوقيع الإلكتروني عامة في ثلاث وظائف أساسية التي سيتم إدراجها فيما يلي:

[1]. لورنس محمد عبيدات، المرجع نفسه، ص 131.

الفرع الأوّل: تمييز هويّة صاحب التوقيع.

ومعنى ذلك بأن يدلّ التوقيع الذي وضع من أجل تحديد هويّة شخص الموقّع حيث يعتبر ذلك دليلا على مشاركة ذلك الشخص بعينه في عملية التوقيع، والربط بين ذلك الشخص ومضمون المحرّر، ولهذا فإنّ التوقيع يمكن أن يؤدي مجموعة متنوّعة من الوظائف حسب طبيعة المستند الذي يحمل التوقيع، فعلى سبيل المثال يمكن أن يكون التوقيع شاهدا على نيّة الطرف في الإلتزام بمضمون العقد الموقّع عليه وعلى نيّة الشخص الإقرار بتحرير النص، أو على نيّته في تأييد مضمون مستند كتبه شخص آخر، وبذلك يتّضح له مدى الإدراك في ترتب النتائج القانونية على عملية التوقيع هذه، والتوقيع الإلكتروني قادر على تحديد هوية الشخص الموقع، خاصة إذا دعم هذا التوقيع بوسائل توفر الثقة الكافية، فالتوقيع بالرقم السرّي قادر على تحديد هوية الشخص الموقع، لأنّ الرقم السري لا يعرفه إلاّ صاحبه، بحيث لا يستطيع أن ينكر الموقع استخدامه للبطاقة المقترنة برقمه السرّي الذي لا يشابه رقما آخرا ولا يعرفه إلاّ هو[1]، وكذلك التوقيع بالخصائص الذاتية يحدّد هويّة الشخص الموقع لأنّ هذه الخصائص تميّزه عن غيره. وبالحال كذلك في التوقيع الرقمي وهو شكل من أشكال التوقيع الذي تطرّقنا إليه سابقا.[2]

الفرع الثاني: التعبير عن إرادة الموقع بمضمون السند.

يمكن ملاحظة أنّ التوقيع يعبّر عن إرادة الموقع بالموافقة على مضمون السند أو

المحرربوصفه أداة صحة، فهو يعبّر عن إرادة صاحبه بالموافقة على ما ورد في السند، وبالتالي فإنّ الموقع عندما يقوم بالتوقيع بإدخال رقمه السرّي أو المفتاح الخاص، أو البصمة

[1]. نضال سليم برهم، المرجع السابق، ص 45.
[2]. لورنس محمد عبيدات، المرجع السابق، ص 152.

الجينية على الشاشة فإنّ معنى ذلك هو قبول الشخص لما ورد في هذا المحرّر والتزامه به، وحتى يكون التوقيع صحيحا يجب أن يكون معبرا عن موافقة صاحبه على مضمون ما جاء به من إلتزامات، وهذا ما أكّده قانون المعاملات الإلكترونية الأردني، حيث نصت المادة 10/ب على أنّه: "يتمّ إثبات صحة التوقيع الإلكتروني ونسبته إلى صاحبه إذا توافرت طريقة لتحديد هويّته والدلالة على موافقاته على المعلومات الواردة في السجل الإلكتروني الذي يحمل توقيعه إذا كانت تلك الطريقة ممّا يعوّل عليها لهذه الغاية في ضوء الظروف المتعلّقة بالمعاملة، بما في ذلك إتفاق الأطراف على استخدام تلك الطريقة". ولهذا نرى أنّ هذا النص يشير إلى استيفاء شرط التوقيع على المحرّر في استخدام التوقيع الإلكتروني، فهو بذلك يحقق أهداف التوقيع التقليدي من حيث الدلالة على موافقته على المعلومات الواردة في السجل الإلكتروني الموقع إلكترونيا، ونص هذه المادة جوهري من حيث أنّها إشارات إلى الإعتراف القانوني بالتواقيع الإلكترونية على السجلات والرسائل الإلكترونية كبديل للتوقيع الخطّي على السجلاّت والرسائل المكتوبة تقليديا.[1]

[1]. لورنس محمد عبيدات، المرجع نفسه، ص 153 وما بعدها.

المبحث الثالث: حجّية التوقيع الإلكتروني في الإثبات.

سنتناول في هذا المبحث **حجّية التوقيع الإلكتروني الموثق** (المطلب الأوّل) ثمّ نعرّج بعد ذلك على **حجّية التوقيع الإلكتروني العادي**(المطلب الثاني).

المطلب الأوّل: حجّية التوقيع الإلكتروني الموثق.

بيّنا فيما سبق أنّ التوقيع الإلكتروني يعد عنصرا فعّالا في المعاملات التجارية المحلية والدولية، فهو جزء من العقد أو المستند، ودون ذلك لا يكون للسند أيّة قيمة قانونية في الإثبات، حيث سنتطرّق في هذا المطلب إلى إجراءات توثيق التوقيع الإلكتروني **(الفرع الأوّل)**، والحجّية القانونية للتوقيع الإلكتروني الموثق **(الفرع الثاني)**.

الفرع الأوّل: إجراءات توثيق التوقيع الإلكتروني.

تتمثل إجراءات توثيق التوقيع الإلكتروني في:

1- إجراءات التوثيق المعتمدة:

يشترط أن تكون إجراءات التوثيق المعتمدة من جهة حكومية أو غير حكومية، فقد ورد في المادة 05 من قانون الأونيسترال النموذجي بشأن القواعد الموحدة الخاصة بالتواقيع الإلكترونية أنّ أيّة طريقة صالحة لإنشاء توقيع إلكتروني قابل للإعتماد عليها من حيث شكل التوقيع الإلكتروني وإجراءات إصداره ومن ثمّ توقيعه، ولا يجوز التمييز بين طرق إصدار التوقيع الإلكتروني وهذا يعني أن لا تكون إجراءات التوثيق المطبّقة عائقا أمام قبول التوقيع الإلكتروني.

كما أنّ المادة الخامسة من قانون المبادلات والتجارة الإلكترونية التونسي[1] تنص على أنّه: "يمكن لمن يرغب في إمضاء وثيقة إلكترونية إحداث إمضائه الإلكتروني بواسطة منظومة موثوق بها يتم ضبط مواصفاتها التقنية بقرار من الوزير المكلّف بالإتصالات".[2]

2- الإجراءات المتفق عليها بين الأطراف:

لقد أعطى المشرع الحريّة للأفراد للخروج عن الإجراءات المعتمدة وتلك المقبولة تجاريا واللجوء إلى إجراءات أخرى قد تكون أكثر ملائمة لطبيعة المعاملات التي يجرونها.[3]

وبشأن إجراءات التوثيق، فقد أوجبت المادة 09/01 من قانون الأونيسترال النموذجي للتواقيع الإلكترونية على مقدم خدمات التصديق ما يلي:

أ. أن يتصرّف وفقا للتأكيدات التي يقدّمها بخصوص سياساته وممارساته.

ب. أن يمارس بعناية معقولة لضمان دقة واكتمال كلّ ما يقدّمه من تأكيدات جوهرية ذات صلة بالشهادة طيلة دورة سريانها أو مدرجة في الشهادة.

ج. أن يوفر وسائل يكون الوصول إليها متيسّرا بقدر معقول وتمكن الطرف المعوّل من التأكيد ممّا يلي:

1. الطريقة المستخدمة في تعيين هويّة الموقع؛

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

---

[1]. قانون المبادلات والتجارة الإلكترونية التونسي عدد 83 لسنة 2000 المؤرخ في 09 غشت 2000، عبد الرحيم بوعيدة وضياء علي أحمد نعمان، موسوعة التشريعات الإلكترونية المدنية والجنائية، المطبعة الوراقة، الطبعة الأولى، 2010، الجزء الثاني، ص 119.

[2]. نضال سليم برهم، المرجع السابق، ص 256.

[3]. تنص المادة 30/ب من قانون المعاملات الإلكترونية الأردني لسنة 2001، الصادر بتاريخ 11 غشت 2001 على أنّه: "تعد إجراءات التوثيق مقبولة تجاريا إذا تمت عند تطبيقها مراعاة الظروف التجارية الخاصة بأطراف المعاملة".

3.أنّ بيانات إنشاء التوقيع صحيحة ولم تتعرّض لما يثير الشبهة؛

4. وجود أي تقييد على نطاق أو مدى المسؤولية التي اشترطها مقدم خدمات التصديق.

الفرع الثاني: الحجّية القانونية للتوقيع الإلكتروني الموثق.

إنّ التوقيع الإلكتروني المؤمن هو التوقيع الذي يستوفي سلامة التعاقد ليرتّب آثاره القانونية المتوخاة ذلك أنّ التوقيع المذكور يعتمد عليه في التعامل بخصوص التصرفات القانونية وهو عبارة عن رقم أو كتابة ولا علاقة له بالبصمة أو الختم المعتمدة في التعاقد التقليدي، ويرتبط ارتباطا عضويا بالتشفير.[1]

وحتى يكون التوقيع الإلكتروني مؤمنا لابدّ أن تتوفّر فيه مجموعة من الشروط نصّت عليها مختلف التشريعات المقارنة، وهي كالتالي:

الشرط الأوّل: أن يكون التوقيع الإلكتروني المؤمن خاص بالموقّع على الوثيقة الإلكترونية، ذلك أنّ الوثيقة الإلكترونية كما تكون مدنية قد تكون تجارية واشتراط خصوصية التوقيع الإلكتروني ونسبته إلى الموقع على العقد ضرورة حتمية في التصرفات القانونية لأنّها لا تتصور دونه وهو مكمل لها.[2]

الشرط الثاني: أن يتم إنشاء التوقيع الإلكتروني المؤمن بوسائل تمكّن الموقع من الإحتفاظ بها تحت مراقبته الخاصة بصفة حصرية.

الشرط الثالث: قيام الإرتباط الوثيقة بين التوقيع الإلكتروني المؤمن والوثيقة المنشئة للتصرّف القانوني، إنّ التوقيع الإلكتروني هو الذي يمنح الحياة للتصرف القانوني وهناك

[1]. المختار بن أحمد العطار، **العقد الإلكتروني**، كطبعة النجاح الجديدة، الدار البيضاء، الطبعة الأولى، 2010، ص 58-59.
[2]. المرجع نفسه، ص 59.

علاقة قانونية قائمة ومرتبطة بينهما وهذا من شأنه أن يساعد المرسل إليه الإيجاب من التعرّف على شخصية الموجب ونوع التصرف القانوني ونطاقه بكيفية مستمرة تمتد إلى ما بعد ترتيب الآثار القانونية للتصرف القانوني، وفي هذا حرص شديد من المشرع على التصرف القانوني الإلكتروني وجعله آمنا فضلا عن حماية كلا المتعاقدين بحيث أنّ كلّ تغيير يلحق بالوثيقة الإلكترونية يستطيع أيّ من المتعاقدين الوصول إليه.[1]

الشرط الرابع: خضوع التوقيع لآلية إنشائه مثبتة بشهادة المطابقة وضوابطها، فإنّ آلية إنشاء التوقيع الإلكتروني تتمثل في معدّات أو برمجيات أو هما معا غرضها هو توظيف معطيات إنشاء التوقيع الإلكتروني التي تحتوي العناصر الفريدة الخاصة بالموقع، كمفتاح الشفرة الخاص المستخدم من الموقّع بغرض إنشاء التوقيع الإلكتروني.

وبالتالي فإنّ شهادة المطابقة تسلّمها السلطات الوطنية المكلّفة باعتماد ومراقبة المصادقة الإلكترونية على التوقيع الإلكتروني وذلك إذا استجابت آلية إنشاء التوقيع الإلكتروني المؤمن الضوابط التالية:

الضابط الأوّل: أن تضمن آلية إنشاء التوقيع الإلكتروني وذلك بوسائل تقنية وإجراءات ملائمة لأنّ معطيات إنشاء التوقيع الإلكتروني لا يمكن إعدادها أكثر من مرّة واحدة وتكون سريّتها مضمونة وأن يكون بالإمكان الوصول إلى معطيات إنشاء التوقيع الإلكتروني عن طريق الإستنباط فضلا عن أنّ التوقيع الإلكتروني يجب أن يكون محميا من كلّ تزوير وأن يكون بالإمكان حمايته من طرف الموقّع بشكل يمنع الغير من استعماله.

الضابط الثاني: أن تحول آلية إنشاء التوقيع الإلكتروني دون أيّ تغيير أو تبديل لمحتوى الوثيقة المراد توقيعها وأن يكون في إمكان الموقع الإطّلاع بسهولة ويسر على الوثيقة الإلكترونية.

[1]. المختار أحمد العطار، المرجع نفسه، ص 61-62.

المطلب الثاني: حجّية التوقيع الإلكتروني العادي.

سنعالج في هذا المطلب حالة وجود إتفاق ينظم حجة التوقيع الإلكتروني في الإثبات **(الفرع الأوّل)**، وحالة عدم وجود إتفاق بين الأطراف على حجّية التوقيع الإلكتروني العادي **(الفرع الثاني)**.

الفرع الأوّل: حالة وجود إتفاق ينظم حجّية التوقيع الإلكتروني في الإثبات.

بداية لابد من الإشارة إلى قواعد الإثبات والتي تقسّم إلى **قواعد إجرائية وقواعد موضوعية**، وذلك على النحو التالي:

أوّلا: القواعد الإجرائية المتعلّقة بإجراءات التقاضي:

وهي قواعد وضعها المشرع لخدمة العدالة وتحقيقها، واحترام حقوق الدفاع وتسهيل عملية الإثبات، فيحدّد على ضوئها إجراءات التقاضي التي يلتزم بها الخصوم والقضاة على حدّ سواء، وهذه القواعد متعلّقة بالنظام العام لا يجوز لأطراف الإتفاق مخالفتها.[1]

ثانيا: القواعد الموضوعية:

وهي تلك التي تتعلّق بمحل الإثبات وطرق الإثبات وعلى من يقع عبء إثباته.

ويرى الدكتور عبد الرزاق السنهوري[2] أنّ إثبات القواعد الموضوعية يمكن الإتفاق على مخالفتها لأنّها تتناول حقوقا فردية ومصالح خاصة، فإذا كان يجوز للأفراد التنازل عن

---

[1]. أيمن علي حسين الحوثي، **التوقيع الإلكتروني بين النظرية والتطبيق**، رسالة لنيل دبلوم الدراسات المعمقة في القانون الخاص، قانون التجارة والأعمال، كلية الحقوق، جامعة محمد الأول، وجدة، 2006-2007، ص 79.

[2]. عبد الرزاق أحمد السنهوري، **الوسيط في شرح القانون المدني، نظرية الإلتزام بوجه عام، الإثبات، آثار الإلتزام**، الجزء الثاني، تنقيح أحمد مدحت مراري، منشأة المعارف، الإسكندرية، طبعة 2004، ص 77 وما بعدها.

حقوقهم أصلا فإنّه من غير المعقول أن نمنعهم من التنازل عن القواعد القانونية التي تهدف إلى حماية هذه الحقوق، لأنّ هذه القواعد لا صلة لها بالنظام العام، ومن ثم يمكن لأطراف الإتفاق صراحة أو ضمنيا مخالفة قواعد الإثبات سواء فيما يتعلّق بطرقه أو بعبئه أو بمحلّه.

ومع ذلك ينبغي عدم إطلاق القول لأنّ قواعد الإثبات الموضوعية لا تتعلّق بالنظام العام، وإنّما يجب النظر إلى الغاية التي تحقّقها قاعدة الإثبات وإذا كانت قاعدة الإثبات تتعلّق بسلطة القاضي في الإثبات، كسلطة توجيه اليمين، أو تتعلق بالضمانات الأساسية لحق الدفاع، كالمجابهة بالأدلّة، أو كانت مشتملة على قيود قانونية واردة على حرية الإثبات فإنّها تعد متعلّقة بالنظام العام، وكمثال لهذه القواعد الأخيرة قاعدة كون الورقة الرسمية حجّة على الناس كافة إلى أن يطعن فيها بالتزوير، وقاعدة كون الورقة العرفية حجّية على الغير في تاريخها الثابت، وحجّية القرائن القانونية القاطعة، ومثل هذه القواعد لا يجوز مخالفتها ويكون كلّ إتفاق بخصوصها باطلا وعديم الأثر لكون موضوعها متعلّق بالنظام العام.[1]

وبالتالي ليس هناك ما يمنع الأشخاص من اللجوء إلى عقد إتفاقات – مادامت لا تتضمن شروطا تعسّفية تضرّ بمصالح أحد الأطراف – يقرّون بموجبها منح التوقيع الإلكتروني حجّية قانونية قابلة لإثبات العكس، وعادة ما يلجأ الأشخاص إلى عقد هذه الإتفاقات في التعاملات التي تتم لمرّة واحدة فقط، لذلك فإنّ هذه الإتفاقيات قليلا ما تبرم في التصرفات التي تتم عن بعد عبر شبكة الإتصالات الحديثة علما أنّه من الجائز إبرام هذه الإتفاقات إذا رغب الأطراف في ذلك وإذا كانت العلاقة بينهم مستمرة.[2]

[1]. أيمن علي حسين الحوثي، المرجع السابق، ص 80-81.
[2]. عيسى غسان ربضي، المرجع السابق، ص 231.

الفرع الثاني: حالة عدم وجود إتفاق بين الأطراف على حجّية التوقيع الإلكتروني العادي.

للقاضي سلطات واسعة في تحديد قيمة الدليل المطروح أمامه، وفي تحديد حجّيته في الإثبات، وفي مراعاة توافر ما يتطلّبه القانون من اشتراطات في المحرّر، والتأكّد من أنّ الطريقة المتّبعة في توقيعه هي طريقة مأمونة وجديرة بالثقة[1] والذي يجعله في مرتبة المحرّر الرسمي، فإنّ المحرّر المذيل بتوقيع إلكتروني عادي لا يمكن تجاهله، وإن لم يكن هناك إتفاق بين الأطراف ينظم ذلك، خصوصا في ظل إجراءات تؤمن الثقة والأمان في التوقيع الإلكتروني وإن لم يكن معزّزا بشهادة توثيق من جهات معتمدة حيث تم منح القاضي سلطة تقديرية في تحديد مدى حجّية السند الإلكتروني غير الموثق، وغير مسبوق بإتفاق بين أطرافه، فإذا تبيّن للقاضي أنّ المحرّر الذي يتمتّع بذات المواصفات التي يتمتع بها المحرّر الكتابي، من حيث توافر الثقة في طريق إنشائه وإرساله، وتخزينه، والإطمئنان إلى أنّ التوقيع منسوب للموقّع، وأنّه تمّ وضعه على المحرّر الإلكتروني بطريقة تحقّق ارتباطا وثيقا بينهما وتتم عن قبوله لمضمونه، فإنّه يعتد به كالمحرّر الكتابي في الإثبات.[2]

[1]. أيمن علي حسين الحوثي، المرجع السابق، ص 86.
[2]. عيسى غسان ربضي، المرجع السابق، ص 239.

المبحث الرابع: آليات حماية التوقيع الإلكتروني.

يتطلب قيام مستخدم ما بالدخول لموقع ما للقيام بتعاملات إلكترونية مثلا باستخدام شبكة الإنترنت، ضرورة تأمين تلك التعاملات في حالة استخدام التوقيع الإلكتروني.

وكلما كان الإجراء المتّبع يحقق الثقة بين المتعاملين زادت كمية المعاملات الإلكترونية والتجارة الإلكترونية، حيث يقع على عاتق القائم على موقع التجارة الإلكترونية التوثق من صحّة الطلب، والذي يتطلب التحقق من أن يخاطبه هو فعلا من سجل إسمه وعنوانه الإلكتروني أو غير ذلك من البيانات والمعلومات التي تتطلبها المواقع الإلكترونية ويكتسب هذا الأمر أهمية كبيرة في ضوء الزيادة الكبيرة في جرائم الإختراقوالإحتيال الإلكتروني المرتكبة باستخدام شبكة الإنترنت. وهذا ما سيتم تناوله في ماهية التشفير كآلية لحماية التوقيع الإلكتروني (**المطلب الأوّل**)، والتوقيع الرقمي (**المطلب الثاني**).

المطلب الأوّل: ماهية التشفير.

تأتي أهمية التشفير لمنع مرتكبي جرائم الإختراقوالإحتيال الإلكتروني من إرتكاب جرائمهم ضدّ هذه التعاملات الإلكترونية[1]، والذي دفع بعض الجهات لإيجاد تقنيات لحماية أمن المعلومات عامة وأمن التجارة الإلكترونية خاصة، من خلال استخدام تقنية **التشفير** لضمان خصوصية تعاملات الأطراف ومنع أيّة تعديلات عليها. ومن هنا سنتناول المقصود بالتشفير (**الفرع الأوّل**)، ضوابط التشفير (**الفرع الثاني**)، الهدف من التشفير (**الفرع الثالث**)، طرق التشفير (**الفرع الرابع**).

[1]. عيسى غسان ربضي، المرجع السابق، ص 177 وما بعدها.
أنظر أيضا: خالد مصطفى فهمي، **النظام القانوني للتوقيع الإلكتروني**، دار الجامعة الجديدة، الإسكندرية، 2007، ص 100 وما بعدها.

الفرع الأوّل: المقصود بالتشفير.

التشفير هو الآلية التي تحمي المعلومات القيّمة مثل المستندات أو الصور أو المعاملات الإلكترونية داخل الإنترنت، من الأشخاص غير المرغوب فيهم للحيلولة دون الوصول إليها أو تغييرها. يعمل التشفير باستخدام "**شفرة**" (صيغة رياضية) ومفتاح لتحويل البيانات المقروءة **(نص عادي)** إلى شكل لا يستطيع الآخرون فهمه **(نص مشفر)** والشفرة هي الوصفة العامة للتشفير. والمفتاح الخاص بك يجعل البيانات المشفرة فريدة من نوعها، يمكن فك تشفيرها فقط لمن يعرف هذا المفتاح، وعادة ما تكون المفاتيح عبارة عن سلسلة طويلة من الأرقام التي تحميها آليات المصادقة المشتركة مثل كلمات المرور أو الرموز أو القياسات الحيوية مثل بصمة الإصبع.[1]

وقد عرّف بعض الفقه التشفير بأنّه تغيير في شكل البيانات عن طريق تحويلها إلى رموز أو إشارات لحماية هذه البيانات من إطّلاع الغير عليها أو من تعديلها أو تغييرها.[2]

وبالتالي ومن خلال التعريف السابق نجد أنّ التشفير يعتمد على بيانات 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 الرسالة يملك مفتاح التشفير الذي يحوّل الإشارات والرموز إلى النص الأصلي.[3]

وبالرجوع إلى المشرع الجزائري نجده نص في المادة 02 من القانون رقم 15-04 الفقرة 08 والفقرة 09 على **مفتاح التشفير الخاص** والذي هو عبارة عن سلسلة من الأعداد

---

[1]. http: www.securing thehuman.org.

[2]. عبد الفتاح حجازي، **النظام القانوني لحماية التجارة الإلكترونية**، دار الفكر الجامعي، الإسكندرية، 2002، ص 203.

[3]. عبد الفتاح حجازي، المرجع نفسه، ص 203.

يحوزها حصريا الموقع فقط، وتستخدم لإنشاء التوقيع الإلكتروني ويرتبط هذا المفتاح بمفتاح تشفير عمومي.

أمّا**مفتاح التشفير العمومي** هو عبارة عن سلسلة من التحقق من الإمضاء الإلكتروني، وتدرج في شهادة التصديق الإلكتروني.[1]

الفرع الثاني: ضوابط التشفير.

1- إباحة تشفير البيانات والمعلومات التي يتم كتابتها أو التعامل فيها باستخدام الوسائل الإلكترونية:

حيث أنّ غالبية التشريعات المقارنة وضعت قواعد ونصوص قانونية تتعامل مع تشفير البيانات والمعلومات وأصدرت تلك الدول قوانين خاصة بالتجارة الإلكترونية لتتعامل مع التشفير. فنجد على سبيل المثال لا الحصر أنّ القانون التونسي الخاص بالمبادلات والتجارة الإلكترونية تعامل معه بشكل مباشر من خلال نصوص التعاملات الإلكترونية التجارية عبر شبكة الإنترنت.

كما أكّد نفس القانون أهمية حماية البيانات المشفرة والعناصر المستخدمة في عملية التشفير وفكّها من أيّ إعتداء عليها سواء تمّ ذلك بإستخدام عناصر التشفير الشخصية الخاصة بتوقيع من غير طرفي العلاقة لإستخدام التشفير في إرتكاب جرائم إحتيالية أو سرقة مفاتيح التشفير التي تفكّ النص المشفر وترجعه إلى النص الأصلي بإستخدام مفاتيح التشفير الخاصة.[2]

[1]. القانون رقم 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين.
[2]. عبد الفتاح حجازي، المرجع السابق، ص 203، أنظر أيضا لورنس محمد عبيدات، المرجع السابق، ص 137.

وقد عالجت التشريعات العربية الخاصة بالتجارة الإلكترونية عملية التشفير بطريقة غير مباشرة، كما أوضحنا سابقا من خلال التوقيع الإلكتروني وذلك بإستثناء**المشرع التونسي** الذي تعامل مع عملية التشفير بشكل مباشر من خلال نصوص خاصة به منعا لإختلاف التفاسير والإجتهادات الفقهية بشأنها.[1]

2- الحق في الحفاظ على سريّة البيانات والمعلومات المشفرة:

ويتطلب ذلك الإعتراف بحق أصحابها في سرّية تلك البيانات والمعلومات وتجريم الإعتداء عليها، فقد اعتبر مشروع قانون التجارة الإلكترونية المصري أنّ الإعتداء على البيانات المرسلة بين طرفي العقد عبر شبكة الإنترنت هو إعتداء على خصوصية وسريّة البيانات والمعلومات المرسلة بين طرفي العلاقة، لأنّ تلك البيانات والمعلومات تتميز بالخصوصية والسرّية وتعبر عن إرادة الطرفين بالقيام بتصرف قانوني، واطّلاع الغير على هذه البيانات والمعلومات يمكن أن يؤدّي إلى إلحاق الضرر بطرفي العلاقة والإعتداء على خصوصيّتهم بمعرفة البيانات التي تم كشفها بعد فكّ التشفير.[2]

وقد وضع المشرع المصري نصوصا في قوانين التجارة الإلكترونية تعاقب كل من يقوم بانتهاك سرّية البيانات المشفرة وإفشائها، سواء كان ذلك بشكل مباشر أو عن طريق النص على أنّ أيّ إعتداء يقع على التجارة الإلكترونية يعد مخالفا لأحكام القوانين وبالتالي يعاقب العقوبة المقرّرة.[3]

---

[1]. مدحت عبد الحليم رمضان، **الحماية الجنائية للتجارة الإلكترونية**، دار النهضة العربية، القاهرة، 2001، ص 31 وما بعدها.

[2]. عبد الفتاح حجازي، المرجع السابق، ص 137.

[3]. مدحت عبد الحليم رمضان، المرجع السابق، ص 31، أنظر أيضا لورنس محمد عبيدات، المرجع السابق، ص 137.

3- اعتبار استخدام التشفير وسيلة يعتد بها قانونا في تحرير البيانات والمعلومات من قبل الجهات المختصة:

كأثر لإقرار المشرع للنص المشفر وحجّيته في إثبات التصرفات القانونية فإنّه يعتبر من المحرّرات الإلكترونية، حيث يمكن تحويل الإشارات والرموز إلى نصوص مقروءة ومفهومة تكون حجّة على من قام بمخالفة الإتفاق المبرم بين الطرفين.[1]

الفرع الثالث: الهدف من التشفير.

تبرز أهمية التشفير في منع الغير من مستخدمي شبكة الإنترنت من الدخول إلى البيانات والمعلومات والحفاظ على سرّيتها وخصوصيّتها للأطراف باستخدام وسائل إلكترونية رقمية أو رموز معيّنة عوضا عن الكتابة التقليدية التي لا يعرفها إلاّ أطراف التعامل التجاري بما لا يسمح باستخدامها من قبل الغير.فاستخدام التشفير يحقق أكبر درجة من الأمن والحماية لمستخدمي شبكة الإنترنت نتيجة لإستعمال أفضل طرق التشفير التي يصعب فكّها.[2]

الفرع الرابع: طرق التشفير.

يتم التشفير من خلال استعمال المفاتيح الخاصة في عملية تشفير الرسالة وفكّ تشفيرها، ويتم ذلك بتحويل الرسائل إلى أشكال تظهر وكأنّها لا يمكن فهمها ومن ثمّ إعادة النص إلى ما كان عليه في السابق. ويتم الإستعانة بمفتاحين مختلفين مرتبطين بشكل حسابي لإنشاء التوقيع الإلكتروني، لتحويل البيانات والمعلومات ثمّ تثبيتها مرّة أخرى بنظام

[1]. عبد الفتاح حجازي، المرجع السابق، ص 204.
[2]. المرجع نفسه، ص 205.

التشفير غير المتماثل ولا يستطيع الغير لو عرفوا مفتاح الشفرة العام اكتشاف المفتاح الخاص بالموقع واستخدامه في التعرّف على محتوى الرسالة.[1]

والمفتاح الخاص يكون معروفا لدى جهة واحدة فقط أو شخص واحد وهو المرسل، ويستخدم لتشفير الرسالة وفك شفرتها، أمّا المفتاح العام فعادة ما يكون معروفا لدى أكثر من جهة أو شخص. ويؤدي فكّ الشفرة إلى إفشاء البيانات والمعلومات وانتشارها ومن ثمّ الإضرار بأصحابها أو بالغير. ومن هذا المنطلق وجب على المشرع أن ينصّ على عقاب من يقوم بفكّ الشفرة وفض المعلومات المشفّرة، نظرا للأضرار الكبيرة التي تترتّب على هذا الفعل.[2]

المطلب الثاني: التوقيع الرقمي.

تأتي أهمية التوقيع الرقمي لمحاكاة خصائص الأمان بشكله الرقمي وليس بشكله العادي (المكتوب)، إنّ التوقيع الرقمي كالتوقيع المكتوب، أي أنّه يستخدم للمصادقة على صحّة مضمون الملف الموقّع عليه والذي يسمى عادة الرسالة والتي يمكن أن تكون على شكل بريد إلكتروني أو عقد معيّن أو حتى رسالة معقدة مرسلة ببروتوكول معيّن، وهذا ما سيتم دراسته من خلال تعريف التوقيع الرقمي (**الفرع الأوّل**)، الصفات المميزة للتوقيع الرقمي (**الفرع الثاني**)، كيفية عمل تقنية التوقيع الرقمي (**الفرع الثالث**)، أهداف وأغراض استخدام التوقيع الرقمي (**الفرع الرابع**).

[1]. عبد الفتاح حجازي، المرجع السابق، ص 204.
[2]. عبد الفتاح حجازي، المرجع نفسه، ص 205، أنظر أيضا لورنس محمد عبيدات، المرجع السابق، ص 139 وما بعدها.

الفرع الأوّل: تعريف التوقيع الرقمي.

لا يوجد تعريف بسيط للتوقيع الرقمي ولكن في حال وجود مثل هذا التعريف فإنّه يمكن أن يكون مشابها للتعريف التالي: "طريقة اتصال مشفرة تعمل على توثيق المعاملات التي تتم عبر الإنترنت".[1]

بشكل أساسي فإنّ الفكرة الكامنة وراء التوقيعات الرقمية هي نفسها كما في التوقيع المكتوب بخط اليد. إنّك تستخدمه للتصديق أو التوثيق، الحقيقة بأنّك وعدت بشيء ما ولا تستطيع التراجع عنه فيما بعد. إنّ التوقيع الرقمي لا يتضمن القيام بتوقيع شيء ما باستخدام القلم والورقة وبعد ذلك إرساله عبر الإنترنت ولكنّه مثل التوقيع على الورق يلتصق بهوية الموقّع على معاملة ما.

الفرع الثاني: الصفات المميّزة للتوقيع الرقمي.

يجب أن يكون للتوقيع بشكل عام الصفات المميّزة التالية:

1- توثيق الموقّع: إنّ التوقيع يجب أن يبيّن أو يشير إلى الشخص الذي قام بتوقيع الوثيقة أو الرسالة أو السجل ويجب أن يكون من الصعب على شخص آخر القيام به دون ترخيص وتفويض.

2- توثيق الوثيقة: أيّ توقيع يجب أن يعرّف عن الطرف الذي قام بتوقيعه بما يجعله غير ممكن تزوير أو تغيير أي من المادة الموقّعة أو التوقيع بدون إنكشاف الحقيقة.

[1]. أمجد قاسم، **التوقيع الرقمي، أهميته وصفاته ومكوّناته**، تقنيات متفرقة، 15 يونيو 2012.

الفرع الثالث: كيفية عمل تقنية التوقيع الرقمي.

يتم عمل تقنية التوقيع الرقمي عن طريق التشفير بواسطة المفتاح العام (شيفرة تستخدم مفتاحين متناظرين أحدهما سرّي ويحفظه مستلم البيانات والآخر عمومي). يتم خلق التوقيعات وكذلك التثبت من صحّتها من خلال التشفير وهو فرع من الرياضيات التطبيقية المختصة بتحويل الرسائل إلى أشكال تبدو وكأنّها لا يمكن فهمها وإعادتها مرّة أخرى كما كانت كما وضّحنا سابقا.

تستخدم التوقيعات الرقمية ما يعرف بنظام شيفرة المفتاح العام والذي يستخدم منهجا معيّنا مستعينا بمفتاحين مختلفين ولكنّهما مرتبطان حسابيا، واحد لخلق التوقيع الرقمي أو لتحويل البيانات إلى أشكال تبدو وكأنّها لا يمكن فهمها والمفتاح الآخر للتثبت من صحّة التوقيع الرقمي أو لإعادة الرسالة إلى شكلها الأصلي.[1]

تدعى أجهزة وبرامج الحاسب الآلي التي تستخدم مثل هذين المفتاحين عادة **بنظام التشفير اللاّتماثلي.** إنّ المفاتيح التكميلية في نظام الشيفرة اللاّتماثلية للتوقيعات الرقمية تدعى عشوائيا المفتاح الخاص والذي يعرفه فقط الموقّع ويستخدم لخلق التوقيع الرقمي والمفتاح العام والمعروف عادة على نطاق أوسع يستخدم من قبل شخص موثوق به للتثبت من صحة التوقيع الرقمي. في حال استدعت الظروف أنّ أكثر من جهة بحاجة للتثبت من صحة التوقيع الرقمي فإنّ المفتاح العام يجب أن يكون متوفرا لتلك الجهات أو يوزع عليهم جميعا أو ربّما يتم نشره في ملف للاتصال المباشر بحيث من الممكن الوصول إليه بسهولة بالرغم من أنّ كلا المفاتيح المرتبطين ببعضها رياضيا فإنّه في حال تمّ تصميم نظام الشيفرة اللاّتماثلية وتمّ تطبيقه بشكل آمن فإنّه حسابيا لا يمكن التوصل إلى معرفة المفتاح العام. وبهذا فإنّه بالرغم من أنّ العديد من الأشخاص يمكن أن يكونوا على علم بالمفتاح العام لموقع وما

[1]. أمجد قاسم، المرجع السابق، ص 19.

يستخدمونه للتثبت من صحة توقيعات موقّع معيّن إلاّ أنّهم لا يستطيعون اكتشاف المفتاح الخاص لذلك الموقّع واستخدامه في تزوير توقيعاته الرقمية.

الفرع الرابع: أهداف وأغراض استخدام التوقيع الرقمي.

إنّ عمليات خلق التوقيع الرقمي والتثبت من صحّته تحقّق التأثيرات الجوهرية المرجوّة من التوقيع لعدّة أغراض قانونية:

1- توثيق الموقع: في حال كان هناك زوج من المفاتيح واحد عام والآخر خاص وكانا مرتبطين بموقع معيّن محدّد فإنّ التوقيع الرقمي ينسب الرسالة إلى الموقع. لا يمكن تزوير التوقيع الرقمي ما لم يفقد الموقع السيطرة على المفتاح الخاص (تعرض المفتاح الخاص للخطر) كأن يقوم بإفشائه أو يفقد الوسط أو الوسيلة المحتفظ به فيها.

2- توثيق الرسالة: كذلك فإنّ التوقيع الرقمي يعمل على تحديد هويّة الرسالة الموقّعة بثقة ودقّة ويقين أكثر من التوقيعات على الورق. إنّ عملية التثبت من الصحة تكشف أي تلاعب حيث أنّ مقارنة نتائج الهامش (واحدة يتم إعدادها عند التوقيع والأخرى عند التثبت من الصحة) تبيّن ما إذا كانت الرسالة هي نفسها عندما تمّ توقيعها.

3- الفعالية: إنّ خلق التوقيع الرقمي والتثبت من صحّته تتطلب مستوى عال من الضمان بأنّ التوقيع الرقمي هو للموقّع بدون تكلف أو رياء مقارنة مع الأساليب الورقية مثل بطاقات نموذج اعتماد التوقيع والتي هي أساليب مملة وتستغرق الكثير من الجهد بحيث أنّه نادرا ما يتم استخدامه في الواقع، فإنّ التوقيعات الرقمية تعطي وتولد درجة ضمان أعلى بدون أن تضيق كثيرا على الموارد المطلوبة للمعالجة.

4- عمل إيجابي: إنّ خلق التوقيع الرقمي يتطلب من الموقّع استخدام مفتاح الموقع الخاص وهذا العمل بإمكانه أن ينجز الوظيفة الرسمية أو الشعائرية في تنبيه الموقّع إلى حقيقة أنّ الموقع يقوم باستكمال معاملة لها عواقب ونتائج قانونية.[1]

[1]. أمجد قاسم، المرجع السابق، ص 20 وما بعدها.

خلاصة الفصل الأول:

يعد التوقيع الالكتروني واقعة مستجدة على الفكر القانوني مما دفع التشريعات الدولية و الإقليمية والوطنية إلى إصدار قوانين لتنظيم التوقيع الالكتروني ولإزالة الغموض عن هذا المصطلح الحديث حيث أوردت أحكاما بينت ماهيته.

وقد أدى اختلاف التقنية المستخدمة في تسجيل منظومة التوقيع الالكتروني إلى ظهور عدة اشكال مختلفة له، من ضمنها ما يعتمد على الارقام أو الأحرف أو الرموز أو الأصوات...، ومنها ما يعتمد على الخواص الطبيعية والفيزيائية لإنسان ولكل شكل من هذه الأشكال قوة ثبوتية تختلف عن الأخرى.

ولقد اعترفت كل التشريعات التي نظمت التوقيع الالكتروني بحجية هذا الأخير في الإثبات توازي الحجية المعترف بها للتوقيع التقليدي، شريطة ان ينشأ بواسطة وسائل خاصة بالشخص الموقع وخاضعة لسيطرته وحده دون سواه، وارتباطه ببيانات المحرر الالكتروني بطريقة يكشف بها عن اي تغيير لاحق لبيانات المحرر او للتوقيع ذاته، كما يتعين ان يعرف التوقيع الالكتروني بهوية صاحبه والتعبير عن رضائه بمحتوى المحرر الالكتروني، واخيرا ان يتميز بشكل فريد بارتباطه بالشخص صاحب العلاقة.

لكن ليس معنى ذلك ان التوقيع الالكتروني الذي لا يحقق هذه العناصر لا يتمتع بأية حجية، بل انه يتمتع بذات حجية التوقيع الالكتروني الذي يستجمع العناصر السابقة اذا استطاع ان يتمسك به لإقامة الدليل على كفاءة منظومة تشغيل هذا التوقيع ، كما انه يمكن للأطراف الاتفاق على تنظيم حجية التوقيع الالكتروني مالم يرد في هذا الاتفاق يخالف النظام العام.

الفصل الثاني

التصديق الإلكتروني

مع ظهور العقود الالكترونية المبرمة عبر الانترنت اصبح من الضروري التصديق الالكتروني على المعلومات المتواجدة بالعقد وتحديد اطراف العقد لسلامة وامن المعاملات والقيام بعملية التصديق الالكتروني والخدمات المتعلقة بما يستلزم وجود هيئات مختصة ذات كفاءة عملية وقانونية موثوق بها وطاقم بشري مؤهل نظرا للمهام المعقدة المنوطة بها وهذا ما يمنح الامان للمتأمل الالكتروني وقد اطلق المشرع الجزائري على هذه الهيئات مصطلح مؤدي خدمات التصديق الالكتروني الذي نظم مختلف مهامها والتزاماتها ومسؤولياتها وفقا للقانون 15_04 الذي يهدف وضع اطار قانوني قصد التكفل بالمتطلبات القانونية والتنظيمية والتقنية التي ستسمح بإرساء جو من الثقة المواتية

لتعميم وتطوير المبادلات الالكترونية بين كافة المستعملين لا سيما في مجال التجارة الالكترونية والتصديق الالكتروني هو مجموع الاجراءات التي تسمح بتسيير الشهادات الالكترونية واصدارها او ابطالها وتستعمل هذه الشهادات للتحقق من التوقيعات الالكترونية وتحديد الطابع الزمني الذي يسمح بمعرفة التوقيت الذي تمت فيها كل عملية وكذا التشفير (تشفير المعطيات) كما ان نشاط تخزين المعلومات يعزز عملية التصديق الالكتروني وهو عملية تضمن اربعة جوانب امنية لتبادل المعلومات على شبكة الانترنت وهي :السرية والتوثيق والنزاهة وعدم الاستنكار كون هذه الجوانب تسمح في ارساء مناخ ثقة عن طريق اقامة بنية ذات مفتاح عمومي مما يساعد على تحديد اصحاب المفاتيح عن طريق اصدار شهادات الكترونية .

وعليه سوف يتم توضيح المقصود بمقدم خدمات التصديق الالكتروني من حيث التشكيلة المؤسساتية والبشرية وهذا في **المبحث الاول** ومسؤولية مقدم خدمات التصديق الالكتروني في **المبحث الثاني** مع ابراز الاطار الوظيفي للتصديق الالكتروني في **المبحث الثالث** .

المبحث الأول: مقدم خدمات التصديق الالكتروني

لخلق مناخ ثقة وضع المشرع الجزائري مخطط ثقة وطني من شانه ضمان التكفل بمقتضيات الأمن والمراقبة والمبادلات بين الاطراف والمرونة في المعاملة لذلك اختارت الجزائر مخططا هيكليا يضم سلطة وطنية للتصديق الالكتروني وهيئتين تؤطران التصديق الالكتروني للفرعين الحكومي والاقتصادي .

وهذا ما سيتم تناوله في :

المطلب الأول: تشكيلة مقدم خمات التصديق الالكتروني .

المطلب الثاني: التزامات مقدم خدمات التصديق الالكتروني .

المطلب الأول: تشكيلة مقدم خدمات التصديق الالكتروني

بحسب ماورد في الباب الثالث من الفصل الثاني من قانون رقم04-15 يتمثل مقدم خدمات التصديق الإلكتروني في ثلاث سلطات هي السلطة الوطنية للتصديق الإلكتروني السلطة الحكومية والسلطة الإقتصادية علما أن لكل سلطة دورا ومسؤوليات خاصة بها تخضع لتنظيم قانوني خاص هدفه التنظيم والسير الحسن لهذا النشاط .

الفرع الأول : السلطة الوطنية للتصديق الالكتروني:

تتشكل السلطة من مجلس ومصالح تقنية وإدارية ومن خمسة أعضاء من بينهم رئيس الجمهورية على أساس كفاءتهم لاسيما في مجال العلوم التقنية المتعلقة بتكنولوجيا الإعلام والإتصال ويتمتع المجلس بجميع الصلاحيات اللازمة لأداء مهام السلطة بما يسمح به

القانون ومنه بإمكانه الإستعانة بأي كفاءة تساعده في أشغاله ،تحدد عهدة أعضاء مجلس السلطة بأربعة سنوات قابلة للتجديد مرة واحدة،يسير المصالح التقنية والإدارية للسلطة مدير عام يعينه رئيس الجمهورية بناء على إقتراح من الوزير الاول حيث يحدد تنظيم هذه المصالح ويسير مهامها عن طريق التنظيم ، حيث تقوم السلطة الوطنية التي هي تابعة للوزير الأول وتتخذ شكل سلطة إدارية مستقلة، بتحديد السياسة الوطنية للتصديق

الإلكتروني وهي مكلفة بترقية إستعمال التوقيع والتصديق الإلكترونيين وتطويرهما ، وكذا مراقبة وضمان صحة استعمالهما[1] ومن المهام التي وكلت لهذه الهيئة مايلي:

√إعداد سياستها للتصديق الإلكتروني والسهر على تطبيقها بعد الحصول على الرأي الإيجابي من قبل الهيئة المكلفة بالموافقة.

√الموافقة على سياسة التصديق الإلكتروني الصادرة عن السلطتين الحكومية والإقتصادية للتصديق الإلكتروني .

√إبرام إتفاقياتالإعتراف على المستوى الدولي.

√إقتراح مشاريع تمهيدية لنصوص تشريعية وتنظيمية تتعلق بالتوقيع أو التصديق الإلكترونيين على الوزير الأول .

√ القيام بعمليات التدقيق علىمستوى السلطتين الحكومية والإقتصادية للتصديق

الإلكتروني ،عن طريق الهيئة الحكومية المكلفة بالتدقيق ، كما أنه تتم إستشارة السلطة عند إعداد أي مشروع أو نص تشريعي أو تنظيمي ذي صلة بالتوقيع أو التصديق الإلكترونيين[1].

[1]زهيدة دردوري، التصديق الإلكتروني ، حوار لوكالة الأنباء الجزائرية،29 نوفمبر2014.

الفرع الثاني: السلطة الحكومية للتصديق الالكتروني

وهي تفرع للسلطة الوطنية التابعة لوزارة البريد وتكنولجيات الإعلام والإتصال ، تؤطر تسيير الشهادات المستعملة في المبادلات الإلكترونية بين الإدارات ، أي إلغاء الطابع المادي للمراسلات بين الوزارات و المؤسسات وبين الإدارات والمواطنين ، لاسيما من خلال سحب وثائق الحالة المدنية عن بعد وتشرف أطراف موثوقة أخرى على الشهادات الإلكترونية في الفرع الحكومي على أن تصادق عليها السلطة الحكومية[2]، وتنشأ لدى الوزير المكلف بالبريد و تكنولوجيا الإتصال والإعلام سلطة حكومية للتصديق الإلكتروني تتمتع بالاستقلال المالي والشخصية المعنوية،تكلف السلطة الحكومية للتصديق الإلكتروني بمتابعة ومراقبة نشاط التصديق الالكتروني للأطراف الثلاثة الموثوقة وكذلك توفير خدمات التصديق الإلكتروني لفائدة المتدخلين في الفرع الحكومي[3]

ومن المهام التي او كلها المشرع لهذه السلطة:

√إعداد سياستها للتصديق الإلكتروني وعرضها على السلطة للموافقة عليها والسهر على تطبيقها .

√الإحتفاظ بشهادات التصديق الإلكتروني منتهية الصلاحية والبيانات المرتبطة بمنحها

---

[1]المواد:(من المادة 16إلى المادة25) من القانون15-04 مؤرخ في 11 ربيع الثاني عام 1436 الموافق لأول فبراير 2015 ، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين.

[2]زهيدة دردوري، مرجع سابق.

[3]المواد:(من المادة 26 إلى المادة 28) من قانون 04-15 المتعلق بالتوقيع والتصديق الالكترونيين .

من قبل الطرف الثالث الموثوق بغرض تسليمها إلى السلطات القضائية المختصة عند الإقتضاء طبقا للاحكام التشريعية والتنظيميةالمعمول بها.

√إرسال كل المعلومات المتعلقة بنشاط التصديق الإلكتروني إلى السلطة الوطنية دوريا أو بناء على طلب منها.

√ القيام بعمليات التدقيق على مستوى الطرف الثالث الموثوق عن طريق الهيئة الحكومية المكلفة بالتدقيق طبقا لسياسة التصديق الإلكتروني .

الفرع الثالث :السلطة الإقتصادية للتصديق الالكتروني:

سلطة التصديق الإلكتروني تابعة لسلطة ضبط البريد والاتصالات وهي مكلفة بتسيير الشهادات المستعملة في المبادلات الالكترونية بين المؤسسات والاشخاص الطبيعية، كما تكلف السلطة الاقتصادية للتصديق الالكتروني بمتابعة ومراقبة مؤدي خدمات التوقيع و التصديقالالكترونيين لصالح الجمهور[1] .

ومن المهام التي اوكلها المشرع للسلطة الاقتصادية مايلي:

√ منح التراخيص لمؤدي خدمات التصديق الالكتروني بعد موافقة السلطة الوطنية.

√ الموافقة على سياسات التصديق الالكتروني الصادرة عن مؤدي خدمات التصديق الالكتروني والسهر على تطبيقها.

[1]زهيدة دردوري ،مرجع سابق.

√ السهر على وجود منافسة فعلية ونزيهة باتخاذ كل التدابير اللازمة لترقية او استعادة المنافسة بين مؤدي خدمات التصديق الالكتروني، من أجل تسليمها إلى السلطات القضائية عند الإقتضاء .

√ التحكيم في النزاعات القائمة يين مؤذي خدمات التصديق الإلكتروني فيما بينهم او مع المستعملين طبقا للتشريع المعمول به.

√ اصدار التقارير و الاحصائيات العمومية وكذا تقرير سنوي يتضمن وصف نشاطاتها مع احترام مبدأ السرية.

√ تقوم بتبليغ النيابة العامة بكل فعل ذي طابع جزائي يكتشف بمناسبة تأدية مهامها[1].

المطلب الثاني: التزامات مقدم خدمات التصديق الالكتروني:

نتيجة للدور الذي يقوم به مقدم خدمات التصديق الالكتروني ، وخطورة النتائج التي تترتب عليهوعمدت معظم التشريعات الى تحديد الالتزامات المترتبة عليه ، سواء كانت هذه الالتزامات في مواجهة صاحب الشهادة الذي يرتبط معها بعلاقة عقدية ام في مواجهة الغير الذي عول على الشهادة الصادرة عنها[2].

[1] المواد :(من المادة 29 إلى المادة 30) من قانون رقم 04-15 السالف الذكر.

[2] لينا ابراهيم يوسف حسان، التوثيق الالكتروني ومسؤولية الجهات المختصة به-دراسة مقارنة- ، دار الراية للنشر والتوزيع، الطبعة الاولى، سنة 2009، ص 106.

الفرع الاول: الالتزام بالتحقق من صحة البيانات:

يلتزم مقدم خدمات التصديق الالكتروني بالتحقق من صحة البيانات المقدمة من الأشخاص المصدر لهم شهادات التصديق وصفاتهم المميزة والتي تمت المصادقة عليها وتضمينها في الشهادة ، ويعتبر هذا الالتزام اكثر الالتزامات دقة ووجوبا للتحقق منه، بالنسبة لعمل مقدم خدمات التصديق الالكتروني وهو يحتاج الى طاقم وظيفي وفني وملائم ومتخصص لذوي الخبرة للتحقق من البيانات المقدمة وأهلية الشخص الصادرة له الشهادة[1]، بالنظر إلى خطورة هذا الإلتزام وما يترتب عليه من آثار سلبية على التجارة الإلكترونية في حالة الإخلال به، فإن مقدم خدمات التصديق الإلكتروني يلتزم بالتعويض في حالة تضمين بيانات غير صحيحة ، مادام المتعامل ليس لديه وسيلة من التيقن من صحة المعلومات والبيانات الواردة في شهادة المصادقة الالكترونية، ويتم ضمان الحصول على بيانات صحيحة ودقيقة الاتصال المباشر او عن طريق ارسال المستندات التي تثبت هوية المتعامل بالبريد او الحصول عليها عن طريق المتعامل شخصيا[2]،

تختلف هذه الالتزامات من حيث التصنيف:

أ- الالتزامات المتعلقة بمزاولة النشاط

تتمثل في الحصول على ترخيص مسبق بمزاولة النشاط المهني من الجهة المختصة ، قبل الشروع في عمل يدخل في حدود الترخيص ، كما يجب على مقدم خدمات التصديق

[1] زهيرة كيسي، النظام القانوني لجهات التوثيق (التصديق) الالكتروني ، دفتر السياسة والقانون ، المركز الجامعي ، تمنراست/ الجزائر ، العدد السابع جوان 2012 ،ص 132 .

[2] لينا ابراهيم، المرجع السابق، ص107 .

الالكتروني عدم التوقف عن مزاولة النشاط المرخص به من جهة اخرى ، أو التنازل عنه للغير إلا بعد الحصول على موافقة كتابية مت الجهة المختصة.

ب- الالتزامات المتعلقة بتفحص صحة البيانات

يلتزم مقرم خدمات التصديق الالكتروني بالتحقق من البيانات المقدمة ومدى صحتها من الاشخاص المصدر لهم شهادات تصديق، التي تم تضمينها في الشهادة ويعتبر هذا الالتزام اكثر الالتزامات دقة و مسؤولية بالنسبة لعمل مقدم خدمات التصديق الالكتروني، لذلك يجب توفر طاقم وظيفي وفني مختص للتحقق من اهلية الشخص الصادرة له الشهادة[1]، إن الإخلال بهذا الالتزام والتقصير في أداءه ينتج آثار سلبية و خسائر مادية تمس الطرف الضعيف، وهو المتعامل في هذه الحالة يلتزم مقدم خدمات التصديق الالكتروني تعويض المتعامل بحسب الضرر الذي ألحقه به نتيجة الاخلال بالالتزام الواجب احترامه[2]

ج-الالتزامات المتعلقة بتأمين وحماية المعلومات

تتمثل هذه الالتزامات في الضرورة التي تقع على عاتق مقدم خدمات التصديق الالكتروني في وضع متطلبات فنية وتقنية مؤمنة، تتفق مع حماية التوقيع الالكتروني وذلك بضرورة توافر التجهيزات المادية من اجهزة و عاملين مختصين بها، وفق منظومة متكاملة إلى جانب ان مقدم خدمات التصديق الالكتروني يجب ان تتوفر لديه ترخيص بإصدار

[1] زهيرة كيسي، مرجع سابق ص 133 .

[2] لينا ابراهيم، مرجع سابق ، ص 107 .

شهادات التصديق الالكتروني ، وانظمة خاصة بتأمين المعلومات وحماية البيانات و تنظيم خاص بإصدارالشهادات و إدارة المفاتيح وفقا لمعايير فنية و تقنية[1].

الفرع الثاني: الالتزام بإصدار شهادة التصديق الالكتروني

ان شهادة التصديق الالكتروني هي عبارة عن رسالة الكترونية تسلم من شخص ثالث موثوق، وتكون لها وظيفة الربط بين شخصين طبيعي أو معنوي وزوج المفاتيح (الخاص والعام)، وتحتوي الشهادة على معلومات عن المتعامل مثل الاسم، العنوان، الأهلية وعناصر تعريفية أخرى وكذلك الممثل القانوني بالنسبة للشخص المعنوي، اسم مصدر الشهادة تاريخ استلام و الشهادة وغيرها من المعلومات الضرورية والواجب توافرها ، ذلك لضمان الأمان كون المتعاملين غايتهم من اللجوء إلى مقدم خدمات التصديق الالكتروني إنما لإسباغ طابع الثقة و الأمان و السرية على رسائلهم وتوقيعاتهم الالكترونية ، وحفظ مصالحهم الخاصة و تكون هذه الشهادة بمثابة هويات في مواجهة من يرغب في التعاقد معهم[2].

إن هذا الالتزام يتمثل في الالتزام بتحقيق نتيجة، والتي هي صدور شهادة تصديق الكترونية مستوفية كامل البيانات الأساسية ، أما في حال إذا كانت شهادة التصديق الالكترونية تخل بأحد الشروط التي يجب توافرها بالشهادة فعلى مقدم خدمات التصديق الالكتروني إلغاء هذه الشهادة، أو تعليق العمل بها في حال توفر سبب يوجب ذلك بناء على صاحب الشهادة أو من تلقاء نفسها ومثال ذلك:

[1] لزهر سعيد، النظام القانوني لعقود التجارة الالكترونية، دار هومة ، الجزائر، 2012، ص178 –179 .

[2] لينا ابراهيم يوسف حسان، مرجع سابق، ص112 .

√ أن تكون الشهادة سلمت بناء على معلومات مغلوطة أو مزيفة، والمقصود منها أن المعلومات تكون صحيحة، وتخص ذات الشخص آخر نتيجة لذلك يتعرض صاحب الشهادة المزيفة إلى المسائلة المدنية و الجزائية.

√ أن تستعمل الشهادة لغرض التدليس وذلك بأن تصدر الشهادة صحيحة وتستعمل من قبل صاحبها لكن استعمالها غير مشروع[1].

الفرع الثالث: الإلتزام بالسرية

من أخطر الإلتزامات الملقاة على عاتق مقدم خدمات التصديق الالكتروني هو الالتزام بالسرية، حيث لا يحصل على المعلومات الشخصية الا الشخص نفسه أو برضائه الصريح، حيث لاتعد بيانات إنشاء التوقيع الالكتروني والمعلومات التي تقدم إلى مزود خدمات التصديق الالكتروني سرية، ولا. يجوز لمن قدمت إليه أو اتصل بها بحكم عمله إفشائها للغير أو استخدامها في غيرالغرض الذي قدمت من اجله.

إلا أن مسؤولية مقدم خدمات التصديق الالكتروني تنتفي في حال إذا رخص صاحب الشهادة كتابياأو الكترونيا في نشرها أو الإعلام عنها، أو في حال صدور حكم قضائي يجيز نشر تلك البيانات أو الإعلام عنها، أو في حال صدور حكم قضائي يجيز نشر تلك البيانات أو الإعلام عنها[2].

وقد ألزم المشرع الأوروبي مقدم خدمات التصديق الالكتروني الحفاظ على البيانات ذات الطابع الشخصي بحيث لا يحصل عليها إلا الشخص نفسه أو برضائه الصريح، ومتى

[1] زهيرة كيسي ، مرجع سابق ، ص 217-216 .

[2] لينا ابراهيم يوسف حسان، مرجع سابق، ص114 .

كانت هذه البيانات ضرورية لإصدار الشهادة كما ألزم المشرع التونسي والمصري مقدم خدمات التصديق الالكتروني وأعوانهم الحفاظ على سرية المعلومات التي عهد بها اليهم في إطار تعاطي أنشطتهم بإستثناء تلك التي رخص صاحب الشهادة كتابيا أو الكترونيا في ان الاعلام عنها أو في الحالات المنصوص عليها في التشريع[1].

ومن هنا نجد بأن مختلف التشريعات أكدت على الحرص الشديد في الحفاظ على سرية المعاملات الالكترونية .

[1]زهيرة كيسي، مرجع سابق، ص 216 .

المبحث الثاني: مسؤولية مقدم خدمات التصديق الالكتروني

المسؤولية عموما تمثل جزاء على مخالفة الشخص أحد الواجبات الملقاة على عاتقه والتي تكون بدورها واجبات مصدرها القانون، فالواجبات القانونية كثيرة يترتب عليها عدة جزاءات بحسب الواجب الذي حدث الإخلال بشأنه ، إن مقدم خدمات التصديق الالكتروني عند إصداره لشهادة التصديق الالكترونية يعمل على تأكيد سلامة وصحة البيانات والمعلومات الواردة بهذه الشهادة إضافة إلى تأكيدها لصحة وقانونية التوقيع الالكتروني.[1]

وكما هو ثابت فإن المسؤولية عن الأضرار التي تحدث بصفة عامة هيأحدالموضوعات القانونية ذات الأهمية الخاصة التي تتعرض لها الانظمة القانونية، وتضع لها قواعد عامة تحكمها، وإلى جانبها تنبهت بعض التشريعات إلى الاهمية المترتبة على تنظيم مسؤولية هذه الجهات، فأفردت لها نصوص خاصة وذلك لعدم كفاية القواعد العامة لتنظيمها ، في حين أغفلت بعض التشريعات الأخرى ذلك التنظيم.

وهذا ما سيتم تناوله من خلال مسؤولية مقدم التصديق الالكتروني وفقا للقواعد العامة في **المطلب الأول** وكذا مسؤولية مقدم التصديق الالكتروني وفقا للقواعد الخاصة في **المطلب الثاني.**

المطلب الأول : مسؤولية مقدم خدمات التصديق الالكتروني وفقا للقواعد العامة

خلافا للتنظيم الذي حظيت به مسؤولية مقدم خدمات التصديق الالكتروني في بعض التشريعات وضعت نصوص خاصة لتنظيم مسؤولية جهات التصديق ، أمام سكوت هذه

[1] أمجد محمد منصور ، النظرية العامة للالتزام مصادر الالتزام، الطبعة الاولى، دار الثقافة، عمان–الاردن 2007 ص 244

التشريعات عن وضع قواعد خاصة لمسؤولية مقدم خدمات التصديق الالكتروني في تعويض الضرر الناتج عن إهمالها وإخلالها بالالتزامات للقواعد العامة للمسؤولية المدنية، وبالرجوع إلى طبيعة النشاط المسند لمقدم خدمات التصديق الالكتروني نجد أنه يطبق بشأنها إحكام المسؤوليتين العقدية والتقصيرية متى توافرت أركانهما و شروطهما بموجب علاقتهما بصاحب الشهادة ونظرا لوجود رابطة عقدية بينهما ، تتمثل في العقد المبرم والذي يرتب التزامات متبادلة في مواجهة كل من الطرفين، فان هذه العلاقة تخضع لأحكام المسؤولية العقدية أما في علاقتهما مع الغير الذي عول على الشهادة الصادرة عنها، ونظرا لعدم وجود رابطة عقدية بينهما فإنها تخضع لأحكام المسؤولية التقصيرية ، فالمسؤولية العقدية تقابل المسؤولية التقصيرية فالأولى جزاء عدم الوفاء بالالتزامات والثانية نتيجة للعمل غير المشروع.

الفرع الأول: المسؤولية العقدية لمقدم خدمات التصديق الالكتروني

من الطبيعي أن المسؤولية العقدية تنهض لوقوع الاخلال بالالتزام العقدي ، وطبيعي أن يستوجب هذا أولا وجود عقد صحيح لم يلتزم أحد الطرفين بتنفيذ التزامه المتعلق به، والعقد الصحيح كما عرفه المشرع الجزائري بالمادة 54 من القانون المدني وهو:" اتفاق يلتزم بموجبه شخص أو عدة أشخاص نحو شخص أو عدة أشخاص آخرين بمنح أو فعل أو عدم فعل شيء ما ، يترتب على العقد إنشاء التزامات تقع على كاهل كل من طرفيه والقوة الملزمة للعقد تقضي بأن يقوم كل طرف بتنفيذ التزامه العقدي"[1]، فالمسؤولية العقدية هي جزاء لعدم قيام المتاعقد بتفيذ التزامه ، أو تأخره في هذا التنفيذ وهي تؤدي إلى

[1] لينا ابراهيم يوسف حسان ، مرجع سابق، ص158

تعويض المتعاقد لما أصابه من ضرر بسبب عدم تنفيذ العقد[1]، وتفترض المسؤولية العقدية وجود عقد صحيح واجب التنفيذ تقوم هذه المسؤولية عند عدم الوفاء بالالتزام المفروض، مما يلحق الضرر بالمتعامل وتقوم المسؤولية عند قيام الأركان الثلاث والمتمثلة:

أولا: ركن الخطأ العقدي

يتحقق الخطأ العقدي لجهة التصديق الالكتروني في حالة الاخلال بأي الالتزامات الملقاة على عاتقها ، بموجب عقد التصديق وهو ما يعرف بالركن المادي والمتمثل فيمايلي:

√ الإهمال في حماية البيانات الخاصة بالتوقيع الالكتروني من خلال تركها في أيدي العابثين.

√عدم التحقق من صحة البيانات أي عدم الالتزام ببذل عناية فيتحقق الخطأ العقدي بعدم بذل العناية اللازمة و الكافية من جانب مقدم خدمات التصديق الالكتروني.

√ عدم الالتزام بتحقيق النتيجة المرجوة مثال كالالتزام بالسرية في حال غياب ذلك يتحقق الخطأ العقدي بعدم تحقيق النتيجة ، أو الغاية المطلوبة ويصبح مقدم خدمات التصديق الالكتروني مجبر على التعويض بقوة القانون[2].

إن المسؤولية العقدية لمقدم خدمة التصديق الالكتروني تجاه الغير لمتضرر من تعويله على الشهادة ، لا تقوم إلا إذا كان هناك عقد يربط الغير المتضرر مع جهة التصديق ، حيث تضمن هذه الجهة بموجب العقد صحة المعلومات التي تتضمنها شهادة التصديق

[1] محمد صبري السعدي، الواضح في شرح القانون المدني، الطبعة الرابعة ، دار الهدى، عين مليلة– الجزائر،2009، ص 310، 311

[2] زهيدة كيسي، مرجع سابق، ص 224 .

الالكتروني ، وفي حالة ثبوت تقصير أي طرف من أطراف التعاقد بهذه الالتزامات ، وتنتج عنه ضرر أصاب الطرف الآخر فإن المسؤولية العقدية هي التي تطبق هنا عند توافر باقي أركانها[1].

ثانيا: ركن الضرر

يعد الضرر الركن الأساسي في قيام المسؤولية المدنية ، فهو السبيل نحو المساءلة المدنية فلا مسؤولية عند انتفاء الضرر لتختلف هذا الركن الجوهري، ويقع عبء إثبات الضرر من يدعيه، والضرر بوجه عام هو الأذى أو التعدي قد ينشأ عن الاخلال بالتزام يفرضه القانون[2].

حتى تقوم مسؤولية مقدم خدمات التصديق الالكتروني ، لا يكفي أن يكون هناك خطأ عقدي فقط ، وإنما يجب أن يكون هناك ضرر لحق بصاحب الشهادة جراء هذا الخطأ ، فإذا توافر سبب موجب لتعليق العمل بشهادة التصديق، أو إلغائها ولم يقم مقدم التصديق الالكتروني بهذينالاجرائين، تكون قد اخلت بالتزام مفروض عليها إذا لحق ضرر بصاحب الشهادة نتيجة لهذا الاهمال، وتتم مساءلة مقدم خدمات التصديق الالكتروني المسؤول عن ذلك ويلتزم بالتعويض للمضرور وفقا لأحكام المسؤولية العقدية، فإذا فقد صاحب الشهادة مفتاحه الخاص وطلب من جهة التصديق إلغاء العمل بشهادة التصديق ولم يستجب لطلبه ، وترتب عن ذلك استعمال الغير لهذا المفتاح في فعل غير مشروع باسم صاحب

[1] آلاء احمد محمد حاج علي، أطروحة استكمال متطلبات الحصول على درجة الماجستير ، قانون خاص، التنظيم القانوني للتصديق الالكتروني على التوقيع الالكتروني، جامعة النجاح الوطنية كلية الدراسات العليا ، فلسطين ، 2013 ، ص 76 .

[2] منذر الفضل، النظرية العامة للالتزامات، الجزء الأول ، دار الثقافة ، عمان ، الأردن،1996، ص 299 ،300 .

المفتاح دون ترخيص منه او علم به فهنا كنتيجة حتمية تقوم المسؤولية العقدية في مساءلة مقدم خدمات التصديق الالكتروني لتعويض صاحب الشهادة عن الضرر الذي لحق به[1].

وقد عالج المشرع الجزائري هذه الحالة بنص المادة 124 من القانون المدني:" كل فعل أيا كان يرتكبه الشخص بخطئه ويسبب ضررا للغير يلزم من كان سببا في حدوثه بالتعويض"[2]، نستنتج من نص المادة أن التعويض يرتبط بتحقق الضرر متى تحقق الضرر هذا الأخير يلتزم مسبب الضرر الذي هو مقدم خدمات التصديق الالكتروني بالتعريض بقدر حجم الضرر، أما في حالة العكس إذا أثبت مقدم خدمات التصديق الالكتروني أن الضرر خارج عن التزاماته ولا يجيز مسائلته به لحق يفرضه القانون ، فلا ضرورة لها بالتعويض وهو ما تضمنه المادة 127 من القانون المدني " إذا اثبت الشخص ن الضرر قد نشأ عن سبب لايد له كحادث مفاجئ ، أو قوة قاهرة ، أو خطأ صدر من المضرور ...كان غير ملزم بتعويض هذا الضرر"، ومنه نستنتج أنه لا يتحقق الضرر حتى تقوم المسؤولية العقدية لمقزم خدمات التصديق الالكتروني وانما على المضرور اي صاحب شهادة التصديق إثبات أن الضرر نتيجة لإهمال هذا الأخير وإخلاله بالتزاماته.

ثالثا: علاقة السببية بين الخطأ والضرر

ان علاقة السببية هي الركن الثالث لقيام المسؤولية العقدية ، فإذا انتفت علاقة السببية انقطعت وانتفت معها المسؤولية، ولا يخرج هذا الضرر من حيث المبدأ عما قررته القواعد العامة في المسؤولية المدنية في مجال الضرر.

[1] لينا إبراهيم يوسف حسان، مرجع سابق، ص 160 -161 .

[2] قانون رقم 05-07 المؤرخ في 13 مايو 2007 من القانون المدني.

العلاقة السببية هي تلك الصلة التي تربط الضرر بالخطأ، فتجعل الضرر نتيجة للخطأ فإذا انعدمت انتفت المسؤولية لانعدام ركن من أركانها ، وتنتفي رابطة السببية عموما إذا تدخل سبب اجنبي ليفصل بين الضرر الذي أصاب صاحب الشهادة ، وبين الخطأ الذي صدر من مقدم خدمات التصديق الالكتروني[1].

فالضرر الذي يصيب صاحب الشهادة، يجب ان يكون سببه الخطأ الذي ارتكبه مقدم خدمات التصديق الالكتروني ، والمتمثل باخلاله بالتزاماته العقدية كان يصدر شهادة تصديق معينة مما يؤدي إلى تفويت الصفقة على صاحب الشهادة ومنه تعرضه إلى خسارة مادية واجبة التعويض من الجهة المسؤولة [2].

كما أن الضرر الناتج عن خطأ ارتكبه مقدم خدمات التصديق الالكتروني يجب أن يكون ضررا مباشر ينحصر داخل الالتزامات التي تقع على عاتق مقدم خدمات التصديق الالكتروني ، كالالتزام ببذل عناية، مثل التحقق من صحة البيانات والمعلومات الشخصية والحفاظ على سرية المعلومات التي مكنت منها ، لأنه المبدأ الأساسي الذي يعطيها مصداقية العمل في مجال التصديق الالكتروني والغاية المرجوة من المتعاملين ، كذلك الالتزام بتحقيق نتيجة والتي تتمثل في اصدار شهادة التصديق مراعية للغاية التي صدرت من اجلها مستوفية لجميع الشروط اللازمة لإصدارها وتكون حجية للمتمسك بحجيتها بما يخدم صالحها[3].

---

[1] دريد محمود علي، النظرية العامة للالتزام، الطبعة الاولى، منشورات الحلبي الحقوقية ، بيروت– لبنان، 2012، ص 301 .

[2] زهيرة كيسي، مرجع سابق، ص 244 .

[3] آلاء محمد حاج علي، مرجع سابق، ص81 .

الفرع الثاني: المسؤولية التقصيرية لمقدم خدمات التصديق الالكتروني

تقوم المسؤولية التقصيرية على الاخلال بالتزام قانوني واحد لا يتغير ، هو الالتزام بعدم الأضرار بالغير ولا ترتبط جهة التصديق مع الغير المتضرر بأي عقد رسمي، قد لاتكون مسؤولية مقدم خدمات التصديق الالكتروني عقدية، وهذا بالطبع عند عدم وجود علاقة عقدية بين مركز التصديق وأولئك المتضررين من طرف آخر، ويعتبر من الغير كل شخص لا تربطه اية علاقة عقدية مع مركز التصديق ، ويشترط لقيام المسؤولية التقصيرية أن يكون الفعل من قبيل الخطأ حيث نصت المادة 124 من القانون المدني:" أن كل فعل يرتكبها لشخص بخطئه ويسبب ضررا للغير يلزم من كان سببا في حدوثه بالتعويض" [1].والمسؤولية التقصيرية بصفة عامة ثلاثة أركان هي:

أولا: ركن الخطأ

إن أي اهمال أو تقصير يسجل على مستوى مقدم خدمات التصديق الالكتروني يخل بالتزاماته من شأنه أن يقيم مسؤولية المركز وفقا لأحكام المسؤولية المدنية التقصيرية، متى توفر الثالوث الشهير الخطأ، الضرر، العلاقة السببية بينهما، إن قيام مسؤولية هذا الأخير يتطلب توافر أركان هذه المسؤولية، أولهما وأهمها الخطأ التقصيري ، أي الاخلال بالالتزام القانوني العام المتمثل في احترام حقوق الاخرين وعدم الاضرار بهم، وهذا الالتزام هو الالتزام ببذل عناية فان الاخلال به يشكل خطأ يوجب المسؤولية ويقوم الاخلال به إذا لم يبذل مقدم خدمات التصديق الالكتروني العناية اللازمة من الحيطة والتبصر ، وهو ما يجب على الغير المتضرر اثباته واقامة البينة عليه وذلك بإقامة الدليل على ان مقدم خدمات التصديق الالكتروني لم يبذل العناية اللازمة المعتادة ، ولاشك أن ذلك ليس بعمل يسير على الغير المتضرر من سلوكه ، لأنه اذا اثبت هذا الأخير أنه قام بالعناية

[1] قانون رقم 05-07 السالف الذكر .

المعتادة والمطلوبة منه، يسقط حق المضرور في مسائلة جهة التصديق وبالتالي يسقط حقه بالتعويض.

إن الخطأ في المسؤولية التقصيرية، هو اخلال بالتزام قانوني سابق يصدر عن تمييز وادراك، يتمثل الالتزام القانوني الذي يعتبر الاخلال به خطأ يبرر المسؤولية التقصيرية، في ضرورة أن يصطنع الشخص في سلوكه قدرا من اليقظة والتبصر حتى لا يضر بالغير فإذا انحرف عن السلوك الواجب، وكان من القدرة على التمييز بحيث يدرك انه قد انحرف فان انحرافه هذا يعد خطأ يستوجب المسؤولية التقصيرية[1].

ثانيا: ركن الضرر

الضرر هو الركن الثاني المسؤولية التقصيرية، لا يكفي لتحقق هذه المسؤولية أن يقع الخطأ بل يجب أن يحدث ضرر نتيجة للخطأ، والمضرور هو الذي يثبت وقوع الضرر به ويجوز إثبات الضرر بأي وسيلة ممكنة، كونه واقعة مادية.

والضرر نوعان ضرر مادي ، وضرر أدبي:

– الضرر المادي هو اخلال بمصلحة المضرور ذات القيمة.المالية ويجب أن يكون هذا الاخلال محققا ولا يكفي أن يكون محتمل الحدوث.

– الضرر الأدبي هو الضرر الذي لا يصيب الشخص في ماله وإنما يصيب مصلحة غير مالية والضرر الأدبي قابل للتعويض بالمال[2].

[1] دريد محمود علي، النظرية العامة للالتزام، مرجع سابق، ص398 –399

[2] عبد الرزاق أحمد السنهوري ، الوسيط في شرح القانون المدني الجديد، المجلد الثاني ، الطبعة الثالثة، منشورات الحلبي الحقوقي ، بيروت– لبنان، 1998، ص984 –982 .

ثالثا: ركن العلاقة السببية

لقيام علاقة السببية بين الضرر والخطأ ، يجب أن يكون الخطأ هو السبب في حصول الأذى للمتضرر، فإذا لم يتحقق هذا الشرط لا تقوم المسؤولية التقصيرية لإنتفاء هذه الرابطة ، فإذا تدخلت عوامل أخرى قطعت ارتباط الضرر والخطأ،فلا تتحقق هذه السببية لأن النتيجة ليست مرتبطة بالسبب ارتباطا طبيعيا[1].

العلاقة السببية هي الركن الثالث للمسؤولية التقصيرية، تتمثل في العلاقة السببية بين الخطأ والفعل الضار والضرر بأن يكون الفعل هو السبب في حدوث الضرر فإذا انتفت علاقة السببية لأي سبب لابد للمدين فيه فلا تقوم المسؤولية التقصيرية[2].

المطلب الثاني: مسؤولية مقدم خدمات التصديق الالكتروني وفقا للقواعد الخاصة

تنبهت بعض التشريعات المنظمة لعمل مقدم خدمات التصديق الالكتروني ، للأهمية المترتبة على تنظيم مسؤولياته في حال إخلاله بالالتزامات المترتبة عليه، فأفردت له نصوصا قانونية خاصة نظمت فيها الحالات التي تنعقد بها مسؤولية هذه الجهات وكذلك إعفائها من المسؤولية وجواز تقييدها، تمثلت هذه التشريعات بكل من التوجيه الأوروبي بشأن التوقيعات الإلكترونية لسنة 1999 ،وقد سلك المشرع الجزائري ذات المنهج.

[1] منذر الفضل ، النظرية العامة للالتزامات، الجزء الاول، مكتبة الثقافة للنشر والتوزيع، ص 449 .

[2] لينا ابراهيم يوسف حسان، مرجع سابق، ص 166 .

الفرع الأول: مسؤولية مقدم خدمات التصديق الالكتروني وفقا للتوجيه الأوروبي بشأن التوقيعات الالكترونية لسنة1999

من أهم المزايا التي يتمتع بها التوجيه الاوروبي بشأن التوقيعات الالكترونية لسنة 1999 تنظيمية لمسؤولية مقدم خدمات التصديق الالكتروني بنصوص خاص، يمكن القول أن تنظيم مسؤولية هذا الاخير تقوم على قاعدتين اساسيتين، أولا المسؤولية المفترضة لمقدم خدمات التصديق الالكتروني، ثانيا جواز تحديد نطاق صلاحية شهادة التصديق الالكتروني[1].

أولا: المسؤولية المفترضة لمقدم خدمات التصديق الالكتروني

وفقا للتشريع الأوروبي فان المكلف بخدمة التصديق الذي يصدر شهادة معتمدة أو الذي يضمن يضمن حصوله على مثل هذه الشهادة ، يكون مسؤولا عن الضرر الذي يتعرض له الشخص الطبيعي أو المعنوي الذي اعتمد على هذه الشهادة فيما يتعلق بالحالات التالية[2]:

1 – ضمان صحة كافة البيانات المتضمنة في الشهادة المعتمدة من التاريخ الذي تم اصدارها فيه، واشتمالها على كافة البيانات المقررة بخصوص شهادة معتمدة.

2 – التحقق خلال لحظة اصدار الشهادة من صاحب التوقيع المحدد الهوية في الشهادة المعتمدة حاز على البيانات الخاصة بإنشاء التوقيع المطابق للبيانات الخاصة بفحص التوقيعات المقدمة أو المحددة في الشهادة.

[1] المواد(1 –2 /5) من التوجيه الاوروربي بشأن التوقيعات الالكترونية لسنة 1999.

[2] لينا ابراهيم يوسف حسان ، مرجع سابق، ص 136 –137

إلا ان التوجيه الأوروبي لم يشر إلى مسؤولية مقدم خدمات التصديق الالكتروني في حالة عدم تعليقها العمل بالشهادة أو الغائها اذا توفر سبب يدعو إلى ذلك ، كما انه لم يشر الى مسؤولية مقدم خدمات التصديق الالكتروني في حال إفشائه الاسرار الخاصة بالعملاء، وتتحقق مسؤولية هذا الاخير سواء كان الشخص الذي اعتمد على الشهادة تربطه علاقة تعاقدية معه" صاحب الشهادة" أم لم تربطه معه أي علاقة " الغير.

ثانيا: جواز تحديد نطاق صلاحية شهادة التصديق الالكتروني

لقد أقر المشرع الأوروبي الحق لمقدم خدمات التصديق الالكتروني بتحديد نطاق صلاحية شهادة التصديق الالكتروني ، بحيث إذا تجاوز هذا النطاق لا يمكن مساءلة مقدم خدمات التصديق الالكتروني عن هذا التجاوز بأي شكل من الأشكال ، لأنه في هذه الحالة يكون صاحب الشهادة قد استخدم الشهادة بصورة تعسفية في حال تجاوز النطاق المحدد لسريان الشهادة ، لا يكون مقدم خدمة التصديق الالكتروني مسؤولا عن الضرر الناتج عن هذا الفعل[1].

الفرع الثاني: مسؤولية مقدم خدمات التصديق الالكتروني وفقا للقانون 04-15

يكون مقدم خدمات التصديق الالكتروني الذي سلم شهادة التصديق الالكتروني الموصوفة مسؤولا عن الضرر الذي يلحق بأي هيئة أو شخص طبيعي كان أو معنوي اعتمد على هذه الشهادة تذلك من خلال:

1 – التأكد من صحة المعلومات الواردة في شهادة التصديق الالكتروني الموصوفة ضمن الشهادة .

[1] لينا ابراهيم يوسف حسان، مرجع سابق، ص 134 -140

2 – التأكد عند منح شهادة التوقيع أن الموقع الذي تم تحديد هويته في شهادة التصديق يحوز كل بيانات إنشاء التوقيع الموافقة لبيانات التحقق من التوقيع المقدم، والمحدد في شهادة التصديق الالكتروني.

3 – التأكد من امكانية استعمال البيانات الموجودة بشهادة التصديق الالكتروني والتحقق منها بدقة.

4 – يكون مقدم خدمات التصديق الالكتروني مسؤولا عن الضرر الناتج عن عدم إلغاء شهادة التصديق الالكتروني هذه والذي يلحق بكل شخص طبيعي أو معنوي اعتمدوا على تلك الشهادة إلا إذا قدم مقدم خدمات التصديق الالكتروني ما يثبت انه لم يرتكب أي إهمال

5 – يمكن لمقدم خدمات التصديق الالكتروني أن يشير في شهادة التصديق الالكترونية إلى الحدود المفروضة على استعمالها بشرط أن تكون الإشارة واضحة و مفهومة من طرف الغير، في هذه الحالة لا يكون مسؤولا عن الضرر الناتج لاستعمالها عند تجاوز الحدود المفروضة على استعمالها.

6 – يمكن لمقدم خدمات التصديق الالكتروني أن يشير في الشهادة إلى الحد الأقصى لقيمة المعاملات التي يمكن أن تستعمل في حدودها شهادة التصديق الالكترونية شريطة أن تكون واضحة و مفهومة للمتلقي، وفي هذه الحالة لا يكون مقدم خدمات التصديق الالكتروني مسؤولا عن الضرر الناتج عن تجاوز ذلك الحد الأقصى.

7 – يجب على مقدم خدمات التصديق الالكتروني إعلام السلطة الاقتصادية للتصديق الالكتروني برغبته في وقف نشاطه المتعلق بتأدية خدمات التصديق الالكتروني أو بأي فعل يؤدي إلى ذلك.

8 – يجب على مقدم خدمات التصديق الالكتروني الذي يوقف نشاطه لأسباب خارجة عن إرادته أن يعلم السلطة الاقتصادية للتصديق الالكتروني بذلك فورا ، كما تقوم هذه الأخيرة بإلغاء شهادته للتصديق الالكتروني بعد تقديره لأسباب المقدمة، في هذه الحالة يتخذ مؤدي الخدمات التدابير اللازمة من اجل حفظ المعلومات المرتبطة بشهادة التصديق الالكتروني الممنوحة[1].

على الرغم مما نظمته تشريعات الدول المختلفة من التزامات تقع على عاتق جهات التوثيق الالكتروني ، ومما يترتب عليه من مسؤولية عن اخلالها بالتزاماته.

الا انني ارى انه من واجب الأطراف التي تعول على شهادات التصديق الالكترونية ان تبذل عناية معقولة للتحقق من صلاحية الشهادة، وفيما اذا كان العمل بها موقوفا او ما اذا كانت ملغاة ، او فيما لو وجد اي قيد على استعمالها ، فكما نلاحظ فقد اجمعت التشريعات المدروسة على ان جهات التصديق الالكتروني تلتزم ببذل عناية وتحقيق نتيجة، فيما يخص بذل العناية تتمثل في التحقق من البيانات وحفظها فإذا اخلت بهذا الالتزام تقوم عليها مسؤولية قد تكون عقدية وقد تكون تقصيرية يتحدد نوعها بحسب من تعرض للاخلال بالالتزام في حقه أكان المتعاقد او الغير اما فيما الالتزام بتحقيق نتيجة هو التزام مقدم خدمات التصديق الالكتروني بسرية المعطيات والبيانات الشخصية الى جانب إصدار شهادة تصديق موافية للشروط التنظيمية المفروضة على مقدم خدمات التصديق الالكتروني .

[1] المواد(من المادة 53 إلى المادة 60) من قانون رقم 15 – 04 السالف الذكر.

المبحث الثالث: الإطار الوظيفي للتصديق الالكتروني

عرف المشرع الجزائري مؤدي خدمات التصديق الالكتروني على أنه: " كل شخص طبيعي أو معنوي يقوم بمنح شهادات التصديق الالكتروني موصوفة وقد يقدم خدمات في مجال التصديق الالكتروني "[1]، بالتالي فالدور أو الإلتزام الأساسي لمقدم خدمات التصديق الالكتروني ، هو اصدار شهادات التصديق الالكتروني وهذه الأخيرة لها دور فعال في تحقيق عنصري الأمان والثقة وعدم قابليتها للتعدي وصلاحية التوقيع الالكتروني[2]، إن شهادة التصديق هي رسالة الكترونية، تسلم من شخص ثالث موثوق ، وتكون لها وظيفة الربط بين شخص طبيعي أو معنوي وزوج من المفاتيح الخاص والعام، وتسمح بتحديد حائز المفتاح العام المذكور فيها، وتحتوي الشهادة على معلومات عن المتعامل اسمه، عنوانه، اهليته، عناصر تعريفية اخرى، والممثل القانوني بالنسبة للشخص المعنوي، واسم مصدر الشهادة والمفتاح العمومي للمتعامل، والرقم التسلسلي ، وتاريخ تسليم الشهادة وتاريخ انتهاء صلاحيتها[3].

وهو ما سيتم تناوله في مطلبين حيث خصصنا **المطلب الاول** بدراسة شهادة التصديق الالكتروني اما **المطلب الثاني** سيخصص لدراسة انواع شهادة التصديق الالكتروني .

---

[1] المادة12 من القانون رقم15 – 04 السالف الذكر.

[2] لينا ابراهيم يوسف حسان ، مرجع سابق، ص 60 .

[3] زيد حمزة مقدم، (النظام القانوني للتوثيق الالكتروني)، مجلة الشريعة والقانون والدراسات الإسلامية، العدد 24 ،شوال 1435 هـ-2014 م، ص 138.

المطلب الأول: شهادة التصديق الالكتروني

نظرا لخطورة وأهمية الدور الذي تلعبه شهادات التصديق الالكتروني في اثبات هوية مرسل الرسالة الالكترونية عن طريق ربطه بمفتاحه العام ،بما يحقق عنصري الثقة والأمان بالمعاملات الالكترونية وبما يحقق من ضمان عدم انكار أحد الطرفين توقيع الوثيقة المرسلة الكترونيا، ودلالة على صحة أن الموقع يملك المفتاح الخاص، وبالتالي فهو الذي قام بالتوقيع، قد اختلفت التشريعات في وضع التعاريف حول شهادة التصديق الالكتروني والتي سنوضحها فيما يلي:

تقوم شهادة التصديق الالكتروني بدور فعال في مجال المعاملات الالكترونية ً فمن شأنها التأكد من شخصية المرسل ومن سلامة وصحة البيانات المدونة بالمحرر، وعدم قابليتها للتعديل، وهو من شأنه أن يرسخ الثقة والأمان لدى المتعاملين عبر الانترنيت وقد اختلفت تعريفاتها باختلاف التشريعات ، فقد عرفها **المشرع الجزائري** وفقا للمادة 07 من القانون 15 -04 على انها :" وثيقة في شكل الكتروني تثبت الصلة بين بيانات التحقق من التوقيع الالكتروني والموقع[1]"، والملاحظ ان المشرع الجزائري أسند تعريف شهادة التصديق الالكتروني إلى وظيفتها ولم يربطه بالجهة المصدرة لهذه الشهادة.

كما عرفها **قواعد الأنسترال** بشأن التوقيعات الالكترونية بأنها:" رسالة بيانات أو سجلا آخر يؤكدان الارتباط بين الموقع وبيانات إنشاء التوقيع "،هذا ما يجعل قواعد الاونسترال بشأن التوقيعات الالكترونية قد عرفت الشهادة على انها سجل الكتروني يتضمن مفتاحا عموميا الى جانب اسم المشترك في الشهادة باعتباره موضوع الشهادة ، يؤكد ان الموقع المحدد هويته في الشهادة يحمل المفتاح الخصوصي للمناظر.

[1] المادة 07 من القانون رقم15 -04 السالف الذكر .

وعرفها **المشرع المصري** في المادة الأولى من فانون التوقيع الالكتروني بأنها:" الشهادة التي تصدر من الجهة المرخص لها بالتصديق ، وتثبت الارتباط بين الموقع ومن انشاء الشهادة"، وكذلك عرفتها المادة 02 من قانون المعاملات والتجارة الالكترونية لإمارة دبي أنها شهادة يصدرها مقدم خدمات التصديق الالكتروني يفيد فيها هوية الشخص او الجهة الحائزة على أداة توقيع معين ويشار إليها في هذا القانون بالشهادة .

وعرفها **المشرع التونسي** على انها "الوثيقة الالكترونية المؤمنة بواسطة الإمضاء الالكتروني للشخص الذي اصدرها والذي يشهد من خلالها اثر المعاينة على صحة البيانات التي تتضمنها"

ان المشرع اشترط في شهادة التصديق الالكتروني ان تكون صادرة عن جهة مرخص لها بالتصديق الالكتروني حتى تكون اداة اثبات للمتعامل بها

يلاحظ من التعريفات السابقة ان معظم التشريعات ركزت على الجانب الوظيفي لشهادة التصديق الالكتروني المتمثل باثبات هوية الشخص مرسل الرسالة الالكترونية او التوقيع الالكتروني صادر عمن نسب اليه بناء على ما تقدم بالعموم ان تعريف شهادة التصديق الالكتروني عبارة عن هوية او بطاقة الكترونية صادرة عن جهة تصديق مختصة، تتضمن مجموعة من البيانات الأساسية المتعلقة بالشهادة وهوية الشخص المرسل ومصدر الشهادة، تقوم بإثبات هوية الشخص مرسل الرسالة الالكترونية عن طريق ربط مفتاحه الخاص بالعام وفق ضوابط معينة.

الفرع الأول: بيانات شهادة التصديق الالكتروني

عرف المشرع الجزائري شهادة التصديق الالكتروني في المادة 07 من قانون رقم 15 – 04 على انها:" وثيقة في شكل الكتروني، تثبت الصلة بين بيانات التحقق من التوقيع الالكتروني والموقع"، في حين انه نص في المادة 15 من نفس القانون اضاف لفظ موصوفة إلى شهادة التصديق الالكترونية حيث ربط بين مصطلح موصوفة ومجموعة من الشروط الواجب توفرها بشهادة التصديق الموصوفة فيما يلي :

√أن تمنح من طرف ثالث موثوق، او من مؤدي خدمات التصديق الالكتروني، طبقا لسياسة التصديق الالكتروني الموافق عليها، اي انه بحسب رأيي الخاص، لو منحت الشهادة من طرف جهة اخرى، لا يعتد بها كشهادة تصديق موصوفة، ويشترط في الجهة المصدرة لهذه الشهادة ان تكون خاضعة لنظام قانوني محدد وفقا لتشريع البلد المتواجد به مقدم خدمات التصديق.

√ ان تمنح للموقع دون سواه، نستنتج انه لو منحت هذه الشهادة لغير صاحب الشهادة تفقد الشهادة مصداقيتها، وبالتالي فهي ترتبط بذات الشخص صاحب التوقيع الالكتروني.

علاوة على ذلك فقد أدرج المشرع الجزائري مجموع البيانات الواجب توافرها في الشهادة وهي:

أ- احتواء الشهادة على اشارة تدل على انه تم منح هذه الشهادة على اساس انها شهادة تصديق الكتروني موصوفة، اي تكون مكتوبة او حاملة لرمز معين يدل على انها شهادة تصديق الالكتروني موصوفة.

ب- تحديد هوية الطرف الثالث الموثوق او مقدم خدمات التصديق الالكتروني المرخص له لشهادة التصديق الالكتروني وكذا البلد الذي يقيم فيه، ومنه ان تكون هوية مقدم خدمات التصديق الالكتروني بارزة وواضحة وألا تكون مبهمة.

ت- اسم الموقع أو الاسم المستعار الذي يحدد هويته، كأن تحمل الشهادة اسم ولقب الموقع المتواجد ببطاقة التعريف خاصته، او ان تكون حاملة اسمه المستعار شرط أن يشير هذا الإسم إلى صاحب التوقيع حقيقة وأن لا يكون خيالي ، أو استخدم بغاية التمويه أو التدليس.

ث- امكانية ادراج صفة خاصة للموقع عند الإقتضاء ، وذلك حسب الغرض من استعمال شهادة التصديق الالكتروني، مثال طبيعة المهنة اذا كان تاجرا ، شركة...الخ.

ج- بيانات تتعلق بالتحقق من التوقيع الالكتروني ، وتكون موافقة لبيانات انشاء التوقيع الالكتروني.

ح- الإشارة إلى بداية ونهاية مدة صلاحية شهادة التصديق الالكتروني.

خ- رمز تعريف شهادة التصديق الالكتروني.

د- التوقيع الالكتروني الموصوف لمؤدي خدمات التصديق الالكتروني أو الطرف الثالث الموثوق الذي يمنح شهادة التصديق الالكتروني[1]، قد يكون رقما تسلسليا أو حروف أجنبية، عبارة عن شيفرات.

ذ- حدود استعمال شهادة التصديق الالكتروني عند الإقتضاء، أي مدة مدة سريان هذه الوثيقة وصلاحيات استعمالها.

ر- حدود قيمة المعاملات التي تستعمل من اجلها شهادة التصديق الالكتروني عند الإقتضاء.

ز- الإشارة الى الوثيقة التي تثبت تمثيل شخص طبيعي أو معنوي عند الإقتضاء.

[1] لينا ابراهيم يوسف حسان، مرجع سابق، ص82 -87 .

الفرع الثاني: البيانات الإلزامية الواجب توافرها في شهادة التصديق الالكتروني

لكي تتمكن شهادة التصديق من أداء مهمتها يجب ان تتضمن بيانات معينة ، والهدف من هذه البيانات هو الإستجابة لمقتضيات السلامة وبث الثقة بهذه الشهادة من حيث صحة التوقيعات التي يطلبها اطراف التعاقد .

أولا: هوية صاحب التصديق الالكتروني:

أي من صدرت الشهادة بإسمه وبناء على طلبه ، وتشمل الهوية اسم صاحب الشهادة سواء اسمه الحقيقي ام كنيته أم اسمه المستعار، مادام يدل على هويته ويعرف به، وكذلك محل اقامته وتاريخ ميلاده، ومهنته وعنوانه، وكافة البيانات الضرورية للتعريف الجامع له.

ثانيا: هوية التصديق الالكتروني المصدرة للشهادة والدولة المقيمة بها أو التابعة لها:

إن التعريف بالجهة المصدرة للشهادة يضفي نوعا من الثقة والأمان على الشهادة الصادرة خاصة وان جهة التصديق تكون مسؤولة في مواجهة الغير المعتمد على الشهادة عن الأضرار التي تلحق به، إذا كانت ناتجة عن إهمال وتقصير منه، ويتم التعريف بجهة التصديق سواء كانت شخصا طبيعيا أو الممثل القانوني للشخص المعنوي[1].

ثالثا: التوقيع الالكتروني للجهة المصدرة لشهادة التصديق الالكتروني:

هذا يضفي على شهادة التصديق الالكتروني المصداقية والثقة والأمان ويؤكد عدم تزويرها في كل الحالات فإن جهة التصديق الالكتروني المصدرة للشهادة، يجب أن توقع الكترونيا

[1] قد عرفه القانون رقم 15 -04 على انه سلسلة من الاعداد التي يحوزها الموقع فقط وقد استعمل المشرع لفظة التشفير الخاص ، ويرتبط هذا المفتاح بمفتاح تشفير عمومي، أما بخصوص مفتاح

على الشهادة الخاصة بها خلال الفترة التشغيلية للشهادة الأخرى المستخدمة للتثبت من صحة التوقيع الالكتروني لجهة التصديق الالكتروني[1].

رابعا: فترة صلاحية شهادة التصديق الالكتروني

وذلك يكون بتحديد سريانها وتاريخ انتهائها وهو من البيانات الجوهرية إذ انه يحدد النطاق الزمني لمسؤولية جهة التصديق عن البيانات الواردة في الشهادة خلال فترة سريان الشهادة ، واذا ما انتهت فترة صلاحية الشهادة فعلى جهة التصديق ان تبين ذلك من خلال نشرها قائمة بالشهادات الصالحة للاستعمال والشهادات الملغية .

خامسا: المفتاح العام لصاحب التوقيع الذي يناظر المفتاح الخاص

وهو ما يؤكد ان الرسالة الالكترونية صادرة عن المرسل نفسه ولم تتعرض لأي تزوير أو تحريف، حيث يمكن مستقبل الرسالة من التحقق من صحة التوقيع الالكتروني للمرسل عن طريق مطابقة المفتاح العام للمفتاح الخاص.

سادسا: البيان المتعلق بحدود استخدام الشهادة وحدود قيمة الصفقات التجارية التي يجري بشأنها استخدام شهادة التصديق الالكتروني

كأن تتضمن الشهادة البيان التالي: أن هذه الشهادة صالحة للاستخدام في أية صفقة تجارية لا تتجاوز قيمتها 500 دينار جزائري أو ما يعادلها بالعملات الأجنبية.

تعتبر هذه البيانات التي اتفقت معظم التشريعات على توحيدها سالفة الذكر إلزامية، لا غنى عنها في أية شهادة تصديق الكترونية لإضفاء الحجية عليها وتمكين الغير من الاعتماد عليها وبث الثقة والأمان في نفوس المتعاملين عبر شبكة الانترنيت[1].

[1] لزهر بن سعيد، مرجع سابق، ص 184 .

المطلب الثاني: أنواع شهادة التصديق الالكتروني

إلى جانب شهادة تصديق التوقيع الالكتروني الرئيسية التي تم ذكرها بياناتها أعلاه، هناك شهادات أخرى تقوم هيئات التصديق بإصدارها تتنوع بحسب الهدف منها، ومن أمثلة ذلك نذكر:

الفرع الأول: شهادات التعاريف

شهادات التعاريف هي التي تقوم بربط اسم معين بمفتاح أو زر معين، وفي هذا النوع من الشهادات تتمثل مهمة جهة التصديق في التحقق من هويات الأشخاص ، إلا أن هذه المهمة المسندة لجهة التصديق ليست بالسهلة ، ذلك أن تكاليف التحقق من هويات الأشخاص الحاملين للبطاقات الشخصية واعادة اصدارهذه البطاقات مرتفعة جدا، وبالطبع فإنه في عالم الاتصالات الرقمية بالضرورة ان يكون الاسم فريدا أو اسما حقيقيا، يجوز استخدام الاسم المستعار، يجب على جهات التصديق ان تضمن هذه الشهادات توقيعها الالكتروني باستخدام مفتاحها الخاص والذي يرتبط بمفتاحها العام[2] بمجرد وضع التوقيع الخاص بجهات التصديق الالكتروني ، فإن الثقة بهذه الشهادة تتحدد وفقا للثقة التي تتمتع بها جهات التصديق الالكتروني .

---

[1]بركان كريم ، التوثيق الالكتروني والمسؤولية المدنية لجهات التوثيق،مذكرة لنيل شهادة ماستر في العلوم القانونية ، تخصص عقود ومسؤولية ، العقيد اكلي محمد أو الحاج، البويرة،2015 ، ص73 -74 .

[2]لزهر بن سعيد ، مرجع سابق، ص184 .

الفرع الثاني: شهادات البصمة الزمنية

التي توثق تاريخ ووقت اصدار التوقيع الرقمي، حيث يقوم صاحب الرسالة بعد التوقيع عليها بارسالها إلى جهة التوثيق التي تقوم بتسجيل التاريخ عليه، وتوقيعها من جهتها ثم تعيدها إلى مرسلها[1].

الفرع الثالث: شهادة الإذن

والتي يتم بمقتضاها تقديم معلومات اضافية عن صاحب التوقيع كمؤهلاته وعمله والترخيصات التي يملكها[2]،ومكان إقامة الشخص و عمره وفيما إذا كان الشخص عضوا في إحدى المنظمات أو النقابات المهنية كنقابة المحامين.

وهناك استخدامات عديدة لهذه الشهادات فعلى سبيل المثال ، فقهاء القانون الذين يتبادلون أسئلة الامتحانات على شبكة الانترنيت ، وهذه الشهادة رغم التشفير العام هو عبارة من الأعداد تكون موضوعة في متناول الجمهور بهدف تمكينهم من التحقق من التوقيع الالكتروني وتدرج في شهادة التصديق الالكتروني تعريفها بالشخص خاصة إذا كانت صادرة عن جهة تصديق ذات سمعة حسنة وتتمتع بدرجة من الموثوقية فإنها تعتريها بعض العيوب تتمثل في أن البيانات التي تقدمها جهة التصديق قد تكون غير دقيقة، وان الشخص قد يفقد السيطرة على توقيعه الرقمي مما يؤدي إلى وقوعه بيد شخص آخر ليس من مواطني الدولة أو غير مقيم فيها، وان الشخص نفسه الذي تصدر الشهادة بإسمه قد

[1] لينا ابراهيم يوسف حسان، مرجع سابق، ص74 –77

[2] بركان كريم، مرجع سابق، ص67 _68 .

تحدث له بعض التغيرات منذ حصوله على الشهادة، فقد يغادر للخارج أو يفقد للخارج أو يفقد جنسيته أو يتوفى وينتقل مفتاحه الخاص لورثته.

الفرع الرابع : شهادة البيان

والتي تثبت صحة واقعة معينة ووقت وقوعه ومحل اقامته لم تنشأ هذه الشهادات لربط شخص معين بمفتاح أو رمز معين وانما نشأت لبيان وقوع حدث ما وقت حدوثه[1].

الفرع الخامس: شهادات خاتم الوقت الرقمي

هي مستند غير قابل للتزوير، يشهد ان الوثيقة موجودة في زمن محدد وانه ليس من الصعب بيان فيما اذا كانت الوثيقة موجودة قبل أو بعد حادث معين ، هذا النوع من الشهادات على درجة كبيرة من الأهمية ذلك ان هناك حالات يكون فيها من المهم جدا بيان متى حدثت الواقعة بالضبط، واثبات انها حدثت قبل وبعد تاريخ معين، تمثل هذه الشهادة مصداقية للتوقيع الرقمي على الوقت الذي جرى فيه التوقيع الرقمي للوثيقة.

الفرع السادس: شهادة التوقيع الرقمي

تعد شهادة التوقيع الرقمي أكثر أنواع الشهادات انتشارا وأكثرها أهمية، حيث تتلخص تقنية شهادة التوقيع بما يلي:

يقوم من يرغب في الحصول على توقيع رقمي موثق بطلب شهادة تصديق من جهة معتمدة، بحيث تحتوي على المفتاح العام الذي يقابل المفتاح الخاص الذي بحوزته آو

[1] قانون رقم 07 –05 السالف الذكر.

الذي ستزوده به جهة التصديق مباشرة أو احد وكلائها ، والذي يطلب من مقدم الطلب اثبات هويته ، كما قد يطلب وثائق تثبت قدرته على ابرام التصرفات القانونية وفي حال موافقة جهة التصديق على الطلب فإنها تصدر توقيعا رقميا خاصا بالعميل وشهادة تصديق فيها هذا التوقيع، وتشهد بمقتضاها بصحة التوقيع ونسبته الى من صدر عنه حيث تحتوي على المفتاح العام وكذلك معلومات تدل على هوية صاحب المفتاح الخاص المقابل، أي هوية من ينسب إليه التوقيع الالكتروني[1]، ان تنوع شهادات التوثيق تزيد من حجية هذه الشهادة في اثبات كافة الوقائع والأحداث المتعلقة بالمعاملة الالكترونية ووقت ثبوتها.

المبحث الرابع: الآثار القانونية لشهادة التصديق الالكتروني

تعتبر شهادة التصديق الالكترونية أهم وسيلة تعتمدها الجهات المختصة في اصدارها لتأمين المعاملة الالكترونية بين المتعاملين، ذلك انها تحتوي على البيانات الصحيحة الموثقة من طرف هذه الجهة والمتعلقة بصاحب التوقيع الالكتروني[2]، حيث بإمكانها التاكد من شخصية المرسل وتشهد بصحة البيانات المدونة بالمحرر وعدم قابليتها للتعديل، وهذا من شأنه أن يمنح الأمان والثقة للمتعاملين المتعاقدين عبر الانترنيت، نظرا لخطورة هذه الشهادة سواء كان ذلك من حيث طبيعة البيانات الشخصية والسرية التي تحتويها ، أو من حيث حجيتها القانونية في الإثبات حيث يجوز لصاحب الحق ان يحتج بهذه الشهادة في حالة التعدي على حق من حقوقه .

[1] ناجي الزهراء ، التجربة التشريعية الجزائرية في تنظيم المعاملات الالكترونية المدنية والتجارية، المؤتمر العلمي المغاربي الأول حول المعلوماتية والقانون المنعقد في الفترة من 28 إلى29 اكتوبر 2009 ، جامعة بومرداس– الجزائر.

[2] القانون رقم 15 –04 السالف الذكر.

وعليه سيتم دراسة في هذا المبحث حجية شهادة التصديق الالكتروني في **المطلب الأول** وكذا التزامات صاحب شهادة التصديق الالكتروني في **المطلب الثاني** .

المطلب الأول: حجية شهادة التصديق الالكتروني

تقوم هذه الحجية لصاحب الحق المحتج به، شرط ان تكون شهادة التصديق الالكترونية متضمنة لجميع الشروط الواجب توافرها في هذه الشهادة وفقا للتشريع الذي أنشئت ضمنه، وان لا تكون قد تعرضت لتعديل او تدليس حتى لا تفقد قيمتها القانونية وتكون حجة أمام القضاء للمطالبة بحق نصت عليه هذه الشهادة ولم ينفذ تكون هذه الشهادة بمثابة دليل اثبات على وجود التزام او عقد الكتروني مبرم بين شخص طبيعي ومعنوي أو العكس، نميز بين نوعين من الشهادات :

√شهادة تصديق الكترونية وطنية .

√شهادة تصديق الكترونية أجنبية.

تقوم حجية شهادة التصديق الالكترونية التي تصدر في داخل تراب الجمهورية متى استوفت الشروط القانونية المنصوص عليها في التشريع .

سنوضح ذلك من خلال ما يلي:

الفرع الأول: حجية شهادة التصديق الوطنية:

أصبح للكتابة في الشكل الالكتروني مكانا ضمن قواعد الإثبات في القانون المدني الجزائري طبقا لنص المادة 323 مكرر:" ينتج الإثبات بالكتابة من تسلسل حروف او

أوصاف أو ارقام ..." ويقصد بالوسيلة الالكترونية المستعملة مثل القرص الصلب او القرص المرن او شكل رسائل الكترونية، وهكذا يتضح مما سبق بأن المشرع الجزائري اعتمد المفهوم الواسع للكتابة المقصود منه سواء الكتابة على الورق أو الكتابة الالكترونية المثبتة على دعائم غير مادية غير ورقية.

ومن اجل إزالة كل الغموض او نزاع يمكن من الناحية القانونية جاء نص المادة 323 مكرر من القانون المدني الجزائري:" يعتبر الإثبات بالكتابة في الشكل الالكتروني كالإثبات بالكتابة على الورق، بشرط إمكانية التأكد من هوية الشخص. الذي أصدرها وان تكون معدة ومحفوظة في ظروف تضمن سلامته[1].

المشرع يعتبر الاثبات بالكتابة في الشكل الالكتروني كالكتابة على الورق بشرط إمكانية التاكد من هوية الشخص الذي اصدرها ، وبهذا يكون المشرع الجزائري قد سوى بين الكتابة الالكترونية والكتابة العادية من حجية الإثبات[2].

الفرع الثاني: حجية شهادة التصديق الالكتروني الأجنبية

قد نص المشرع الجزائري في المادة 63 من القانون رقم 15 -04 الذي يحدد القواعد العامة للتوقيع والتصديق الالكترونيين مايلي:" تكون لشهادة التصديق الالكتروني التي يمنحها مؤدي خدمات التصديق الالكتروني المقيم في بلد أجنبي نفس قيمة الشهادات الممنوحة من طرف مؤدي خدمات التصديق الالكتروني المقيم في الجزائر شرط ان يكون

[1] إياد محمد عارف، مرجع سابق،ص 129 -130 .

[2] عبد اللطيف بركات ، الاثبات الالكتروني في المعاملات الادارية، مذكرة لنيل شهادة الماستر في الحقوق، تخصص قانون اداري، جامعة محمد خيضر -بسكرة-، 2012 ،ص 73 .

مؤدي خدمات التصديق الالكتروني الأجنبي هذا قد تصرف في اطار اتفاقية للاعتراف المتبادل ابرمتها السلطة "[1]

يعكس هذا النص مدى التعاون الدولي في مجال التجارة الالكترونية سيما وانها تجارة عابرة للحدود الإقليمية، بمعنى ان البائع قد يكون في فرنسا والمشتري في الجزائر ، ومقدم الخدمة في الصين، والشخص راغب الخدمة كاستشارة الكترونية قانونية مثلا مقيم في الأردن ، فكل هذه الأمور تبرر الرغبة في ضرورة الاعتراف بالأثر القانوني لشهادات التصديق الأجنبية ويجعلها بنفس مرتبة الشهادات المحلية ، ولكن بتوافر جملة من الشروط:

√ وجود اتفاقية بين الجزائر وهذا البلد الاجنبي الصادر منه الشهادة تبرمها سلطة ضبط البريد والمواصلات باعتبارها هي المخولة قانونا براقبة عملية التصديق بموجب هذه الاتفاقية تكون لشهادة كلا البلدين نفس القيمة القانونية.

√ مبدأ المعاملة بالمثل، والمتمثل في سريان شهادة التصديق الجزائرية في البلد الأجنبي، وسريان شهادة التصديق الالكتروني الاجنبية في الجزائر.

√ من جانب اخر هناك شرط تستلزمه القواعد العامة للقانون، هو ان لا تكون شهادات التصديق الالكتروني الاجنبية المعترف بها في الجزائر مخالفة للنظام والآداب العامة[2]

نستنتج ان القانون الجزائري ركز على ضرورة استيفاء تلك الشهادات على الشروط المنصوص عليها في قوانينها الوطنية، حول التاكد من استيفاء تلك الشهادات على العناصر اللازمة لبث الثقة والأمان فيها فكلما توافرت الشهادة الالكترونية على الشروط

[1] بركان كريم، مرجع سابق، ص 78 .

[2] زيد حمزة مقدم، مرجع سابق، ص143 -145 .

المنصوص عليها كلما اكتسبت المحررات الموقعة الكترونيا حجية اثبات المعاملات الالكترونية[1]هناك ثلاث معايير اساسية يستند اليها للاعتراف بشهادة التصديق الالكترونية الاجنبية وهي كالتالي:

√ ان تكون هذه الشهادات صادرة من هيئات تصديق تضمن على الأقل مستوى من الثقة الذي يضمنه مزود خدمات التصديق الوطني.

√ ان تتمتع بالكفاءة التي تخضع في تقديرها للمعايير الدولية المعترف بها في هذا المجال.

√ان يكون هناك اتفاق ثنائي او جماعي بين الدول المعنية[2].

الفرع الثالث: حالات تعليق وإلغاء العمل بشهادة التصديق الالكترونية

يقصد بتعليق العمل بشهادة التصديق الالكترونية الوقف المؤقت لسريان الشهادة، وهو ما يعني تعطيل العمل بالأثر القانوني المترتب على الشهادة تمهيدا لإلغائها وعلى ذلك نخص بالذكر الحالات التالية:

أولا: حالات تعليق العمل بشهادة التصديق الالكترونية

1 – بناء على طلب صاحب الشأن:

ويقصد بصاحب الشأن الشخص الذي تقدم بطلب لإصدار الشهادة سواء كان شخصا طبيعيا أو معنويا ، وتتعدد الأسباب التي قد يطلب فيها صاحب الشأن من جهات التوثيق

[1]المادة 08 من قواعد الأنسترال الموحدة بشأن التوقيعات الالكترونية.

[2]لينا ابراهيم يوسف حسان، مرجع سابق، ص130 .

تعليق العمل بالشهادة الصادرة ، فقد يصرف النظر عن اتمام الصفقة او الصفقات التي أراد استعمال التوقيع الالكتروني فيها، أو أن يكتشف تلاعبا في منظومة احداث التوقيع الالكتروني ، او اختلاف الشركاء فيما بينهم، وغير ذلك من الأسباب التي تواجه صاحب الشأن وتدفعه إلى طلب تعليق الشهادة.

2 – ان تكون الشهادة سلمت بالاعتماد على معلومات مغلوطة او مزيفة:

ان مسؤولية الجهة التي تصدر الشهادة مستمرة طول مدة سريانها، فإذا تبين لها خلال هذه الفترة أن الشهادة التي أصدرت قد سلمت بناء على معلومات مغلوطة أو مزيفة ، يتعين عليها الاسراع إلى ايقاف العمل بالشهادة ، وإلا تعرضت للمسؤولية في مواجهة صاحب الشهادة أو الغير حسن النية الذي اعتمد على هذه الشهادة .

3 – ان تستعمل الشهادة لغرض التدليس

اذا علمت جهة التصديق ان صاحبها قد اصدرها لتحقيق غرض غير مشروع ، كأن يهدف من اصداره إلى اقناع الغير بملائمة مركزه المالي مما يدفعه للتعاقد معه، ففي هذه الحالات وحالات التدليس الأخرى يجب على الجهة مصدرة الشهادة تعليق سريانها ومن ثم الغائها إذا تأكدت من صحة وجود التدليس ، أو يثبت عدم صحته فيلغي التعليق.

4 – ان يطرأ التغيير على البيانات التي تتضمنها الشهادة:

من المفروض أن البيانات التي يقدمها العميل لإصدار شهادة التصديق ان تبقى صحيحة طول فترة سريانها ، خاصة البيانات الجوهرية ، فإذا طرأ تغيير على اي بيان من هذه البيانات يتعين على صاحب الشهادة إعلام جهة التصديق بهذا التغيير، وان لم يفعل لا يكون امام جهة التصديق إلا تعليق العمل بشهادة التصديق لحين تصحيح البيان الذي

طرأ على هذا التغيير، سواء ارتبط هذا البيان بشخص صاحب الشهادة أم كان بيانا موضوعيا يتعلق بموضوع الشهادة ومجالات استعمالها[1].

ثانيا: حالات إلغاء العمل بشهادات التصديق الالكتروني

1 – بطلب من صاحب الشهادة.

2 – عند اعلام مزود خدمات التصديق الالكتروني بوفاة الشخص الطبيعي او حل الشخص الاعتباري صاحب الشهادة.

3 – عند ثبوت إحدى الاحالات التالية:

√عدم صحة المعلومات المتضمنة في الشهادة المعلقة، أي احتواء الشهادة على معلومات لا تخص صاحب التوقيع وغير صحيحة.

√ تغير المعلومات المتضمنة في الشهادة ، ويكون هذا التغيير دون علم مسبق من طرف مقدم خدمات التصديق الالكتروني ، ويكون مصير هذه الشهادة الالغاء وعدم المصادقة على صحة مضمونها من طرف مقدم خدمات التصديق الالكتروني.

√ استعمال الشهادة بغرض التدليس أو الغش، ويكون ذلك وفقا للحالات السابق ذكرها.

√ انتهاك منظومة انشاء التوقيع الالكتروني.

هذا ويقوم مقدم خدمات التصديق الالكتروني بإعلام صاحب الشهادة وبإعلام صاحب الشهادة وبإعلام الهيئة في حال تعليق العمل بشهادة التصديق الالكتروني أو الغائها واسباب ذلك، ويجري رفع التعليق فورا عند زوال الاسباب التي ادت اليه، كما يحق لصاحب الشهادة أو للغير التظلم أمام الهيئة على قرار مزود خدمات التصديق الالكتروني

[1] زيد حمزة مقدم، المرجع السابق، ص 143– 145.

بتعليق أو الغائها، وذلك خلال مدة اقصاها خمسة عشر يوما من تاريخ اعلامه به، وتقوم الهيئة بالفصل في التظلم خلال مدة اقصاها ثلاثون من تاريخ تقديمه.

المطلب الثاني: التزامات صاحب شهادة التصديق الالكتروني

بحسب ما اورده المشرع الجزائري في نص المادتين 61 -62 من القانون رقم 15 -04 الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين ، تتمثل التزامات صاحب شهادة التصديق الالكتروني في ما يلي:

√ يعتبر صاحب شهادة التصديق الالكتروني فور التوقيع عليها.المسؤول الوحيد عن سرية بيانات إنشاء التوقيع ، وذلك وجب عليه أن يتخذ العناية اللازمة والكافية للحفاظ على سرية بياناته وعدم استخدامها من طرف الغير وهذا يتفق ونص المادة 8 /1 /أ من قانون الأونسترال النموذجي حيث جاء فيه:" على الموقع إن يمارس عناية معقولة لتفادي استخدام أداة توقيعه استخدام غير مأذون به"[1]

√ في حالة الشك في الحفاظ على سرية بيانات إنشاء التوقيع الالكتروني أو في حالة ما إذا أصبحت هذه البيانات غير مطابقة للمعلومات المتضمنة في شهادة التصديق الالكتروني ، فإنه يجب على صاحب الشهادة ان يعمل على الغائها من طرف مؤدي خدمات التصديق الالكتروني ، ومنه على صاحب الشهادة إعلام جهة التصديق الالكتروني بدون تأخير عن أي خرق لمنظومة إحداث التوقيع الخاصة به وفيما اذا كانت

[1]قانون رقم 15 -04 السالف الذكر.

قد تعرضت لما يثير الشبهة ، أو تم استعمالها من قبل الغير بصورة غير مشروعة وذلك ليتم وقف العمل بالشهادة فورا[1].

√ لا يجوز لصاحب شهادة التصديق الالكتروني عند انتهاء صلاحيتها او عند الغائها استعمال بيانات انشاء التوقيع الموافقة لها من اجل توقيع أو تصديق هذه البيامات نفسها من طرف مؤد آخر لخدمات التصديق الالكتروني.

√لايجوز لصاحب شهادة التصديق الالكتروني الموصوفة استعمال هذه الشهادة لأغراض أخرى غير تلك التي منحت من اجلها[2].

ومنه نستنتج ان صاحب الشهادة هو المسؤول الوحيد عن سرية وسلامة منظومة احداث الإمضاء التي يستعملها، وكل استعمال لهذه المنظومة يعتبر صادرا منه، ويتعين على صاحب الشهادة إعلام مزود خدمات المصادقة الالكترونية عن كل تغيير حصل للمعلومات المضمنة بالشهادة ، وعناصر التشفير الشخصية للإمضاء موضوع الشهادة المعينة والمصادقة على هذه العناصر من جديد لدى مزود آخر لخدمات المصادقة الالكترونية[3].

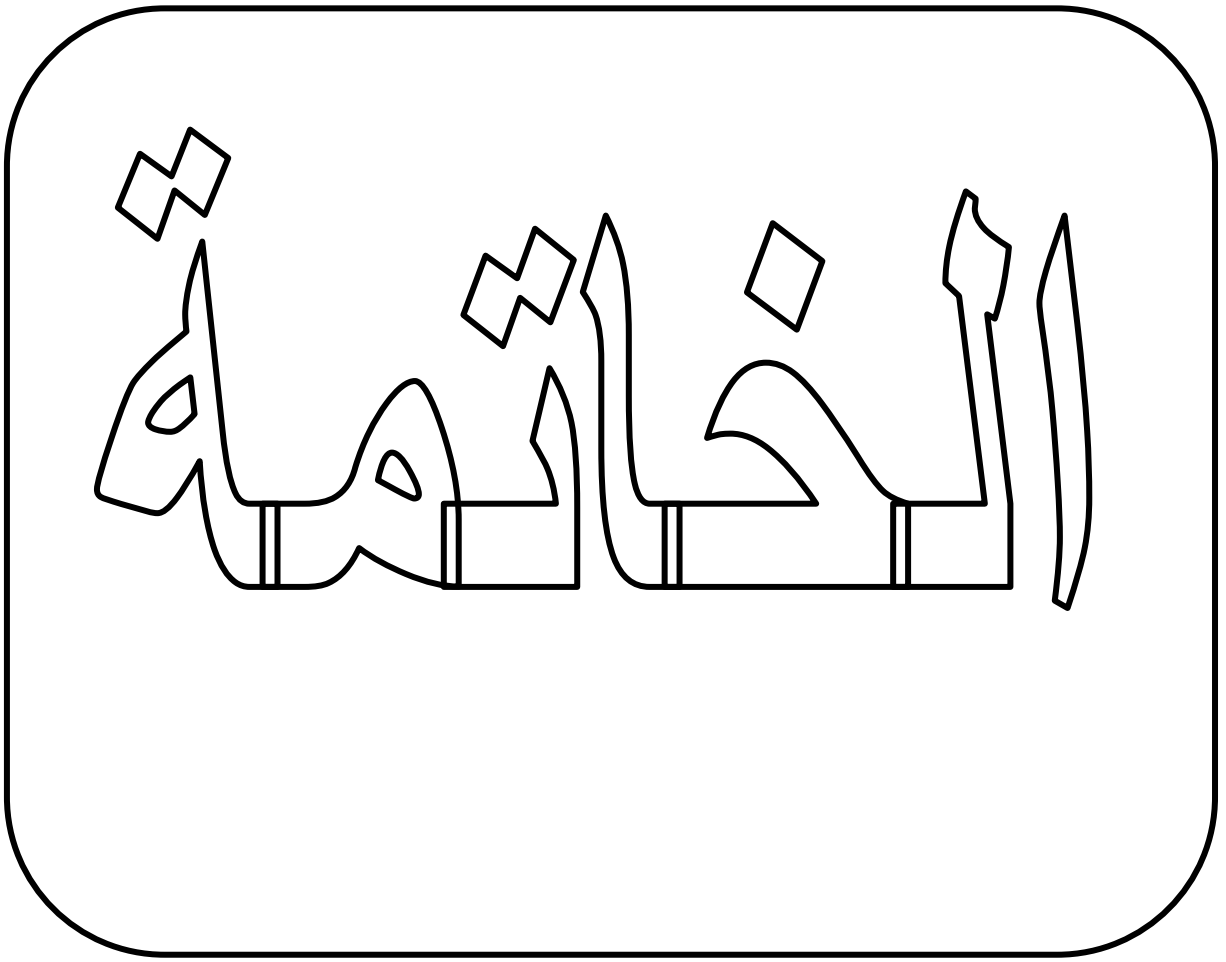
[1] لينا إبراهيم يوسف حسان، المرجع السابق، ص 130.

[2] قانون رقم 15 – 04 السالف الذكر .

[3]قانون المبادلات والتجارة الالكترونية التونسي ، الباب الأول، الفصل الحادي والعشرون، العدد 83 لسنة2000،المؤرخ في09غشت 2000.

خلاصة الفصل الثاني:

نخلص مما سبق إلى القول ان على الرغم مما نظمته تشريعات الدول المختلفة من التزاما ت تقع على عاتق جهات التصديق الالكتروني ومما يترتب عليه من مسؤولية عن اخلالها ا بالتزاماتها، الا انه من واجب الاطراف التي تعول على على شهادات التصديق الالكترون ية ان تبذل عناية معقولة للتحقق من صلاحية الشهادة وفيما اذا كان العمل بها موقوفا او اذا كانت ملغاة، او فيما وجد اي قيد على استعمالها ، كل ذلك للتقليل من حجم الخسائر التي قد تتكبدها.


الخاتمة

تحقيقا لمستلزمات الثقة و الأمان التي تعتبر من الضمانات الأساسية للتعاملات الالكترونية ظهرت الحاجة لوجود طرف ثالث مستقل من أطراف العلاقة القانونية، هذا الطرف يمكن تسميته بجهة التصديق الالكتروني تلعب هذه الجهة دورا هاما ورئيسيا في توفير بيئة آمنة للمتعاملين بالوسائط الالكترونية وذلك لكونه يربط بين شخص المتعاقد وبيانات الرسالة الالكترونية ، وبالنتيجة التأكيد على ان التوقيع الالكتروني الوارد على الرسالة يعود للموقع نفسه دون سواه.

وبالرجوع للقواعد العامة للمسؤولية المدنية وتطبيقهاعلى الجهات التصديق والتوقيع الالكترونيين ، نجد انها تخضع لأحكام المسؤولية العقدية من خطأ وضرر وعلاقة سببية بينهما، أما في إطار علاقتها بالغير الذي عول على الشهادة الصادرة عنها فإنها تخضع لأحكام المسؤولية التقصيرية نظرا لعدم وجود علاقة عقدية بينهما متى توافرت أركانها من فعل وضرر وعلاقة سببية.

التوصيات:

– زيادة الوعي لدى المتعاملين بالمعاملات بأهمية التوقيع والتصديق الالكترونيين و إجرائتهما ، وذلك بعدعقد الندوات والدورات المتخصصة والمؤتمرات التي تعالج هذا الموضوع.

– على الدولة الجزائرية العمل على تحسين جودة جودة خدمات الانترنيت، فإذا كانت هذه الاخيرة ضعيفة فلا يمكن انتظار خدمات نوعية في مجال الخدمات والتجارة الالكترونية.

– إضافة المزيد من التوضيح للنصوص القانونية المتعلقة بالتوقيع و التصديق الالكترونيين.

– الإستفادة من تشريعات الدول المتطورة والتي لها الأسبقية في المعاملات الإلكترونية من أجل صياغة تشريع مرن يواكب التطور.

– العمل على تحفيز العمل بالمعاملات الالكترونية بين الأفراد.

– إذا كنا مع التقدم العلمي والتكنولوجي في مجال المعاملات القانونية إلا اننا يجب ان نتعامل مع هذا التقدم القادم علينا بحذر وحيطة شديدين، فلا نتعامل معه إلا بما يتماشى مع ديننا الحنيف وتقاليدنا الراسخة وأعرافنا المتفق عليها لأن ما يصلح لغيرنا لا يصلح لنا.

– تشديد الجزاءات الجنائية على الجرائم المتعلقة بالقرصنة وإختراق الحسابات ، و التزوير التي يتم بواسطة الحاسوب ، والتي تؤثر سلبا على سمعة التجارة الالكترونية، مما يجعل من التعاملات الالكترونية امر يفتقر إلى الأمان والثقة واللذان يعدان جوهرة المعاملات.

– اشراك الفنيين المختصين في مجال الإعلام والتكنولوجيا في وضع مشاريع قانونية، وذلك لخبرتهم في فهم المسائل التقنية والمصطلحات التكنولوجية أكثر من رجال القانون.

– إدماج كامل التوقيع والتصديق الالكترونيين في كل القطاعات من أجل حماية أكيدة للم عاملات الالكترونية، وعصرنة التعاملات التجارية.