الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

جامعة أبو بكر بلقايد -تلمسان-

كلية الحقوق

التوقيع الإلكتروني كوسيلة من وسائل الإثبات

مذكرة تخرج لنيل شهادة الماجستير في القانون الخاص

إعداد الطالب:

أزرو محمد رضا

أعضاء اللجنة:

أ.قلفاط شكري	أستاذ التعليم العالي	جامعة تلمسان	رئيسا.
أ.دنوني هجيرة	أستاذة التعليم العالي	جامعة تلمسان	مشرفة و مقررة.
أ.بوعزة ديدن	أستاذ محاضر	جامعة تلمسان	مناقشا.
أ.مامون عبد الكريم	أستاذ محاضر	جامعة تلمسان	مناقشا.

السنة الجامعية :2007-2008

24. 10. 2323

تشكرات

أقدم خالص تحياتي إلى أستاذتي دنوني هجيرة

لتوجيهاتها القيمة

وكل من الأستاذ قلفاط

والأستاذ مامون

والأستاذ بوعزة

على جهودهم في تصحيح المذكرة

وشكري الكبير لكل العاملين في الإدارة

وبالخصوص الأستاذ كحلولة عميد الكلية

نظرا لتسهيلات الكبيرة

وكل شخص ساعدني لإتمام هذه المذكرة

24 OCT. 2007

جامعة أبي بكر بلقايد - تلمسان
كلية الحقوق
المكتبة
رقم الجرد : 17/104
تاريخ الدخول: .....

الإهداء

إلى أعز الناس على قلبي

إلى من ربياني صغيرا

إلى أمي وأبي

وإلى أخي الوحيد ...

وكل شخص ساعدني في إتمام هذا البحث

أهديهم ثمرة بحثي وجهدي.

قائمة أهم المختصرات

بالعربية

أ	أستاذ
ج	جزء
د	دكتور
ص	صفحة
س	سنة
دج	دينار جزائري
ق إ م	قانون الإجراءات المدنية
ق م ج	قانون المدني الجزائري

بالفرنسية

PSC	prestataire
P	Page
Op.cit	Opere citatis
Cass.civ	cassation civil.
Cass.crim	cassation criminelle
Civ,rej	civil , rejetet
Bull.civ	Bulletin civil
N₀	Numéro
UNICTRAL	United Nation Commission on International Trade Law
CNUDCI	Commission des Nations Unies pour le Droit Commercial International
Art	Article
Art. prec	Article précité
Ch.soc	la Chambre sociale
CSN	La conseil suprême de notariat
CNHJ	Chambre nationale des huissiers de justice
SCSSI	Le service central de la sécurité des systèmes d'information

المقدمة

يعد الرضا من أهم أركان العقد، فلا يكون صحيحا ولا يرتب أثاره إلا بتوافره ، ويتم التعبير عنه إما بمجرد تبادل الأشياء أو التصافح أو بالكتابة.

إذ تعتبر هذه الأخيرة(الكتابة) الوسيلة الأكثر استعمالا لكونها تحفظ حقوق الأطراف المتعاقدة و تكون حجة في حال وقوع نزاع .

تكون هذه الكتابة إما على شكل ورقة رسمية أو عرفية، إلا أنه وفي جميع الأحوال يجب أن تذيل في الأخير بتوقيع الأطراف.

بل إن بعض التشريعات[1]، وبعض الفقهاء[2] اعتبرت التوقيع هو الشرط الوحيد لصحة الورقة العرفية، إلا أن هذا لا يعني بالضرورة عدم وجود شروط أخرى بجانبه حتى يتم قبول الكتابة كدليل إثبات.

فنجد مثلا أن الورقة الرسمية إضافة إلى توقيع الأطراف، فإنه يجب أن تتم بواسطة موظف أو ضابط عمومي أو شخص مكلف بخدمة عامة في حدود سلطاته اختصاصه، ويدون ما تلقاه من ذوي الشأن وفق الأشكال القانونية[3].

بل حتى الورقة العرفية التي تكتسب قوتها من توقيع الأطراف عليها لا تكون حجة على الغير في تاريخه إلا منذ أن يكون له تاريخ ثابت وفق ما تنص عليه المادة 328من القانون المدني الجزائري بقولها :«لا يكون العقد العرفي حجة على الغير في تاريخه إلا منذ أن يكون له تاريخ ثابت ...»، وبالتالي فإنه يحق لنا التساؤل عن دور ومكانة التوقيع في الإثبات ؟

---

[1] مثل القانون الإثبات المصري

[2] أنظر د عبد الرزاق السنهوري ،الوسيط في شرح القانون المدني الجديد ،الإثبات وآثار الالتزام ،ج2 ،ص.176و د- سليمان مرقس، الوافي في شرح القانون المدني ، أصول الإثبات وإجراءاته في المواد المدنية، الطبعة الخامسة ،1991، ص.230

[3] وهو ما نصت عليه المادة 324 من القانون المدني الجزائري بقولها:«العقد الرسمي عقد يثبت فيه موظف أو ضابط عمومي أو شخص مكلف بخدمة عامة، ما تم لديه أو ما تلقاه من ذوي الشأن وذلك طبقا للأشكال القانونية وفي حدود سلطته واختصاصه

إلا أن التوقيع لم يعد مقتصرا على الصورة التقليدية التي تتم فوق دعامة ورقية، فدخول الكمبيوتر والانترنيت بشكل كبير في حياة الأفراد واعتمادهم عليه في إبرام الصفقات التجارية ومختلف تصرفاتهم القانونية ، أدى إلى ظهور دعامات جديدة مثل الأقراص المضغوطة و الأقراص اللينة[1] ،أصبح لزاما إيجاد بديل مناسب للتوقيع التقليدي ، فكان ظهور التوقيع الإلكتروني كوسيلة الجديدة لإبرام الصفقات سواء على الشبكات المفتوحة (الانترنيت) أو الشبكات المغلقة(الأنترانات) .

إذ أصبح هذا الأخير ظاهرة اجتماعية صار من الضروري دراستها وإيجاد الإطار القانوني الذي يحميها وذلك حماية للأفراد والمجتمعات الذين يتعاملون مع هذا النوع من التوقيع.

فتحول التوقيع الإلكتروني إلى أداة أمنة لإبرام العقود التجارية، والمنفذ لتجنب القرصنة ومختلف الأعمال الإجرامية.

إلا أنه يجب أن نعرف بداية ما هو التوقيع الإلكتروني ؟ و ما هي مكانته في الإثبات؟ ومن هم أطرافه ؟ وما هي مسؤولياتهم أثناء إعمال التوقيع الإلكتروني؟

نظرا للدور الكبير الذي بات يلعبه التوقيع الالكتروني من الناحية الاقتصادية ، فإن وضع القوانين الخاصة به أصبح أمرا لا مفر منه ، سواء على المستوى الدولي كقانون الأونيسترال النموذجي بشأن التوقيعات الإلكترونية أو التعليمة الأوروبية المتعلقة بالتوقيع الالكتروني رقم 93-199، أو على مستوى الدول كفرنسا بموجب المرسوم 30 مارس 2001 التي بموجبها تم إدخال التوقيع الالكتروني كوسيلة إثبات في القانون المدني الفرنسي، وتونس بموجب القانون الخاص بالتوقيع الالكتروني عدد 83 لسنة 2000 المؤرخ في 9 أوت 2000 يتعلق بالمبادلات والتجارة الالكتروني ، ثم تبعتها بعد ذلك العديد من الدول العربية كإمارة دبي بموجب القانون رقم (2) لسنة 2002 بشأن المعاملات والتجارة الالكترونية ومصر إلخ ...

---

[1] وهو ما يعرف ب cd و disquette

كما سندرس في هذا البحث بالتفصيل موقف المشرع الجزائري من التوقيع الإلكتروني وهل سن قوانين خاصة به أسوة ببقية الدول الأخرى.

تتميز على العموم التجارة الإلكترونية من أنها تتم بين أشخاص لا تربط بينهم أي علاقة أو معرفة مسبقة .

إلا أنه قد تم حل هذا الإشكال بواسطة ما يعرف ب« مزود الخدمات» الذي يعتبر الوسيط بين الموقع والمرسل إليه، بحيث يتكفل بإنشاء التوقيع الإلكتروني لصالح الموقع، كما يصدر هذا الأخير شهادة التصديق الإلكتروني في حال ما إذا طلبها المرسل إليه، بل الأكثر من ذلك فإن القانون قد حمله المسؤولية المدنية والجنائية في حال ما إذا أخل بالتزاماته المنصوص عليها قانونا، غير أنه يجب أن نعرف أولا من هو مزود الخدمات؟ وما هي التزاماته؟ وما هي الشروط القانونية التي وضعها المشرع لمزاولة مهنته ؟

من المعروف أن الجريمة المعلوماتية تشكل خطرا كبيرا على المعاملات الإلكترونية بصفة عامة وعلى التوقيع الإلكتروني بصفة خاصة، ولهذا كان إقرار الحماية الجنائية للتوقيع الإلكتروني أمرا ضروريا من جهة حتى نزرع في الأشخاص المستخدمة له نوعا من الأمان والطمأنينة في نفوسهم ، ومن جهة أخرى تكون رادعا لكل شخص يحاول التلاعب بالتوقيع الإلكتروني ، لكن ما هي أنواع الجرائم الوقعة على التوقيع الإلكتروني؟ ، وما هي عقوبة كل جريمة؟

وللإجابة على هذه التساؤلات قسمنا البحث إلى فصلين ، ففي الفصل الأول سنتطرق إلى مكانة التوقيع الالكتروني من التوقيع التقليدي ، وفي الفصل الثاني سنتحدث على التوقيع و الأمان القانوني أو ما هي الضمانات والوسائل التي بها نحمي التوقيع الإلكتروني.

الفصل الأول : طبيعة التوقيع الإلكتروني

على الرغم من استعمال التوقيع بكثرة من طرف الأشخاص في حياتهم اليومية، ودوره الكبير في الإثبات، إلا أن القانون لم يحاول إعطاء تعريف دقيق له ولا حتى تبيان مكوناته ووظائفه ، وترك هذه المهمة للفقهاء.

حيث أن الورقة الرسمية أو العرفية لا تكون دليل إثبات إلا إذا احتوت على توقيع الأطراف، الذي يعني بالضرورة موافقتهم على ما احتواه السند، وعلى هذا الأساس فإن المبحث الأول سنتطرق فيه إلى محتويات ووظائف التوقيع.

كما أن ظهور التوقيع الإلكتروني واعتباره امتدادا للتوقيع التقليدي ألزم رجال القانون دراسته ومحاولة إبراز مكانته كوسيلة إثبات حديثة، غير أن هذا لا ينفي الجدل القائم حول مدى حجية التوقيع الإلكتروني وهل بالفعل وصل إلى نفس درجة التوقيع التقليدي؟ وهو ما سنجيب عنه في المبحث الثاني

المبحث الأول : دور التوقيع في الإثبات

حاول الكثير من الفقهاء إعطاء مفهوم دقيق للتوقيع ومن بينهم الأستاذ Christophe Dervs الذي عرفه بأنه:«كل علامة توضع على سند تميز هوية وشخصية الموقع وتكشف إرادته بقبول التزامه بمضمون هذا المستند وإقراره له»[1]

من خلال هذا التعريف يمكن استخلاص عناصر و وظائف التوقيع، مع إجراء مقارنة ذلك بالتوقيع الإلكتروني باعتباره امتدادا للتوقيع التقليدي (المطلب الأول).

[1] المستشار عمرو عيسى الفقي،وسائل الاتصال الحديثة وحجيتها في الإثبات،المكتب الجامعي الحديث ،2006 ،ص . 22

بعد ذلك سنتطرق في المطلب الثاني إلى مجال إعمال التوقيع في الكتابة الرسمية والعرفية لأهميته البالغة .

المطلب الأول : شروط ووظائف التوقيع

إن التوقيع سواء كان خطيا أو الكترونيا حتى يكون صحيحا ويولد أثار قانونية ترتب التزاما على الموقع فإنه يشترط أن يكون محددا بصفة كافية لهوية الشخص الموقع ،ولذلك هناك من رأى أن يحتوي التوقيع(الإمضاء) على لقب واسم الموقع كاملا ويمكن أن يكون باسم الشهرة وهو ما سنتطرق إليه بالتفصيل في الفرع الأول .

عندما يصبح التوقيع صحيحا ومستوفي لجميع الشروط فإن ذلك يعني بالضرورة رضا الموقع بمحتوى السند الكتابي وهو الدور الأساسي للتوقيع لكن مع ظهور التوقيع الإلكتروني ظهرت مهام جديدة للتوقيع وهي مراقبة مدى نزاهة الوثيقة وأخيرا منح الوثيقة الموقعة صفة «الأصل» وهو ما سندرسه بالتفصيل في الفرع الثاني .

الفرع الأول : شروط ومحتوى التوقيع

1- شروط الأخذ بالتوقيع :

ليكون التوقيع صحيحا ويعتد به قانونا يجب أن يكون بيد الموقع نفسه أو من ينسب إليه المحرر ولا يجوز أن يكون بخط شخص أخر ولو كان موكلا عنه لأن الوكيل يوقع باسمه باعتباره وكيلا لا باسم الموكل [1]، إذ لا قيمة للمحرر إذا وقع عليه شخص باسم غير اسمه أو

[1] المستشار عمرو عيسى الفقي،وسائل الاتصال الحديثة وحجيتها في الإثبات ،ص. 23

بختم غيره طالما أن هذه الواقعة ثابتة أو غير منكرة[1]، ولا يمكن بأي حال من الأحوال تعويض التوقيع بالختم أو الصليب (croix)[2].

بما أن الهدف من التوقيع الإلكتروني هو إيجاد بديل مناسب للتوقيع التقليدي في إطار المعاملات الإلكترونية فقد حرصت التشريعات على توفر هذا الشرط ، إذ يجب أن يكون هذا التوقيع مرتبط بالموقع دون سواه ،وأن يسيطر الموقع وحده على الوسيط الإلكتروني[3].

كما يجب أن يترك التوقيع أثرا مميزا يبقى ولا يزول مع مرور الزمن، بحيث يكون منفصلا عن الكتابة غير متداخل فيها أو مختلطا معها[4]

2- أنواع التوقيع :

إن للتوقيع عدة أنواع فقد يتم بالإمضاء بخط اليد أو بالختم أو ببصمة الأصبع، وإن كان المشرع الجزائري في المادة 327 من القانون المدني قبل التعديل لم يكن يعترف إلا بالإمضاء حيث تنص هذه المادة :«يعتبر العقد العرفي صادرا ممن وقعه ما لم ينكر صراحة ما هو منسوب إليه من خط أو إمضاء...» ، ثم أقر بصحة التوقيع ببصمة الأصبع وهذا بموجب القانون 05-10المؤرخ في 20جوان 2005 المعدل والمتمم للقانون المدني وإن لم يقر بالختم كنوع من أنواع التوقيع حيث تنص المادة 327 بعد التعديل على :«يعتبر العقد العرفي صادرا ممن كتبه أو وقعه أو وضع عليه بصمة إصبعه...»، وهذا ربما نظرا لسهولة تزوير الختم وهو أغلب ما ذهب إليه الفقهاء[5] .

---

[1] د-سليمان مرقس،المرجع السابق،ص.234

[2] Meme Mostefa-Kara Farida née Settouti: «La preuve écrit en droit civil algérien» , mémoire pour le diplôme de magistère en droit , université d'Alger , Institut des Sciences Juridiques et administratives , 1982, p.43

[3] سنتحدث بأكثر تفصيل عن شروط التوقيع الإلكتروني في المبحث الثاني من هذا الفصل.

[4] المستشار عمرو عيسى الفقي،المرجع السابق،ص.29

[5] أنظر في ذلك د-سليمان مرقس،المرجع السابق ،ص.237 و238 ود-عبد الرزاق السنهوري ،المرجع السابق، ص.177و178

عكس ذلك فإن المشرع المصري قد اعترف بالختم وهذا ما ذهبت إليه المادة 14 من قانون الإثبات.

زيادة على ذلك فقد اقترح الأستاذ stenuit ضمن المشروع الأول للقانون المدني المصري أن تضاف فوق ختم الشخص إمضاء شخص أخر مرخص له ذلك قانونا ويتعين في هذه الحالة أن يذكر موقع الورقة بإمضائه أنه يعرف صاحب الختم أو أن يبين المستندات المثبتة لشخصه وأن يوضح سبب عجزه عن الإمضاء والتجائه إليه بدلا منه ؛ وقد رأت لجنة تنقيح التقنين المدني عدم الاعتداد بهذا المقترح لأنه يؤدي إلى تعطيل التعامل[1].

ولقد أحسن المشرع الجزائري فعلا عندما اعتد ببصمة الأصبع ،وهذا نظرا لانتشار الأمية ، وكذلك لاستحالة تزويرها إذ أنها عمليا تختلف من شخص لأخر.

3- محتويات التوقيع(تحديد هوية الموقع):

حتى يكون الإمضاء صحيحا يجب أن يحتوي على اسم ولقب الموقع كاملا أو بالأحرف الأولى فقط أو حتى باسم الشهرة، المهم أن يحدد هوية الموقع؛ وهو ما أقره المشرع الفرنسي صراحة في المرسوم 230-2000 المادة 4 فقرة 1 عندما نص على :« التوقيع اللازم لإتمام تصرف قانوني يحدد الشخص الذي يجريه. وهو يعبر عن رضى الأطراف بالالتزامات الناشئة عن هذا التصرف. »

اللقب : هو ناتج أساسا عن روابط الزواج والنسب ، ويمكن في فرنسا وفق قانون 23ديسيمبر 1985 لكل فرنسي وفرنسية إذا أرادوا أن يضيفوا لقب أمهم أو لقب أبيهم في جميع التصرفات اليومية وفي بطاقات التعريف وبالتالي يمكنهم الإمضاء باللقبين معا [2] .

---

[1] د-عبد الرزاق السنهوري،المرجع السابق،ص.177هامش1

[2] Delphine Majdanski:« la signature et les mentions manuscrites dans les contrats» ;Presses Universitaires de Bordeaux.2003 , p.83

أما في الجزائر ووفق المادة 28 فقرة 1 من القانون المدني تنص صراحة على عدم إمكانية حمل الشخص للقبين معا إذ:«يجب أن يكون لكل شخص لقب واسم فأكثر ولقب الشخص يلحق أولاده».

الاسم: على الرغم من أهمية وضع اللقب أثناء التوقيع إلا أنه هناك من اشترط وضع الاسم بجانبه حتى نتمكن من تمييز هوية الموقع عن بقية الأشخاص، ويعرف على أنه الاسم الخاص المرتبط باللقب والذي يميز الشخص عن بقية أفراد عائلته [1] .

حتى وإن كان وضع الاسم وحده أثناء التوقيع لا يثير مشاكل في المجال التعاقدي إلا انه قد طرح في فرنسا العديد من المشاكل خاصة في مجال الوصية المكتوبة.

لقد كان موقف القضاء الفرنسي مضطربا ولم يستقر على رأي واحد فتارة نجده يقر بصحة التوقيع المحتوي على الاسم وحده دون اللقب، وتارة أخرى لا يقر بصحته، غير أن الملاحظ أنه أخذ بمعيار «الاعتياد» لإقرار صحة توقيع دون أخر.

إلا أنه استبعد هذا المعيار في بعض أحكامه ، مثل ذلك الحكم الصادر من مجلس النقض الغرفة المدنية الصادر 24جوان 1952[2] ،حيث أن موصي حرر وصيته في بطاقة بريدية ووقعها باسمه فقط «pierre» لصالح الآنسة ب.

فقام ورثة الميت برفع دعوى أمام القضاء مشككين في نزاهة الوصية على اعتبار أنها لم تستكمل الشروط المنصوص عليها في المادة 97من القانون المدني، حيث اعتبروا أن التوقيع بالاسم فقط لا يوضح هوية الموقع (الموصي) بشكل كافي.

لكن المحكمة في حكمها اعتبرت أن :«التوقيع بالاسم فقط في الوصية المكتوبة مطابق لما يتطلبه القانون بمجرد التأكد من هوية الموقع ومن إرادته حتى وإن لم يكن توقيعه

[1] Delphine Majdanski ;op .cit ;p.85
[2] Cass.civ.24 juin 1952,JCP 1952,II,7179 cité par Delphine Majdanski ;op.cit ;p.86

المعتاد في تصرفاته القانونية ذلك متى كان ظاهرا أن تحرير الوصية في البطاقة كان بكتابته الشخصية».

كما جاء موقف الفقيه الأستاذVoirin مساندا لما توصل إليه القضاء الفرنسي حيث اعتبر أن التوقيع بالاسم فقط كافي بالنسبة للموصي متى كانت تجمعه بالموصى له علاقات حميمية ناتجة عن العلاقات الأسرية أو الصداقة وما عدى في هذه الحالات فإن توقيع الموصي يجب أن يحتوي على لقبه في التوقيع [1]

نستخلص في الأخير أن التوقيع بالاسم يعتبر صحيحا متى كان الموقع معتادا التوقيع به و يحدد هويته بشكل كافي، ولا يكون هذا في جميع الأحوال بل تدرس كل حالة على حدا.

اسم الشهرة: هناك من يوقع باسم الشهرة وعرفته محكمة نقض باريس في القرار الصادر 25 أكتوبر 1961على أنه « هو الاسم المختار من الشخص ليتنكر به عن الجمهور بشخصيته الحقيقية بمناسبة ممارسته نشاط معين »[2]

المعروف أن اسم الشهرة لا يحمل أي طابع رسمي فهو غير موجود في وثائق و لا بطاقة تعريف الشخص، وبالتالي يحق لنا التساؤل حول مدى الاعتداد بتوقيع الشخص بهذا الاسم.

غير أنه البعض يرى أن هذا التوقيع يجب أن يكون محدودا في مجالات معينة ولا يستعمل في التصرفات الهامة والخطيرة والتي يستوجب فيها تحديد هوية الموقع بشكل قطعي[3].

عبر القضاء الفرنسي عن رأيه في هذا الموضوع بان اعترف بالتوقيع باسم الشهرة مع إمكانية إثبات العكس ، وذلك في قراره الصادر عن محكمة نقض باريس بتاريخ 16ماي 1988 [1].

---

[1] Delphine Majdanski ;op.cit ;p.86

[2]Paris, 25 octobre 1961, JCP, 1961 , II ,12377,cité par Delphine Majdanski ;op.cit ;p.84

[3] Julien Esnault :« la signature électronique» ;université de droit, d'économie et de science sociales paris II pantheon-assas ,p.7

الأحرف الأولى من الاسم واللقب : قد طرح هذا النوع من التوقيع على القضاء الفرنسي خاصة في مجال الوصية، حيث يرى مجلس Caen في القرار الصادر بتاريخ 11ديسمبر 1822 بأنه:« لا يجد في الوصية المكتوبة أن الأحرف الأولى من لقب واسم الموصي فهي لا تعادل التوقيع ؛ حيث أن التوقيع هو كتابة اسم ولقب الموقع كامل ولا يمكن أن يكون مجرد كتابة الحرف الأولى من اسمه ولقبه[2]»

إلا انه وفيما يخص الوصية الرسمية والتي تتم أمام الموثق فقد اعترف القضاء الفرنسي بالتوقيع بالأحرف الأولى واعتبره توقيعا صحيحا، وهذا ما أقره مجلس Nancy في 1مارس 1831، على أساس أن الموثق الذي تم أمامه تحرير الوصية أكد أن الشهود قد رأوا الموصي يوقع هذا من جهة ومن جهة أخرى فإن هذا الأخير كان معتادا التوقيع بالأحرف الأولى من اسمه ولقبه[3].

أما في الوقت الحاضر فإن هذا النوع من التوقيع تدرس مدى صحته على حسب كل حالة على حدا.

غير أنه وقع خلاف حول التوقيع على الورقة العرفية إن تعددت أوراقها فهناك من يرى أنه يستلزم أن يتم التوقيع على كل ورقة ولا يكفي توقيع الورقة الأخيرة فقط[4]، وهناك من رأى عكس ذلك بأن جعل التوقيع في أخر الصفحة كافيا دون أن توقع باقي الصفحات[5] .

إلا أنه في الواقع أن الورقة العرفية لا تكون لها أي حجية أو قيمة قانونية إلا بتوقيعها أو الإمضاء عليها، وبالتالي فإنه يستحسن بحسب رأينا متى تعددت الأوراق أن توقع كل ورقة حتى تكون كل تلك الأوراق حجة بما احتوت وتجنبا لإضافة ورقة أو أوراق فيما بعد

---

[1] Cass.crim. 16 mai 1988, lexilaser, pourvoi N0 87-80.769. ,cité par Delphine Majdanski ;op.cit ;p.85

[2]Caen. 11décembre 1822. s.1823. sur pourvoit Civ,rej.,25 avril 1825,s.1825,1,71, cité par Delphine Majdanski ;op.cit ;p.88

[3] Delphine Majdanski ;op.cit ;p.89

[4] أنظر د-سليمان مرقس،المرجع السابق،ص.232

[5] د-عبد الفتاح بيومي حجازي،التوقيع الإلكتروني في النظم القانونية المقارنة ،دار الفكر الجامعي-2005،ص.389

لم يكن الموقع قد التزم بها أثناء توقيعه على الورقة العرفية ، ولكن هذا لا ينفي أنه يستطيع الأفراد أن يوقعوا على الورقة الأخيرة فقط ما دام أن أغلب التشريعات لم تتطرق إلى هذه الحالة ،خاصة إذا ما كانت هذه الأوراق مرتبطة ببعضها البعض بشكل يستحيل معها القيام بزيادة أية ورقة .

لا يطرح هذا المشكل فيما يخص الورقة الرسمية التي اشترط فيها المشرع أن تكون كل ورقة موقعة ومؤشرة من طرف الموثق والموقع[1].

أما مكان التوقيع فلم لم يشترط المشرع أن يرد في مكان معين فيمكن أن يكون في أخر الورقة وهو الغالب وقد يأتي على هامش الورقة في اتجاه طولي أول الورقة.

على العكس من ذلك نجد أن القضاء وخاصة الفرنسي قد أوضح رأيه في هذه النقطة بالذات ، بأن رفض وصية موقعة بيد الموصي في أول الورقة إذ لا يمكن أن نتصور أنه قد وقع منذ البداية على الوصية دون أن تكون هناك إمكانية أن يكون الموصي قد عدل الوصية لصالحه ، ولا يصلح التوقيع في أول الورقة إلا في حالة التوقيع على بياض[2].

وهو نفس ما اتجه إليه القضاء المصري إذ اعتبر أن التوقيع في أخر المستند شرط على نسبته لصاحبه ودليل على التزامه بمضمونه، أما التوقيع في مكان أخرمن المحرر فلا يكفي لكي ينسب المحرر إلى موقعه[3].

4-تحديد هوية الموقع في التوقيع الإلكتروني:

إن تحديد هوية الشخص في المعاملات الإلكترونية يختلف بشكل جذري عن ما هو متعارف عليه في المعالات الكلاسيكية ،فإن كان هذا الأخير تتيح معرفة الموقع عن طريق

---

[1] في فرنسا بموجب المادة9 فقرة 4 من المرسوم 26 نوفمبر 1971 والجزائر بنص المادة 324 مكرر 2 فقرة1 من القانون المدني :« توقع العقود الرسمية من قبل الأطراف والشهود عند الاقتضاء، ويؤشر الضابط العمومي على ذلك في أخر العقد »

[2] Delphine Majdanski ;op.cit. ,p.88

[3] أنظر د-سليمان مرقس،المرجع السابق،ص.234

بطاقة التعريف الوطنية والحضور المادي للشخص، فإن ذلك غير ممكن في الفضاء الإلكتروني .

إلا أنه يجب التمييز في هذا المجال بين الشبكات المغلقة والمفتوحة ،فهذه الأخيرة غالبا ما تتم التصرفات بين أشخاص لم يسبق أن تعاملوا مع بعضهم البعض وبالتالي ليس لهم معرفة مسبقة بالأطراف المتعاملة معهم ،وهو ما شكل أهم عائق لتطور التجارة الإلكترونية .

إلا أنه وبمجيء التوقيع الإلكتروني فقد تم تجاوز هذه العقبة ، حيث تتيح هذه الوسيلة معرفة الطرف المتعامل، بواسطة شهادة التصديق الإلكتروني فكل موقع يجب أن تحدد هويته بشكل دقيق وكامل (الاسم اللقب ،المهنة)، مع إمكانية ذكر حتى اسم الشهرة.

كما أن تدخل مزود الخدمات في التوقيع الإلكتروني يضمن أمن المبادلات على الشبكات ويساعد على تحديد المرسل والمرسل إليه[1].

غير أن هذه المشكلة لا تطرح بتاتا في الشبكات المغلقة التي يفترض أنها مسيرة من طرف كيان واحد هو الذي يقوم بتحديد هوية مستعملي هذه الشبكة[2].

بالإضافة إلى ذلك فإنه غالبا ما يتم اللجوء إلى استعمال رقم سري حتى يتم تحديد هوية الموقع ، وهو ما يخفض بشكل كبير احتمالات التزوير ،بحيث أن هذا الرقم السري عادة ما يتكون من أربعة أرقام وتكون للشخص الحق في ثلاث محاولات فقط[3] .

---

[1] أ/قارة مولود ،التوقيع الإلكتروني كدليل إثبات في القانون الخاص،ماجستير في القانون الخاص ،جامعة فرحات عباس سطيف (الجزائر)،سنة 2004، ص. 16

[2] Didier Gobert et étienne Montero :« La signature dans les contrats et les paiements» ; édition Bruylant Bruxelles , 2000 ; p.62

[3] Anne lise Vilerrubla :«Les apports de la signature électronique» ;www.signelec.com

الفرع الثاني : وظائف التوقيع

متى استوفى التوقيع شروطه التي بينتها التشريعات والفقهاء والقضاء وكانت محتوية على عناصرها ، فإنه يصبح يلعب دورا هاما في الإثبات ، فهو يعني بالضرورة رضا الموقع على ما ورد في السند الكتابي ، كما أنه يؤدي مهام أخرى سندرسه بالتفصيل في هذا الفرع .

أولا: التوقيع هو تعبير عن رضا الموقع بمحتوى السند الكتابي

يعتبر التوقيع في الحقيقة الصورة المثلى للتعبير عن إرادة الموقع والتزامه بما ورد في السند الكتابي ، وإن ذكر اسم شخص في السند لا يعني بالضرورة أنه ملتزم بما ورد فيها فلا يعتبر هذا رضاء من الشخص حتى يوقع على السند ومن دون التوقيع لا يعتبر الشخص طرفا في هذه العلاقة ولا ملتزما بما ورد في السند.

أما إذا تعددت الأطراف فإنه يشترط توقيع كل طرف على حدا ولا يلتزم بها أحد الأطراف إلا إذا وقعها الطرف الثاني كعقد البيع مثلا، أو على الأقل توقيع الطرف الملتزم في حالة العقود الملزمة لجانب واحد مثل عقد الوديعة.

إضافة إلى ذلك فإنه ليس لزاما في الورقة العرفية أن يكون توقيع الأطراف جميعا في وقت واحد أو مكان واحد بل يجوز أن يتم التوقيع في زمان ومكان مختلفين، إلا إذا تبين من الظروف أن أصحاب الشأن إنما أرادوا ألا يرتبطوا إلا بتوقيعهم جميعا[1].

أما الورقة الرسمية فلا يمكن أن نتخيل أن يتم توقيعها من الأطراف في أزمنة وأمكنة مختلفة إذ أنه يشترط في هذه الحالة أن يتم توقيع الأطراف أمام موظف أو ضابط عمومي أو شخص مكلف بخدمة عامة مختص وفق ما تنص عليه المادة 324 من القانون المدني .

---

[1] د-عبد الرزاق السنهوري،المرجع السابق،ص179

بل الأكثر من ذلك فإن المشرع الفرنسي في المادة 1325 من القانون المدني يلزم الأطراف في حالة الالتزامات المتبادلة أن تكون لكل طرف نسخة من السند الكتابي موقعة من طرفهم ، إذ تضمن لكل طرف نفس درجة الأمان من ناحية الإثبات لأن كل منهم يحوز على التزام كتابي من الطرف الأخر، وفي حال العكس فإن ذلك يؤدي إلى جعل أحدهم تحت رحمة الشخص الحائز للدليل الكتابي[1] .

على الرغم من أهمية هذا الإجراء الشكلي من الناحية الإثباتية إلا أنه لم يشترطه المشرع المصري والجزائري الذي اكتفى بتوقيع الأشخاص على السند حتى يكون حجة ضدهم دون أن تكون لكل منهم نسخة .

لكن الأستاذ الغوثي بن ملحة ذهب إلى أن مخالفة هذا الشرط هو بطلان الورقة العرفية باعتبارها دليلا كتابيا ، غير أن هذا البطلان يترتب على المحرر ولا يمس التصرف القانوني ذاته والذي يظل صحيحا ، ويجوز إثباته بطرق أخرى غير الكتابة[2] .

كما اشتراط المشرع الجزائري في نص المادة 327 من القانون المدني المعدل أن يكون التوقيع بيد الموقع دون سواه خاصة في الورقة العرفية التي لا تصلح حتى كمبدأ ثبوت بالكتابة إلا إذا كانت مكتوبة بيد الموقع ، والذي يعني استبعاد استعمال ورق الكربون بما أن هذا الأخير يؤدي إلى تحرير السند بغير يد من تنسب إليه الورقة وهذا في حقيقة الأمر ما هو إلا حماية لرضا الموقع، وإن كانت محكمة النقض المصرية قد خالفت ذلك بأن اعترفت بالتوقيع بالكربون بشرط أن يكون التوقيع منسوبا للطاعن [3].

أما التوقيع الإلكتروني فتحقق هذه الوظيفة بمجرد استعمال مفتاح التشفير بطريقة إرادية وشخصية، بشرط أن يكون هذا التوقيع مرتبط بشكل منطقي بالوثيقة [4]

---

[1] Meme Mostefa-Kara Farida née Settouti, op.cit., p.39

[2] د.الغوثي بن ملحة ، قواعد وطرق الإثبات ومباشرتها في النظام القانوني الجزائري، الطبعة الأولى، مطبوعات الديوان الجزائري للأشغال التربوية ،2001 ،ص 46

[3] الطعن رقم 527 سنة 44 جلسة 1978/1/31 س 29 ص 357 مأخوذ عن المستشار محمد أحمد عابدين،حجية الورقة الرسمية والعرفية،دار الكتب القانونية،سنة1997،ص37

[4] Didier Gobert et étienne Montero ;op.cit ;p 62

ثانيا : مراقبة مدى سلامة الوثيقة ونزاهتها

كلمة السلامة أو النزاهة نادرا ما استعملت في القانون ومعناها تقنيا حالة الشيء الذي يحتوي على جميع أجزائه ولم يتعرض للتغير أو التحويل[1] .

لم يكن الفقه التقليدي قد عالج هذه الوظيفة إذ أنها كانت تؤدى من طرف التوقيع بصفة آلية ليس على أساس وسيلة التوقيع ذاتها وإنما لكون التوقيع بصورته التقليدية يتم فوق دعائم ورقية وهو ما يمنح الورقة الموقعة ضمانات كبيرة نظرا لصعوبة التزوير من جهة ونظرا أن الورق يتم الاحتفاظ به لمدة طويلة .

غالبا ما يتم رقابة مدى نزاهة الوثيقة بمراقبة صحة التوقيع أو الخط وفق ما يعرف بمضاهاة الخطوط، المنصوص عليها في قانون الإجراءات المدنية الجزائري من المواد 76 إلى غاية المادة 80ق إ م .

من خلال استقراء هذه المواد نلاحظ أن المشرع قد ترك السلطة التقديرية للقاضي في إجراء المضاهاة أو عدم إجرائها بحسب أهمية هذا الإجراء في الفصل في النزاع وأثره في الدعوى فإن كان منتجا أقره وإلا صرف النظر عنه .

كما تم تحديد الأوراق القابلة للمضاهاة في المادة 77 ق إ م وهي :

- العقود الرسمية التي تحمل الإمضاءات.
- الخطوط والتوقيعات المعترف بها من الخصم .
- الجزء من المستند الذي لا ينكره الخصم .

وأوراق المضاهاة يؤشر عليها بتوقيع القاضي .

مما يمكن أن نلاحظه من هذه المادة أن جميع الأوراق القابلة للمضاهاة إما أن تحمل توقيع الشخص المنسوبة إليه الورقة أو أن تكون بخطه أو يكون معترفا بها ، وهو ما يظهر

[1] Julien Esnault ;op.cit ;p15

جليا أن حماية الوثيقة أو السند من التزوير وتوفير السلامة والنزاهة فيها لا يتم إلا عبر التوقيع أو الكتابة التي تنسب دون أدنى شك إلى الخصم دون سواه ، وهو ما يتوافق مع شروط التوقيع التي يستوجب فيها أن يكون التوقيع أو الخط بيد من تنسب إليه الورقة.

غير أنه ومع ظهور صور أخرى للتوقيع وخاصة ما يعرف بالتوقيع الالكتروني أصبح التساؤل مطروحا بشدة حول نزاهة الوثيقة الموقعة الكترونيا خاصة في مجال الشبكات المفتوحة، ويرى البعض استحالة تزوير أو تقليد التوقيع الالكتروني نظرا لما وصل إليه من تأمين وحماية[1].

إذ تقضي التعاملات الالكترونية أن يضع المتعاقد أو الموقع مفتاحه الخاص في خانة العرض ويرسله إلى المتعاقد الأخر حتى يتمكن من التأكد من هوية المرسل وتتحقق خاصية التوقيع بصفة عامة[2]، ويستتبع لا حقا أن جهة التصديق على صحة التوقيع سوف تمنح لاحقا شهادة تفيد صحة التوقيع الالكتروني وبالتالي الوصول إلى وثيقة نزيهة وسليمة موقعة الكترونيا.

ثالثا : منح الوثيقة صفة« الأصل»

هناك وظيفة أخرى للتوقيع نادرا ما تم التطرق إليها وهي منح الوثيقة الموقعة صفة الأصل وتمييزها عن النسخة وهو ما يظهر خصوصا في الورقة العرفية التي تستوجب أن تكون مكتوبة أو موقعة من الشخص الذي تنسب إليه.

أما فيما يخص الورقة الرسمية فإنه لا فرق بين الصورة الخطية والصورة الفوتوغرافية ما دامت كلتاهما صورة رسمية، بل لعل الصورة الفوتوغرافية هي الأدق من الناحية الفعلية[3].

---

[1] د-عبد الفتاح بيومي حجازي، المرجع السابق، ص.340

[2] د-عبد الفتاح بيومي حجازي، المرجع السابق، ص.341

[3] د-عبد الرزاق السنهوري ، المرجع السابق، ص.163

كما أن أصل الورقة الرسمية نادرا ما يضيع إذ هو محفوظ دائما في مكتب التوثيق فإن وجد الأصل فإن الصورة تعتبر حجة بالقدر الذي تكون فيه مطابقة للأصل وفق المادة 325 ق م ج.

ويشترط في هذا الفرض شرطان أولهما أن يكون أصل الورقة الرسمية موجودا وثانيهما أن تكون الورقة التي يحتج بها ليست هي الأصل بل صورة من الأصل أما إذا فقد الأصل فإن الصورة تكون حجة على الوجه الآتي :

- يكون للصور الرسمية الأصلية تنفيذية كانت أو غير تنفيذية حجية الأصل متى كان مظهرها الخارجي لا يسمح بالشك في مطابقتها للأصل.

- ويكون للصور الرسمية المأخوذة من الصور الأصلية الحجة ذاتها ولكن يجوز في هذه الحالة لكل من الطرفين أن يطلب مراجعتها من الصورة الأصلية التي أخذت منها.

- أما ما يؤخذ من صور رسمية للصورة المأخوذة من النسخ الأولى فلا يعتد به إلا لمجرد الاستئناس تبعا للظروف[1].

هذا ما يؤدي إلى أن الورقة الرسمية متى كانت أصلية لا تحتاج إلى توقيع حتى نستطيع تمييزها عن النسخة عكس الورقة العرفية التي يعتبر التوقيع فيها عنصرا جوهريا لتمييز النسخة من الأصل.

إلا أنه ومع ظهور الدعائم الالكترونية أصبح من الصعب بمكان تمييز الأصل من النسخة وذلك نظرا لسهولة إعادة طبع ونسخ المعطيات والوثائق الالكترونية.

ولا يمكن في جميع الأحوال أن نتصور أن كل استنساخ لوثيقة الكترونية يمنحها صفة النسخة، كما لا يفهم من كون الوثيقة وحيدة وغير قابلة للنسخ من أنها حتما الأصل، ووجود وسيلة تضمن نزاهة وسلامة الوثيقة لا يكفي بتاتا لمنح الوثيقة صفة الأصل ، وإنما في حقيقة الأمر وجود التوقيع الالكتروني على الوثيقة هو الذي يمنحها هاته الصفة، فبمجرد أن يكون التوقيع مرتبطا بالوثيقة مع إمكانية مراقبة مدى سلامة التوقيع فإن هذه الوثيقة تعتبر أصلا[2].

---

[1] هذه الحالات مذكورة في المادة 326 ق م ج.

[2] Didier Gobert et étienne Montero , op.cit ; p.67

نجد أن المشرع المصري قد تبنى هذا الموقف في المادة 16 من قانون التوقيع الإلكتروني والتي تنص:«الصورة المنسوخة على الورق من المحرر الإلكتروني الرسمي حجة على الكافة بالقدر الذي تكون فيها مطابقة لأصل هذا المحرر، وذلك مادام المحرر الإلكتروني الرسمي والتوقيع الإلكتروني موجودين على الدعامة الإلكترونية »، ولا تعتبر النسخة في هذه الحالة إلا كبداية ثبوت بالكتابة أو مجرد قرينة بسيطة فقط.

كما يجب التمييز في هذه الحالة بين الكتابة الأصلية والدعامة الأصلية، إذ أن الكتابة لا تفقد صفة الأصل إذا ما وجدت في غير الدعامة التي كتب بواسطتها[1].

سنلاحظ لاحقا أنه على الرغم من وجود عدة أنواع من التواقيع الالكترونية إلا أن التوقيع الرقمي(الالكتروني) يبقى هو الوحيد الذي باستطاعته أن يضفي وبكل جدارة صفة الأصل على الوثيقة الالكترونية دون سواها باعتبار أن هذا النوع من التوقيع قد أصبح محاطا بمجموعة من النصوص القانونية التي تحميه وتجعله في نفس درجة التوقيع التقليدي كما أن هناك عدة وسائل تقنية تجعل من الصعب تزويره ، بل من السهل تزوير التوقيع التقليدي مقارنة بالتوقيع الالكتروني.

المطلب الثاني: نطاق حجية التوقيع في الإثبات

إن التوقيع يهدف أساسا إلى إثبات واقعة معينة أو تصرف قانوني وهذا الأخير اشترط الفقه شروطا معينة يجب أن تتوفر فيه وهو ما سنتطرق إليه في الفرع الأول.

فإذا ما استوفى محل الإثبات تلك الشروط فإنه يمكن إعمال التوقيع في الأوراق سواء منها الرسمية أو العرفية (الفرع الثاني)

[1] Stéphane Caïdi «:La preuve et la conservation de l'écrit dans la société de l'information» ; UNIVERSITÉ DE MONTRÉAL Faculté des études supérieures ; 2002 ;p.17

الفرع الأول : شروط الواقعة مراد إثباتها

يكاد الفقهاء[1] يتفقون على الشروط التي يجب أن تتوافر في محل الإثبات وقد قسمها البعض منهم إلى شروط بديهية وشروط أساسية وهي:

1- الشروط البديهية:

يجب أن تكون الواقعة محددة تحديدا كافيا لا إبهام فيه، فالإقناع لا يرد على أمر مبهم أو ليست له حدود[2]، فالمالك مثلا عليه أن يقيم الدليل على واقعة معينة كانت سببا في ملكيته له كعقد شراء مع تبيان نوعه ومحله كأن يذكر أنه عقد بيع سيارة معينة بأوصافها وأن يعين تاريخه وإن كان وفاء بدين وجب بيان زمانه ومكانه وأصل الدين الموفى به ومقداره.

زيادة على ذلك يلزم أن يكون تحديد الواقعة عند نظر القاضي في أمر إثباتها سواء تم تعيينها في عريضة الدعوى أم في مذكرات الخصوم المقدمة في الدعوى أم في طلب الإحالة إلى التحقيق إلخ...[3]

كما أن الواقعة محل الإثبات إما أن تكون ايجابية والتي يمكن إثباتها من طريق مباشر مثاله إثبات حصول التعاقد أو الوفاء كما في الأمثلة السابقة؛ أوقد تكون الواقعة سلبية يمكن إثباتها بأمر منافي لها فإذا أراد الطبيب مثلا أن يثبت عدم تقصيره في علاج المريض فإنه يكفي أن يقيم الدليل على أنه قام بكل ما يفرضه واجب العلاج وأنه اتخذ في ذلك كل الاحتياطات اللازمة[4] .

كون الواقعة محددة تحديدا كافيا مسألة موضوعية تخضع لرقابة قاضي الموضوع.

---

[1] أنظر في ذلك د-سليمان مرقس، المرجع السابق، ص 62 وما بعدها ود-جلال علي العدوي ،الإثبات،منشأة المعارف بالاسكندرية-سنة1996،ص317 وما بعدها ود-عبد الفتاح بيومي حجازي، المرجع السابق، ص 373 وما بعدها

[2] د-سليمان مرقس، المرجع السابق، ص63

[3] د-سليمان مرقس، المرجع السابق، ص63وص64

[4] د-سليمان مرقس، المرجع السابق، ص65

لكن هذا لا ينفي أن الواقعة غير المحددة يمكن إثباتها باليمين أو الإقرار ولا يجوز إثباتها بغيرها من الأدلة[1]، وهو ما ينتج عنه في هذا الفرض عدم إمكانية إثبات الواقعة بالكتابة وبالتالي استبعاد التوقيع لكونه مرتبط بالكتابة.

فإن صح أن الواقعة غير محددة لا يمكن إثباتها فإن هذا يؤدي حتما إلى استحالة إثباتها وبالتالي يتلاقى الشرطان ويصبحان شرطا واحدا فالواقعة يجب أن تكون محددة وإلا فإنها تصبح مستحيلة الإثبات.

الاستحالة في هذه الحالة ترجع إما إلى عدم تصديقها عقلا كمن يدعي بنوة شخص لأخر يصغره سنا أو كالأعمى الذي يدعي أنه رأى هلال رمضان أو مورث المدعى قد صدمه بسيارته في تاريخ ثبت أن المورث المذكور كان قد مات قبله ،أو ترجع إلى أن الواقعة قابلة للتصديق عقلا ولكن لا سبيل إلى إثباتها كالشخص الذي يدعي أنه لم يكن مدانا طوال حياته، إذ أن إثبات المستحيل عبث فلا يجوز السماح بها حرصا على وقت المحكمة وهيبتها من الضياع.

تعتبر مسألة إمكان الواقعة أو استحالتها ترجع لتقدير قاضي الموضوع باعتبارها من المسائل الموضوعية ولا رقابة لقاضي القانون عليها إلا فيما يخص بتسبيب الحكم [2].

إضافة إلى ذلك يشترط أن تكون الواقعة مراد إثباتها متنازعا حولها أما إذا كانت ثابتة بطبيعتها كساعة شروق الشمس أو معترفا بها من الخصم فلا جدوى من إثباتها وإضاعة وقت المحكمة من التحقق فيها.

فيتحدد مجال الواقعة المتنازع حولها بادعاء المدعي وجواب المدعى عليه فإن وافق الجواب الإدعاء انتفت المنازعة[3] وإن خالف الإدعاء جواب المدعى عليه كان النزاع شاملا

---

[1] د.جلال علي العدوي ،المرجع السابق،ص.318
[2] د.سليمان مرقس، المرجع السابق، ص.66و67
[3] د.سليمان مرقس، المرجع السابق، ص.67

أما إذا خالفه في جزء منه ووافقه في جزء أخر أستبعد الجزء المتفق عليه ، بشرط أن يكون التسليم قاطعا وشاملا وغير مخالف للنظام العام.

2- الشروط الأساسية:

سنتعرض الآن للشروط الأساسية المذكورة في المادة 61 ق إ م بقولها: «يجوز الأمر بالتحقيق لإثبات الوقائع التي تكون بطبيعتها قابلة للإثبات بشهادة الشهود، والتي يكون التحقيق فيها جائزا ومنتجا في الدعوى»

حيث رأى المشرع أنها تكتسي أهمية بالغة ويجب على أطراف الدعوى متى أرادوا إثبات واقعة معينة أن يحترموا هاته الشروط وهي :

أ-أن تكون الواقعة متعلقة بالدعوى :

زيادة على المشرع الجزائري الذي أقر هذا الشرط نجد أن معظم التشريعات نصت عليه منها مثلا المشرع المصري في المادة 2 من قانون الإثبات والمادة 4 من قانون البيانات الأردني ولم ينص عليه المشرع الفرنسي.

المقصود بهذا الشرط أن يكون الأمر المراد إثباته مرتبطا ارتباطا وثيقا بالدعوى خاصة إذا كان مصدر الحق أو واقعة مرتبطة بمصدر الحق ومؤثرة فيه، وبالتالي استبعاد كل الوقائع التي لا صلة لها بالدعوى أولا أثر لها على الموضوع ، فإذا طالب المؤجر المستأجر باجرة شهر معين فلا يجوز لهذا الأخير أن يثبت أنه قد وفى بأجرة الأشهر السابقة ولكن يجوز له أن يثبت أنه قد أنفق أجرة الشهر في ترميمات تقع على عاتق المؤجر[1] .

تبرز أهمية هذا الشرط عند لجوء المدعي إلى طريق الإثبات غير المباشر أي إثبات واقعة أخرى تسمح باعتبار الواقعة المدعاة ثابتة فيشترط فيها أن تكون ذات صلة قوية بالواقعة الأصلية وقريبة الاحتمال وهو ما يعرف بفكرة «تحويل الدليل»[2].

---

[1] د-سليمان مرقس، المرجع السابق،ص .69

[2] د-عبد الرزاق السنهوري،المرجع السابق،ص.61

ب-أن تكون الواقعة منتجة في الدعوى:

المقصود بهذا الشرط أن يكون من شأن إثبات الواقعة تأثير على الحكم الذي يصدر في الدعوى فإن لم يؤثر فيها فإنه لا حاجة لإثبات هذه الواقعة.

لا يلزم أن تكون هذه الواقعة منتجة لوحدها في الدعوى بل يكفي أن تكون منتجة إذا تضافرت معها وقائع أخرى[1].

إلا أنه يصعب الأمر في حالة الدعاوى التي يجيزها القانون لمجرد تقرير واقعة للاستدلال مثل أمر بإثبات حالة المنصوص عليه في المادة 172 ق إ م ، فيجب أن تكون الواقعة المثبتة في هذه المحاضر منتجة في الدعوى .

ففي حال ما إذا تم رفع دعوى على أساس عيب في المبيع وتم تحرير محضر إثبات حالة بذلك فلا قيمة له في البيوع القضائية والإدارية والبيع بالمزاد العلني لأنه لا ضمان للعيوب في هذه البيوع ، وبالتالي تصبح الواقعة غير منتجة في الدعوى .

تختلف رقابة محكمة الموضوع عن محكمة القانون فيما تفصل فيه بحسب ما إذا كانت الواقعة مرتبطة بالدعوى ارتباطا مباشرا أو غير مباشر ، فإن كانت الواقعة غير مباشرة فإن محكمة الموضوع تفصل فيه على أساس أنه مسألة موضوعية، لا رقابة لمحكمة القانون عليه إلا على أساس التسبيب أو خطأ قانوني، أما إذا كانت الواقعة مباشرة فإن محكمة الموضوع تفصل فيه باعتباره مسألة قانونية ومن ثم يخضع لرقابة محكمة القانون .

غير أنه قد يتساءل البعض عن جدوى التمييز بين الشرطين بما أن أحدهما مستغرق للأخر، وهو صحيح من الناحية النظرية إلا انه يستحسن من الناحية العملية التمييز بينهما.

فقد يطلب الخصم إثبات واقعة يتضح من أول وهلة أنها متعلقة بالدعوى فهذا يكفي لقبول إثبات هذه الواقعة قبولا مبدئيا حتى تبين فيما بعد أنها غير منتجة في الإثبات رفض

---

[1] د-جلال علي العدوي ،المرجع السابق،ص326

القاضي استمرار السير في إثبات الواقعة أو أضاف إليها وقائع أخرى تتساند معها، أما إذا أدمج الشرطان في شرط واحد وكان لا بد من أن تكون الواقعة منتجة من مبدأ الأمر لم يستطع القاضي قبول إثبات الواقعة قبولا مبدئيا فيتعطل بذلك طريق الإثبات[1].

فكل واقعة منتجة في الدعوى تكون حتما متعلقة بها، ولكن العكس غير صحيح، إذ ليس بالضرورة أن كل واقعة متعلقة بالدعوى تكون منتجة فيها[2].

ج-أن تكون الواقعة جائزة الإثبات قانونا:

أخيرا يشترط في الواقعة أن تكون جائزة الإثبات وقد يكون ذلك لمانع قانوني أو طبيعي[3].

فالمانع الطبيعي هو الذي يجعل الواقعة مستحيلة الوقوع كما هو الشأن في طلب إثبات بنوة شخص لأخر يصغره سنا، وإن كان هناك بعض الفقهاء لا يورد هذه الحالة لكونها مرتبطة بشرط أخر بديهي هو أن تكون الواقعة غير مستحيلة، فالمستحيل حدوثه لا يجوز قبول إثباته[4].

أما المانع القانوني فهو عدم جواز إثبات الواقعة لسبب قانوني مثل عدم جواز إثبات الوقائع التي تشملها حجية الأمر المقضي فيه.

يمكن توسيع الأمر إلى مقتضيات النظام العام والآداب العامة فلا يجوز إثبات دين القمار أو إفشاء سر المهنة والمعاشرة الغير مشروعة.

تقدير كون الواقعة جائزة الإثبات قانونا من مسائل القانون التي يخضع فيها قاضي الموضوع لرقابة محكمة النقض[5] .

---

[1] د-عبد الرزاق السنهوري،المرجع السابق،ص.63

[2] د-عبد الفتاح بيومي حجازي، المرجع السابق،ص.379

[3] أنظر في ذلك د-جلال علي العدوي ،المرجع السابق،ص.327 وما بعدها

[4] د-جلال علي العدوي ،المرجع السابق،ص.328

[5] د-عبد الفتاح بيومي حجازي،المرجع السابق، ص381

الفرع الثاني :مجال إعمال التوقيع

إذا ما توافرت في الواقعة المراد إثباتها الشروط المذكورة أنفا، فإنه يمكن إثباتها كتابة سواء كانت كتابة رسمية أو عرفية، ولا يتصور صحة هذه الكتابة من دون أن تحتوي على التوقيع .

لكن على الرغم من صحة التوقيع وتوافر الشروط اللازمة للواقعة محل الإثبات إلا أن هذا لا يعد كافيا ، بل يفرض القانون في الورقة العرفية أو الرسمية توافر عناصر أخرى حتى يكون التوقيع صحيحا.

وعلى هذا الأساس فإننا سنتطرق إلى إعمال التوقيع في الورقة العرفية باعتباره عنصرا أساسيا فيه ثم التطرق إليه في الورقة الرسمية وأخيرا حالات الإثبات دون وجود عنصر التوقيع.

1-التوقيع في الورقة العرفية :

لقد رأينا الأهمية البالغة للتوقيع في الورقة العرفية فهي لا تكتسب حجيتها إلا بتوقيع الأطراف عليها ، وعلى الرغم من ذلك فإن المشرع اعتبر ذلك غير كافي لإضفاء الحجية على الورقة العرفية سواء اتجاه المتعاقدين أو الورثة أو الغير وهو ما سندرسه إتباعا.

أولا :حجية التوقيع اتجاه المتعاقدين: تنص المادة 327 من القانون المدني الجزائري على : «يعتبر العقد العرفي صادرا ممن كتبه أو وقعه أو وضع عليه بصمة إصبعه ما لم ينكر صراحة ما هو منسوب إليه ...»

من خلال هذه المادة نستنتج أن التوقيع على الورقة العرفية كمبدأ عام كافي لتكون الورقة حجة على أطراف إلى أن يثبت العكس ، أما الكتابة غير الموقعة لا تعدوا إلا أن تكون

مشروعا يحتمل الاعتماد عليه أو عدمه[1] ،وهو ما نصت عليه المادة 363 من قانون الموجبات اللبناني :«العقد الخطي الذي يكتب عند التعاقد لا يكتسب قوة الإثبات التامة إلا إذا وقعه المتعاقدون».

كما أقرته محكمة النقض المصرية بقولها:«لما كان قانون الإثبات في المادة 14 منه يعتبر المحرر العرفي صادرا ممن وقعه ما لم ينكر صراحة ما هو منسوب إليه من خط أو إمضاء أو ختم أو بصمة ، بما مؤداه أن ثبوت صحة التوقيع يكفي لإعطاء الورقة العرفية حجيتها في أن صاحب التوقيع قد ارتضى مضمون الورقة والتزم به ، فإذا أراد نفي هذه الحجية بادعائه اختلاس التوقيع منه كرها وغشا أو أن الورقة كانت موقعة على بياض وحصل عليها المتمسك بها بغير رضاه ،كان على صاحب التوقيع إثبات ما يدعيه»[2] .

اشترط المشرع المصري والجزائري أن يكون الإنكار صريحا من الموقع و أن مجرد سكوته يعتبر إقرارا منه بصحة توقيعه ومن ناقش موضوع السند لا يقبل منه إنكار الخط أو التوقيع أو البصمة[3]، ولا يجوز لصاحب التوقيع في هذه الحالة إلا أن يطعن بالتزوير[4].

أما إذا أنكرها الموقع صراحة سواء كلها أو جزء منها فعلى المحتج بها أن يحيلها إلى القضاء وفق إجراءات التحقيق[5] ، أما في حالة إدعاء الموقع تزوير توقيعه فإنه يقع عليه عبء إثبات التزوير.

ثانيا حجية التوقيع اتجاه الغير: والمقصود بالغير هو كل شخص يجوز أن يسري في حقه التصرف القانوني الذي تثبته الورقة العرفية وهو بوجه عام الخلف الخاص والخلف العام والدائن.

---

[1] د-سليمان مرقس، المرجع السابق،ص233

[2] نقض 1982/1/28 طعن رقم 664 لسنة 47 قضائية مأخوذة من عبد العزيز سليم،شرح قانون الإثبات ،طبعة 1998، ص 72

[3] وهو ما نصت عليه المادة 151 من قانون أصول المحكمات المدنية اللبناني والفقرة الثانية من المادة 14 قانون إثبات مصري.

[4] د-عبد الرزاق السنهوري، المرجع السابق،ص189

[5] الواردة في قانون الإجراءات المدنية الجزائري من المواد 76 إلى 80 ق إ م

يكفي على الورثة أن يحلفوا يمينا بأنهم لا يعلمون أن الخط أو الإمضاء أو البصمة هو لمن تلقوا منه هذا الحق [1] ، وبالتالي يقع على من يحتج بالورقة العرفية إثبات صحة التوقيع الوارد فيها بموجب إجراءات تحقيق الخطوط .

وقد قضت المحكمة العليا في قرارها الصادر بتاريخ 1985/02/06 عن الغرفة المدنية بأن إثبات عقد عرفي دون توجيه اليمين للورثة مخالفة للقانون ومتى كان ذلك استوجب نقض وإبطال القرار المطعون فيه[2]

أما إذا بدأ الورثة أو الخلف في مناقشة الموضوع فإن ذلك يؤدي إلى سقوط حقهم في الدفع بعد ذلك بجهالة توقيع المورث أو السلف وإنما عليه في هذه الحالة أن يسلك طريق الطعن بالتزوير[3]

كما أن وفاة أحد الذين لهم على العقد خط أو إمضاء في الورقة العرفية يجعلها تكتسب التاريخ الثابت وفق المادة 328 من القانون المدني الجزائري، ولا يشترط توقيع الشخص باعتباره متعاقدا بل يكفي توقيعه عليها باعتباره شاهدا[4].

2-التوقيع في الورقة الرسمية :

بداية يجب أن لا نحصر مهمة إصدار الأوراق الرسمية في الموثق أو ضابط الحالة المدنية فقط، بل يدخل في هذا المجال القاضي أثناء إصداره للأحكام القضائية ومحاضر الخبراء عند انتدابهم قضائيا[5] .

---

[3] المادة 327 فقرة 1 من القانون المدني الجزائري التي تنص :«يعتبر العقد العرفي صادرا ممن كتبه أو وقعه أو وضع عليه بصمة إصبعه ما لم ينكر صراح ما هو منسوب إليه ،أما ورثته أو خلفه فلا يطلب منهم الإنكار ويكفي أن يحلفوا يمينا بأنهم لا يعلمون أن الخط أو الإمضاء أو البصمة هو لمن تلقوا منه هذا الحق»

[2] أ.بن شنات صالح ،الكتابة كدليل إثبات في المواد المدنية ، رسالة ماجستير في القانون الخاص ، جامعة السانيا وهران ، ص .89

[3] د.محمد حسن قاسم،الإثبات في المواد المدنية والتجارية،ص169،الدار الجامعية

[4] د.الغوثي بن ملحة ، المرجع السابق، ص. 49

[5] Meme Mostefa-Kara Farida née Settouti, op.cit., p.43

فعندما يقوم الضابط العمومي أو الشخص المكلف بالخدمة العامة بتحرير ورقة رسمية يجب أن تحتوي على التوقيع إذ أن المشرع الجزائري فرض في المادة 324 مكرر 2 فقرة 1 من القانون المدني أن توقع العقود الرسمية من قبل الأطراف والشهود عند الاقتضاء ، ويؤشر الضابط العمومي على ذلك في أخر العقد.

فتوقيع الأطراف هو تعبير خارجي عن رضاهم بمحتوى الورقة الرسمية، أما توقيع الشهود والموثق فإنه في الحقيقة لا يلعبون فيه إلا دور شهود مميزين[1].

وفي حالة إذا كان أحد الأطراف أو الشهود لا يستطيع التوقيع فيضع بصمته إلا إذا وجد مانع قاهر كأن تكون يده مقطوعة أوبها عاهة يبين الضابط العمومي ذلك في أخر العقد[2]؛ وقد تبنته المادة 29 من قانون التوثيق المؤرخ في 2006/02/20 التي جعلت من توقيع الأطراف والشهود والموثق والمترجم (عند الاقتضاء) من البيانات الإجبارية التي يجب أن يتضمنها العقد.

بل الأكثر من ذلك اشترط المشرع الجزائري في المادة 324 مكرر3 من القانون المدني أن تكون العقود الاحتفائية بحضور شاهدين؛ وبالتالي توقيعها من طرفهم إذ لا يتصور حضور الشاهدين دون توقيعهم وهو يتفق بما ورد في المادة 324 مكرر 2 من نفس القانون.

نصت المادة 26 الفقرة الثانية من قانون التوثيق أنه يصادق على الإحالات في أسفل الصفحات وعلى عدد الكلمات المشطوبة في العقد بالتوقيع بالأحرف الأولى من قبل الموثق والأطراف وعند الاقتضاء الشهود والمترجم؛ والهدف من هذا الإجراء هو التأكد من علم الجميع بوجود هذه الهوامش حتى لا يدعي أحد منهم بعدم علمه بها ،وإبعاد شبهة التزوير

---

[1] Delphine Majdanski ;op.cit ;p48

[2] وهو ما تنص عليه المادة 324 مكرر 2 فقرة 2 بقولها :«وإذا كان بين الأطراف أو الشهود من لا يعرف أو لا يستطيع التوقيع يبين الضابط العمومي في أخر العقد تصريحاتهم في هذا الشأن ويضعون بصماتهم ما لم يكن هناك مانع قاهر.»

عنها، وفي حال إخلال الموثق بهذا الواجب فإنه يتعرض للعقوبات التأديبية الواردة في المادة 54 من نفس القانون [1]

أعطت المادة 38 من قانون التوثيق إمكانية حيازة الموثق على طابع وختم خاص به يسلم له من طرف وزير العدل والأختام وهو المعمول به حاليا ولكن بشرط أن يودع توقيعه وعلامته لدى كتابة الضبط لمحكمة محل إقامة المكتب والغرفة الجهوية للموثقين.

أما في حال وفاة الموثق أو وقوع مانع وعدم توقيعه على الورقة الرسمية وكان جميع الأطراف والشهود قد وقعوا عليها منحت المادة 36 من قانون التوثيق إمكانية توقيع الورقة الرسمية من قبل موثق أخر بموجب أمر من رئيس المحكمة بناءا على طلب الأطراف وتعبر كأنها وقعت من طرف الموثق المتوفى.

على الرغم من أهمية التوقيع في الورقة الرسمية إلا انه يجب أن تتوافر بجانبها شروط أخرى أوجبها المشرع حتى تكون لهذه الورقة الصفة الرسمية وهي :

- صدور الورقة الرسمية من موظف عام أو ضابط عمومي أو شخص مكلف بخدمة عامة.
- أن يكون هذا الموظف العام أو الضابط العمومي أو الشخص المكلف بخدمة عامة مختصا بتحرير الورقة الرسمية من حيث الموضوع والمكان وفي حدود سلطته.
- مراعاة الأوضاع التي قررها القانون لتحرير الورقة الرسمية.

أما إذا أصبحت الورقة الرسمية باطلة لعدم توافر الشروط القانونية المذكورة سابقا فتتحول إلى ورقة عرفية بشرط أن تكون موقعة من الأطراف[2].

كما تجدر الإشارة إلى توقيع الأطراف في الورقة الرسمية يعتبر من البيانات التي تدخل في حدود مهمة الموظف العام وهي بالتالي حجيتها تبقى قائمة إلى أن يطعن فيها بالتزوير[3].

---

[1] هذه العقوبات هي :الإنذار، التوبيخ ، التوقيف عن ممارسة المهنة لمدة أقصاها 6 أشهر، العزل

[2] لمزيد من التفاصيل أنظر أبن شنات صالح ،المرجع السابق، ص 43 وما يليها .

[3] أبن شنات صالح ، المرجع السابق ،ص65

المبحث الثاني: مكانة التوقيع الالكتروني في الإثبات

رأينا في المبحث الأول أهمية ودور التوقيع التقليدي في الإثبات سواء كان ذلك في الورقة العرفية أو الرسمية

غير أنه ومع الطفرة التكنولوجية الهائلة التي يعيشها العالم واعتماد الأفراد على الكمبيوتر والانترنيت لإبرام مختلف العقود، أصبح التوقيع بصورته التقليدية لا يلبي حاجات الأفراد.

إلا أن أهم عيب يميز شبكة الأنترنيت والمعاملات الإلكترونية على العموم هي مشكلة الأمن والخصوصية.

أصبحت هذه المشكلة تثير قلق الكثير من الناس مما يسبب نوعا من انعدام الثقة في شبكة الانترنيت، فكان التوقيع الالكتروني المنفذ لحل هذه الإشكالية ، وبالتالي أصبح لزاما إعادة النظر في القواعد العامة للإثبات الخطي بإدخال التوقيع الإلكتروني كوسيلة إثبات جديدة تتلاءم مع التطور الذي نعيشه في وقتنا الحاضر (المطلب الأول).

مع مرور الوقت أصبح التوقيع الالكتروني ظاهرة لا يمكن تفاديها أو تجاهلها فتم إقرارها في العديد من الدول ولكن هل هذا يعني أن له نفس حجية التوقيع التقليدي ؟ وهو ما سنجيب عنه في المطلب الثاني.

المطلب الأول: ضرورة إعادة التعريف بالإثبات الخطي

لقد كان القضاء الفرنسي من الأوائل الذي أقر حجية الوسائل الحديثة وهذا في حكم صادر من محكمة النقض الفرنسية التي اعترفت بالتوقيع الالكتروني الذي يصاحب عملية

السحب على أساس وجود اتفاق بين البنك والعميل يعطي لهذا الأخير الحق في إثبات تصرفات العميل استنادا إلى التسجيلات التي بحوزة البنك[1].

يقر غالبية الفقهاء أن قواعد الإثبات لا تتعلق بالنظام العام بل بالمصلحة الشخصية للأفراد وبالتالي تجيز لهم الاتفاق على مخالفة الأحكام العامة للإثبات[2] ، إلا أن هذه الإرادة تبقى مقيدة خاصة في العلاقات التي تربط المحترفين بالمستهلكين فلا يجب أن تحتوي اتفاقيتهم على شرط تعسفي[3].

نلاحظ أن إقرار حجية التوقيع الإلكتروني في تشريعات الدول تختلف طرقه من دولة إلى أخرى فنجد مثلا أن المشرع الألماني مثلا قد سن قانونا خاصا بالتوقيع الإلكتروني في ماي 2001، بينما المشرع الفرنسي اتجه أولا إلى إدخاله في قواعد القانون المدني بموجب المادة 4-1316ثم بعد ذلك أصدر مرسوم 30 مارس 2001 المتعلق بالتوقيع الإلكتروني[4] .

انتهجت الجزائر نفس الطريق الذي اتبعه المشرع الفرنسي حيث اعترف مؤخرا بحجية التوقيع الالكتروني ومعها الكتابة الكترونية في القانون المدني[5]، ومن المنتظر إصدار مرسوم تنظيمي في هذا الشأن.

الملاحظ أن التوقيع الإلكتروني ما هو إلا صورة من صور الكتابة الإلكترونية، وهو ما يستلزم بالضرورة المساواة بين الكتابة الخطية والكتابة الإلكترونية (الفرع الأول)

---

[1] CA Montpellier,1re ch.,9avril 1987, confirmé par Cass.civ.,1re ch., 8 novembre 1989 -, Sté Crédicas, *Bull.civ.*I.no 342., cité par Alain Bensoussan et Yves le roux :« Cryptologie et signature électronique aspects juridiques», Hermes Science Publication, Paris, 1999, p.79

[2] د-عبد الرزاق السنهوري، المرجع السابق، ص94 وما يليها

[3] Guenièvre Bordinat :« Introduction à la notion de signature électronique» ; www.signelec.com

[4] Béatrice jaluzot :«Transposition de la directive signature électronique:comparaison franco-allemande» ,Recueil Dalloz,2004,No 40

[5] المادة 327 فقرة 2 من القانون المدني التي تنص على الأخذ بالتوقيع الالكتروني والمادة 324 مكرر1 التي تقربالمساواة بين الكتابة على الورق والكتابة الالكترونية.

كما يبقى التوقيع الإلكتروني على الرغم من أهميته ودوره الكبير في التعاملات الإلكترونية مجهولا لدى الكثير من الناس، ولهذا سنحاول تعريفه في الفرع الثاني.

وهل إقرار حجية التوقيع الالكتروني يعني الأخذ بكل أنواعه على سبيل الإطلاق؟(الفرع الثالث) .

الفرع الأول:المساواة بين الكتابة الخطية والكتابة الإلكترونية

لقد قد كانت الكتابة ومنذ زمن بعيد ترتكز على الدعامة الورقية وتعبر المجال الطبيعي لها، ولذلك كان متفق عليه أن الكتابة المقصودة في الإثبات هي التي تتم على الورق.

إلا أن ظهور الانترنيت واعتماد الأفراد عليها لما توفره من سرعة في التعامل ومن قدرة على شراء السلعة بأقل ثمن [1] ،حتم على المشرعين والفقهاء الاهتمام بهذا المجال حيث لم يصبح الورق أفضل وسيلة لإبرام هذه التصرفات بل ظهرت إلى جانبها ما يعرف بالكتابة الإلكترونية،وإن كان الأستاذ Eric Caprioli يفضل مصطلح «الكتابة بالشكل الإلكتروني» على عبارة «الكتابة الإلكترونية» إذ هي ليست إلا عبارة عن شكل من أشكال الكتابة [2]

وقع جدل فقهي كبير حول مسألة الإثبات بالوسائل الحديثة بصفة عامة والكتابة الإلكترونية بصفة خاصة، وبرزت ثلاث اتجاهات حاولت معالجة هذه المسألة.

هناك من دعا إلى إقرار حجية الوسائل الحديثة ومعها الكتابة الإلكترونية عن طريق الاتفاق وهو ما سماه الأستاذان Didier Gobert et étienne Montero «الطريق الإتفاقي»[3]، حيث بموجبها يتفق الأطراف أنه في حال وجود نزاع بينهما فإن الكتابة الإلكترونية تكون حجة فيما بينهما وغالبا ما تكون هذه النوعية من الاتفاقيات في المعاملات

---

[1] -محمد الأمين الرومي،المرجع السابق،ص.21

[2] Eric caprioli :«,le juge et la preuve électronique, juriscom.net, 10 janvier 2000

[3] Didier Gobert et étienne Montero ,op.cit.,p.54et 55

البنكية والشبكات المغلقة، ويشترط في هذه الحالة أن يكون الطرفين قد تعاملا مع بعضهما البعض سابقا.

أما برأي البعض الأخر فإن إقرار حجية الكتابة الإلكترونية يفرض تعديلا شاملا للقواعد القانونية المتعلقة بالإثبات ،بل إن هناك من اقترح أن يتم استبعاد الكتابة التقليدية كليا ضمن قواعد الإثبات واستبدالها بنظام الإثبات الحر[1] ،وفي هذه الحالة فإن كل وسائل الإثبات تكون على نفس قوة درجة الإثبات،وهو ما كان يسعى إليه المحترفون الذين يستخدمون أنظمة الإعلام الآلي من أجل تسيير الأنظمة الآلية للدفع أو لإبرام العقود الإلكترونية[2]

أما الاتجاه الثالث فيرى أن قواعد الإثبات الحالية تستوعب بشكل كامل الكتابة الإلكترونية ولسنا بحاجة إلا للتفسير السليم لتلك القواعد، فالمقصود بالكتابة في الإثبات ليست فقط الكتابة الخطية بل تشمل كذلك الكتابة الإلكترونية وهو ما سار عليه المشرع التونسي أثناء تعديله لمجلة الالتزامات والعقود [3] .

فيما يخص المجال الدولي فتعتبر لجنة الأمم المتحدة لقانون التجارة الدولية[4] الأولى التي نبهت الدول إلى أهمية الاعتراف بحجية وسائل الإثبات الحديثة، وضرورة المساواة بين الكتابة الخطية والكتابة الإلكترونية عندما أصدرت قانون التجارة الإلكتروني حيث أوصت اللجنة الدول في هذا القانون مراعاة بعض الضوابط التالية:

أ-إعادة النظر في القواعد القانونية التي تمثل عائقا في استخدام الوسائط والدعامات الإلكترونية كأدلة في الدعاوى القضائية.

ب- توفير الوسائل المناسبة التي تمنح البيانات حجية ومصداقية أمام الأطراف والقضاء.

---

[1] قد تم إقرار هذا المبدأ في القانون المدني الهولندي في سنة 1988.

[2] Jérôme Huet: «le code civil et les contrat électronique», www.actoba.com

[3] أ/علي كحلون،المرجع السابق،ص. 245

[4](بالإنجليزيةUNICTRAL) و(بالفرنسيةCNUDCI)

ج- ضرورة إعادة النظر في القواعد القانونية الخاصة بالكتابة والتوقيع وحجيتهما في الإثبات.

لم تكتفي هذه اللجنة بإصدار قانون التجارة الإلكتروني، بل أتبعته بقانون نموذجي بشأن التوقيعات الإلكترونية سنة 2001 ومنحت بموجبه الحجية الكاملة للتوقيع الإلكتروني قصد مسايرة مستجدات التجارة الإلكترونية[1].

كما لم يقتصر الاعتراف بحجية الكتابة الإلكترونية على لجنة الأمم المتحدة بل شمل كذلك الإتحاد الأوروبي عندما أصدر التعليمة المتعلقة بالتوقيع الإلكتروني حيث يمكن للأشخاص أن يبرموا عقودهم بالشكل الإلكتروني شريطة أن تكون هذه العقود موقعة إلكترونيا[2] .

أما على مستوى الدول فقد كانت فرنسا السباقة في هذا المجال التي اعترفت بالكتابة الإلكترونية في المادة 1316من القانون المدني حيث نصت :«الإثبات الخطي أو الإثبات بالكتابة ينتج عن تتابع للحروف ،للخصائص ، للأرقام ولكل رمز أو إشارة مخصصة لعلامة مفهومة واضحة أيما كانت دعامتها وشكل إرسالها»، وهو تقريبا نفس التعريف الموجود في القانون المدني الجزائري في المادة 323 مكرر التي تنص :«ينتج الإثبات بالكتابة عن تسلسل حروف أو أوصاف أو رموز ذات معنى مفهوم ،مهما كانت الوسيلة التي تتضمنها، وكذا طرق إرسالها»

غير أنه يجب أن تتوافر في هذا النوع من الكتابة شروط معينة حتى يتم قبولها كوسيلة إثبات أمام القضاء، فالمشرع الفرنسي لم يهتم بالدعامة التي تكون فيها الكتابة الإلكترونية فقد

---

[1] د-سعيد سيد قنديل،التوقيع الإلكتروني بين التدويل والاقتباس، دار الجامعية الجديدة للنشر2004،ص.18.

[2] Directive 1999/93/CE Du parlement européen et du conseil du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques.

تكون في أقراص لينة أو أية واسطة إلكترونية وإنما يجب أن تكون الكتابة مفهومة وقابلة للقراءة وأن يتم حفظها بشكل آمن ودائم مع إمكانية التصرف فيها بطلبها والاستدلال بها[1].

أن يتضمن الدليل كتابة أي أن تكون البينة الإلكترونية رسمية أو عرفية متضمنة كتابة مثبتة لتصرف قانوني ، ولا يشترط في هذا المجال أن تكون فوق دعامة مادية محددة بالذات، يضاف إلى ذلك أن تكون هذه الكتابة مقروءة ومفهومة بشكل قطعي من طرف الجميع[2].

نجد هذه الشروط في المادة 1316 فقرة 1و3 من القانون المدني الفرنسي التي تنص على أنه :«يقبل السند الإلكتروني بالمقدار نفسه لقبول الكتابة القائمة على سند ورقي شريطة أن يمكن من تعيين الشخص الذي ينسب إليه ،ويكون قد نظم وتم حفظه وفقا للأوضاع والشروط التي تضمن توثيقه وصدق ما ورد به»[3] ، وكذلك لدى المشرع الجزائري وفق المادة 323 مكرر 1 قانون مدني[4] .

يرى المستشار عبد الفتاح بيومي حجازي أنه حتى يتم الاعتراف بالكتابة الإلكترونية فإنه يجب أن تتم فوق دعامة مادية يمكن فصلها عن جهاز الكمبيوتر وإلا فإنه لا يعترف لها بهذه الصفة[5].

إلا أن أهم مشكل قد يواجه الكتابة الإلكترونية هي صعوبة قراءتها بعد مرور مدة زمنية معينة وهذا بفعل تغير برامج الكمبيوتر وتطورها بشكل مستمر ، إلا أنه قد تم حل هذا المشكل عن طريق أنظمة خاصة ببرامج فك الشفرة أو ما يسمى بالوسيط الإلكتروني[6]

---

[1] أ/قارة مولود ،التوقيع الإلكتروني كدليل إثبات في القانون الخاص،ماجستير في القانون الخاص ،جامعة فرحات عباس سطيف (الجزائر)،سنة 2004،ص.11.

[2] Jérôme Huet .op.cit,p.5

[3] Art,1316-c ;f- L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier,sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature a en garantir l'intégrité

[4] المادة 323 مكرر 1 قانون مدني تنص:«يعتبر الإثبات بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة على الورق،بشرط إمكانية التأكد من هوية الشخص الذي أصدرها وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها.

[5] د-عبد الفتاح بيومي حجازي،المرجع السابق، ص.45.

[6] أ/قارة مولود ،المرجع السابق،ص11. ،الهامش رقم 12

ينتج عن المساواة بين الكتابة الإلكترونية والكتابة الخطية أثار مهمة من بينها:

- على القاضي أن يقبل هذا النوع من الكتابة ويقدر حجيتها مقارنة بالأدلة الكتابية الأخرى، بمجرد توافر الشروط المذكورة سابقا وهو ما يعرف بمبدأ الحياد التكنولوجي .
- يجب أن تكون الوثيقة محفوظة بشكل أمن ،
- يجب تحديد هوية الأطراف خاصة في الشبكات المفتوحة وهو ما يقوم به التوقيع الإلكتروني بشكل جيد وآمن بصورة شبه مؤكدة .

الفرع الثاني : تعريف التوقيع الالكتروني

إن التوقيع الالكتروني ما هو في حقيقة الأمر إلى مزيج بين التقنية والقانون ،وأول تعريف تقني أتت به منظمة ISO بقولها :«التوقيع(الرقمي) معطيات مضافة إلى وحدة معطيات والتي تحول تلك الوحدة إلى شفرة تسمح للمرسل بالبرهنة على مصدر وسلامة وحدة المعطيات وحمايتها ضد كل تزوير»[1].

جاءت التعليمة الأوربية لحمل الدول التي تحت لوائها على الاعتراف بالتوقيع الإلكتروني مثله مثل التوقيع التقليدي وجعله كوسيلة إثبات مقبولة لدى القضاء[2].

فميزت هذه الأخيرة بين نوعين من التوقيع الإلكتروني الأول هو ما نصت عليه المادة 2-1«هو عبارة عن معطى على شكل إلكتروني المرتبط أو المتصل منطقيا بمطيات إلكترونية أخرى والتي تستعمل كوسيلة للتصديق»[3] ،ثم في المادة2-2 عرفت التوقيع

---

[1] Thierry Piette-coudol:«échanges électroniques Certification et sécurité » , édition litec ,2001p.126

[2] المادة 5الفقرة 2 من التعليمة الأوروبية.

[3] article 2-1 de la Directive : " la signature électronique une donnée sous forme électronique, qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification ".

الإلكتروني المتقدم والذي يجب أن يستوفي مجموعة من الشروط[1] ،وهو وحده الذي له الحجية الكاملة مع ترك السلطة التقديرية للقضاء في بقية الأنواع الأخرى.

نلاحظ على هذين التعريفين يرتكزان أساسا على البعد التقني للتوقيع الإلكتروني أكثر من البعد الوظيفي ،ومن دون الإشارة إلى التشفير الأسيميتري الذي يلعب دورا كبيرا في هذا المجال [2].

بعد ذلك عرفه قانون الأونيسترال النموذجي في مادته الثانية بأنه :«بيانات في شكل الكتروني مدرجة في رسالة بيانات أو مضافة إليها أو مرتبطة بها منطقيا ، يجوز أن تستخدم لتعيين هوية الموقع بالنسبة إلى رسالة البيانات ،ولبيان موافقة الموقع على المعلومات الواردة في رسالة البيانات»

أول التعاريف على مستوى الدول كان من طرف الولايات المتحدة الأمريكية بموجب القانون الفيدرالي الأمريكي المتعلق بالتجارة الالكترونية الصادر في 30 جوان 2000 والذي ينص على أن التوقيع الالكتروني هو «عبارة عن أصوات أو إشارات أو رموز أو أي إجراء أخر يتصل منطقيا بنظام معالجة المعلومات إلكترونيا، ويقترن بتعاقد أو مستند أو محرر ويستخدمه الشخص قاصدا التوقيع على المحرر» .

كما عرفه المشرع الفرنسي في المادة 4-1316 مدني فرنسي بأنه:«التوقيع الضروري لاكتمال التصرف القانوني والتعريف بهوية صاحبه والمعبر عن رضاء الأطراف بالالتزامات الناشئة عنه .

ومتى كان التوقيع الكترونياً، فإنه يتمثل في استعمال وسيلة تعريف مأمونة تؤكد ارتباط التوقيع بالتصرف المعني، ويكون الأمان الذي تمنحه هذه الوسيلة مفترضاً ما لم يثبت العكس إذا تمَّ إنشاء التوقيع الالكتروني، وتحقق تحديد شخص الموقع، وأمكن ضمان سلامة التصرف بمراعاة تطبيق الشروط التي تصدر بها لائحة عن مجلس الدولة» ، بالتالي فإن هذا

---

[1] وهذه الشروط هي : - يسمح بتحديد هوية الموقع - ارتباط التوقيع الإلكتروني بالموقع دون غيره.- سلامة مضمون الرسالة الإلكترونية التي ارتبط بها التوقيع - إمكانية كشف أي تبديل أو تعديل في بيانات التوقيع الإلكتروني.

[2] Guenièvre Bordinat :«Introduction a la notion de signature électronique».www.signelec.com

التعريف يرتكز أساسا على المعيار الوظيفي للتوقيع(عكس التعليمة) ويجعل من الكتابة الإلكترونية لها نفس حجية الكتابة على الورق[1].

أما في مصر فقد عرفته المادة الأولى من القانون تنظيم التوقيع الإلكتروني بأنه:«...ج- ما يوضع على المحرر الإلكتروني ويتخذ شكل حروف أو أرقام أو إشارات أو غيرها ويكون له طابع متفرد يسمح بتحديد شخص الموقع ويميزه عن غيره».

انتقد هذا التعريف على أساس أنه يوسع بشكل كبير من نطاق التوقيع الإلكتروني ، ورأى البعض أنه يجب أن يكون تعريفه على النحو التالي:«هو البصمة الإلكترونية التي توضع على المحرر الإلكتروني الذي يدل على اتصال منطقي بين شخص معين وبين الوثيقة الإلكترونية على وجه يدل على أنه منشئها ويدل على هويته ويدل على قبوله بمحتواها»[2].

أما تعريف التوقيع الإلكتروني في إمارة دبي فتم بموجب المادة الثانية من قانون التجارة الإلكتروني التي تنص بأنه:« توقيع مكون من حروف أو أرقام أو رموز أو صوت أو نظام معالجة ذي شكل إلكتروني وملحق أو مرتبط منطقيا برسالة إلكترونية وممهورة بنية توثيق أو اعتماد تلك الرسالة».

في القانون الأردني عرفه قانون التجارة الإلكتروني بأنه:«الأصوات الإلكترونية أو الرموز أو المعالجة أو التشفير الرقمي التي تبين هوية الشخص المعني الذي وضع هذه الإشارات على المستند من أجل توقيعه وبغرض الموافقة على مضمونه».

كما عرف التوقيع الإلكتروني في قانون مملكة البحرين في شأن المعاملات الإلكترونية بأنه:«معلومات مصاغة بطريقة إلكترونية، أو محتواة أو مثبتة في سجل إلكتروني أو مرتبطة به منطقيا قد يستخدمها الموقع لإثبات هويته»

---

[1]Guenièvre Bordinat ; op.cit, www.signelec.com

[2]المستشار عبد الفتاح بيومي حجازي،المرجع السابق،ص.60

نلاحظ على العموم أن تعريف التوقيع الالكتروني في مختلف التشريعات سواء منها العربية أو الأوربية جاء بمفهوم واحد تقريبا مع اختلاف في الألفاظ ولكن مع وحدة المضمون[1].

نستنتج من هذه التعريفات أن معظم التشريعات سواء على المستوى الدولي أو الداخلي حاولت أن تتجنب التعريف الضيق للتوقيع الإلكتروني والهدف من ذلك الانفتاح على التطورات التكنولوجية في هذا المجال وما قد تفرزه من تغيرات ،إلا أنه في حقيقة الأمر لا يوجد إلا نوع واحد من التواقيع الإلكترونية الذي يستجيب للشروط القانونية وهو ما يسمى بالتوقيع الإلكتروني المؤمن والمرتكز على التشفير بالمفتاح العام [2]

القانون التونسي عكس التشريعات الأخرى لم يعرف التوقيع الإلكتروني التي ترك هذه المهمة للفقه بل اهتم فقط بتعريف العناصر المؤدية إلى هذا التوقيع ،وهذا نظرا لارتباطها الوثيق بالتوقيع الالكتروني ومن أمثلتها ، شهادة المصادقة الالكترونية ، المحرر الالكتروني إلخ...

حيث لا يكتمل تعريف التوقيع الإلكتروني دون أن نتطرق إلى الوسيط الإلكتروني، وقد عرفته المادة الأولى من قانون التوقيع الإلكتروني المصري بأنه «أداة أو أدوات أو أنظمة إنشاء التوقيع الإلكتروني » ، وهو نفس ما اتجهت إليه المادة الثانية من قانون التجارة الإلكترونية في إمارة دبي حيث عرفته ب«أداة التوقيع» ،أما المشرع التونسي فعرفها في المادة الثانية من قانون المبادلات الإلكتروني بأنه:«مجموعة وحيدة من عناصر التشفير الشخصية أو مجموعة من المعدات المهيأة خصيصا لإحداث الإمضاء الإلكتروني».

---

[1] محمد منير الجنبيهي و ممدوح محمد الجنبيهي ،التوقيع الالكتروني وحجيته في الإثبات، دار الفكر الجامعي 2005، ص.11

[2] Béatrice Jaluzot op.cit ,p2866

نلاحظ على هذه التعريفات أنها وردت غامضة ومبهمة ولا توضح ما المقصود بالوسيط الإلكتروني وإن كانت على العموم هي عبارة عن الوسيلة التي يمكن عن طريقها لصاحب التوقيع أن يوقع.

فيمكن أن يتم التوقيع الإلكتروني مثلا بواسطة القلم الإلكتروني أو عن طريق بطاقة الائتمان أو بواسطة المميزات البيولوجية للعميل أو ما يعرف بالتوقيع البيومتري.

وكل هذه الوسائط الإلكترونية هي التي جعلت للتوقيع الإلكتروني أنواعا عدة ولا تقتصر على صورة واحدة فقط وهو ما سنتطرق إليه في الفرع الثالث من هذا المطلب.

الفرع الثالث: أنواع التوقيع الإلكتروني

لقد أفرزت لنا المعاملات الإلكترونية عدة أنواع لما يعرف بالتوقيع الإلكتروني ، فقد يتم نقل التوقيع الخطي إلى وثيقة إلكترونية بواسطة الماسح الضوئي (**أولا**) أو التوقيع الكودي (**ثانيا**) أو اللجوء إلى فكرة الخواص الشخصية (**ثالثا**) وأخيرا قد يتم التعامل الإلكتروني من خلال التوقيع الرقمي الذي يعتمد على فكرة اللوغارتميات (**رابعا**)

أولا : نقل التوقيع الخطي بالماسح الضوئي(التوقيع بالقلم الإلكتروني):

إن أساس هذا النوع من لتوقيع يقوم على فكرة تحويل التوقيع من الدعامة الورقية إلى الدعامة الإلكترونية بواسطة الماسح الضوئي(scanner) حيث يخزن هذا التوقيع فيما بعد في مذكرة الكمبيوتر أو في دعامة مغناطيسية مثل أقراص مغناطيسية (Disquette) أو أقراص ضوئية مكتنزة(CD. ROM) ثم يوضع هذا التوقيع فيما بعد فوق الوثيقة

الإلكترونية وتحول هذه الوثيقة إلى الشكل الورقي بعد طباعتها، وتكون النتيجة النهائية مطابقة بشكل كبير للأصل إذا كان الورق المستعمل والطابعة من النوع الجيد [1].

يظهر لنا من الوهلة الأولى أن هذا النوع من التوقيع لا يشكل صعوبات تقنية للموقع كما لا يكلف الأطراف أعباء مالية كبيرة كما أن استعمال هذه الوسيلة يعتبر سهلا ولا يحتاج إلى معارف تقنية في مجال الإعلام الآلي.

على الرغم من هذه الميزات التي يوفرها هذا النوع من التوقيع إلا أنه يأخذ عيه عدة مأخذ وسلبيات فهو لا يوفر الأمان القانوني للأطراف الموقعة إذ يمكن لأي شخص سيء النية أن يدخل إلى مذكرة الكمبيوتر أو أن يتحصل على الدعامة المغناطيسية ويقوم بنسخ هذا التوقيع واستعماله لأغراض لم تنصرف إرادة الموقع عليها وبالتالي فإن هذه الوثيقة الموقعة لا تربط بالموقع أي علاقة بينهما ،وقد استقر الوضع على عدم الاعتداد بهذا النوع من التوقيع[2].

ثانيا : التوقيع الكودي:

إن هذه التقنية جعلت أساسا لتسهيل إبرام الصفقات التجارية والحصول على النقود في أي وقت، وتطورت بشكل كبير في المجال البنكي التي تعتمد على الشبابيك الآلية .

أحسن مثال عليها استعمال بطاقة الائتمان التي تحتوي على رقم سري لا يعرفه سوى العميل حيث يقوم بإدخال البطاقة في ماكينة السحب بالشكل الصحيح ثم بعد ذلك يدخل رقمه السري الخاص به (P.I.N) وأخيرا يقوم بالضغط على الاختيار المناسب لإتمام العملية ومن دون هذه الخطوات لا يمكن للعميل أن يتمم العملية[3].

---

[1] Didier Gobert et étienne Montero ,op.cit ;p.57

[2] أنظر في ذلك د-سعيد سيد قنديل،المرجع السابق ،ص.66

[3] أنظر في ذلك د-سعيد سيد قنديل، المرجع السابق،ص.67 والمستشار عبد الفتاح بيومي حجازي ،المرجع السابق،ص.27 وما بعدها

يرى البعض أن هذا النوع من التوقيع الإلكتروني لا تشكل فقط آلية للدخول إلى نظام معلوماتي بل تؤدي وظائف التوقيع التقليدي بشكل كامل[1].

حتى هذا النوع من التوقيع لا يخلو من عيوب إذ يمكن للغير متى تحصل على بطاقة الائتمان وكان عارفا بالرقم السري لها أن يقوم بالعمليات المصرفية وهذا ما يؤدي إلى عدم تحديد هوية الموقع بشكل صحيح من جهة ومن جهة ثانية عدم انصراف إرادة هذا الأخير للقيام بهذا التصرف.

كما أنه يمكن تقليد بطاقة الائتمان وإن كان هذا لا يجدي نفعا من دون معرفة الرقم السري للبطاقة، كما أن الموقع ملزم بكل الأحوال على الحفاظ على الرقم السري وعدم تسريبه إلى أي شخص أخر لأنه بمثابة مفتاح خزانة النقود وفي حالة خطئه أو إهماله في الحفاظ على الرقم السري فإنه يتحمل المسؤولية المدنية عن العمليات المنفذة قبل إخطاره للبنك[2] .

وقد امتد استعمال التوقيع الكودي باعتباره يحدد هوية الشخص الحامل لها بشكل دقيق إلى التساؤل حول مدى اعتماد الدولة على هذا النظام لإصدار ما يعرف ببطاقات التعرف الإلكترونية[3]، وهو ما يتم الإعداد له حاليا في العديد من الدول كفرنسا وبلجيكا وسويسرا إلخ...

ثالثا : التوقيع البيومتري:

ظهر مؤخرا اعتماد البنوك على ما يعرف بالتوقيع البيومتري ويرتكز أساسا على الخواص الذاتية للعميل أو الموقع والتي لا يمكن من الناحية العملية أن تتشابه مع شخص أخر .

---

[1]Didier Gobert et étienne Montero ,op.cit., p.58

[2] المستشار عبد الفتاح بيومي،المرجع السابق،ص.28 و29

[3]Thierry Piette-Coudol ,op.cit ,p.132

إذ يتم تمييز العميل إما بواسطة بصمة أصبعه (dactyloscopie) أو بقزحية العين (rétinoscopie)،وهناك كذلك ما يعرف بالبصمة الصوتية للشخص أو حتى اللجوء إلى تمييز العميل عن طريق دراسة توقيعه مثل طريقه تخطيطه للتوقيع وسرعة الحركة والضغط على القلم إلخ...

المهم أن تكون الميزات البيومترية مرتبطة بالشخص وأن تكون مؤمنة ، وأصبح تطبيق هذه التقنيات مستعملا في عدة مجالات مثل الدخول إلى القاعات المؤمنة أو إلى الخزائن المحمية إلخ...

إن أغلب هذه التقنيات لا تزال في المرحلة التجريبية ولم تصل بعد إلى مرحلة الاستعمال العادي لها ، كما يواجه هذا النوع من التوقيع عدة عوائق لتطبيقه مثل غلاء هذه المعدات هذا من جهة ومن جهة أخرى فإن الميزات الفيزيائية للشخص مثل البصمة الصوتية قد تتغير بحسب الحالة التي يكون فيها الشخص ،فالصوت يتغير بسبب القلق مثلا .

فكل هذه السلبيات جعلت من التوقيع البيومتري قليل الاستعمال ولا يتم تطبيقه إلا في مجالات قليلة ومحدودة.

رابعا: التوقيع الرقمي:

يعتمد التوقيع الرقمي أساسا على نظام التشفير واللوغرتميات والتي تهدف إلى تحقيق وظائف التوقيع كما رأيناه سابقا وضمان سرية المعاملات الإلكترونية .

يجب أن ندرك أن التشفير يمكن أن ينصب على العقد الإلكتروني أو على المحرر الإلكتروني أو على التوقيع الإلكتروني.

ففي حالة العقد الإلكتروني والموقع عليه إلكترونيا يمكن أن تشفر بيانات العقد وفي حالات أخرى تكون البيانات غير مشفرة بالرغم من أن التوقيع على ذلك العقد يكون مشفرا[1].

التشفير قد يتم على صورتين فإما يكون على شكل التشفير التماثلي (symétrique) أو بصورة التشفير اللاتماثلي (Asymétrique).

فالطريقة الأولى تعتمد أساسا على فك الشفرة بمفتاح واحد سواء في التشفير أو فك الشفرة وتتطلب إحالة المفتاح بين الأطراف(الموقع والمرسل إليه) بطريقة يجب أن تضمن سلامته[2].

تطور هذا النظام ليصبح يعتمد على نظام التشفير اللاتماثلي أو ما يعرف بالتشفير بالمفتاح العام والتي لا تعتمد فقط على مفتاح واحد كما رأينا في الطرقة الأولى بل تعتمد على مفتاحين أحدهما عام والأخر خاص ،وحتى وإن عرف المفتاح العام فلا يمكن معرفة المفتاح الخاص ، وهذا النظام يسمح بالتأكد من مصدر الوثيقة[3]، ومن سلامتها[4].

فالتوقيع اللاتماثلي هو عبارة عن رموز غير متناسقة والتي يكون فيها مفتاح إدخال الشفرة والرمز مختلف عن المفتاح الذي يقوم بحل التشفير قصد قراءة الرسائل المشفرة ، وعلى سبيل المثال فإنه يمكن استخدام الرقمين 127،997للوصول إلى الرقم 126619 فيكون في غاية الصعوبة الوصول على الرقمين انطلاقا من أحدهما[5].

يقوم الموقع في هذه الحالة بإرسال المفتاح العام فقط للمرسل إليه ويحتفظ بالمفتاح الخاص الذي يبقى بحوزته ويكون سريا بالنسبة للأطراف الأخرى.

---

[1] محمد أمين الرومي،المرجع السابق،ص .30و31

[2] أ/علي كحلون،المرجع اسابق،ص.282

[3] authentification

[4] integrité

[5] د-سعيد السيد قنديل، المرجع السابق،ص62. و63

عند توقيع الرسالة الإلكترونية من طرف الموقع بقوم المرسل إليه بالتأكد من صحة هذا التوقيع، وغالبا ما يتدخل طرف ثالث في هذه العملية وهو ما يعرف «بمزود الخدمات »الذي يؤكد على صحة التوقيع وذلك بمقارنة المفتاح المرسل من طرف المرسل إليه بما هو موجود عنده من مفاتيح عامة فإن تطابق المفتاح المرسل مع المفاتح الموجود عند مزود الخدمات يقوم هذا الأخير بتزويد المرسل إليه بشهادة تؤكد صحة التوقيع ويتم إرسالها بشكل آمن ومن دون التعرض لتزوير أو القرصنة عليها[1].

حيث يكون المفتاح العام في هذه الحالة معروفا بالنسبة للغير ،أما المفتاح الخاص فلا يتصور معرفته إلا من صاحبه ويبقى سرا على الآخرين.

غالبا ما تعتمد الشركات في هذا المجال على تقنية طبقة الفتحات الآمنة (SSL) وهو عبارة عن برنامج متخصص لنقل البيانات والمعلومات بين جهازين عبر شبكة الانترنيت بحيث لا يمكن لأحد غير المرسل والمستقبل قراءتها ويصعب فك شفرتها[2].

وقد سارت الدول في اتجاه تحرير استعمال هذه الوسائل التي كنت حكرا على الجهاز العسكري والأمني لاقتناعها بأن تقدم التجارة الإلكترونية مشروط بأمان وسلامة المعلومات على الشبكة المفتوحة، ولا يمكن أن يتحقق ذلك إلا بتحرير استعمال وسائل التشفير[3].

المطلب الثاني : مدى حجية التوقيع الإلكتروني

على الرغم من الوسائل الحديثة والمتطورة التي تستعمل لإنشاء وإعمال التوقيع الإلكتروني إلا أن الناس مازالوا يتخوفون من استعمال هذا النوع من التوقيع ، ولذلك

---

[1] Thierry Piette-Coudol ;op.cit ;p.129

[2] المستشار عبد الفتاح مراد،شرح قوانين التوقيع الإلكتروني في مصر والدول العربية،شركة البهاء للبرمجيات والكمبيوتر والنشر الإلكتروني

[3] أ/علي كحلون،المرجع السابق ،ص.283

حرصت معظم التشريعات على منح التوقيع الإلكتروني ضمانات شروط معينة حتى يصبح له نفس حجية التوقيع الكتابي (الفرع الأول).

يبقى مشكل الحفاظ على التوقيع الإلكتروني الذي يتم على المستندات الإلكترونية دون المساس بمحتوى السند من أهم المعوقات التي تنقص من القيمة الإثباتية للتوقيع الإلكتروني، وهو ما تم تجاوزه في إطار ما يعرف بالأرشيف الإلكتروني (الفرع الثاني)

إذ بمجرد أن يستوفي التوقيع الإلكتروني شروطه ويتم الحفاظ عليه دون المساس به فإن استخدامه كوسيلة إثبات يتم في العديد من المجالات وإن كانت معظم التشريعات قد استبعدت استعمال التوقيع الإلكتروني في بعض المجالات(الفرع الثالث).

الفرع الأول:شروط صحة التوقيع الإلكتروني

إن معظم التشريعات قد جعلت من التوقيع الإلكتروني له نفس حجية التوقيع الكتابي إذا استوفى مجموعة من الشروط ويطلق عليه« التوقيع الإلكتروني المحمي» ونصت عليها المادة 18من قانون التوقيع الإلكتروني المصري المادة 6 من قانون االأونيسترال النموذجي بشأن التوقيعات الإلكترونية والمادة 20 من قانون التجارة الإلكترونية في إمارة دبي والمادة 2/2 من التعليمة الأوروبية.

وهذه الشروط هي:

1-يسمح بتحديد هوية الموقع

2-ارتباط التوقيع الإلكتروني بالموقع دون غيره.

3-سلامة مضمون الرسالة الإلكترونية التي ارتبط بها التوقيع

4-إمكانية كشف أي تبديل أو تعديل في بيانات التوقيع الإلكتروني.

أولا : يسمح بتحديد هوية الموقع:

إن تحديد هوية الموقع في إطار الكتابة على الورق يعتبر شرطا بديهيا فبمجرد التوقيع على الوثيقة يعتبر كافيا لتحديد هوية الأطراف، ولكن الأمر يبدوا ذو أهمية كبرى في إطار المعاملات الإلكترونية والتي من الصعب تحديد هوية أطرافها.

لذلك فإن التوقيع الإلكتروني يجب أن يحدد وبصفة كافية هوية الأطراف ،وإن كان ذلك لا يلغي إمكانية أن يكون الدفع الإلكتروني بطريق الإغفال أو ما يعرف «المجهول»إذ أن دفع الثمن ما هو في حقيقة الأمر إلا أثرا من أثار العقد وبالتالي لا يؤثر بوجود العقد[1].

كما أن القانون المدني الفرنسي في المادة 1316 فقرة4 نصت على أن تكون هوية الموقع ثابتة ، ويتم تحقيق هذا الشرط بواسطة ما يعرف باستعمال المفتاح الخاص (يشترط أن يكون سريا) الذي هو في مكانة القلم وينتج عن استعماله من طرف الموقع أثار التوقيع ويدعم برقم سري يحتفظ به الموقع دون سواه والذي يسمح بالدخول إلى المفتاح الخاص[2].

يعتبر قرار مجلس Besançon بتاريخ 20 أكتوبر 2000 الأول في مجال التوقيع الإلكتروني حيث اعتبرت أن الثقة في إجراءات التوقيع التي قام بها المحامي مشكوك فيها بمجرد أن الرقم السري يمكن أن يتعرف عليه شخص أخر وبالتالي فإن تحديد هوية الموقع تبقى غير مؤكدة[3].

وقد كان لقرار الغرفة المدنية الثانية لمجلس النقض الفرنسي الصادر بتاريخ 30 أفريل 2003 الحل النهائي لهذه الإشكالية بأن رفضت توقيع إلكتروني خارج أحكام قانون

---

[1] Thirry Piette-Coudol ;op.cit ;p134

[2] Julien ESNAULT ;op.cit ;p 8 et 9

[3] CA Besançon, ch.soc., 20 octobre.2000, *Sarl Chalets Boisson c/ Bernard Gros* : JCP G 2001, II,no 10606 , cité par Julien ESNAULT ;op.cit ;p9

13 مارس 2000 والذي لا يحدد بشكل كافي وكامل هوية الموقع ، ولا يمكن الاعتماد على الهاتف النقال (بواسطة الرسائل القصيرة SMS)لإتمام إجراءات التوقيع الإلكتروني مادام أن إمكانية استعمال الهاتف النقال من طرف الغير يصبح ممكنا وبالتالي عدم تحديد هوية الموقع بصورة كاملة[1].

ثانيا :ارتباط التوقيع الإلكتروني بالموقع دون غيره:

إن التوقيع سواء كان تقليديا أو إلكترونيا يجب أن يتم من طرف الموقع دون سواه، إذ هو تعبير عن إرادة الموقع ورضاه بمحتوى السند (كتابي أو إلكتروني) وبالتالي يجب أن تكون هناك علاقة مباشرة بين التوقيع والموقع .

ففي التوقيع التقليدي العلاقة المباشرة بين الموقع والتوقيع لا إشكال فيها فتكون بواسطة اليد أما في التوقيع الإلكتروني فالعلاقة بين الموقع والتوقيع تكون بالاستعمال المنفرد للموقع للتوقيع وعدم السماح للغير باستعمال توقيعه، أي اغتصاب التوقيع الإلكتروني[2].

لهذا قام المشرع الفرنسي بتعديل المادة 1326من القانون المدني فيما يخص الأعمال الملزمة لجانب واحد فقد كانت تنص على كتابة المبالغ يدويا بواسطة «اليد» ثم عدلت لتصبح «بواسطة الشخص نفسه» ،وبالتالي لم يعد مشترطا في التوقيع باعتباره كتابة أن يكون بيد الموقع حتى يكون صحيحا بل يجب أن يتم بواسطة شخص الموقع .

[1] Julien ESNAULT ;op.cit ;p9

[2] المستشار عبد الفتاح بيومي حجازي،المرجع السابق،ص444

ثالثا: سلامة مضمون الرسالة الإلكترونية التي ارتبط بها التوقيع:

إن الهدف الأساسي للتوقيع بصفة عامة هو انصراف إرادة الموقع إلى الالتزام بمحتوى السند.

فالتوقيع الكتابي مثلا تنصرف فيه إرادة الموقع إلى الالتزام بما ورد في الورقة(عرفية أو رسمية)بشرط عدم تزوير ما ورد في الورقة أو السند ، وإلا فإن الموقع يكون غير ملزم بتوقيعه ويحقه له أن يرفع دعوى تزوير وفق ما تنص عليه القوانين.

كذلك فإن التوقيع الإلكتروني يسعى إلى تحقيق نفس غرض التوقيع التقليدي ،فعند إبرام عقد إلكتروني في إطار التجارة الإلكترونية فإن الموقع على السند الإلكتروني يكون ملزما بما ورد في هذا السند على أن الاعتراف بسلامة التوقيع الإلكتروني في هذه الحالة يستلزم عدم تغيير محتوى ومضمون الرسالة الإلكترونية وإلا فقد التوقيع الإلكتروني أهميته[1].

رابعا: إمكانية كشف أي تبديل أو تعديل في بيانات التوقيع الإلكتروني:

لقد رأينا في الشرط السابق أن التوقيع الإلكتروني يجب أن ينفرد به صاحبه دون غيره من الأشخاص لأنه يحدد هوية الموقع ولذلك يجب على هذا الأخير أن يحتفظ بمنظومة التوقيع الإلكتروني سرا وأن لا يطلع عليه الغير، وأن يذل في ذلك عناية معقولة[2].

يلتزم الموقع بموجبها أن يبذل عناية الرجل العادي في الحفاظ على صحة بيانات التوقيع الإلكتروني الذي يكون بحوزته إذ أنه يعتبر مستهلكا(الطرف الضعيف) ولا يمكن أن نلزمه بتحقيق نتيجة ،وبالتالي فإنه وفي حالة ما إذا تم تعديل التوقيع الإلكتروني يتحمل المدعي عبء إثبات ذلك.

---

[1] المستشار عبد الفتاح بيومي،المرجع السابق،ص128

[2] وهو ما نص عليه الفصل 6 من قانون المبادلات والتجارة الإلكترونية التونسي ،المادة 8 من قانون الأونيسترال النموذجي بشأن التوقيعات الإلكترونية ،المادة 20 من قانون إمارة دبي الخاص بالمبادلات والتجارة الإلكترونية إلخ...

يقع على عاتق المتعامل أن يتحقق من صحة التوقيع المقدم له وذلك بطلب الشهادة الخاصة بالتوقيع من طرف مزود الخدمة.

كما أن هذا الأخير إن كان التوقيع موقفا أو منتهي الصلاحية أن يذكر ذلك وأن يتم منح توقيع إلكتروني وحيد وغير مشابه لأي توقيع أخر.

الفرع الثاني:إشكالية حفظ التوقيع الإلكتروني وسلامته

تتم معالجة هذه المشكلة تتم عبر مستويين، الأول معالجة مشكلة سلامة الوثيقة الإلكترونية بشكل عام باعتبار أن التوقيع الإلكتروني عادة ما يتم فوق هذا النوع من السندات ثم دراسة سلامة التوقيع الإلكتروني في المستوى الثاني[1].

أولا: سلامة الوثيقة الإلكترونية:

الاحتفاظ بالسند الكتابي يختلف بحسب طبيعة المعاملة فتكون 10سنوات بالنسبة للمعاملات التي تتم بين التجار و30سنة للمعاملات المدنية و100 سنة بالنسبة للورقة الرسمية ،وإن كان هذا يبدوا سهلا بالنسبة للتصرفات المحررة على الدعائم الورقية إلا أن ذلك يبدو في غاية الصعوبة بالنسبة للوثيقة الالكترونية.

فإن كانت هذه الأخيرة تتميز على العموم بخاصيتين أولها أنها سهلة التعديل والتغيير وثانيهما إمكانية استقلالها عن الدعامة المادية التي كتبت فيها ووضعها في دعامة أخرى من دون أن تفقد قيمتها الأولى[1].

إلا أن الكتابة الإلكترونية بصفة عامة والتوقيع الإلكتروني بصفة خاصة حتى يعتبر دليل إثبات ويكون له نفس حجية التوقيع التقليدي يجب أن يتم الاحتفاظ به لمدة معينة من دون

[1] Stéphane Caïdi ;op.cit ;p.14

تغيير وهو ما تنص عليه صراحة المادة 323مكرر 1 من القانون المدني الجزائري :«يعتبر الإثبات بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة على الورق ،بشرط إمكانية التأكد من هوية الشخص وأن تكون معدة في ظروف تضمن سلامتها ».

أحال المشرع الجزائري في المادة 327 فقرة 2 من القانون المدني للمادة 323مكرر1 في صحة التوقيع الإلكتروني ، وهو نفس ما نص عليه المشرع التونسي في الفصل الرابع من قانون المبادلات والتجارة الإلكترونية و المادة 1-1316من القانون المدني الفرنسي.

في تقرير لمجلس الدولة الفرنسي المعنون ب«الانترنيت والشبكات الرقمية»يقر أنه يجب الاحتفاظ بسلامة الوثيقة الإلكترونية بصفة مستمرة[1].

فالتطور التكنولوجي السريع والمستمر للمعلوماتية أصبح من الصعب توفير هذه الشروط فما كان مقروءا قبل سنة أصبح غير ممكن في الوقت الحالي وهذا بسبب تطوير البرامج الخاصة بالكمبيوتر والتي تسمح بقراءة الوثيقة الإلكترونية.

بل الأكثر من ذلك أنه ما يمكن قراءته على كمبيوتر لا يمكن قراءته في كمبيوتر أخر بسبب عدم توافق البرامج ، وكثيرا ما تصل الرسالة الالكترونية إلى المرسل إليه بغير حالتها الأولى ومعها التوقيع الالكتروني باعتباره عنصر من الوثيقة الإلكترونية وذلك بسبب تدخل الغير سيء النية وتغييره لمحتوى السند أو التوقيع الإلكتروني[2]

إلا أن ظهور ما يعرف ب«الأرشيف الإلكتروني» والذي يتم عن طريق شركات متخصصة أصبح بموجبه للوثيقة الإلكترونية الموقعة إلكترونيا نفس حجية الوثيقة الموقعة كتابيا، إذ أمكن الاحتفاظ بالوثيقة الإلكترونية لمدة طويلة دون تغيير محتواها، ولكن بشرط

[1] Julien ESNAULT ;op.cit ;p.19
[2] Julien ESNAULT ;op.cit ;p.15

الصيانة التكنولوجية الدائمة للبرامج الخاصة بالأرشيف الإلكتروني حتى يمكن مواكبة التطور التكنولوجي الحاصل في عالم الإعلام الآلي[1].

الملاحظ على المشرع الجزائري لم ينص صراحة على تقنية الأرشيف الإلكتروني ولا على الأحكام القانونية المنظمة لهذا النشاط .

إلا أن المشرع البحريني في المادة 9 من قانون التجارة الإلكتروني اشترط صراحة حفظ السندات الإلكترونية بمجرد توافر مجموعة من الشروط وهي:

أ- أن يتم حفظ السجل الإلكتروني بالصيغة التي تم بها إنشاؤه أو إرساله أو تسلمه، أو يتم حفظه في صيغة يثبت أنها تمثل بدقة المعلومات الأصلية التي تم إنشاؤها أو إرسالها أو تسلمها.

ب- أن تكون المعلومات التي تضمنها السجل الإلكتروني الذي تم حفظه قابلة لأن يتم لاحقا الدخول عليها وعرضها واستخراجها بشكل قابل للفهم.

ج- بيان المعلومات – إن وجدت – التي تحدد مصدر المستند والجهة المرسل إليها وتاريخ ووقت إرساله أو تسلمه، وذلك إذا كان المستند المحفوظ قد أرسل أو تم تسلمه إلكترونياً.

د- موافقة الجهة العامة التي يخضع النشاط لإشرافها – إن وجدت – على أن يتم الحفظ في شكل سجل إلكتروني واستيفاء أية اشتراطات تحددها هذه الجهة.

نتج عن ذلك تغير مفهوم الأرشيف الذي كان ولوقت قريب يهدف فقط إلى الاحتفاظ بالوثائق لمدة معينة، لكن مع التطور التكنولوجي وظهور التقنيات الحديثة أصبح الأرشيف يهدف كذلك إلى ضمان نزاهة وسلامة الوثيقة الإلكترونية.

[1] Stéphane Caïdi ;op.cit ;p.21

إلا أن المحافظة على سلامة الوثيقة الإلكترونية لا يجب أن يكون مرتبطا بالوسائل التقنية للأرشيف ولكن يجب أن يخضع في ذلك للمدة المنصوص عليها في القانون[1].

ثانيا: سلامة التوقيع الإلكتروني:

تظهر أهمية الأرشيف الإلكتروني في مجال التوقيع الإلكتروني مثلا المرسوم 30مارس 2001 (فرنسا) الذي ألزم مزود الخدمات بالحفاظ على المميزات والمرجعيات الخاصة بتحديد هوية وصفة الحائز على الشهادة.

كما أن التوقيع الإلكتروني القائم على أساس المفتاح العام يستوجب حفظ الكثير من المعطيات والوثائق، منها مثلا الشهادات ومختلف العقود المبرمة مع مزود الخدمات ونسخ الأوراق المثبتة لهوية وصفة الموقع وكل المعلومات الضرورية لجعل الشهادة الإلكترونية صالحة كدليل إثبات أمام القضاء[2].

لضمان سلامة التوقيع الإلكتروني ومعه الوثيقة الإلكترونية وفي نفس الوقت التحقق من هوية المرسل ،فيمكن الاستعمال المزدوج لمنظومة الإمضاء أو ما يعرف ب

« hachage ou condensé du message[3]» حيث تسمح عملية hachage بتغير حجم المراسلة إلى ما يعرف بالبصمة والتي لها مميزات خاصة مختلفة عن مثيلتها، فيقوم المرسل بإمضائها عن طريق الإمضاء الإصبعي ثم يرسلها إلى الطرف الثاني والذي يقوم هو الأخر بإعادة صيغة البصمة انطلاقا من المعطيات المتوافرة بالمراسلة فإن كانت متطابقة تأكد المرسل إليه من سلامة الوثيقة والتوقيع وفي نفس الوقت تأكد من هوية المرسل والذي لا يمكن إنكار مراسلته[4].

---

[1] Julien ESNAULT ;op.cit ;p.19

[2] المادة 6 من المرسوم 2001

[3] أ علي كحلون،المرجع السابق،ص.282

[4] أ علي كحلون،المرجع السابق،ص.282هامش 92

يشترط في هذه العملية أن تتم المراسلة بين الطرفين بطريقة أمنة لا تسمح للغير السيئ النية التدخل في العملية وتغيير محتوى الوثيقة أو التوقيع الإلكتروني ولا يتم هذا إلا باستعمال وسائل تشفير ذات مستوى عال من الأداء.

إن كان توفير السلامة أثناء إعمال التوقيع الإلكتروني يشغل حيزا كبيرا من فكر رجال القانون إلا أن ذلك لا ينفي أن أهم مشكل يواجه التوقيع الإلكتروني هو بالخصوص تحقيق مبدأ السلامة أثناء عملية الحفظ و هو ما يفرض توفير أعلى درجات الأمن أثناء القيام بهذه العملية لما يترتب عنها من أثار قانونية.

يفضل في هذا المجال أن تتم الأرشفة الإلكترونية عن طريق الغير وأن لا نعتمد على طريقة الأرشيف الداخلي الذي يجعل الوثائق الإلكترونية تحت السيطرة المباشرة لأحد الأطراف[1] وهو ما يجعل الوثيقة محل شك وعدم الثقة فيما تحتويه من معلومات وذلك لإمكانية تعديلها بما يتوافق ومصلحة الشخص الذي تكون بحوزته .

وعملية الأرشيف الإلكتروني تمر بعدة مراحل :

- أولا : يقوم المستعمل بجمع الوثائق الإلكترونية المرتبطة بالعقد والتوقيع.
- ثانيا : يتم إرسال هذه الوثائق إلكترونيا إلى الشركة المختصة بالأرشيف الإلكتروني ، بحيث يمنح لهذه الوثائق الموقع إلكترونيا تاريخ «مؤكد»عن طريق horodatage .
- وأخيرا تقوم الشركة المختصة بوضع الوثائق التي بحوزتها في الأرشيف الإلكتروني.

هذه العملية الأخيرة قد تدوم لفترة طويلة وهو ما يترب على عاتق الشركة تطوير أنظمتها بشكل مستمر حتى يمكن قراءة هذه الوثائق متى تطلب الأمر ذلك.

[1] Julien ESNAULT ;op.cit ;p.20

إلا أن هناك البعض من اقتراح إعادة وضع التوقيع الإلكتروني فوق هذه الوثائق أو إعادة نفس التوقيع الإلكتروني على الوثائق، إلا أن هذا لا يسمح بقراءة الوثائق بشكل وواضح ومفهوم ومن جهة أخرى لا يتيح الفرصة للتأكد من صحة التوقيع[1].

وهو ما أدى على الاعتماد في هذا المجال على معيارISO المعروف ب-NZ42 013، والتي تسمح بالحفاظ على نزاهة التوقيع والوثيقة الإلكترونية طوال مدة حفظها.

الفرع الثالث: مجال إعمال التوقيع الإلكتروني

عندما يستوفي التوقيع الإلكتروني شروطه المذكورة سابقا وتم حفظه ضمن شروط تضمن سلامته أصبح له نفس حجية التوقيع التقليدي.

لكن هل هذا يعني بالضرورة أن التوقيع الإلكتروني يمكن إعماله في جميع المحررات سواء منها الرسمية أو العرفية ؟

لقد حرصت التعليمة الأوروبية بشأن التوقيعات الإلكترونية في المادة 5 على تحديد مجال التوقيع الإلكتروني والتي نستخلص منها ما يلي:

1-يرجع للقانون الوطني تحديد مجال إعمال التوقيع الإلكتروني والاتفاقيات المتعلقة بالإثبات.

2-كل نظام قانوني يمنح حجية للتوقيع الخطي يجب أن يمنح كذلك نفس الحجية للتوقيع الإلكتروني

3- أن تكون حجية التوقيع الإلكتروني المتقدم في نفس درجة حجية التوقيع الخطي في المجالات المرخص لها من طرف القانون الوطني.

4التوقيع الإلكتروني البسيط يمكن أن يرفض ولكن ليس على أساس أنه جاء على شكل إلكتروني[1].

[1] Julien ESNAULT ;op.cit ;p.21

إن الأسس التي وضعتها التعليمة الأوربية في مجال إعمال التوقيع الإلكتروني حرصت عليه تشريعات الدول فيما بعد ،فنجد مثلا أن المشرع البحريني قد أقر نفس هذه المبادئ[2] والمشرع التونسي[3] ، ومشرع إمارة دبي [4] إلخ...

الجدير بالذكر أن إمكانية إعمال التوقيع الإلكتروني لا تقتصر فقط على الورقة الرسمية أو العرفية بل يمكن إعمالها حتى في مجالات لم يشترط فيها المشرع الكتابة ولا التوقيع لإثبات التصرف القانوني ،وهو ما يمنح لهذا الأخير أهمية بالغة كوسيلة إثبات في مجالات لم تتسع قواعد الإثبات التقليدية لاحتوائها.

أولا :التوقيع الإلكتروني في الورقة الرسمية:

لقد رأينا سابقا دور التوقيع في الورقة الرسمية (توقيع الأطراف والموظف) والتي من دونها لا يمكن أن إصباغ الصفة الرسمية على المحرر.
غير أن ظهور المحررات الإلكترونية بمختلف أشكالها ومنها الورقة الرسمية الإلكترونية أصبح لزاما التطرق إلى دور التوقيع الإلكتروني في هذا النوع من الأوراق، وهل هناك استبعاد لهذا النوع من التوقيع في الأوراق الرسمية ؟

على العموم إن ظهور الورقة الرسمية الإلكترونية مرتبط بما يعرف ب«الحكومة الإلكترونية»[5] التي تعتمد في تسييرها على أجهزة الحاسب الآلي المرتبطة فيما بينها بشبكة داخلية (الانترانت) وبغيرها عن طريق شبكة الانترنيت، حيث يقوم الموظفين المختصين في الحكومة الإلكترونية بإصدار مختلف المحررات الإلكترونية وتوقيعها إلكترونيا[6] وهو ما

---

[1] Arnaud-f .Fausse :«La signature électronique transaction et confiance sur Internet» ,Dunod paris 2001 ;p48

[2] المادة 5 من قانون التجارة الإلكتروني
[3] الفقرة 2 من الفصل الأول من قانون المبادلات والتجارة الإلكترونية
[4] المادة 7 من قانون إمارة دبي الخاص بالمبادلات والتجارة الالكترونية
[5] المستشار عبد الفتاح بيومي حجازي ، المرجع السابق ،ص.418
[6] المستشار عبد الفتاح مراد،المرجع السابق،ص.11

يضفي عليها صفة المحررات الرسمية وذلك بهدف الرفع من كفاءة العمل الإداري بما يتفق ومتطلبات العصر.

تم إقرار صحة الكتابة الإلكترونية على الوثائق الرسمية في فرنسا بموجب الفقرة الثانية من المادة 1317 من القانون المدني، ولكن ترك تحديد شروط صحة هذه الكتابة لمجلس الدولة[1]، وهو ما تم بالفعل عندما أصدر هذا المجلس في 2005 مرسومين الأول مرسوم 973-2005 المعدل والمتمم للمرسوم 941-71 المتعلق بالعقود المحررة من طرف الموثق، أما المرسوم الثاني فهو 972-2005 المعدل للمرسوم 222-56 المتعلق بنظام المحضرين.

بما أن الموثق والمحضر القضائي يصدران محررات رسمية ذات قوة ثبوتية كبيرة فإن كل التشريعات اشترط لصحة هذه المحررات حضور الموظف أو الضابط العمومي أو شخص مكلف بخدمة عمومية[2].

إلا انه وفي مجال إبرام العقود الرسمية الإلكترونية فإن الحضور الجسدي سواء للموثق أو المحضر يعتبر من أهم العوائق التي تعترض تحرير هذا النوع من المحررات ويقلل من ثقة الأفراد في الأوراق الرسمية الإلكترونية.

تجاوز المشرع الفرنسي هذا المشكل حيث اشترط على الموثق أو المحضر أن تكون الأنظمة المعلوماتية المستعملة من طرفهم معتمدة من طرف الهيئة المختصة (بالنسبة للموثقين المجلس الأعلى للتوثيقCSN أو الغرفة الوطنية للمحضرين القضائيين CNHJ كما أنه يجب استعمال توقيع إلكتروني مؤمن وفق الشروط المذكورة سابقا[3].

---

[1] l'article 1317 du Code civil par un alinéa 2. Désormais, l'acte authentique " *peut être dressé sur support électronique s'il est établi et conservé dans des conditions fixées par décret en Conseil d'Etat* ".

[2] المادة 324من القانون المدني الجزائري

[3]Pascal Agosti: « Le régime juridique des actes authentiques électroniques» ;www.caprioli-avocats.com

يمكن للموثق في فرنسا انطلاقا من 1 فيفري 2006 من تحرير العقود الرسمية حتى في غياب الأطراف المعنية، ولكن يستوجب في هذه الحالة أن يكون الطرف الغائب حاضر معه موثق ليتلقى منه رضاه وتصريحاته وتكون موقعة إلكترونيا من طرف هذا الموثق.

يجب على هذا الأخير أن يضع التاريخ للمحرر الرسمي بنفسه ويشير إليه بالكلمات ولا يعتمد على تقنية Horodatage[1] .

أما فيما يخص الحفاظ على التوقيع الإلكتروني فإنه يشترط أن يتم في ظروف تضمن سلامة الوثيقة وتسمح بقراءتها و أن يقوم الموثق أو المحضر بإرسالها خلال مدة 4 أشهر اللاحقة من تاريخ إعداد المحرر لتتم مراقبتها من طرف المجلس الأعلى للتوثيق أو من طرف الغرفة الوطنية للمحضرين القضائيين[2].

على الرغم من ذلك فإن معظم التشريعات لم تعتد بالتوقيع الإلكتروني في بعض الأوراق الرسمية مثل ذلك ما تنص عليه المادة 2 من قانون التجارة الإلكتروني البحريني :

« : التطبيق 1- تسري أحكام هذا القانون على السجلات والتوقيعات الإلكترونية .

2- يستثني من أحكام هذا القانون ما يلي :-

أ -كافة المسائل التي ينعقد الاختصاص بشأنها للمحاكم الشرعية طبقاً لأحكام المرسوم بقانون رقم (13) لسنة 1971 بشأن تنظيم القضاء وتعديلاته.

ب- مسائل الأحوال الشخصية لغير المسلمين مثل الزواج والطلاق والحضانة والتبني والميراث وإنشاء الوصايا وتعديلها.

ج- المعاملات والتصرفات التي يشترط القانون للاعتداد بها أن تكون مثبتة في محررات رسمية.

د - السندات القابلة للتداول .

---

[1] المادة 8 فقرة 2 من المرسوم 71-941

[2] المادة 28 فقرة 3 من المرسوم 71-941 و المادة 4-29 فقرة 4 من المرسوم 56-222

هـ - سندات الملكية، فيما عدا تلك المنصوص عليها في المادة (20) من هذا القانون.»

وهو نفس ما تم اتجهت إليه المادة 5 من قانون دبي الخاص بالمبادلات والتجارة الإلكترونية والمادة 6 من قانون التوقيع الإلكتروني والتجارة الإلكترونية في المملكة الأردنية الهاشمية.

إذ يرى البعض أن تحديد مجال إعمال التوقيع الإلكتروني على بعض المعاملات دون الأخرى هو نوع من التقصير لا لزوم له مادام أنه اعترف له بالحجية الكاملة مثله مثل التوقيع التقليدي ،كما أنه يعتبر تفرقة بين أنواع المعاملات وقصور في تطبيق القانون لا داعي له[1].

ثانيا:المعاملات المدنية أو التجارية:

إن الورقة العرفية قد تكون إما بمناسبة القيام بمعاملات مدنية أو تجارية، وبالتالي فإن التوقيع الإلكتروني يمكن استعماله في هذا المجال بل هو وجد لهذا الغرض أساسا ،ولهذا سنتطرق أولا إلى إعمال التوقيع الإلكتروني في المعاملات التجارية وثانيا في المعاملات المدنية .

أ:المعاملات التجارية:

إن المواد التجارية كمبدأ عام تخضع لحرية الإثبات[2] إلا فيما يخص بعض التصرفات التي تخضع لشكليات معينة[3] ،ولذا فإن الاعتماد على وسائل الإثبات الحديثة ومنها التوقيع

---

[1] المستشار عمرو عيسى الفقي، المرجع السابق،ص 141و14

[2] المادة 30 من القانون التجاري الجزائري

[3] مثل ذلك بيع المحل التجاري يجب أن يتم بعقد رسمي وفق المادة 79 من القانون التجاري الجزائري والشركات التجارية كذلك وهو ما تنص عليه المادة 545 قانون تجاري جزائري.

الإلكتروني ممكن في هذا المجال، ويترك أمر تقديرها إلى قاضي الموضوع بحسب ظروف وملابسات الدعوى المطروحة عليه[1].

يقصد بالمواد التجارية في هذا المجال هي تلك التي يكون أطرافها تجارا وموضوعها متعلق بأعمالهم التجارية، أما في حالة العقود المختلطة والتي يكون فيها أحد طرفي العقد غير تاجر فهو وحده الذي يستفيد من قاعدة الإثبات الحر في مواجهة التاجر المتعاقد معه[2] .

نلاحظ بالتالي أن القواعد الإثبات المقررة في المواد المدنية لا تطبق في مجال الأعمال التجارية

إذ يؤدي تطبيق هذه القواعد تعطيل التعامل وهو ما لا يتلاءم مع الطبيعة الخاصة للمعاملات التجارية والتي تقوم على عنصري السرعة في التعامل و الثقة الموجودة بين المتعاقدين ،فالتوقيع الإلكتروني يوفر هاته الميزات ما دام مستوفي شروطه المذكورة سابقا فإنه يصبح موثوقا به ويوفر عنصر السرعة لكون شبكة الانترنيت توفر الوقت بشكل كبير عن طريق البريد الإلكتروني .

ب :المعاملات المدنية:

1-حرية الإثبات في التصرفات التي لا تتجاوز حد معين:

معظم التشريعات تركت للأفراد حرية الإثبات في التصرفات المدنية إذا لم تتجاوز مبلغا معينا ففي الجزائر حدد ب 100000دج [3] وفي مصر 500جنيه [4] ،وبالتالي فإنه يمكن استعمال التوقيع الإلكتروني كوسيلة إثبات في هذا المجال مع ترك السلطة التقديرية للقاضي في الأخذ بها أو عدم الأخذ بها .

---

[1] د-سعيد سيد قنديل،المرجع السابق،ص38
[2] المستشار عمرو عيسى الفقي المرجع السابق،ص55
[3] المادة 333 قانون مدني جزائري
[4] المادة 60فقرة1 من قانون الإثبات المصري

2حالة المانع الأدبي أو المادي:

نصت عليه المادة 336 من القانون المدني الجزائري دون ذكر تعريف له .

يكون هذا المانع متوافرا متى استحال على الشخص الحصول على دليل كتابي لإثبات التصرف ، أو إذا أحاطت بالعلاقة التعاقدية ظروف خارجية لم تمكن المتعاقد من إعداد الدليل الكتابي[1]، مثل كإقراض شخص مالا طرأت الحاجة إليه وهو في الميناء على وشك السفر ، وعلى العموم يشترط أن يكون الحادث غير منتظر الوقوع أو جسيم بحيث يجعل التعاقد على الالتزام أمرا بلغ حدا من الاستعجال لا يتسع معه الوقت للحصول على السند الكتابي .

أما المانع الأدبي فهو يقوم على ظروف نفسية تجعل من الشخص المتعاقد لا يحصل على السند الكتابي وهذه الموانع هي :1-الزوجية والقرابة 2-علاقة الخدمة 3-العرف المتبع.

وتقدير ما إذا كان هناك مانع أدبي أو معنوي متروك للسلطة التقديرية لقاضي الموضوع[2].

ولكن هل يعتبر التعامل بوسائل الاتصال الحديثة مانعا من إعداد دليل كتابي ؟

هناك من اعتبر أن التعاقد عبر الهاتف يشكل مانعا ماديا للحصول على السند الكتابي[3]، إلا أن هذه الاستحالة لا تتحقق فيما لو أبرمت الصفقات عبر الانترنيت وهذا لاعتراف معظم التشريعات بالسند الإلكتروني مثله مثل السند المحرر على الورق.

إلا أن هناك البعض من حاول إقرار وجود المانع الأدبي في هذه الحالات وهذا ناتج عما فرضه العرف في هذه الصفقات، إذ أن معظم التجار اعتادوا أن لا يأخذوا دليلا كتابيا على ما يرسلونه إلى المنازل من مبيعات.

---

[1] د.الغوثي بن ملحة ، المرجع السابق، ص 44

[2] المستشار عمرو عيسى الفقي،المرجع السابق،ص67

[3] انظر في ذلك المستشار عمرو عيسى الفقي،المرجع السابق،ص71 و د-سعيد سيد قنديل،المرجع السابق،ص26

3-مبدأ الثبوت بالكتابة:

مقرر هذا المبدأ منصوص عليه في المادة 335 من القانون المدني الجزائري ويشترط في هذه الصورة شرطان وهما :

1-وجود الكتابة: مثل السند الغير موقع أو السجلات أو المراسلات ولا يكفي مجرد الأعمال المادية، أما الأوراق الموقعة فهي أدلة كاملة.

2-أن تكون صادرة من الخصم : ويكون هذا الصدور من الخصم إما ماديا أو معنويا، ويتحقق الصدور المادي بكتابة الخصم للورقة أما الصدور المعنوي فعندما يمليها الخصم وهذا عندما يكون أميا أو إثبات أقواله في محضر[1] ،ويعتبر في حكم الخصم من يمثله قانونا أمام القضاء كالوكيل أو الوصي.

أما مستخرجات الوسائل التكنولوجية الحديثة فالرأي الراجح هو إعطائها صفة بداية الثبوت بالكتابة كالرسائل الإلكترونية أو مستخرج الحاسب الآلي الناتج عن جهاز الصرف الآلي لكونه صادر من الخصم و لا يظهر بهذا الشكل إلا بعد أن يقوم بعدة إجراءات [2]، كما يعتبر مبدأ ثبوت بالكتابة للبنك لأنه يخضع للتشغيل من طرف البنك .

بعدما أوضحنا في الفصل الأول مكانة التوقيع الإلكتروني ضمن وسائل الإثبات الحديثة، فإننا سنتطرق في الفصل الثاني إلى الضمانات القانونية التي تجعل من التوقيع الإلكتروني طريقة آمنة في إبرام العقود ومختلف التصرفات التي تتم بالطريقة الإلكترونية.

---

[1] المستشار عمرو عيسى الفقي،المرجع السابق،ص.61

[2] هذه الإجراءات هي أولا إدخال البطاقة ثم إدخال الرقم السري ثم تحديد المبلغ المطلوب.

الفصل الثاني: التوقيع الإلكتروني و الأمان القانوني

ستنصب دراستنا في المبحث الأول إلى عملية التصديق التي تعتبر الحجر الزاوية للتوقيع الإلكتروني، حيث يتدخل بموجبها طرف ثالث يسمى «مزود الخدمات»، ويجب أن يتحصل إما على تفويض أو ترخيص للممارسة نشاطه ، بعدما يستوفي الشروط التي أوجبتها القوانين، مع تحمله للمسؤولية المدنية إذا ما أضر بأحد الأطراف سواء كان موقعا أو مرسل إليه أو حتى طرفا معولا فقط .

يصدر هذا الأخير « شهادة التصديق الإلكتروني» لدلالة على صحة التوقيع عندما يتم طلبها من المرسل إليه، والتي يجب أن تحتوي على بيانات معينة، إذ يجب إلغائها أو تعليق العمل بها في حال وجود شك فيها أو نهاية العمل بالتوقيع الإلكتروني.

أما المبحث الثاني فسنعالج فيه كيف تتم حماية التوقيع الإلكتروني أثناء إعماله من طرف الموقع والمرسل إليه باعتبارهم وحدهم الذين يقومون بإعمال التوقيع الإلكتروني ثم دراسة الحماية الجنائية للتوقيع الإلكتروني بعد إعماله، ومختلف الجرائم الواقعة على التوقيع والعقوبات المقررة لكل جريمة التي غالبا ما تكون إما غرامة أو عقوبة الحبس.

المبحث الأول: مقومات الأمان : التصديق

يتميز التوقيع الإلكتروني عن التوقيع التقليدي بتدخل طرف ثالث تكون مهمته الأساسية تأكيد أن المفتاح العام هو فعلا للمرسل الرسالة، وبمعنى أخر تأكيد لشخصية هذا المرسل وصلاحيته وهو ما يطلق عليه ب «مزود الخدمات» (المطلب الأول).

حيث يقوم هذا الأخير بإصدار« شهادة التصديق الإلكتروني» التي تهدف أساسا لتأكيد صحة التوقيع الإلكتروني وأنه منسوب للموقع دون سواه وهو ما يتيح للأطراف المتعاقدة التعارف فيما بينهم وتحديد هويتهم بشكل يوفر الطمأنينة في نفوسهم (المطلب الثاني)

المطلب الأول: مزود الخدمات (PSC)

إن تدخل طرف ثالث في التوقيع الإلكتروني يعتبر ضروريا بل أساسيا ،لكون الأطراف المتعاقدة مع بعضها البعض خاصة في الشبكات المفتوحة(الانترنيت)ليس لها معرفة مسبقة فيما بينها وهو ما يقوم به مزود الخدمات .

كما أن عدم التأكد من هوية المتعاقدان يجعل حجية التوقيع الموضوع على الصفقة بطيء والصفقة كلها محل منازعة وشك[1].

لقد أصبح بالتالي لمزود الخدمات دور هام في مجال التجارة الإلكترونية على العموم والتوقيع الإلكتروني على الخصوص ،ونظرا للثقل الاقتصادي الكبير الذي أصبح يشكله مزود الخدمات في توفير الأمان القانوني على مستوى شبكة الانترنيت فإن الدول وضعت شروطا معينة يجب على هذا الأخير أن يستوفيها حتى يتمكن من ممارسة نشاطه وهو ما سنتطرق إليه في الفرع الأول.

بمجرد أن يستوفي مزود الخدمات الشروط القانونية الموضوعة من طرف الدولة فإنه تقع على عاتقه مجموعة من الالتزامات تجاه الهيئة المختصة أو المتعاملين بالتوقيع الإلكتروني (الفرع الثاني).

غير أنه إذا ما أخل بهذه الالتزامات تترتب على عاتقه المسؤولية المدنية سواء كان ذلك على أساس المسؤولية العقدية أو التقصيرية حسب كل حالة (الفرع الثالث).

---

[1] د-سعيد سيد قنديل،المرجع السابق،ص 74

الفرع الأول : شروط ممارسة عملية التصديق

أطلقت عدة تسميات على القائم بعملية التصديق فهناك من سماه مقدم خدمات التصديق[1] أو جهة التصديق[2] أو مزود خدمات التصديق[3] إلخ...

لقد وردت عدة تعريفات له فمثلا المشرع التونسي عرفه في الفصل الثاني من القانون المتعلق بالمبادلات والتجارة الإلكترونية بأنه« كل شخص طبيعي أو معنوي يحدث ويسلم ويتصرف في شهادات المصادقة ويسدي خدمات أخرى ذات علاقة بالإمضاء الالكتروني»،أما مشرع إمارة دبي عرفه ب« ـ أي شخص أو جهة معتمدة أو معترف بها تقوم بإصدار شهادات تصديق الكترونية أو أية خدمات أو مهمات متعلقة بها وبالتواقيع الالكترونية والمنظمة بموجب أحكام الفصل الخامس من هذا القانون»، و المشرع الفرنسي عرفه في المادة 1 من المرسوم 272-2001 بأنه :«كل شخص يسلم شهادات إلكترونية أو خدمات أخرى متعلقة بالتوقيع الإلكتروني»[4]

نظرا للدور الكبير الذي يلعبه مزود الخدمات في التوقيع الإلكتروني باعتباره الرابط الوحيد بين الموقع والمرسل إليه، إضافة إلى ذلك فهو الذي يقوم بتحديد هوية الموقع ومدى صلاحية توقيعه الإلكتروني ،فإن التشريعات في هذا المجال رأى من الضرورة بمكان أن تنص على شروط معينة حتى يستطيع مزود الخدمات ممارسة نشاطه ، و أهمها هي إصدار الترخيص أو التفويض الإداري .

---

[1] مثل قانون الأونيسترال النموذجي بشأن التوقيعات الإلكترونية

[2] وهو المصطلح المستعمل من طرف المشرع المصري في قانون التوقيع الإلكتروني

[3] يستعمل هذا المصطلح لدى مشرع إمارة دبي

[4] 11. « Prestataire de services de certification électronique » : toute personne qui délivre des certificats électroniques ou fournit d'autres services en matière de signature électronique ;»

أولا: منح الترخيص أو التفويض لمزاولة عملية التصديق :

إن ممارسة أي عمل مهني بشكل غير منتظم قد يترتب عليه في بعض الحالات فوضى وعدم استقرار في المعاملات وضياع حقوق الأطراف المعنيين بالتصرف[1] ،ولذلك فإن الدول والتشريعات قد فرضت إما أن يتحصل مزود الخدمات على تفويض أو ترخيص وهو ما سنتعرض إليه بالتفصيل إتباعا.

1-التفويض الإرادي « accréditation volontaire» :

وفقا للتعليمة الأوروبية بشأن التوقيع الإلكتروني فإن القيام بمهام مزود الخدمات لا يخضع إلى أي ترخيص مسبق[2].

إلا أنه يمكن لكل دولة أن تنص على ضرورة وجود تفويض للقيام بمهمة مزود الخدمات بناءا على طلب من هذا الأخير إلى الجهات المختصة المعهود إليها أساسا بهذه الحقوق والالتزامات ، ولهذه الجهة الترخيص بعد ذلك إذا توافرت لمقدم الخدمات ما يؤهله للقيام بهذه المهمة وفق ما يتم وضعه من ضوابط في هذا الشأن[3] .

سار المشرع الفرنسي على هذا النهج حيث لم يفرض على الشركات العاملة في هذا المجال أي ترخيص مسبق للممارسة عملية التصديق، وإنما يمنح لمزود الخدمات صفة«المؤهل[4]»،بمجرد أن يستوفي الشروط المذكورة في المادة 6 من المرسوم 2001-272[5].

---

[1] د-سعيد سيد قنديل،المرجع السابق،ص 77

[2] المادة 1/3من التعليمة الأوروبية تنص : « Les états membres ne soumettent la fourniture des services de certification à aucune autorisation préalable»

[3] د-سعيد سيد قنديل،المرجع السابق،ص78

[4] qualifié

[5] المادة 7 فقرة 1 من المرسوم 2001-272 تنص :

«Les prestataires de services de certification électronique qui satisfont aux exigences fixées à l'article 6 peuvent demander à être reconnus comme qualifiés.»

حيث منح المشرع الفرنسي لهيئات خاصة منح التفويض لمزودي الخدمات، وتكون معينة بواسطة قرار من وزير الصناعة[1] .

حيث تقوم هذه الأخيرة قبل منحها التفويض بتقييم مزود الخدمات بموجب شروط محددة في القرار الصادر عنها[2] ، وهو ما يعتبر مطابقا لما ورد في المادة 2-13 من التعليمة الأوروبية التي أقرت بحق الدول بأن يكون لها هيئات خاصة بمنح التفويض لمزود الخدمات لممارسة مهامه، [3] وهو عبارة عن ترخيص يشار فيه إلى واجبات وحقوق مزود الخدمات.

تهدف أنظمة التفويض الإرادي بحسب التعليمة الأوروبية إلى ضمان أحسن الخدمات من طرف مزود الخدمات ،وإيجاد الإطار الملائم لتطوير خدماتهم من أجل الوصول إلى درجة الثقة والأمان والجودة المطلوبة ، ولهم الحرية الكاملة للالتزام بهذه الأنظمة والاستفادة منها[4].

كما سار على هذا المنهج المشرع الفرنسي عندما أقر هذه الحرية عندما استعمل عبارة «يمكنهم» في المادة 7 من المرسوم 272 -2001 ،أي أن لهذا الأخير حرية الخضوع لنظام التفويض الإداري أو عدم الخضوع له.

---

[1] على سبيل المثال نجد حاليا مركز الخدمة الرئيسي لأمن نظم المعلومات في فرنسا ويرمز لهذا المركز ب SCSSI Le service central de la sécurité des systèmes d'information وهناك BSI في ألمانيا و NSA في الولايات المتحدة الأمريكية إلخ...

[2] المادة 7 فقرة 2 من نفس المرسوم:

«Cette qualification, qui vaut présomption de conformité auxdites exigences, est délivrée par les organismes ayant reçu à cet effet une accréditation délivrée par une instance désignée par arrêté du ministre chargé de l'industrie. Elle est précédée d'une évaluation réalisée par ces mêmes organismes selon des règles définies par arrêté du Premier ministre.»

[3] «accréditation volontaire »,toute autorisation indiquant les droits et obligations spécifiques à la fourniture de services de certification,accordée,sur demande du prestataire de service de certification concerné,par l'organisme public ou privé chargé d'élaborer ces droits et obligations et d'en contrôler le respect,lorsque le prestataire de service de certification n'est pas habilité à exercer les droits découlant de l'autorisation aussi longtemps qu'il n'a pas obtenu la décision de cet organisme»

[4] les régimes volontaires d'accréditation visant à assurer un meilleur service fourni peuvent constituer pour les prestataires de service de certification le cadre propice à l'amélioration de leurs services afin d'atteindre le degré de confiance,de sécurité et de qualité exigés par l'évolution du marché;il est nécessaire que de tels régimes incitent à mettre au point des règles de bonne pratique entre prestataires de service de certification;il y a lieu que ces derniers restent libres de souscrire à ces régimes d'accréditation et d'en bénéficier;

2-الترخيص:

أما نظام الترخيص المعمول لدى معظم الدول العربية فهو يختلف عن نظام التفويض، فالأول يعطي الحرية كاملة لمزود الخدمات في الخضوع إليه أو عدم الخضوع له ويبقى هذا الأخير يمارس مهامه حتى ولو لم يتحصل على التفويض .

أما الثاني فإنه يجبر مزود الخدمات أن يتحصل على الترخيص حتى يمارس مهامه على أراضي الدولة .

غير أن الحصول على الترخيص يختلف من دولة إلى أخرى، ولهذا فسنتطرق إلى موقف كل مشرع على حدة.

أ- المشرع البحريني:

لقد ميز المشرع البحريني في قانون التجارة الإلكتروني بين نوعين من مزودي خدمات الشهادات[1] ،فهناك المعتمد والغير معتمد والمعيار الفاصل بينهما هو أن الأول يخضع لأحكام المادة 16و 17 والتي تفرض على هذا الأخير الحصول على رخصة أو اعتماد وتتم وفق خطوات يجب على مزود الخدمة احترامها وهي:

- يجب على هذا الأخير أن يتقدم بطلب إلى الوزارة للموافقة على اعتماده
- يصدر قرار من الوزير بالموافقة على الطلب وإدراجه في سجل« مزودي الخدمات المعتمدين» بعدما يكون قد استوفى الشروط المقررة في هذا الشأن ،
- يجب على مزود الخدمة أن يدفع الرسوم المترتبة عن عملية التسجيل
- أخيرا ينشر القرار في الجريدة الرسمية.

أما النوع الثاني من مزودي الخدمات فلا يخضع لهذه الشروط ، و لا يحق لهم حتى ممارسة أنشطتهم على إقليم الدولة حتى يصبحوا معتمدين.

---

[1] هذا هو المصطلح المعتمد عند المشرع البحريني بالنسبة لمزود الخدمات

غير أن التساؤل يبقى مطروحا حول جدوى هذا التقسيم ، إذ كان الأجدر أن يقوم المشرع البحريني في هذه الحالة بذكر الشروط الضرورية واللازمة للحصول على الترخيص من دون السعي إلى التمييز بين مزود خدمات معتمد وأخر غير معتمد ما دام أن هذا الأخير لن يستطيع في جميع الأحوال ممارسة نشاطه على إقليم الدولة.

ب-مشرع إمارة دبي:

كما تبنى المشرع في إمارة دبي نفس الموقف عندما نص صراحة في المادة 23 من قانون المبادلات والتجارة الإلكترونية على ضرورة تعيين مراقب لخدمات التصديق من طرف رئيس سلطة منطقة دبي الحرة للتكنولوجيا والتجارة الإلكترونية والإعلام تكون من بين مهامه منح التراخيص الضرورية لمزودي الخدمات.

نظرا لجسامة المهام التي يقوم بها المراقب أعطى مشرع إمارة دبي لهذا الأخير أن يفوض أي شخص تحت مسؤوليته للقيام بهذه المهمة بشرط أن يكون هذا التفويض مكتوبا حتى يستطيع هذا الأخير أن يثبت الصلاحيات المخولة له أثناء تعامله مع مزودي الخدمات[1].

ج- المشرع المصري:

أما في مصر وبموجب المادة 4 من قانون التوقيع الإلكتروني فإن مهمة إصدار وتجديد التراخيص لمزاولة أنشطة خدمات التوقيع الإلكتروني فإنها موكلة إلى هيئة تنمية صناعة تكنولوجيا المعلومات.

---

[1] **مادة (23)** (1) لأغراض هذا القانون يعين الرئيس بقرار يصدره، مراقباً لخدمات التصديق وعلى وجه الخصوص لأغراض ترخيص وتصديق ومراقبة أنشطة مزودي خدمات التصديق والإشراف عليها، وينشر هذا القرار في الجريدة الرسمية.

(2) يجوز للمراقب أن يفوض كتابة أياً من مسئولياته بموجب هذا الفصل لمن يراه.

(3)يعتبر المراقب أو المفوض من قبله موظفاً عاماً.

(4) على المفوض إن يبرز عند ممارسته أيا من الصلاحيات المخولة له واستجابة لطلب الشخص الذي يتصرف تجاهه، ما يثبت الصلاحية التي خوله إياها المراقب.

بالإضافة إلى ذلك ووفق المادة 5 من نفس القانون فإن مزود الخدمات ملزم بدفع رسم لصالح الهيئة بقيمة واحد في المائة من إيرادات مزود الخدمات حتى يتم إصدار وتجديد التراخيص.

يعتبر مزود الخدمات في مصر في نفس مركز صاحب الامتياز لأنه يقوم بعمل من المفروض أن تقوم به إحدى جهات الإدارة العامة ،إلا أنه لا تطبق عليه أحكام عقد الامتياز حتى يعطيه قدرا من الحرية في العمل بالنظر إلى طبيعة المعاملات الإلكترونية التي يقوم بها[1] .

كما أن هيئة تنمية صناعة تكنولوجيا المعلومات ملزمة عند إصدار الترخيص بإتباع الإجراءات التالية :

1- يتم اختيار المرخص له في إطار المنافسة العلنية قصد إعطاء الفرصة لأكبر عدد ممكن من مزودي الخدمات التقدم للحصول على الترخيص.

2- على مجلس إدارة هيئة تنمية صناعة تكنولوجيا المعلومات تجديد التراخيص وأن لا تزيد عن 99 سنة ومن الممكن أن تقل عن ذلك.

3-لا بد أن تحدد سلطة الترخيص الضوابط التي عن طريقها سوق يتم الإشراف والمتابعة للمرخص له سواء من الناحية الفنية أو المالية.

4- على المرخص له الاستمرار في النشاط المرخص له وأن لا يتوقف عنه أو يندمج في جهة أخرى للقيام بذات العمل أو يتنازل عن الترخيص للغير إلا بموافقة سلطة الترخيص، حتى لا تجد السلطة المذكورة نفسها أمام آخرين لم ترخص لهم[2].

---

[1] المستشار عبد الفتاح بيومي حجازي،المرجع السابق ،ص455

[2] راجع المادة 19 من قانون التوقيع الإلكتروني المصري.

د- المشرع التونسي:

أما المشرع التونسي فبدوره لم يخرج عن هذا الإطار و أكد على وجوب أن يتحصل مزود الخدمات على ترخيص مسبق من الوكالة الوطنية للمصادقة الإلكترونية [1].

مع ضرورة أن يخضع مزود الخدمة إلى دفتر شروط يتضمن ما يلي:

- كلفة دراسة ومتابعة ملفات مطالب الشهادات .
- آجال دراسة الملفات.
- الإمكانيات المادية والمالية والبشرية التي يجب توفرها لتعاطي النشاط.
- شروط تأمين التفاعل المتبادل لأنظمة المصادقة وربط سجلات شهادات المصادقة .
- القواعد المتعلقة بالإعلام والخاصة بخدماته والشهادات التي سلمها والتي يتعين على مزود خدمات المصادقة الالكترونية حفظها [2].

ثانيا: شروط أخرى

1-بالنسبة للتعليمة الأوروبية و فرنسا:

فحتى وإن كانت التعليمة الأوروبية رفضت أن تضع الدول الترخيص المسبق كشرط لممارسة مهنة مزود الخدمات، إلا أنها وضعت مجموعة من الشروط في الملحق رقم 2 يجب على هذا الأخير أن يحترمها وهي:

- ضمان عمل خدمة الدليل بشكل سريع و آمن وخدمة العدول كذلك .
- مراقبة هوية الشخص الممنوح له الشهادة بوسائل ملائمة ومطابقة للقانون الوطني .
- استعمال أنظمة موثوقة.

---

[1] الفصل 11 من القانون المتعلق بالمبادلات والتجارة الإلكترونية التونسي
[2] الفصل 12 فقرة 2 من نفس القانون

- أرشفة المعلومات المرتبطة بالشهادات خلال المدة المطلوبة لذلك وبالخصوص إعطاء الشهادة الحجية أمام القضاء.
- التوفر على موارد مالية كافية.

أما فرنسا فقد جاء المرسوم 272- 2001 مسايرا لما ورد في التعليمة الأوروبية بشأن التوقيعات الإلكترونية حيث لم تضع الترخيص كشرط مسبق لممارسة مهام مزود الخدمات، وإنما وضعت شروطا أخرى الهدف منها أن يصبح مزود الخدمات معتمدا أو مؤهلا وقد وردت هذه الشروط في المادة 6 الفقرة 2 من المرسوم 272-2001 ومن خلالها يمكن أن نلاحظ أن المشرع الفرنسي ركز على ما يلي:

-أن يثبت مزود الخدمات أن خدمات التصديق الإلكتروني موثوق فيها .

- يوفر شهادات تصديق إلكترونية معتمدة وآمنة وغير قابلة للتعديل بحيث يحدد هوية الموقع بشكل كافي بحيث يمكن أن تستعمل كدليل إثبات أمام القضاء.
- يجب أن تكون له الإمكانيات المادية والبشرية لمزاولة نشاطاته.
-حفظ المعلومات المتعلقة بالتوقيع الإلكتروني في مدة معينة.

كما نجد أن أغلبية الدول قد ربطت منح الترخيص لمزود الخدمات بضرورة أن يستوفي هذا الأخير مجموعة من الشروط ، وهي تختلف من دولة إلى أخرى .

3-بالنسبة للمشرع التونسي:

لقد وضع القانون التونسي شروطا معينة حتى يمنح الترخيص لمزود الخدمات وهي:- الجنسية التونسية –الإقامة في تونس –أن يكون طالب الترخيص متمتعا بحقوقه المدنية و السياسية ونقي السوابق العدلية –الحصول على الشهادات العلمية الضرورية لذلك وهي على

الأقل الشهادة الإعدادية أو ما يعادلها –وأخيرا عدم الارتباط بنشاط مهني أخر[1]

4-بالنسبة للمشرع البحريني:

إن المشرع البحريني عكس المشرع التونسي لم يشترط الجنسية والإقامة لممارسة مهنة التصديق الإلكتروني بل ركز بشكل كبير على الوسائل التقنية الكفيلة بجعل التوقيع الإلكتروني يشكل وسيلة آمنة في التعامل بها وهو ما يظهر جليا في المادة 4 فقرة 2 من قانون التجارة الإلكتروني البحريني وهذه الشروط هي كما يلي :

أ- الأسلوب والصيغة – بما في ذلك معايير أنظمة المعلومات – التي يجب الالتزام بها في إنشاء و إرسال و بث و تسلم و حفظ السجلات الإلكترونية، والأنظمة التي تستعمل لذلك .

ب- إذا كان مطلوباً استعمال توقيع إلكتروني لاعتماد سجل إلكتروني ، فإنه يلزم تحديد نوع التوقيع الإلكتروني المطلوب ، ومعايير نظام المعلومات المطلوب استعمالها ، وأسلوب وصيغة وضع التوقيع على السجل ، وأية اشتراطات أخرى يلزم توافرها للتحقق من صحة هذا التوقيع .

ج- أنظمة وإجراءات السيطرة المناسبة لحفظ وسلامة وأمان وخصوصية السجل الإلكتروني وقابليته للتدقيق وكيفية التخلص منه .

د- أية خصائص أخرى للسجلات الإلكترونية تعتبر ضرورية أو مناسبة في هذا الشأن.

هـ- أية اشتراطات بشأن الإقرار بتسلم السجلات الإلكترونية من قبل الجهات العامة .

الفرع الثاني: التزامات مزود الخدمات

بمجرد أن يستوفي مزود الخدمة الشروط التي تضعها الدول له فإن ذلك يعني بالضرورة أنه تقع عليه التزامات عديدة يجب أن يوفي بها.

---

[1] هذه الشروط مذكورة في الفصل 11 من قانون المبادلات والتجارة الإلكترونية

إن هذه الالتزامات تنصب أساسا على إنشاء التوقيع الإلكتروني والتأكد من صحته و ذلك بإصدار شهادات الإلكترونية، والموارد المالية المستخدمة من طرف مزود الخدمات.

فعند إنشاء المفاتيح العامة يعتبر مقدم خدمة التوثيق[1] جهازا مستقلا تتحدد وظائفه في التحقق والتأكد من هوية وطبيعة الشخص الحامل للمفتاح العام ،وإصدار الشهادات الإلكترونية التي تربط بين الشخص والمفتاح العام .

إضافة إلى وظيفة أخرى تتعلق بالإشهار الكافي لتلك الشهادات الصادرة منه وتوفير المعلومات الخاصة بالموقعين المحددين في الشهادات، وتوفير المعلومات اللازمة للأطراف المعتمدة على خدمات التصديق[2] .

غير أن هناك من الفقهاء من حدد مهام والتزامات مزود الخدمات في ثلاث نقاط أساسية وهي:

1- تحديد هوية المتعاملين في التعاملات الإلكترونية وتحديد أهليتهم القانونية للتعامل والتعاقد، والتحقق من مضمون هذا التعامل وسلامته، وكذلك جديته وبعده عن الغش والاحتيال.

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

3- تقوم جهات التصديق بإصدار التوقيع الرقمي وشهادات توثيق هذا التوقيع التي تشهد بمقتضاها على صحته ونسبته إلى من صدر عنه[3] .

---

[1] هو نفسه مزود الخدمات

[2] أ/قارة مولود ،المرجع السابق،ص84

[3] المستشار عبد الفتاح بيومي حجازي،المرجع السابق ،ص134

1- التزامات مزود الخدمات في إمارة دبي وقانون الأونيسترال :

من خلال استقراء المادة 24 من قانون إمارة دبي الخاص بالمبادلات والتجارة الالكترونية نستنتج أن التزامات مزود الخدمات تنحصر في :

-إصدار شهادة تصديق تحتوي على البيانات الجوهرية وتكون مرتبطة بالموقع[1].

-إعطاء الضمانات القانونية بشأن أداة التوقيع وتحديد هوية الموقع بشكل كافي، إذ يجب على مزود الخدمات أن تكون لديه وسائل فعالة لإلغاء منظومة التوقيع الإلكتروني في حال تعرضه للاعتداء وهذا حماية للموقع والمتعاملين به[2]،

-يجب على مزود الخدمات أن تتوفر لديه إجراءات وموارد بشرية جديرة بالثقة وفق معايير حددها المشرع [3].

تجدر الملاحظة أن المشرع في إمارة دبي قد تبنى نفس الشروط الواردة في قانون الأونيسترال النموذجي بشأن التوقيعات الإلكترونية ،حيث أن المادة 9 منه بينت السلوك الواجب إتباعه من طرف مقدم الخدمات (الواجبات) ، ثم عنون المادة 10 ب«الجدارة بالثقة» حيث وضح على وجه الدقة الشروط التي يجب أن تتوافر في مزود الخدمات حتى يمكن الثقة في النظم والموارد البشرية المستعملة لديه وهي:

أ- الموارد المالية والبشرية بما في ذلك توافر الموجودات ،أو

ب- جودة نظم المعدات والبرمجيات ،أو

ت- أو إجراءات تجهيز الشهادات وطلبات الحصول على الشهادات والاحتفاظ بالسجلات ،أو

ث- إتاحة المعلومات للموقعين المعينة هويتهم في الشهادات والأطراف المعولة المحتملة ،أو

---

[1] المادة 24 فقرة 3 من قانون إمارة دبي الخاص بالمبادلات والتجارة الإلكترونية

[2] المستشار عبد الفتاح بيومي حجازي،المرجع السابق ،ص207

[3] المادة 24 فقرة 2 من نفس القانون

ج- انتظام ومدى مراجعة الحسابات من جانب هيئة مستقلة، أو

ح- وجود إعلان من الدولة أو من هيئة اعتماد أو من مقدم الخدمات التصديق بخصوص الامتثال لما سبق ذكره أو بخصوص وجوده، أو

خ- أي عامل أخر.

2- التزامات مزود الخدمات في مصر:

هذه الالتزامات هي نفسها الموجودة في مشروع قانون التوقيع الإلكتروني المصري،إذ يجب أن يصدر مزود الخدمات شهادة تصديق دقيقة من حيث محتوياتها بحيث تسمح بتحديد هوية منشأ الوثيقة وإمكانية الإطلاع عليها وذكر كل القيود الواردة على هذه الشهادة ومدة صلاحيتها ، ويجب عليه أن يتعامل وفق أصول الأمانة بأن يحافظ على سرية البيانات والمعلومات التي يقدمها طالب التوقيع الإلكتروني[1]، و أن يستخدم وسائل وإجراءات فنية من العاملين يعتمد عليهم في أداء الخدمة المطلوبة.

3- التزامات مزود الخدمات في تونس:

لقد ركز المشرع التونسي في القانون المتعلق بالمبادلات والتجارة الإلكترونية على أن يقوم مزود الخدمات بإصدار وتصميم وحفظ الشهادات[2] وأن تكون هذه الأخيرة موثوق بها وتستجيب لمعايير السلامة ،واستعمال وسائل موثوقة بها من أجل هذا الغرض[3].

كما أنه يلتزم بمسك سجل الكتروني لشهادات المصادقة يحتوي على شهادات المصادقة وعند اللزوم، تاريخ تعليق الشهادات أو إلغاؤها[4].

---

[1] المادة 9 من مشروع قانون لتنظيم التوقيع الإلكتروني

[2] الفصل 12 من قانون المبادلات والتجارة الإلكتروني

[3] الفصل 13 من نفس القانون

[4] الفصل 14 من نفس القانون

بالإضافة إلى ذلك يتولى تعليق العمل بالشهادة أو إلغائها إن اقتضى الأمر ذلك وأن يعلم صاحب الشهادة بهذا القرار.

يمكن أن يقوم مزود الخدمات بمهام أخرى لها علاقة بالتوقيع الإلكتروني وخاصة منها:

-ترقيم وبيان تاريخ الإمضاء horodotage

- ضمان سلامة وعدم إنكار التبادل الإلكتروني hachage

-إنشاء منظومات الإحداث والتدقيق في التوقيع.

-تسجيل تاريخ وساعة إرسال البيانات وتاريخ وساعة وصولها.

-التعريف بالمتعاملين التجاريين ومقراتهم وعناوينهم.

-مسك قاعدة بيانات تدرج بها أنشطة العاملين بالقطاع التجاري وجميع ما يرتبط بذلك.

إلا أن المشرع التونسي قد سكت عن جميع هذه المهام وخاصة ما يتعلق بتنظيم مسألة التاريخ وتحديد مفاهيمها وضبط نظامها وأركانها، لما لتأريخ التوقيع من أهمية كبرى في معارضة الغير بالورقة العرفية[1] .

يعتبر ذلك مفهوما موسعا لمهام مزود الخدمات وهو نفس المفهوم الذي تبناه الإتحاد الأوروبي في التعليمة المتعلقة بالتوقيع الإلكتروني[2].

4- التزامات مزود الخدمات في التعليمة الأوروبية و فرنسا:

لقد ركزت التعليمة الأوروبية على ضرورة أن يستخدم مزود الخدمات أشخاص لهم معارف محددة والخبرة اللازمة لأجل القيام بمهمة تزويد الخدمات، خاصة الكفاءة في التسيير والمعارف في مجال تكنولوجيا التوقيع الإلكتروني.

---

[1] أ /علي كحلون،المرجع السابق،ص 302

[2] أ/علي كحلون،المرجع السابق،ص300

إضافة إلى ذلك أن يستعمل مزود الخدمات أنظمة ومواد موثوق فيها محمية من أي تعديل وأن يضمن الأمن التقني للمهام التي يقوم بها.

أن يمتلك هذا الأخير الموارد المالية اللازمة للقيام بمهامه وفق الشروط المنصوص عليها في التعليمة وخاصة تغطية مسؤوليته في حال ما إذا سبب أضرارا[1]

أما المشرع الفرنسي في المادة 11 من المرسوم 535-2002 أوجب على مزود الخدمات أن يثبت قيامه بالتزامات معينة حتى يمكن أن يمنح له التفويض وهي كما يلي:

- مطابقته لمعايير الجودة وفق قواعد ومقاييس التفويض المعمول بها.
- كفاءته لتطبيق معايير التقييم المعمول بها والمنهجية الملائمة لذلك بالإضافة إلى ضمان السرية المطلوبة أثناء التقييم .
- القدرة التقنية لأن يسير هذا التقييم.

على العموم يتمثل الالتزام الرئيسي لمزود الخدمات في منح صاحب الشأن شهادة الإلكترونية تحقق الغرض من وظيفته وهو التصديق على التوقيع الإلكتروني المستخدم في صفقة معينة بما يجعل هذا التصديق إقرارا بمضمون الصفقة[2] .

هناك من الفقهاء من رأوا أن مزود الخدمات يجب أن تهدف إلى إرساء الثقة في التوقيع الإلكتروني ،وبالتالي فإن التزاماته تتمثل أساسا في :

- حفظ المفتاح الخاص وجعله سري.
- استعمال المفتاح الخاص من طرف الموقع دون سواه.
- المراقبة الأكيدة من طرف صاحب الوثيقة قبل التوقيع .
- عدم تزوير شهادة التصديق.
- التفسير الصحيح للرسالة.

---

[1] Arnaud-f .Fausse ;op.cit. ,p161

[2] د-سعيد سيد قنديل،المرجع السابق ،ص 90

وهذا ما يستلزم أن يوفر مزود الخدمات قسمين أساسيين هما:

أولا : توفير منتجات أمنة مثل البرمجيات ،العتاد ،البطاقات الممغنطة إلخ...

ثانيا : يجب أن تكون له أنظمة أمن ومعلومات خاصة فيما يتعلق بتحديد الهوية والمفاتيح إلخ...[1]

الفرع الثالث : مسؤولية مزود الخدمات :

إن تحميل مزود الخدمات المسؤولية المدنية سواء منها العقدية أو التقصيرية يعتبر أمرا بديهيا إذ من الضروري توافر الضمانات القانونية في حال ما إذا لم يحترم هذا الأخير التزاماته[2] ،ويكون حق التعويض عن الأضرار المترتبة على الخطأ أيا كان مصدره أو سببه مكفول للمضرور سواء لصالح أحد المتعاقدين أو الغير أو ضدهما[3] .

حيث لم تخرج عن نطاقه معظم التشريعات، فمنحت الحق للمرسل إليه والغير والموقع الحق في التعويض عن الأضرار الناجمة عن إخلال مزود الخدمات بالتزاماته المذكورة في الفرع السابق.

من أهم التزامات مزود الخدمات إصدار شهادة تصديق صحيحة وموثوق فيها ،وإلا يحق لكل شخص يثق بمحتوى شهادة التصديق ثم وجد سبب للشك في محتواها أو تم اكتشاف عدم صحة المعلومات الواردة فيها أن يطلب التعويض عن الأضرار اللاحقة به وفق قواعد المسؤولية التي تقع على مزود الخدمات المنصوص عليها في المادة 6 من التعليمة الأوروبية[4]،وكذلك يكون مسئولا عن صحة العلاقة بين الموقع والمفتاح العام[5]

---

[1] Arnaud-f .Fausse ;op.cit. ,p59

[2] Valérie Sédaillian :« ,Preuve et signature électronique,Juriscom .»net,9 mai 2000

[3] المستشار عبد الفتاح بيومي حجازي،المرجع السابق ،ص117

[4] Pierre bresse :«guide juridique de l'internet et du commerce électronique»,entreprendre informatique,1998 ,p319

[5] د.سعيد سيد قنديل،المرجع السابق ،ص 94

نجد أن المشرع التونسي في الفصل 22 الفقرة 1و2 من قانون المبادلات والتجارة الإلكترونية قد وضع قاعدة عامة لهذه المسؤولية حيث نص:« يكون مزود خدمات المصادقة الالكترونية مسئول عن كل ضرر حصل لكل شخص وثق عن حسن نية في الضمانات المنصوص عليها بالفصل 18 من هذا القانون .

ويكون مزود خدمات المصادقة الالكترونية مسئولا عن الضرر الحاصل لكل شخص نتيجة عدم تعليق أو إلغاء شهادة طبقا للفصلين 19 و 20 من هذا القانون.»

حيث أنه قام بالجمع بين المسؤولية العقدية والتقصيرية لمزود الخدمات عندما استعمل عبارة « لكل شخص» ، فالمقصود بها هو إما الموقع فنكون هنا بصدد المسؤولية العقدية لوجود عقد بينهما،أو المرسل إليه فيتم إعمال قواعد المسؤولية التقصيرية .

لقد كان مشرع إمارة دبي أكثر وضوحا في هذا المجال فميز بين المسؤولية التقصيرية والعقدية لمزود الخدمات في المادة 24 فقرة 4 من قانون المبادلات والتجارة الالكترونية التي نصت :« إذا حدثت أية أضرار نتيجة لعدم صحة الشهادة أو نتيجة لأي عيب فيها، يكون مزود خدمات التصديق مسئولاً عن الخسائر التي يتكبدها:

(أ)- كل طرف تعاقد مع مزود خدمات التصديق حول تقديم الشهادة .

(ب) -أي شخص اعتمد بصورة معقولة على الشهادة التي أصدرها مزود خدمات التصديق.»

من خلال استقراء هذه المادة نلاحظ أن المسؤولية المدنية لمزود الخدمات قد تكون عقدية اتجاه الموقع (أولا)،وقد تكون تقصيرية اتجاه المرسل إليه(ثانيا).

أولا: مسؤولية مزود الخدمات تجاه الموقع:

يرى الأستاذ السنهوري أن المسؤولية العقدية على العموم يجب أن تتوافر فيها شرطان أساسيان هما :

أولا أن يقوم عقد صحيح بين الدائن والمدين، وثانيا أن يكون الضرر الذي أصاب الدائن قد وقع بسبب عدم تنفيذ العقد[1]، وهو ما يتوفر في علاقة مزود الخدمات بالموقع إذ من المفترض أنه قد أبرم عقد بينهما يسمى ب«عقد الاشتراك» ،بموجبه يبين شروط منح شهادة التصديق[2].

كما أن الضرر الذي قد يلحق بالموقع غالبا ما يكون بسبب منح مزود الخدمات شهادة تصديق مغلوطة وغير صحيحة.

إلا أنه يجب أن تتوافر في المسؤولية العقدية أركان ثلاث وهي :الخطأ العقدي ،الضرر والعلاقة السببية بين الخطأ والضرر[3] .

المقصود بالخطأ هو عدم تنفيذ التزام تعاقدي ،ويجب علينا أولا أن نعرف طبيعة التزام مزود الخدمات، فهناك من اعتبره بأنه التزام ببذل العناية وليس التزام بتحقيق النتيجة ،فنجد مثلا المادة 24 فقرة1 من قانون المبادلات والتجارة الإلكترونية في إمارة دبي تنص على :«... (ب) أن يمارس عناية معقولة لضمان دقة واكتمال كل ما يقدمه من بيانات جوهرية ذات صلة بالشهادة أو مدرجة فيها طيلة سريانها».

غير أن التفسير الموسع للمادة 40 من مشروع تطبيق التعليمة الأوربية يتضح لنا أن مزود الخدمات يجب عليه أن يثبت عدم وجود خطأ أو إهمال من جانبه ،وتكون مسؤوليته

---

[1] د- عبد الرزاق السنهوري –الوسيط في شرح القانون المدني الجديد ، نظرية الالتزام بوجه عام ،مصادر الالتزام ،المجلد الثاني ،منشورات الحلبي الحقوقية 2000،ص854

[2] Julien esnault ,op,.cit.,p43

[3] أنظر د- عبد الرزاق السنهوري،،المرجع السابق،ص735وما بعدها

مفترضة عن الأضرار التي يسببها للأشخاص الذين اعتمدوا بشكل معقول على شهادات التصديق التي أصدرها[1] .

كما أن الخطأ الذي يرتكبه مزود الخدمات يرتب على عاتقه المسؤولية بمجرد عدم صحة البيانات الواردة في شهادة التصديق أو وجود عيب فيها وبالتالي يقع عليه عبء إثبات عدم وجود الخطأ أو الإهمال.

يجب أن يكون الخطأ العقدي مرجعه المدين نفسه(مزود الخدمات)وليس شخصا أخر[2]، والغالب أن مزود الخدمات يقع عليه واجب تحقيق نتيجة في التزاماته التعاقدية.

يمكن اعتبار الموقع بأنه:« كل شخص اعتمد بشكل معقول على الشهادات التي أصدرها مزود الخدمات»، إلا أن استعمال كلمة الشهادات بالجمع قد يجعل الكثير منا يتجه إلى أن المقصود من هذه المادة هو المرسل إليه وليس الموقع ،فالمرسل إليه هو الذي يراقب مدى صحة شهادات التصديق أما الموقع فإنه لا يمتلك إلا شهادة تصديق واحدة.

لكن حقيقة الأمر أن استعمال عبارة الجمع في الشهادة المقصود بها عمل مزود الخدمات الذي يرتكز حول تسليم شهادات التصديق[3].

نلاحظ أن التزام مزود الخدمات في هذه الحالة هو التزام بتحقيق نتيجة ،إذ يجب عليه أن يحقق نتيجة معينة حتى يكون التزامه منفذا وهو في هذه الحالة إصدار شهادة رقمية مضمونها صحة البيانات الواردة فيها سواء اعتمد في ذلك على تحرياته الشخصية أو ثقته في الأطراف التي أدلت له بالمعلومات عن هذه الشهادة[4]، وهي مسؤولية عن الفعل الشخصي ويطلب الرجوع إلى المبادئ العامة في الإثبات لإقامة الدليل على مسؤولية المزود[5].

---

[1] Sauf à démontrer qu'elles n'ont commis aucune faute intentionnelle ou négligence, les personnes physique ou morales prestataires de services de certification électronique ou fournissant d'autres services liés aux signatures électroniques sont présumées responsables du préjudice causé au personnes qui sont fiées raisonnablement aux certificats qu'elles délivrent .

[2] المستشار عبد الفتاح بيومي حجازي،المرجع السابق ،ص 218

[3] Julien Esnault ,op.cit.,p44

[4] المستشار عبد الفتاح بيومي حجازي،المرجع السابق ،ص 119

[5] /علي كحلون،المرجع السابق،ص 305

انتهج المشرع السويسري نهجا مختلفا مقارنة ببقية التشريعات الأخرى حيث حمل الموقع صاحب المفتاح الخاص أن يثبت أن مقدم خدمات التصديق قد استعمل مفتاحه الخاص دون رضاه مع إثباته في الوقت نفسه أنه قد بذل العناية اللازمة للحفاظ على سرية مفتاحه الخاص[1]

ثانيا: مسؤولية مزود الخدمات تجاه المرسل إليه :

لا يقع على عاتق مزود الخدمات التزام ببذل عناية أو تحقيق نتيجة اتجاه المرسل إليه إذ لا وجود لأي عقد بينهما[2]، فلا يمكن إعمال قواعد المسؤولية العقدية في هذه الحالة .

بالتالي يتم اللجوء إلى قواعد المسؤولية التقصيرية (المادة 124 من القانون المدني الجزائري ويقابلها المادة 1382من القانون المدني الفرنسي)حتى يمكن تعويض الأضرار التي تلحق المرسل إليه بسبب إخلال مزود الخدمات بالتزاماته المذكورة سابقا،أي يجب على المرسل إليه إثبات وجود الخطأ والضرر والعلاقة السببية بينهما [3].

إلا أن إثبات الخطأ يعتبر أمرا صعبا فالتوقيع الإلكتروني تستخدم فيه إجراءات معقدة، بالإضافة إلى أن المرسل إليه لا يستطيع الدخول إلى البنية التحتية لمزود الخدمات وبالتالي لا يستطيع إثبات الخطأ لذا فإنه في غالب الأحيان يتم اللجوء إلى الخبرة القضائية[4].

تحديد ما إذا كانت الأعمال التي يقوم بها مزود الخدمات تشكل ضررا اتجاه المرسل إليه متروكة للسلطة التقديرية لقاضي الموضوع، إذ أنه لا وجود لنصوص قانونية تحدد الأعمال التي يتحقق بها الفعل الضار[5].

---

[1] د.سعيد سيد قنديل،المرجع السابق ،ص 96و97

[2] Julien Esnault ,op.cit.,p47

[3] ومن دون إثبات الخطأ والضرر والعلاقة السببية بينهما لا يمكن أن توجد المسؤولية التقصيرية

[4] Julien Esnault ,op.cit.,p47

[5] المستشار عبد الفتاح بيومي حجازي،المرجع السابق ،ص 220

إذ يمكن للمرسل إليه في أن يثبت خطأ مزود الخدمات على أساس إخلاله بالتزاماته المذكورة في القانون، خاصة إذا تعلق العمل بالشهادة أو إلغائها قد سبب ضررا للغير[1]

كما أن المشرع التونسي أبقى على هذه المسؤولية إذ يجب تعويض الضرر اللاحق بالغير حتى ولو كان سبب الضرر لا علاقة له بالفصل 18 من قانون المبادلات والتجارة الإلكترونية ،وهذا استنادا للقواعد العامة التي تلزم كل من تسبب بخطئه في الإضرار بالغير بتعويض ذلك الغير[2].

نظرا للصعوبات التي قد تواجه المرسل إليه في إثبات الخطأ فإن التعليمة الأوروبية في مادتها 6 رأت ضرورة إعمال مسؤولية مزود الخدمات بصفة شبه آلية ،إذ عليه أن يثبت عدم إهماله أثناء إصداره لشهادات التصديق المعتمدة .

ثالثا: الإعفاء من المسؤولية وتحديدها:

إلا أنه يمكن لمزود الخدمات أن يعفي نفسه من المسؤولية إذا أثبت أن المرسل إليه لم يحترم حدود عمل شهادة التصديق ،بحيث اعتمد عليها في مجالات لم تكن مذكورة في الشهادة ، أو كان بإمكانه أن يعلم بحسب المجرى العادي للأمور بأن الشهادة قد انتهى العمل بها أو ألغيت أو تم تعليق العمل بها ، أو أن اعتماد مزود خدمة الشهادات قد تم إلغاؤه[3] أو أثبت بأنه لم يقترف أي خطأ أو إهمال[4]، أو أن الضرر نشأ عن سبب أجنبي لا يد له فيه[5]، أو أن الطرف المضرور قد أخل بالتزام جوهري وهو أن يتخذ خطوات مناسبة ومعقولة للتأكد من صحة البيانات الواردة في الشهادة وأن تكون هذه البيانات قد وفرها له مزود الخدمات[6].

---

[1] المستشار عبد الفتاح بيومي حجازي،المرجع السابق ،ص192
[2] المستشار عبد الفتاح بيومي حجازي،المرجع السابق ،ص 114
[3] المادة 18 فقرة 2 من قانون التجارة الإلكتروني البحريني
[4] المادة 6 فقرة c من التعليمة الأوروبية
[5] المادة 25 فقرة 5 من قانون المعاملات والتجارة الإلكترونية في إمارة دبي
[6] المستشار عبد الفتاح بيومي حجازي،المرجع السابق ،ص 221

كما يمكن لمزود الخدمات أن يحدد ويقيد من نطاق مسؤوليته طبقا للقواعد العامة ،وهو ما أقره مشرع إمارة دبي في المادة 24 فقرة 5 :«... (أ) إذا أدرج في الشهادة بياناً يقيد نطاق ومدى مسئوليته تجاه أي شخص ذي صلة، ومدى ذلك القيد. »،وهذا البيان يكون صالحا اتجاه الموقع أو الغير.

لقد حدد الأستاذ Julien Esnault ثلاث شروط يجب احترامها حتى يكون تحديد المسؤولية صحيحا وهي:

1- يجب أولا أن يتم استبعاد الخطأ الجسيم .

2- إبتداءا من قرار Chronopost يجب أن لا تكون الشروط المحددة أو المعفية للمسؤولية تستبعد السبب الرئيسي للالتزام وإلا أعتبر باطلا.

فيعتبر الشرط المحدد لمسؤولية مزود الخدمات باطلا إذا كان الهدف منه عدم إعطاء شهادة التصديق لقيمتها القانونية في إنشاء التوقيع ،باعتباره السبب الرئيسي لالتزام مزود الخدمات.

3- يجب أخذ الحذر من الشروط التعسفية والتي يمكن أن تدرج في العقد، وفي حال ما إذا وجد خلل واضح بين حقوق وواجبات أطراف العقد، فهذه الشروط تعتبر باطلة وفق المواد (L.132-1à L134-1 من قانون الاستهلاك)[1].

المطلب الثاني: شهادة التصديق الإلكتروني

لقد رأينا في المطلب الأول أن مزود الخدمات الهدف الأساسي الذي وجد من أجله هو إصدار شهادة تصديق صحيحة ،فالشروط الموضوعة الخاصة به وكذا التزاماته وترتيب المسؤولية ترتكز كلها على شهادة التصديق .

[1] Julien esnault ,op.cit.,p45 et 46

غالبا ما يخطأ الكثيرون ويعتقدون أن هذه الشهادة تنصب على التوقيع الإلكتروني ككل ولكن حقيقة الأمر أنها توثق للمفتاح العام فقط[1].

كما تعتبر الشهادة وفق التشريع الألماني الرابط المادي بين الموقع والتوقيع[2]، فالتعليمة الأوروبية مثلا لا تقر بالمساواة بين التوقيع الخطي والإلكتروني إلا إذا كان هذا الأخير مرتكزا على شهادة معتمدة[3] ،والتي يجب أن تتوفر فيها بعض المعلومات حتى تكتسب هذه الصفة وهو ما سنتطرق إليه في الفرع الأول.

غير أن عمل مزود الخدمات لا يقتصر فقط على أرض الدولة المتواجد فيها بل يشمل كذلك المستوى الدولي ولذلك وجب على الدول الاعتراف بصحة شهادة التصديق الأجنبية الصادرة من طرف هذا المزود (الفرع الثاني).

ولضمان الأمن القانوني للتوقيع الإلكتروني وشهادة التصديق، فإنه يمكن إلغاء الشهادة أو تعليق العمل بها بمجرد الشك في محتواها أو انتهاء مدة العمل بها(الفرع الثالث).

الفرع الأول: محتويات شهادة التصديق

يجب علينا أولا أن نعرف شهادة التصديق ، والتي أوردتها التشريعات والقوانين في المواد الأولى .

فنجد مثلا المشرع التونسي قد عرفها في الفصل الثاني من قانون المبادلات والتجارة الإلكترونية بأنها:« -شهادة المصادقة الالكترونية: الوثيقة الالكترونية المؤمنة بواسطة الإمضاء الالكتروني للشخص الذي أصدرها والذي يشهد من خلالها اثر المعاينة، على صحة

---

[1] Thierry Piette-coudol ;op.cit.,p173

[2] Béatrice jaluzot :« Transposition de la directive«signature électronique» :comparaison franco- allemande»

[3] Eric A.caprioli :«Régime juridique du prestataire de services de confiance au regard de la directive du 13 décembre 1999» www.caprioli-avocats.com, Date de la mise a jour : mai 2003

البيانات التي تتضمنها.»، وعرفها مشرع إمارة دبي بما يلي:« - شهادة يصدرها مزود خدمات التصديق يفيد فيها تأكيد هوية الشخص أو الجهة الحائزة على أداة توقيع معينة، ويشار إليها في هذا القانون بـ «الشهادة» .

أما المشرع الفرنسي فقد عرفها في المادة الأولى من المرسوم 272-2001 ب:«وثيقة على شكل إلكتروني تثبت صحة العلاقة بين معطيات مراقبة التوقيع الإلكتروني والموقع »[1].

كذلك المشرع الألماني:«شهادة إلكترونية التي تمنح مفتاح مراقبة التوقيع إلى شخص والتي تؤكد هوية ذلك الشخص»،وهو تعريف مطابق لما جاء في التعليمة الأوروبية»[2] .

إلا أنه وبمقارنة التعريفين(الألماني والفرنسي) نجد أن القانون الألماني قد أعطى لشهادة التصديق مهمة منح المفتاح العام إلى الموقع وبالخصوص ضمان هوية ذلك الموقع، إلا أن القانون الفرنسي قد ركز على الرابطة الموضوعية بين العنصرين(المفتاح العام والموقع)،ورفض ضمنيا فكرة الضمان[3].

على العموم فإن شهادة التصديق الإلكتروني هي شهادة تؤكد هوية الموقع وصحة العلاقة بين أداة التوقيع والموقع أي تأكيد نسبة أداة التوقيع للموقع دون سواه بالإضافة إلى مهام أخرى تتمثل فيما يلي :

- عدم إنكار إرسال التوقيع .
- عدم إنكار وصول التوقيع
- تشفير المعطيات[4] .

---

[1] « Certificat électronique » : un document sous forme électronique attestant du lien entre les données de vérification de signature électronique et un signataire ;

[2] Art.2.9 :««certificat »,une attestation électronique qui lie des données afférentes à la vérification de signature à une personne et confirme l'identité de cette personne;»

[3] Béatrice jaluzot :« Transposition de la directive«signature électronique» :comparaison franco- allemande»

[4] Arnaud-f .Fausse ;op.cit. ,p 106

بالتالي فإنه يشترط في هذه الشهادة أن تذكر فيها بعض المعلومات حتى يمكن لها أن تؤدي مهامها على أحسن وجه.

إلا أن الملاحظ أن التشريعات والقوانين قد انقسمت إلى ثلاث اتجاهات في هذا المجال، فهناك من قسمها إلى نوعين شهادة تصديق «بسيطة » وشهادة تصديق «معتمدة»، وهناك اتجاه ثاني من حدد محتوياتها ومكوناتها بغض النظر عن التقسيم المذكور سابقا، واتجاه ثالث ذكر محتويات شهادة التصديق المعتمدة دون التطرق إلى شهادة التصديق البسيطة.

من بين البلدان والقوانين التي تبنت الاتجاه الأول نجد مثلا التعليمة الأوروبية والقانون الفرنسي،غير أنه لم يهتموا ولم يتطرقوا إلى محتويات وشكل شهادة التصديق البسيطة ، وبالتالي فإن هذا النوع من الشهادة لا تحتاج إلى ترخيص إذ بمجرد اعتماد مزود الخدمات جاز له إصدارها ، أما النوع الثاني بالإضافة إلى الاعتماد المسبق يشترط أن يتحصل مزود الخدمات على رخصة مسبقة حتى يتمكن من إصدار شهادة تصديق معتمدة[1] ، غير أنه يمكن إصدار هذا النوع من الشهادات على الرغم من عدم الحصول على التفويض بشرط أن يستعمل مزود الخدمات أنظمة ومواد موثوق فيها لعمل الشهادة والحفاظ عليها وأشخاص مؤهلين[2]

عكس ذلك فإن شهادة التصديق المعتمدة فقد تم تنظيمها بشكل دقيق ولم يترك تنظيمها إلى إرادة المتعاقدين.

فالقانون الفرنسي بموجب المادة 6 من المرسوم 2001-272 حدد بيانات شهادة التصديق المعتمدة ب :

- التنويه بأن الشهادة الممنوحة لها صفة شهادة إلكترونية معتمدة.
- هوية مزود الخدمات وكذلك الدولة المقيم فيها .
- اسم الموقع أو اسم الشهرة ، الذي يعرف به.

---

[1] أ.قارة مولود،المرجع السابق،ص101

[2] Eric A.caprioli :«Régime juridique du prestataire de services de confiance au regard de la directive du 13 décembre 1999 »www.caprioli-avocats.com, Date de la mise a jour : mai 2003

-في حال وجود الأجل، ذكر صفة الموقع بالنسبة لاستعمال شهادة التصديق الموجهة له.

-معطيات مراقبة التوقيع الإلكتروني المتطابقة مع معطيات إنشاء التوقيع الإلكتروني.

-التنويه إلى بداية ونهاية فترة صلاحية الشهادة الإلكترونية.

-رمز الهوية الشهادة الإلكترونية.

-التوقيع الإلكتروني المؤمن لمزود الخدمات الذي منح الشهادة الإلكترونية.

-في حال وجود الأجل، ذكر شروط استعمال الشهادة الإلكترونية ،بالخصوص المبلغ الأقصى في المعاملات والتي من أجلها يمكن استعمال شهادة التصديق [1] .

بالتالي فإن المشرع الفرنسي لم يخرج عن توجيهات التعليمة الأوروبية فيما يخص هذا الشأن، حيث تبناها بشكل كامل ولم يخرج عن نطاقها[2]

أما الاتجاه الثاني فقد اتبعه كل من المشرع التونسي و مشرع إمارة دبي حيث ذكرا محتويات شهادة التصديق مباشرة دون الاهتمام بالتفرقة بين شهادة التصديق العادية و

---

[1] a) Une mention indiquant que ce certificat est délivré à titre de certificat électronique qualifié ;
b) L'identité du prestataire de services de certification électronique ainsi que l'Etat dans lequel il est établi ;
c) Le nom du signataire ou un pseudonyme, celui-ci devant alors être identifié comme tel ;
d) Le cas échéant, l'indication de la qualité du signataire en fonction de l'usage auquel le certificat électronique est destiné ;
e) Les données de vérification de signature électronique qui correspondent aux données de création de signature électronique ;
f) L'indication du début et de la fin de la période de validité du certificat électronique ;
g) Le code d'identité du certificat électronique ;
h) La signature électronique sécurisée du prestataire de services de certification électronique qui délivre le certificat électronique ;
i) Le cas échéant, les conditions d'utilisation du certificat électronique, notamment le montant maximum des transactions pour lesquelles ce certificat peut être utilisé

[2] الملحق II من التعليمة الأوروبية

المعتمدة ،إلا أنه يمكن أن نستخلص من خلال استقراء المواد بأن الشهادة يجب أن تكون معتمدة في جميع الأحوال ولا مجال لحرية الأطراف لتحديد محتوياتها.

فنجد أن الفصل 17 فقرة 2 من قانون المبادلات والتجارة الإلكتروني التونسي قد ركز على معيار الأمان والسلامة عند إصدار الشهادة حتى يمكن الثقة فيها، ولا يتأتى ذلك إلا إذا احتوت على ما يلي:

- هوية صاحب الشهادة.

-هوية الشخص الذي أصدرها وإمضاء الكتروني

-عناصر التدقيق في إمضاء صاحب الشهادة.

-مدة صلاحية الشهادة

-مجالات استعمال الشهادة.

أما قانون إمارة دبي في المادة 24 فقرة3 ففرض أن تحتوي شهادة التصديق على ما يلي :

«يجب أن تحدد الشهادة ما يلي :

أ- هوية مزود خدمات التصديق.

ب- أن الشخص المعينة هويته في الشهادة لديه السيطرة في الوقت المعني على أداة التوقيع المشار إليها في الشهادة.

ج- أن أداة التوقيع كانت سارية المفعول في أو قبل تاريخ إصدار الشهادة.

د- ما إذا كانت هناك أية قيود على الغرض أو القيمة التي يجوز أن تستخدم من اجلها أداة التوقيع أو الشهادة.

ه- ما إذا كانت هناك أية قيود على نطاق أو مدى المسئولية التي قبلها مزود خدمات التصديق تجاه أي شخص»

أما الاتجاه الثالث فقد تبناه المشرع البحريني الذي تطرق مباشرة إلى محتويات الشهادة المعتمدة دون الطرق إلى الشهادة البسيطة، وهو ما نلاحظه جليا في المادة الأولى

من قانون التجارة الإلكتروني حيث نص :« - شهادة معتمدة : سجل إلكتروني يتسم بأنه :

أ - يربط بيانات تحقق من توقيع بشخص معين .

ب- يثبت هوية ذلك الشخص .

ج- يكون صادراً من قبل مزود خدمة شهادات معتمد .

د -مستوفٍ للمعايير المتفق عليها بين الأطراف المعنية أو المنصوص عليها في القرارات التي تصدر استناداً لأحكام هذا القانون.

من خلال كل هذه النصوص القانونية فإن التشريعات قد اتفقت على بعض البيانات التي يجب أن تكون مذكورة في شهادة التصديق، ومن أهم هذه البيانات :

أ- تحديد هوية الموقع: وذلك ببيان اسمه ولقبه ومهنته ومحل إقامته والبيانات التي تشير إلى أنه صاحب هذه الشهادة[1]،وإمكانية حتى ذكر اسم الشهرة وهو ما أقره المشرع الفرنسي .

بحيث أن شهادة التصديق لا تتيح فقط مراقبة هوية الشخص ولكن حتى سلطاته وقدراته وصفته المهنية (مثال يمكن معرفة هل الشخص طبيب أم محامي...)[2].

غير أن مشرع إمارة دبي لم ينص على هذا البيان بشكل صريح ،وإنما ذكره بشكل ضمني عندما تحدث على شرط السيطرة على أداة التوقيع حيث يجب أن يكون الشخص المحدد هويته في الشهادة مسيطرا على أداة التوقيع.

إلا أنه لا يحق لمزود الخدمات أن يتحصل على المعطيات الشخصية المحددة لهوية الموقع إلا بعد موافقته[1] ،بشرط أن تكون هذه المعلومات ضرورية[2].

---

[1] المستشار عبد الفتاح بيومي حجازي،المرجع السابق ،ص 170

[2] Valérie Sédaillian :«Preuve et signature électronique»,www. Juriscom .net

وطبقا للمادة الثانية من التعليمة الأوروبية المتعلقة بكيفية معالجة المعلومات الشخصية فإنها تعرف المعلومات الشخصية ب:«كل معلومة تتصل بشخص محدد الهوية أو قابل للتحديد».

غير أن التساؤل المطروح في هذا المجال هو، هل يمكن للمشترك أن يخفي اسمه الحقيقي ويستعمل اسما مستعارا؟

إن التعليمة الأوروبية والقانون الفرنسي لم تمنع ذلك[3]، بحيث تركت حرية وضع اسم الموقع سواء كان اسمه الحقيقي أو اسمه المستعار ،مادام أن أي منهما يمكن أن يؤدي إلى التحقق من هوية الموقع[4].

إلا انه يفضل أن يحتفظ مقدم خدمات التصديق ببعض المعلومات التي تمكن من معرفة شخصية الموقع عندما تطلب منه بموجب اللوائح والتشريعات[5].

أ- هوية مزود الخدمات: يجب أن تحتوي شهادة التصديق هوية مزود الخدمات من حيث اسمه والمكان الذي يباشر فيه عمله ورقم الترخيص الصادر له من السلطة المختصة وأية بيانات لم ينص عليها القانون تساهم في تحديد هويته ،وهذا حتى يمكن الرجوع عليه بالتعويض في المسؤولية المدنية في حال وقوع خطأ من جانبه[6].

ج- السيطرة على أداة التوقيع: يجب أن تشير شهادة التصديق الإلكتروني إلى أن أداة التوقيع تحت سيطرة الموقع ،وهو من الشروط الأساسية حتى نكون بصدد توقيع

---

[1] الفصل 38 من قانون المبادلات والتجارة الإلكترونية التونسي

[2] الفصل 39 من نفس القانون.

[3] المادة 3/8 من التعليمة الأوروبية المتعلقة بالتوقيع الإلكتروني تنص:

«3.Sans préjudice des effets juridiques donnés aux pseudonymes par la législation nationale,les États membres ne peuvent empêcher le prestataire de service de certification d'indiquer dans le certificat un pseudonyme au lieu du nom du signataire.»

[4] د-سعيد سيد قنديل،المرجع السابق ،ص 89

[5] د-سعيد سيد قنديل،المرجع السابق ،ص 90

[6] المستشار عبد الفتاح بيومي حجازي،المرجع السابق ،ص 213

إلكتروني محمي ،وهذا بقصد توفير الثقة لدى المتعاملين بمثل هذه الوثائق ،وحتى لا يتفاجأ الطرف المعول على الشهادة من أن هذه الأخيرة موقوفة العمل أو قد تم إساءة استعمالها .

إن السيطرة الفعلية على أداة التوقيع من طرف الموقع تتمثل أساسا في إمكانية هذا الأخير وقف التعامل بها في أي وقت بناءا على طلبه وذلك لأسباب التي يحددها القانون[1].

د-تحديد مجال استعمال الشهادة وصلاحيتها : على الرغم من اعتراف معظم التشريعات بحجية التوقيع الإلكتروني ومساواته للتوقيع الخطي إلى أن هذه المساواة تبقى غير كاملة حيث أنه غالبا ما يتم إنشاء التوقيع الإلكتروني لأغراض معينة دون سواها، ولهذا فإن شهادة التصديق يجب أن يذكر فيها مجال استعمال هذا التوقيع ،ولا يسأل مزود الخدمات في حال ما إذا أثبت أن المرسل إليه لم يحترم حدود عمل الشهادة .

كما أن على مزود الخدمات أن يذكر الحد الأقصى للمبلغ الذي يمكن التعامل به خاصة إذا كانت هذه الشهادة محددة المدة أو معلقة على أجل.

غالبا ما تكون مدة الصلاحية محددة بسنة قابلة للتجديد، وبالتالي فيجب ذكر تاريخ بداية ونهاية العمل بشهادة التصديق، وفي حال تعليقها أو إلغائها يجب التنويه بذلك حتى لا يعتمد المرسل إليه على شهادة تصديق غير صالحة.

هناك من جعل لفترة صلاحية الشهادة عدة وظائف منها:

-إنه بمجرد انتهاء العمل بشهادة التصديق بشكل طبيعي، فإن ذلك يسمح بتجديد الشهادة وبالتالي منح الفرصة لتغيير المفاتيح سواء تعلق الأمر بصاحب الشهادة أو المرسل إليه، هذه الآلية تسمح بحماية أولية في حال كشف المفتاح الخاص للموقع.

-الشهادات التي تحتوي على استعمالات موسعة غالبا ما تكون محددة المدة مثال ذلك : شهادة تصديق تتيح الدخول إلى موقع انترنيت يوفر خدمة الدفع لن تكون هذه الأخيرة صالحة إلا في فترة الدفع التي تتم بواسطة حامل الشهادة ،ولكن يجب أن

---

[1] المستشار عبد الفتاح بيومي حجازي،المرجع السابق ،ص 214

تكون هذه الشهادة المستعملة صالحة وهو شرط ضروري ولكنه غير كافي ،فإذا ما اكتشف صاحب الشهادة أن مفتاحه الخاص قد تم كشفه أثناء فترة الصلاحية ،فكل الشهادات الموقعة يجب أن تلغى أي تصبح غير صالحة[1] .

يلاحظ أن تدوين هذه البيانات هي مسؤولية مزود الخدمات دون غيره ،ولذلك ففي حالة عدم تدوين بيان ما فإنه هو من يقع عليه تعويض الضرر الذي لحق الطرف المضرور من جراء هذا الخطأ[2].

الفرع الثاني : الاعتراف بشهادة التصديق الأجنبية .

إن عمل مزود الخدمات يتسم بالطابع العالمي إذ غالبا ما يتم استعمال التوقيع الإلكتروني في صفقات وعقود ذات طابع دولي ،وبما أن التوقيع الإلكتروني مرتبط بشهادة التصديق فإن عدم اعتراف دولة من الدول بصحة الشهادة لمجرد أنها غير صادرة على أرض دولتها يشكل عائقا وحاجزا لتطور المعاملات الإلكترونية.

لهذا حرصت قوانين الدول على المساواة بين شهادة التصديق الوطنية والأجنبية ،وقد كان قانون الأونيسترال النموذجي بشأن التوقيعات الإلكترونية السباق لذلك بأن وضع الأسس التي يجب على الدول اتباعها حتى تكون لشهادة التصديق الأجنبية نفس الأثر والمفعول مقارنة بشهادة التصديق الوطنية .

حيث يفترض أن يكون للشهادات والتواقيع الأجنبية نفس الأثر القانوني إذا كانت تتمتع بنفس مستوى المصداقية ويمكن تحديد هذه المصداقية بالرجوع إلى المقاييس الدولية

---

[1] Arnaud-f .Fausse ;op.cit. ,p 107

[2] الفصل 22 من قانون المبادلات والتجارة الإلكترونية التونسي

المعترف بها إضافة إلى بعض العوامل الأخرى المتعلقة بهذه المقاييس والتي تصدر في دليل تشريعي خاص[1]،ولا أهمية لمكان إصدار شهادة التصديق .

وهو ما أخذ به مشرع إمارة دبي في نص المادة 26 فقرة 2 من قانون المبادلات والتجارة الإلكترونية حيث اشترطت على مزودي الخدمات مستوى من الوثوق يوازي على الأقل ما تتطلبه المادة 24 من هذا القانون والأخذ بالمعايير الدولية في هذا المجال[2].

كما يمكن للدول أن تضع شروطا أخرى حتى يمكن الاحتجاج بالشهادة الأجنبية، كأن يتصرف بصدق في حدود البيانات الإلكترونية التي لديه عن أصحابها والتي تدل عن الشخص المعين الهوية وأنه يسيطر سيطرة تامة على أداة التوقيع ،وأن يبذل عناية الرجل الحريص لضمان دقة واكتمال ما يقدمه من بيانات جوهرية ذات صلة بالشهادة إلخ...[3]

على العموم يمكن تحديد ثلاث حالات للاعتراف بشهادة التصديق الأجنبية[4] :

الحالة الأولى : إذا لم يطلب مزود الخدمات الأجنبي اعتماده إصدار الشهادات والتواقيع الإلكترونية ،فكل ما يشترط في ذلك أن يقدم هذا الأخير مستوى من الثقة يساوي على الأقل ما هو مطلوب قانونا في دولته أو ما هو معترف به دوليا.

يعتبر هذا الشرط منطقيا فلا يمكن بأي حال من الأحوال الاعتراف بشهادة تصديق إلكترونية صادرة من مزود خدمات لم يتم الاعتراف به حتى في الدولة التي يمارس فيها مهامه أو ثبت أن هذا الأخير لم يوفر مستوى من الثقة مساويا لما هو معمول به في الدولة الممارس فيها نشاطه.

---

[1] المستشار عبد الفتاح بيومي حجازي،المرجع السابق ،ص 273

[2] المادة 26 فقرة 2 تنص :«(2) تعتبر الشهادات التي يصدرها مزودو خدمات التصديق الأجانب، كشهادات صادرة من مزودي خدمات التصديق الذين يعملون بموجب هذا القانون، إذا كانت ممارسات مزودي خدمات التصديق الأجانب ذات مستوى من الوثوق يوازي على الأقل المستوى الذي تتطلبه المادة (24) من مزودي خدمات التصديق العاملين بموجب هذا القانون، ومع الأخذ بالاعتبار المعايير الدولية المعترف بها.»

[3] أ/قارة مولود ،المرجع السابق،ص 93

[4] أنظر في ذلك أ/قارة مولود ،المرجع السابق،ص 94و 95

لم ينكر هذا الشرط حتى قانون الأونيسترال النموذجي بشأن التوقيعات الإلكترونية الذي نص في المادة 12 فقرة 2 على:« 2- يكون للشهادة التي تصدر خارج (الدولة المشرعة) المفعول القانوني نفسه في (الدولة المشرعة) الذي للشهادة التي يصدر في (الدولة المشرعة) إذا كانت تتيح مستوى مكافئا جوهريا من الموثوقية.»

لا يمكن تصور هذه الحالة إلا في الدول التي تعتمد على نظام التفويض والاعتماد (مثل فرنسا ودول الاتحاد الأوروبي) بينما الدول التي تفرض الترخيص لمزاولة نشاطات مزود الخدمات ، فلا يمكن لهذا الأخير أن يمارس مهامه على إقليم هذه الدولة دون الحصول على الترخيص(مثل تونس مصر البحرين وإمارة دبي).

الحالة الثانية : إذا ما طلب مزود الخدمات اعتماد ما يصدره من شهادات لدى دولة أجنبية غير الدولة التي يمارس فيها نشاطه وجب عليه التكيف وقانونها الوطني وهو ما تنص عليه المادة 7 من التعليمة الأوروبية [1].

وهو ما سار عليه القانون الفرنسي حيث نص في المادة 8 من المرسوم 2001-272 على أن شهادة التصديق الصدارة من مزود خدمات يقع خارج الإتحاد الأوروبي لها نفس القيمة القانونية الممنوحة لمزود خدمات يقع في الإتحاد الأوروبي بشرط أن يأخذ بعين الاعتبار الشروط التالية:

أ- أن يكون مستوفي للشروط المذكورة في المادة 6 من هذا المرسوم وأن يكون مفوضا وفقا للتعليمة الأوروبية[2] .

---

[1] Les États membres veillent à ce que les certificats délivrés à titre de certificats qualifiés à l'intention du public par un prestataire de service de certification établi dans un pays tiers soient reconnus équivalents,sur le plan juridique,aux certificats délivrés par un prestataire de service de certification établi dans la Communauté:
a)si le prestataire de service de certification remplit les conditions visées dans la présente directive et a été accrédité dans le cadre d'un régime volontaire d'accréditation établi dans un État membre
ou
b)si un prestataire de service de certification établi dans la Communauté,qui satisfait aux exigences visées dans la présente directive,garantit le certificat.

[2] المقصود بالمادة 6 من هذا المرسوم هي أن يكون مزود الخدمات مستوفي للشروط القانونية وفقا للقانون الفرنسي

ب- أن تكون الشهادة الالكترونية الممنوحة من طرف مزود الخدمات مضمونة من طرف مزود خدمات يقع في الاتحاد الأوروبي مستوفي للشروط المذكورة في المادة 6 من هذا المرسوم [1].

أما الحالة الأخيرة فإنه يجب الأخذ بعين الاعتبار الاتفاقيات وقد تكون هذه الاتفاقيات بين الدول أو اتفاق بين طرفين حول المعاملة التي يستخدم فيها ذلك التوقيع أو الشهادة، إلا أن هناك من الدول من اقتصرت على الإعترف بحجية شهادة التصديق على ضرورة وجود اتفاقية بين الدولتين ولم تتطرق إلى اتفاق الطرفين وهو ما يمكن اعتباره استبعاد لهذا النوع من الاتفاقيات.

تبنى هذا الموقف كل من المشرع التونسي وفق الفصل 23 من قانون المبادلات والتجارة الإلكترونية[2] ،والمشرع الفرنسي في المادة 8 حيث نص في الشرط الأخير لقبول شهادة التصديق الأجنبية على :« ج- أو أن يكون اتفاق يكون الإتحاد الأوروبي طرفا فيه .»

بالتالي فإن المشرع الفرنسي وفق الحالة الأخيرة لم ينكر القيمة القانونية لشهادة التصديق الإلكترونية التي يصدرها مزود خدمات يقع خارج الإتحاد الأوروبي بشرط أن يكون الإتحاد الأوروبي طرفا فيه .

إلا أن مشرع إمارة دبي أقر بهذه النوعية من الاتفاقيات، مع وضع شروطا معينة حتى يتم قبولها وهي :

---

[1] Art. 8. - Un certificat électronique délivré par un prestataire de services de certification électronique établi dans un Etat n'appartenant pas à la Communauté européenne a la même valeur juridique que celui délivré par un prestataire établi dans la Communauté, dès lors :
a) Que le prestataire satisfait aux exigences fixées au II de l'article 6 et a été accrédité, au sens de la directive du 13 décembre 1999 susvisée, dans un Etat membre ;
b) Ou que le certificat électronique délivré par le prestataire a été garanti par un prestataire établi dans la Communauté et satisfaisant aux exigences fixées au II de l'article 6 ;
c) Ou qu'un accord auquel la Communauté est partie l'a prévu.

[2] ينص الفصل 23 على :« تعتبر الشهادات المسلمة من مزود خدمات المصادقة الالكترونية الموجود ببلد أجنبي كشهادات مسلمة من مزود خدمات المصادقة الالكترونية موجود بالبلاد التونسية اذا تم الاعتراف بهذا الهيكل في إطار اتفاقية اعتراف متبادل تبرمها الوكالة الوطنية للمصادقة الالكترونية.»

- أن يحدد الأفراد مزودي خدمات محددين أو فئة معينة منهم أو فئة معينة من الشهادات فيما يتصل بالرسائل أو التوقيعات الالكترونية المقدمة لهم.

- أن لا يكون هذا الاتفاق غير مشروع وفق قوانين الإمارة[1] ،وهو بالتالي قد طبق بشكل حرفي ما أتى به قانون الأونيسترال الذي أقر بحجية هذه الاتفاقيات بموجب المادة 12 فقرة 5 من هذا القانون التي تنص :«5- إذا اتفقت الأطراف فيما بينها ،برغم ما ورد في الفقرات 2 و 3 و4 على استخدام أنواع معينة من التوقيعات الإلكترونية أو الشهادات ،يتعين الاعتراف بذلك الاتفاق باعتباره كافيا لأغراض الاعتراف عبر الحدود ،ما لم يكن من شأن ذلك الاتفاق أن يكون غير صحيح أو غير ساري المفعول بمقتضى القانون المنطبق »

الفرع الثالث: تعليق وإلغاء شهادة التصديق

لقد رأينا في الفرع السابق أن شهادة التصديق لها مدة صلاحية محددة وغالبا ما تكون بسنة ولذا وجب على مزود الخدمات تحديد تاريخ إصدارها و نهايتها على وجه الدقة، وهو ما أقرته التعليمة الأوروبية في الملحق رقم 2[2] ،و عادة ما تنتهي صلاحية الشهادة أليا بحلول تاريخ نهاية الصلاحية أو بإشعار من صاحبها كما لو فقدها، كما قد يكون الطلب من تلقاء نفسه دون عناء تسبيبه[3] .

غير أنه يجب التمييز بين التعليق وإلغاء شهادة التصديق ،فالحالة الأولى تعني تعطيل العمل بالأثر القانوني المترتب على الشهادة بشكل مؤقت وهذا تمهيدا لإلغائها أو استئناف

---

[1] المادة 26 فقرة 6 من قانون المعاملات والتجارة الإلكتروني :« (6) على الرغم من أحكام الفقرتين (2)، (3) السابقتين:
(أ) يجوز للأطراف في المعاملات التجارية والمعاملات الأخرى أن يحددوا وجوب استخدام مزودي خدمات تصديق معينين أو فئة معينة منهم أو فئة معينة من الشهادات فيما يتصل بالرسائل أو التوقيعات الالكترونية المقدمة لهم.
(ب) وفي الحالات التي يتفق فيها الأطراف فيما بينهم على استخدام أنواع معينة من التوقيعات الالكترونية أو الشهادات فإن ذلك الاتفاق يعتبر كافياً لأغراض الاعتراف المتبادل بين الاختصاصات القضائية المختلفة للدول، شريطة ألا يكون مثل هذا الاتفاق غير مشروع وفقاً لأحكام القوانين المطبقة في الإمارة.

[2] [2] Annex II,c :« veiller à ce que la date et l'heure d'émission et de révocation d'un certificat puissent être déterminées avec précision;»

[3] أ/قارة مولود ،المرجع السابق،ص 95

العمل بها[1] أما الإلغاء فهدفه إنهاء العمل بشهادة التصديق بشكل تجعلها عديمة الأثر وكأنها لم تكن.

تظهر أهمية إلغاء شهادة التصديق عندما ألزمت التعليمة الأوروبية مزود الخدمات أن تكون لديه خدمة الإلغاء بشكل أكيد وفوري[2]،كما يعتبر مزود الخدمات مسئولا في حال ما إذا لم يقم بتسجيل أو نشر بيان بانتهاء أو إلغاء أو تعليق العمل بالشهادة المعتمدة[3] .

كما ألزم قانون إمارة دبي بشأن المعاملات والتجارة الإلكترونية مزود الخدمات أن يوفر وسيلة مناسبة لإلغاء شهادة التصديق وأن يوفر للموقعين وسيلة تمكنهم من إشعار بأن أداة التوقيع قد تعرضت لما يثير الشبهة وأن تضمن توفر خدمة إلغاء التوقيع يمكن استخدامها في الوقت المناسب[4].

أما المشرع التونسي فقد نظم حالات تعليق وإلغاء شهادة التصديق بشكل دقيق، فنجده نص عليهما في الفصلين 19 و 20 من قانون المبادلات والتجارة الالكترونية وهي كما يلي :

1-عند طلب صاحب الشهادة : يحق لصاحب الشهادة أن يطلب إما إلغاء العمل بالشهادة وفق الفصل 20 من هذا القانون ،كما يحق له أن يطلب تعليق العمل بها وفق الفصل 19 من نفس القانون، بما أنها تحمل الصفة الشخصية لصاحب الشهادة حيث أنها تحتوي على هوية الموقع، وبالتالي فهو المعني بها أولا وأخيرا.

المقصود بصاحب الشهادة هو الشخص الطبيعي الذي طلب إصدار الشهادة ،سواء كانت له صفة أصلية أو باعتباره الممثل القانوني لأحد الأشخاص المعنوية العامة أو الخاصة ،وهو ما نصت عليه المادة 2 فقرة 3 من التعليمة الأوروبية في تعريفها للموقع بأنه:«الشخص

---

[1] المستشار عبد الفتاح بيومي حجازي،المرجع السابق ،ص 174

[2] Annex II,b :« assurer le fonctionnement d'un service d'annuaire rapide et sûr et d'un service de révocation sûr et immédiat; »

[3] المادة 18 فقرة 1 من قانون التجارة الإلكتروني البحريني:« د- تسجيل أو نشر بيان بانتهاء أو إلغاء أو تعليق العمل بالشهادة المعتمدة ، طبقاً للقرارات التي تصدر في هذا الشأن تنفيذاً لأحكام هذا القانون »

[4] المادة 24 فقرة 1 من قانون المعاملات والتجارة الإلكترونية

الطبيعي أو المعنوي الحائز لأداة توقيع إلكتروني خاصة به ويقوم بالتوقيع أو يتم التوقيع بالنيابة عنه على الرسالة الإلكترونية باستخدامه هذه الأداة[1] »،وهو ما أقره قانون إمارة دبي بشأن المعاملات والتجارة الإلكترونية [2]

فلا يجوز للغير أن يطلب إلغاء الشهادة إنما يمكن له أن يضع الواقعة سبب الإلغاء تحت تصرف مزود الخدمات الذي يقدر بدوره إمكانية إلغاء الشهادة من عدمه[3].

إلا أن طلب صاحب الشهادة بإلغائها يجب أن يكون مبررا، خاصة إذا علمنا أن شهادة التصديق فور صدورها واستعمالها فإنه ترتب أثارا وحقوقا للغير.

من المبررات التي يمكن لصاحب الشهادة أن يعتمد عليها في طلبه، في حال اكتشافه تلاعبا بمنظومة التوقيع الإلكتروني.

2-عند إعلامه بوفاة الشخص الطبيعي أو انحلال الشخص المعنوي صاحب الشهادة:

لقد رأينا أن شهادة التصديق مرتبطة بالموقع فهي تصدر باسمه سواء كان شخصا طبيعيا أو ممثلا قانونيا لشخص معنوي، المهم أن تصدر الشهادة باسم شخص طبيعي.

ففي حال وفاة الشخص الطبيعي فلا حاجة للتوقيع الإلكتروني الخاص به أو شهادة المصادقة الصادرة في هذا الخصوص، وكذلك في حال انحلال الشخص المعنوي أو انقضائه.

لكن قد يثار المشكل في حالة دمج الشركات، يمكن أن تطلب هذه الشركة أن تعدل الشهادة، والأفضل أن تستصدر شهادات جديدة تفاديا للغموض الذي قد يحدث[4] .

---

[1] Art02 :«signataire »,toute personne qui détient un dispositif de création de signature et qui agit soit pour son propre compte,soit pour celui d'une entité ou personne physique ou morale qu'elle représente;»

[2] المادة 1 من قانون المعاملات والتجارة الإلكتروني اتلي تنص :« الموقع ـ الشخص الطبيعي أو المعنوي الحائز لأداة توقيع الكتروني خاصة به ويقوم بالتوقيع او يتم التوقيع بالنيابة عنه على الرسالة الالكترونية باستخدام هذه الأداة.

[3] المستشار عبد الفتاح بيومي حجازي،المرجع السابق ،ص 182

[4] أ/قارة مولود ،المرجع السابق،ص 96

3-الشهادة المحتوية على معلومات مغلوطة أو مزيفة : يجب أن نعلم أن هناك فرقا كبيرا بين المعلومة المغلوطة وتلك المزيفة، فالأولى هي معلومات صحيحة ولكن تخص شخصا أخر كأن يسلم مزود الخدمات الشهادة إلى شخص له ذات الاسم الثلاثي ،فيتوجب على مود الخدمة أن يسارع بتعليق الشهادة من تلقاء نفسه لأنه قد يسبب ضررا للغير[1] .

أما المعلومات المزيفة فهي معلومات غير حقيقية يصدر على أساسها مزود الخدمات شهادة التصديق، كأن يقوم أحدهم بتزوير بطاقته الشخصية.

من خلال استقراء الفصلين 19 و 20 من القانون التونسي نلاحظ أن هذه الحالة يجب أن تمر على مرحلتين:

أولا: يجب على مزود الخدمات أن يقوم بتعليق العمل بشهادة التصديق كما أوضحناه سابقا بمجرد أن يعلم بأن المعلومات الواردة في شهادة التصديق مزيفة أو مغلوطة .

ثانيا : يتعين على مزود الخدمات أن يتحرى بنفسه بالوسائل المشروعة ودون الإخلال بالقواعد القانونية المتعلقة بحماية المعطيات الشخصية[2] عن مدى سبب الوقف المؤقت، فإما يلغي شهادة التصديق كليا أو أن تكون المعلومات الواردة في الشهادة صحيحة وبالتالي يتم رفع حالة التعليق فورا.

كذلك الشأن في حالة انتهاك منظومة التوقيع الإلكتروني أو الاستعمال المدلس للشهادة،كأن تفقد الشهادة من صاحبها ويقوم أخر باستعمالها بوصفه صاحب الشهادة على نحو يؤدي إلى التدليس على إرادة الغير.

4-تعليق الشهادة بسبب تغيير البيانات المتضمنة فيها: من المفترض أن تكون المعلومات المذكورة في شهادة التصديق صحيحة طوال مدة سريانها، فيتوجب على صاحب الشهادة إذا

---

[1] المستشار عبد الفتاح بيومي حجازي،المرجع السابق ،ص 176

[2] هذه النصوص واردة في القانون التونسي في الباب السادس تحت عنوان «في حماية المعطيات الشخصية»

ما حدث أي تغيير في الشهادة إعلام مزود الخدمات بذلك[1] ،وان يمارس عناية معقولة لضمان دقة واكتمال كل ما يقدمه من بيانات وتصريحات جوهرية ذات صلة بالشهادة طيلة فترة سريانها[2].

على هذا الأساس فإنه يجب على مزود الخدمات في هذه الحالة متى أبلغه صاحب الشهادة بتغير أحد بيانات الشهادة أن يعلق العمل بها حتى يتأكد من المعلومة، فإما يلغي الشهادة نهائيا إذا ثبت صحة سبب التعليق أو يلغي قرار التعليق .

فمنح المشرع التونسي لصاحب الشهادة والغير الحق في معارضة قرار مزود الخدمات بتعليق العمل بالشهادة من تاريخ نشره في السجل الإلكتروني ؛ وهو أمر منطقي إذ غالبا ما يرتب هذا القرار أثارا سلبية سواء على صاحب الشهادة أو الغير الذي ارتبطت مصالحه بهذه الشهادة.

المبحث الثاني: حماية التوقيع الإلكتروني

إن توفير الأمان القانوني الضروري للتوقيع الإلكتروني لا يقع فقط على عاتق مزود الخدمات .

بل تفرض القوانين كذلك على الموقع والمرسل إليه أن يتبعا سلوكا معينا أثناء عملية التوقيع لأنهما المعنيان بالدرجة الأولى وأصحاب المصلحة وأن أي إخلال من طرفهما قد يمس بصفة مباشرة بمركز الطرف الأخر(المطلب الأول).

---

[1] الفصل 6 فقر 3 من نفس القانون التونسي

[2] المادة 22 فقرة 1 من قانون المعاملات والتجارة الإلكترونية بإمارة دبي تنص:«(ج) ان يمارس عناية معقولة لضمان دقة واكتمال كل ما يقدمه من بيانات وتصريحات جوهرية ذات صلة بالشهادة طيلة فترة سريانها، وذلك في الحالات التي تستلزم فيها اداة التوقيع استخدام شهادة.

يتميز التوقيع الإلكتروني بأنه وسيلة هامة في مجالات المعاملات الالكترونية، والتي غالبا ما تتم في الانترنيت، و نظرا لما يميز هذه الأخيرة من كثرة الأعمال الإجرامية وعمليات التزوير والقرصنة، فإن التوقيع الإلكتروني بدوره يصبح عرضة لهذه الأعمال الإجرامية.

لهذا نجد أن معظم التشريعات والقوانين في هذه الدول قد وفرت حماية جنائية للتوقيع الإلكتروني ، وهذا حتى يكون حاجزا ورادعا أمام أي شخص سيئ النية يسعى إلى زعزعة ثقة الأفراد بالتوقيع الإلكتروني والتجارة الإلكترونية(المطلب الثاني) .

المطلب الأول: حماية التوقيع الإلكتروني أثناء استعماله

إن استخدام التوقيع الإلكتروني يكون من طرف الموقع الذي يقوم بعملية التوقيع وما ترتب هذه العملية من التزامات ومسؤولية على عاتقه ،كما فرض القانون عليه أن يتبع سلوكا معينا أثناء التوقيع(الفرع الأول).

أما المرسل إليه أو الطرف المعول فإنه لم تهمله القوانين وألزمته أن يتبع بعض الخطوات حتى يتأكد من صحة التوقيع وإلا فإنه يتحمل تبعة ذلك (الفرع الثاني)

الفرع الأول : التزامات ومسؤولية الموقع

إن الموقع هو الشخص الطبيعي أو المعنوي الحائز لأداة توقيع الكتروني خاصة به ويقوم بالتوقيع أو يتم التوقيع بالنيابة عنه على الرسالة الالكترونية باستخدام هذه الأداة[1].

لم [1] ورد هذا التعريف تقريبا في كل التشريعات مثل القانون البحريني وإمارة دبي والقانون الفرنسي إلا أن المشرع التونسي يورد تعريفا للموقع عكس بقية التشريعات.

لكن عند استعمال التوقيع الإلكتروني من طرفه فإن علاقته مع المرسل إليه هي علاقة بين غائبين ،فلا الموقع متأكد من أن الوثيقة هي من طرف المرسل إليه ولا المرسل إليه يمكن له مشاهدة توقيع الموقع وهو ما يولد إحساس بعدم الأمان من الجهتين[1]

وبالتالي فإن للموقع دور هام في استعمال أداة التوقيع وفي توفير جو من الطمأنينة في نفسية المرسل إليه وكل شخص متعامل معه.

لذلك أعطت التشريعات والقوانين أهمية بالغة في تحديد سلوك الموقع اتجاه المرسل إليه أو اتجاه مزود الخدمات ،فنجد مثلا أن قانون الأونيسترال قد أفرد المادة 8 لتحديد مسؤولية الموقع المعنونة ب«سلوك الموقع» التي تنص :«1- حيثما يمكن استخدام بيانات إنشاء التوقيع لإنشاء توقيع يكون له مفعول قانوني ،يتعين على كل موقع :

أ- أن يمارس عناية معقولة لاجتناب استخدام بيانات إنشاء توقيعه استخداما غير مأذون به.

ب- أن يبادر دون تأخر لا مسوغ له ،إلى استخدام الوسائل التي يوفرها مقدم خدمات التصديق بمقتضى المادة 9 من هذا القانون ، أو على نحو أخر إلى بذل جهود معقولة لإشعار أي شخص يجوز للموقع أن يتوقع منه على وجه معقول أن يعول على التوقيع الإلكتروني أو أن يقدم خدمات تأييد التوقيع الإلكتروني، وذلك في حالة :

1- معرفة الموقع بأن بيانات إنشاء التوقيع تعرضت لما يثير الشبهة أو

2- كون الظروف المعروفة لدى الموقع تؤدي إلى احتمال كبير بأن بيانات إنشاء التوقيع ربما تكون تعرضت لما يثير الشبهة .

ج- أن يمارس في حال استخدام شهادة لتأييد التوقيع الإلكتروني ،عناية معقولة لضمان دقة و اكتمال كل ما يقدمه الموقع من تأكيدات مادية ذات صلة بالشهادة طيلة دورة سريانها ،أو يتوخى إدراجها في الشهادة .

---

[1] Thierry Piette-coudol ;op.cit , 162

2- يتحمل الموقع التبعات القانونية لتخلفه عن الوفاء باشتراطات الفقرة 1»

يمكن أن نستخلص من هذه المادة ما يلي :

1- التزام عام من الموقع بأن يمارس عناية معقولة لمنع استخدام الغير لتوقيعه الإلكتروني من دون إذنه وهو ما نص عليه كذلك مشرع إمارة دبي في المادة 22 فقرة 1 :«أ- أن يمارس عناية معقولة لتفادي استخدام أداة توقيعه استخداما غير مأذون» ، وهذا الالتزام يرد عموما على الاتفاقيات المتعلقة باستخدام بطاقات الائتمان[1]، وينبغي أن مثل ذلك الالتزام أيضا على أية بيانات إنشاء توقيع إلكتروني يمكن استخدامها لأغراض التعبير على نية ذات دلالة قانونية[2].

أما المشرع التونسي فقد استعمل عبارة «الاحتياطات الدنيا» لإلزام الموقع ببذل العناية بعدم استعمال أداة توقيعه استعمالا غير مشروع [3] ،وهو ما يؤدي إلى تحقيق شرط أساسي في التوقيع الإلكتروني المحمي وهو ارتباط التوقيع الإلكتروني بالموقع دون غيره ،فلا يمكن أن تصور ارتباط التوقيع الإلكتروني بالموقع من دون أن يبذل هذا الأخير عناية معقولة أو يتخذ الاحتياطات الدنيا لتفادي استخدام أداة توقيعه من طرف الغير من دون إذنه

2- من ناحية أخرى يجب على الموقع أن يخطر من دون تأخير كل طرف معول على توقيعه الإلكتروني من أن أداة التوقيع الخاصة به قد تعرضت لما يثير الشبهة [4].

المقصود بالشخص المعول على التوقيع الإلكتروني ليس فقط المرسل إليه بل أيضا شخصا مثل مقدم الخدمات.

---

[1] أ-منير محمد الجنبيهي وأ-ممدوح منير الجنبيهي ،المرجع السابق ،ص 48

[2] أ-إبراهيم سيد أحمد ،المرجع السابق،ص 345

[3] حيث ينص الفصل 21 من القانون التونسي على :« يتعين على كل من يستعمل منظومة إمضاء الكتروني :
-اتخاذ الاحتياطات الدنيا التي يتم ضبطها في القرار المنصوص عليه بالفصل 5 من هذا القانون لتفادي كل استعمال غير مشروع لعناصر التشفير او المعدات الشخصية المتعلقة بإمضائه »

[4] وهو ما تنص عليه المادة 22 من قانون إمارة دبي :« (ب) أن يخطر الأشخاص المعنيين بدون تأخير غير مبرر، وذلك في حالة :
- معرفة الموقع بأن أداة توقيعه تعرضت لما يثير الشبهة في درجة أمانها.
- دلالة الظروف المعروفة لديه على احتمال كبير بأن تكون أداة التوقيع قد تعرضت لما يثير الشبهة في أمانها.»

كما أن التزام الموقع في هذه الحالة هو التزام ببذل العناية بنصه على «بذل جهود معقولة » فيستحيل على الموقع أن يتتبع كل شخص قد يعول على التوقيع الإلكتروني، لذا فتحميل هذا الأخير تحقيق نتيجة المتمثل في إشعار كل شخص يمكن تصور أنه يعول على التوقيع الإلكتروني يعتبر عبئا مفرطا ،ولهذا ينبغي تفسير مفهوم «الجهود المعقولة» على المبدأ العام لحسن النية [1] .

ذلك ما يتوافق مع شرط أساسي في التوقيع الإلكتروني المحمي وهو إمكانية كشف أي تعديل أو تبديل في بيانات التوقيع الإلكتروني ،فبمجرد أن يستعمل التوقيع من أي طرف أخر غير الموقع ذاته فإن ذلك يعني أن التوقيع الإلكتروني قد تعرض للتعديل والتغيير ومن واجب الموقع في هذه الحالة أن يخبر كل طرف معول على هذا التوقيع من أنه قد تعرضت بياناته للتعديل .

3- في حال صدور شهادة مصادقة إلكترونية فإنه يجب على الموقع أن يمارس عناية معتادة ومعقولة تضمن دقة بيانات الشهادة واكتمالها خلال مدة سريانها لتعلق حقوق الغير بهذه الشهادات والبيانات الواردة فيها [2] ، وهذا الالتزام لا يكون إلا في حالة التوقيعات الإلكترونية المدعومة بالشهادات ،عكس الالتزامات الأخرى التي تكون في جميع التوقيعات الإلكترونية[3] .

أما الفقرة 2 من المادة 8 من قانون الأونيسترال النموذجي فقد رتبت المسؤولية على عاتق الموقع في حال ما لم يستوفي الشروط المذكورة في الفقرة الأولى ،وإن كانت لم تنص على نتائج المسؤولية ولا حدودها بل ترك الأمر للقانون الوطني في تقدير هذه المسؤولية ،إلا أنها توجه إشارة واضحة إلى الدول مفادها أنه ينبغي أن تترتب مسؤولية على التخلف عن استيفاء الالتزامات المبينة في الفقرة الأولى[4] . وهو ما أقره المشرع مثلا المشرع في إمارة

---

[1] أ.إبراهيم سيد أحمد ،المرجع السابق،ص 345

[2] المستشار عبد الفتاح بيومي حجازي،المرجع السابق ،ص 86

[3] أنظر في ذلك أ.منير محمد الجنبيهي وأ.ممدوح منير الجنبيهي ،المرجع السابق ،ص48 و أ.إبراهيم سيد أحمد ،المرجع السابق،ص 346

[4] أ.منير محمد الجنبيهي وأ.ممدوح منير الجنبيهي ،المرجع السابق ،ص 49

دبي في المادة 22 فقرة 2 التي تنص:

« يكون الموقع مسئولاً عن تقصيره في استيفاء متطلبات الفقرة (1)السابقة» ،وكذلك المشرع التونسي في الفصل 21 عندما اعتبره هو المسئول الوحيد على سرية وسلامة منظومة إحداث الإمضاء التي يستعملها.

بالإضافة إلى ذلك ألزم المشرع التونسي الموقع أن يخبر مزود الخدمات بأي تغيير قد يطرأ على المعلومات الواردة مثل أن يغير الموقع محل إقامته أو مهنته إلخ ... وهو أمر بديهي لأن أي تغيير في البيانات الواردة في شهادة التصديق تمس بصفة مباشرة مصالح الأشخاص الذين وثقوا بما ورد في هذه الشهادة ،وفي حال ما لم يلتزم الموقع بذلك فإن هذه الشهادة تصبح مزيفة ويمكن لمزود الخدمات في هذه الحالة إلغائها [1]

كما يقع على الموقع تعويض الأضرار التي قد تلحق المرسل إليه أو الأطراف المعولة التي اعتمدت على هذه الشهادة.

الفرع الثاني: دور المرسل إليه في التوقيع الإلكتروني

أطلقت التشريعات عدة تسميات على المرسل إليه فقانون الأونيسترال مثلا أسماه بالطرف المعول ، أو الطرف المعتمد كقانون إمارة دبي وهناك من أسماه المرسل إليه كالقانون البجريني أو المتعامل مثلما ورد في القانون المصري.

لا يهمنا في هذا النطاق إلا تحديد تعريف واضح للمرسل إليه وهو كل شخص سواء كان طبيعي أو اعتباري يتعامل استنادا إلى شهادة تصديق إلكترونية أو توقيع إلكتروني.

على هذا الأساس فإن المرسل إليه في علاقته مع مزود الخدمات يبقى محميا بموجب قواعد المسؤولية التقصيرية إذا ما سبب هذا الأخير أضرارا له. [2]

---

[1] أنظر ما قلناه عن حالة تزييف شهادة التصديق في الفرع الثالث من المطلب الثاني من المبحث الأول تحت عنوان « تعليق وإلغاء شهادة التصديق»

[2] أنظر ما قلناه في مسؤولية مزود الخدمات اتجاه الموقع

فرض القانون على المرسل إليه أن يتخذ خطوات مناسبة ومعقولة للتأكد من صحة البيانات الواردة في الشهادة و التأكد من صحة التوقيع الإلكتروني، وهذه الخطوات هي:

- عندما تصل الرسالة الإلكترونية إلى المرسل إليه، فإنه يجد التوقيع الإلكتروني ملحقا أو موجود داخل الرسالة (وهو الحالة الغالبة في الواقع العملي).

غير أن التوقيع في هذه المرحلة لا يمكن استغلاله لكونه مشفر وبالتالي يكون غير مقروء، لذا فمن الضروري أن تكون لديه شهادة إلكترونية تحتوي على المفتاح العام.

في بعض الحالات يمكن إرسال الشهادة بواسطة الموقع نفسه، إلا أنه يجب على المرسل إليه أن يسأل إلكترونيا مزود الخدمات عن طريق عريضة من أجل الحصول على الشهادة.

لكن السؤال المطروح ماذا لو لم يبذل المرسل إليه العناية المطلوبة في الحصول على الشهادة الإلكترونية؟

في هذه الحالة فإن المرسل إليه لا يكون له الحق في الحصول على التعويضات عن الأضرار المترتبة عن ذلك لأنه قد أخل بالتزام جوهري وهو أن يتحصل على شهادة التصديق و يتخذ خطوات مناسبة ومعقولة للتأكد من صحة البيانات الواردة في الشهادة.

-بالشهادة المتحصل عليها يقوم المرسل إليه بفك الشفرة ثم مراقبة التوقيع الإلكتروني .

-أخيرا التوقيع الإلكتروني المعالج والغير مشفر يصبح صحيحا ،ولكن ذلك لا يتم بصورة آلية فقد يكون التوقيع منتهي الصلاحية أو تم تجاوز مجالات استعماله ،لذا يجب على المرسل إليه التأكد من مجالات استعمال التوقيع الإلكتروني بواسطة عريضة إلكترونية موجهة لمزود الخدمات للحصول على« قائمة الشهادات الملغية» أو قائمة الشهادات المعلقة[1] وهو ما يعتبر مطابقا لما ورد في المادة 11 من قانون

[1] Thierry Piette-coudol; op.cit,p.164 et 165

الأونيسترال النموذجي بشأن التوقيعات الإلكترونية حيث نصت :«يتحمل الطرف المعول التبعات القانونية الناجمة عن تخلفه عن:

ب-اتخاذ خطوات معقولة، إذا كان التوقيع الإلكتروني مؤيدا بشهادة لأجل:

1- التحقق من صلاحية الشهادة أو وقفها أو إلغائها.

2-مراعاة وجود أي تقييد بخصوص الشهادة.»

إلا أنه ينبغي إبقاء مسألة صحة التوقيع الإلكتروني منفصلة عن مسألة ما إن كان من المعقول من الطرف المعول أن يعول على توقيع لا يستوفي المعايير القانونية المذكورة في المادة 6 من قانون الأونيسترال[1].

كما أن المادة 5 من مشروع قانون تنظيم التوقيع الإلكتروني المصري ألزم المتعامل(المرسل إليه) أن يتحقق من صحة التوقيع لإلكتروني المقدم له، وصلاحية هذا التوقيع أي التأكد من مجالات استعمالاته و أخيرا التأكد من صدور هذا التوقيع من الموقع دون سواه[2]

وهو ملزم كذلك بإثبات نزاهته واستقامته و يثبت أنه احتفظ بالوثيقة كما تسلمها وهو ما جاء به القانون التونسي في الفصل الرابع [3].

كما أن المادة 22 من القانون البحريني قد منحت لصاحب المصلحة (الموقع أو المرسل إليه) الحق في الطعن بالتزوير في السجلات الإلكترونية والتوقيع الإلكتروني

---

[1] أ-إبراهيم سيد أحمد ،المرجع السابق،ص 352

المادة 5 من مشروع تنظيم التوقيع الإلكتروني المصري تنص:«يلتزم المتعامل بأن يتحقق من صحة التوقيع الإلكتروني [2]المقدم له ،وصلاحيته للاستخدام وصدوره من الموقع وذلك كله وفقا للشروط والضوابط الواردة في القانون ولائحته لتنفيذية»

[3] Arnaud-f .Fausse ;op.cit. ,p 274

الذي عليها، وأعطت الحق في الطعن بالبطلان باستعمال التوقيع الإلكتروني إذا ما تم من دون تفويض من صاحب الحق (الموقع)[1].

المطلب الثاني: الحماية الجنائية للتوقيع الإلكتروني

لقد رأينا في المطلب الأول من هذا المبحث دور الموقع والمرسل إليه في حماية التوقيع الإلكتروني أثناء إعماله والسلوك الذي يجب عليهم أن يتبعوه وفق ما ينص عليه القانون وما يقتضيه سلوك الشخص المعتاد أثناء تعامله مع التوقيع الإلكتروني.

إلا أن هذه القواعد لن تكون كافية من دون نصوص جنائية تعاقب كل شخص سواء كان طرفا في التوقيع(مثل الموقع أو المرسل إليه أو مزود الخدمات) أو كان شخص سيء النية لم يكن طرفا فيه .

إلا أن الفقه الجنائي تردد كثيرا في اعتبار المعلومات والبيانات من قبيل المال المنقول، غير أنه استقر على إعطائها هذه الصفة حتى يمكن حماية البيانات والمعلومات وبرامج الحاسب الآلي وتطبيقاتها هذا من جهة ومن جهة أخرى فإن ثورة المعلومات ساهمت في ظهور كيانات اقتصادية جديدة تتطلب الحماية الجنائية وهذه الكيانات من قبيل المعلومات أو البيانات[2].

---

[1] **مادة (22):** الطعن في صحة السجلات والتوقيعات الإلكترونية 1- لصاحب المصلحة الطعن بالتزوير في السجلات الإلكترونية والتوقيع الإلكتروني عليها ، والطعن ببطلان استعمال هذا التوقيع ، إذا تم ذلك بدون تفويض من صاحب الحق ، أو لغير ذلك من أسباب البطلان المقررة قانوناً في شأن التوقيع الخطي . 2- تفصل المحكمة المختصة في الطعون المشار إليها في البند السابق ، أو الدفوع المتعلقة بشأنها، طبقاً للإجراءات وقواعد الإثبات المقررة قانوناً ، وبما يتفق وطبيعة السجلات والتوقيعات الإلكترونية وفقا للأحكام المنصوص عليها في هذا القانون .

[2] المستشار عبد الفتاح بيومي حجازي،المرجع السابق ،ص 477

على هذا الأساس فإن التوقيع الإلكتروني أصبح يشكل كيانا هاما يجب حمايته جنائيا وهذا نظرا للأهمية الاقتصادية التي يشكلها في إطار التجارة الإلكترونية باعتباره مال منقول ويحتوي على معلومات وبيانات مهمة يجب حمايتها.

من أهم الأطراف الفاعلة في هذا المجال هو مزود الخدمات باعتباره فهو من يمنح التوقيع للأشخاص الراغبين فيه بمقابل مادي وغالبا ما يخضع إلى شروط والتزامات دقيقة يجب أن يوفي بها وأي إخلال بها قد يرتب على عاتقه المسؤولية الجنائية (الفرع الأول).

بالإضافة إلى ذلك فإن شهادة التصديق تعتبر المحرك الأساسي لإعمال التوقيع بشكل يوفر أكبر قدرا من التعارف بين الأطراف المتعاقدة، وبالتالي فإن أي تلاعب بهذه الشهادة يعتبر مساسا مباشر بمصداقية التوقيع الإلكتروني ككل، وبالتالي فإن التشريعات والنصوص القانونية قد رتبت عقوبات قد تصل إلى الحبس والغرامة على كل شخص قد يتلاعب بهذه الشهادة (الفرع الثاني).

كما وسعت التشريعات الحماية الحنائية لتشمل التوقيع والكتابة الإلكترونية ،لكونهما عنصران مرتبطان ببعضهما البعض وأي مساس بأحدهما فإنه سيؤدي حتما للمساس بالأخر،ولم يتم إغفال الوسيط الإلكتروني ففرضت القوانين الحماية له لأنه الوسيلة التي يتم بها التوقيع (الفرع الثالث).

الفرع الأول: المسؤولية الجنائية لمزود الخدمات

أولا: جريمة ممارسة نشاط مزود الخدمات من دون ترخيص:

إن أول جزاء يترتب على إخلال مزود الخدمات بالتزاماته وفق الفصل 44 من قانون المبادلات والتجارة الالكترونية التونسي هو سحب الترخيص وإيقاف نشاطه، ولا يشترط في هذه الجريمة العمد بل يكفي مجرد الإهمال حتى تقع العقوبة[1].

إذا أخذنا بعين الاعتبار أن الترخيص هو من أهم الشروط الضرورية لمزالة نشاط مزود الخدمات فإن القانون التونسي أقر عقوبة السجن لمدة تتراوح بين شهرين و 3 سنوات وبخطية تتراوح بين 1.000 و 10.000 دينار أو بإحدى هاتين العقوبتين[2] .

وهو نفس ما أقره القانون المصري في المادة (23 /أ)عندما نص في عقوبة الحبس والغرامة التي لا تقل عن عشرة ألاف جنيه في حال قيام مزود الخدمات بنشاطاته قبل الحصول على الترخيص من الجهة المختصة .

كما يحق للهيئة بالإضافة إلى هذه العقوبات أن تلغي ترخيص مزود الخدمات أو توقف سريانه إلى غاية إزالة أسباب المخالفة [3]

والسبب الأساسي لتجريم هذا الفعل من طرف القوانين والتشريعات هي الآثار الخطيرة المترتبة عن هذا الفعل إذ أنه يقضي على مبدأ الثقة والأمان التي يجب أن تتوافر في

---

[1] المستشار عبد الفتاح بيومي حجازي،المرجع السابق ،ص 490

[2] **الفصل 46:**« يعاقب كل من يمارس نشاط مزود خدمات المصادقة الالكترونية بدون الحصول على ترخيص مبق طبقا للفصل 11 من هذا القانون بالسجن لمدة تتراوح بين شهرين و 3 سنوات وبخطية تتراوح بين 1.000 و 10.000 دينار أو بإحدى هاتين العقوبتين. »

[3] المادة 26 تنص:«مع عدم الإخلال بأحكام المادة (23) من هذا القانون يكون للهيئة إذا خالف المرخص له بإصدار شهادات تصديق إلكتروني شروط الترخيص أو خالف أيا من أحكام المادة (19) من هذا القانون أن تلغي الترخيص ،كما يكون لها أن توقف سريانه حتى إزالة أسباب المخالفة ،وذلك كله وفقا للقواعد والإجراءات التي تحددها اللائحة التنفيذية لهذا القانون »

المعاملات الإلكترونية، فالغير قد سلم بصحة الشهادة التي يصدرها مزود الخدمات إلا أنه يتبين له فيما بعد أن هذه الشهادة غير صحيحة وغير معترف بها قانونا مما يسبب ضياعا لحقوق ومصالح الغير .

بالإضافة إلى ذلك فإن مزود الخدمات قد خالف نصا صريحا بوجوب حصوله على الترخيص لمزاولة وممارسة نشاطاته على إقليم الدولة، وهو ما ينص عليه مثلا الفصل 11 فقرة 1 من القانون التونسي :« يتعين على كل شخص طبيعي أو معنوي يرغب في تعاطي نشاط مزود خدمات المصادقة الالكترونية الحصول على ترخيص مسبق من الوكالة الوطنية للمصادقة الالكترونية .» ، والمادة 19 فقرة 1 من القانون المصري التي تنص :« لا تجوز مزاولة نشاط إصدار شهادات التصديق الإلكتروني إلا بترخيص من الهيئة ...».

من جهة فإن هذه الجريمة من الجرائم العمدية ،ذلك أن الجاني كان عالما بأن سلوكه المتمثل في إصدار الشهادة دون الحصول على الترخيص من السلطة المختصة يشكل جناية، ومع ذلك فقد اتجهت إرادته إلى هذا السلوك الإجرامي وقبل الآثار المترتبة عليه[1].

ثانيا : جريمة إفشاء الأسرار :

لا تقتصر هذه الجريمة على مزود الخدمات بل تشمل كل شخص أعطى له القانون سلطة الإطلاع على معلومات وبيانات شخصية متعلقة بالأفراد مثل مزود الانترنيت.

إلا أنه وفي مجال التوقيع الإلكتروني غالبا ما تقع هذه الجرائم من طرف مزود الخدمات أو أحد أعوانه لأن القانون قد منح له سلطة الحصول على معلومات وبيانات شخصية متعلقة بالموقع، بحيث يجب أن تبقى هذه البيانات سرية لأنها ضامن أساسي للممارسة التجارة الإلكترونية بشكل أمن وعدم إطلاع الغير على هذه البيانات.

---

[1] المستشار عبد الفتاح بيومي حجازي،المرجع السابق ،ص 540

أما إذا قام مزود الخدمات أو أحد أعوانه بإفشاء هذه البيانات فإنه تترتب اتجاهه عقوبات جنائية، وهو ما نص عليه الفصل 52 من القانون التونسي[1] ، والمادة 31 فقرة 1 من قانون إمارة دبي[2] (1) ،والمادة (23/د) من القانون المصري[3] .

نلاحظ من خلال هذه المواد أن مشرع إمارة دبي لم يجعل من العمد شرطا لقيام هذه الجريمة بل يكفي أن تتم بإهمال مزود الخدمات ، إلا أنه في هذه الحالة فالعقوبة تقتصر على الغرامة وحدها دون أن تشملها عقوبة الحبس.

غير أنه يعفى مزود الخدمات من هذه العقوبات إذا ما قام بنشر المعلومات الشخصية بموافقة المعني بالأمر، سواء تمت هذه الموافقة كتابيا أو إلكترونيا ، أو تم نشر هذه المعلومات وفق ما ينص عليه القانون كما لو تم ذلك بناءا على إذن من السلطات القضائية في الدولة.

أخيرا فإنه يجب التمييز بين هذه الجريمة وجريمة انتهاك السرية والخصوصية في التجارة الإلكترونية التي تشبهها إلى حد كبير إلا أن المعيار الفاصل بينهما هو أن هذه الأخيرة تتم من طرف شخص غير مخول له قانونا الإطلاع على هذه البيانات بينما الجريمة التي نحن بصدد دراستها تقع دائما من طرف شخص مخول له قانونا الإطلاع على هذه المعلومات[4] .

---

[1] **الفصل 52** :«يعاقب طبقا لأحكام الفصل 254 من المجلة الجنائية مزود خدمات المصادقة الالكترونية وأعوانه الذين يفشون او يحثون او يشاركون في إفشاء المعلومات التي عهدت إليهم في إطار تعاطي نشاطاتهم باستثناء تلك التي رخص صاحب الشهادة كتابيا او الكترونيا في نشرها أو الإعلام بها أو في الحالات المنصوص عليها في التشريع الجاري به العمل» .

[2] التي تنص:« يعاقب كل شخص تمكن بموجب أية سلطات ممنوحة له في هذا القانون من الاطلاع على معلومات في سجلات أو مستندات أو مراسلات الكترونية، وأفشى متعمدا أيا من هذه المعلومات، بالحبس وبغرامة لا تجاوز 100.000 درهم، أو بإحدى هاتين العقوبتين. وتكون العقوبة الغرامة التي لا تجاوز 100.000 درهم في حالة تسببه بإهماله في إفشاء هذه المعلومات. »

[3] المادة (23/د) تنص:«...د- خالف أيا من أحكام المادتين 19 ،21 من هذا القانون

[4] المستشار عبد الفتاح بيومي حجازي،المرجع السابق ،ص 527

أضاف المشرع المصري في المادة 23 الفقرة الأخيرة منه عقوبة لا تقل عن 5000 جنيه ولا تجاوز 50000 جنيه في حالة ما إذا لم تلتزم الجهات والشركات العاملة في مجال التوقيع الإلكتروني بموافاة الهيئة بما تطلبه من تقارير أو إحصاءات أو معلومات تتصل بنشاط الهيئة، وفي حال تكرار هذا السلوك فإن العقوبة تضاعف في حدها الأقصى والأدنى، مع نشر أحكام الإدانة في جريدتين يوميتين وعلى الانترنت على حساب المحكوم عليه، ولا نجد هذه العقوبة في قانون من قوانين الدول الأخرى .

الفرع الثاني: الجرائم المتعلقة بشهادة التصديق

هناك عدة جرائم مرتبطة بشهادة التصديق عاقبت عليها التشريعات وسنتعرض إليها بالتفصيل على الشكل الأتي :

أولا: جريمة نشر الشهادة بقصد الاحتيال:

نصت عليه المادة 29 من قانون إمارة دبي بقولها:«_: يعاقب كل من أنشأ أو نشر عن معرفة أو وفر أية شهادة أو بيانات غير صحيحة لأي غرض احتيالي أو أي غرض آخر غير مشروع، بالحبس وبغرامة لا تجاوز 250.000 درهم أو بإحدى هاتين العقوبتين.» ، والمادة(24 فقرة1 /ج) من القانون البجريني :« العقوبات 1 - مع عدم الإخلال بأية عقوبة أشد ينص عليها أي قانون آخر ، يعاقب بالسجن مدة لا تزيد على عشر سنوات ، وبغرامة لا تجاوز مائة ألف دينار أو بإحدى هاتين العقوبتين كل من ارتكب عمداً فعلاً من الأفعال الآتية :... ج- إنشاء أو نشر أو تحريف أو استعمال شهادة ، أو توقيع إلكتروني لغرض احتيالي أو لأي غرض غير مشروع . ».

يجب توافر الركنين المادي والمعنوي لقيام لهاته الجريمة :

1- الركن المادي : إنشاء أو نشر أو توفير شهادة أو بيانات غير صحيحة ،ويتم ذلك بخلق شهادة لا وجود لها أو نشر هذه الشهادة بقصد استعمالها .

أما توفير الشهادة أو البيانات فهو حصول الجاني على شهادة أو بيانات كانت موجودة لدى الغير واستعملها لنفسه[1].

يشترط كذلك في هذه الجريمة أن تتم عن طريق الاحتيال أو أي غرض غير مشروع، إذ يجب أن يهدف من خلالها الجاني لخداع المجني عليه كأن يوهمه بصحة مركزه المالي قصد إبرام صفقة وهمية.

2- الركن المعنوي : يجب أن تتوافر في هذه الجريمة القصد الجنائي العام بركنيه العلم والإرادة ، أي أن يكون الجاني عالما بأن الشهادة التي يستعملها غير صحيحة ومع ذلك تنصرف إرادته للسلوك الإجرامي ويقبل النتائج المترتبة على هذا الفعل.

نلاحظ أنه إذا ما توافر الركن المادي والمعنوي للجريمة فإنه تترتب على عاتق الشخص المرتكب للفعل المسؤولية الجنائية وما ينتج عنها من حبس تتراوح مدته بين شهر و 3 سنوات (المادة 69 عقوبات اتحادي) وقد تصل عند المشرع البحريني إلى 10 سنوات كحد أقصى ،وبالغرامة لا تتجاوز 250.000 درهم (عند مشرع إمارة دبي) أو مائة ألف دينار(بالنسبة للمشرع البحريني) أو بعقوبة أشد إن وجدت ،ويكون للقاضي السلطة التقديرية في الاختيار بين العقوبتين أو الحكم بكليهما وذلك وفق ظروف القضية المعروضة أمامها.

[1] المستشار عبد الفتاح بيومي حجازي،المرجع السابق ،ص 520

ثانيا : جريمة نشر الشهادة

إن النص على هذه الجريمة هدفه الأساسي منع الأشخاص من نسبة شهادة التصديق إلى شخص لم يوقعها أو لم تصدر من مزود الخدمات ،أو استعمال هذه الشهادة بعدما تم إلغائها أو إيقاف العمل بها .

صور هذه الجريمة ذكرت في المادة 28 من قانون إمارة دبي التي تنص:« لا يجوز لأي شخص أن ينشر شهادة تشير إلى مزود خدمات تصديق مدرج اسمه في الشهادة، إذا كان الشخص يعرف أن: (أ) مزود خدمات التصديق المدرج اسمه في الشهادة لم يصدر الشهادة.
(ب) الموقع المدرج اسمه في الشهادة لم يقبل الشهادة.
(ج) الشهادة قد ألغيت أو أوقفت، إلا إذا كان ذلك النشر بغرض التحقق من توقيع الكتروني أو رقمي تم استعماله قبل الإيقاف أو الإلغاء.» .

كما أقره أقره المشرع البحريني في المادة 24 فقرة 1 /ه التي تنص :« العقوبات 1 - مع عدم الإخلال بأية عقوبة أشد ينص عليها أي قانون آخر ، يعاقب بالسجن مدة لا تزيد على عشر سنوات ، وبغرامة لا تجاوز مائة ألف دينار أو بإحدى هاتين العقوبتين كل من ارتكب عمداً فعلاً من الأفعال الآتية :

...هـ - نشر شهادة أو وضعها في متناول أي شخص ، يحتمل أن يعتمد عليها أو على توقيع إلكتروني وارد بها من خلال الاستناد لأية بيانات مدرجة بهذه الشهادة مثل الرموز أو كلمات السر أو الغوريثمات أو مفاتيح التشفير العامة أو أية بيانات تستعمل لأغراض التحقق من صحة التوقيع الإلكتروني ، إذا كان من ارتكب ذلك الفعل على علم بأي من الآتي :- – عدم إصدار الشهادة من قبل مزود خدمة الشهادات المدون في تلك الشهادة . – عدم قبول الشهادة من قبل صاحبها المدون بها . – إلغاء الشهادة أو وقف العمل بها ، بشرط ألا يكون نشر الشهادة أو وضعها في متناول الجمهور قد تم بغرض تمكين الغير من التحقق من صحة توقيع إلكتروني تم إنشاؤه قبل إلغاء الشهادة أو وقف العمل بها أو لغرض الإخطار بالإلغاء أو الوقف ».

وعلى ذلك فإن صور الركن المادي لهذه الجريمة وفق المادتين هي ثلاث صور :

1-استعمال شهادة تصديق من أحد الأشخاص سواء كان شخصا طبيعيا أو معنويا وينسبها إلى مزود خدمات معين وهي في حقيقة الأمر لم تصدر أبدا من هذا المزود.

2-أو يستعمل هذا الشخص شهادة تصديق ينكر الشخص الموقع من أنها منسوبة إليه أو لا يقبلها ،وفي هذه الحالة لا يمكن استعمال هذه الشهادة .

3-أو استعمال شهادة تصديق ملغاة أو موقوفة العمل إلا إذا كان بغرض التحقق من توقيع الكتروني أو رقمي تم استعماله قبل الإيقاف أو الإلغاء.

ثالثا : جريمة تزييف الطلب وانتحال هوية شخص أخر

1- جريمة تزييف الطلب:

إن الموقع أو نائبه ملزم أن يقدم بياناته إلى مزود الخدمات وهذا إما لاستصدار أو إيقاف أو إلغاء الشهادة ، لذلك نصت المادة 30 من قانون إمارة دبي على عقوبات في حال ما إذا أخل هذا الأخير بالتزامه حيث تنص هذه المادة : «مع عدم الإخلال بأية عقوبة اشد ينص عليها أي قانون آخر، يعاقب كل من قدم متعمداً بيانات غير صحيحة عن هويته أو تفويضه إلى مزود خدمات التصديق بغرض طلب استصدار أو إلغاء أو إيقاف شهادة، بالحبس لمدة لا تزيد على ستة أشهر، وبغرامة لا تجاوز 100.000 درهم أو بإحدى هاتين العقوبتين» ، والفصل 47 من القانون التونسي التي تنص :« يعاقب كل من صرح عمدا بمعطيات خاطئة

لمزود خدمات المصادقة الالكترونية ولكافة الأطراف التي طلب منها أن تثق بإمضائه بالسجن لمدة تتراوح بين 6 أشهر وعامين وبخطية تتراوح بين 1.000 و 10.000 دينار أو بإحدى هاتين العقوبتين.»

بالتالي يشترط في هذه الجريمة أن تتم بتقديم بيانات غير صحيحة عن هويته أو تفويضه بشكل عمدي ،ويتحقق هذا الفعل حتى لو تحققت الواقعة إلى طرف ثالث غير مزود الخدمات من ذلك مثلا بنك أحد الأطراف[1] .

فإن تحقق هذا الفعل فإن المسؤولية الجنائية تقوم بحق الموقع أو المفوض ،وينتج عنها عقوبة الحبس لا تقل عن شهر ولا تزيد عن 6 أشهر وغرامة لا تتجاوز 100.000 درهم ، أما المشرع التونسي فقد أقر عقوبة أشد بالمقارنة مع ما ورد لدى مشرع إمارة دبي حيث نص على عقوبة السجن من 6 أشهر إلى عامين وخطية تتراوح بين 1000و 10.000 وفي كلا النصين ترك السلطة التقديرية للمحكمة في فرض إحدى هاتين العقوبتين أو كلاهما .

2-انتحال هوية شخص أخر :

قد يتم إصدار شهادة التصديق لغير الشخص المقصود وهذا إما لكون هذا الأخير قد انتحل شخصية طالب شهادة التصديق أو تحصل على هذه الشهادة من تفويض مزور وهو ما ينص عليه القانون البحريني في المادة(24 /1 /د) : « د- انتحال هوية شخص آخر ، أو الإدعاء زوراً بأنه مفوض من قبله في طلب الحصول على شهادة أو قبولها ، أو طلب تعليق العمل بها أو إلغائها» .

المقصود بالانتحال كل من تدخل بغير صفة واستعمل اسم الغير ، أو لجأ إلى تزوير تفويض بموجبه يستطيع طلب الشهادة أو إلغائها أو طلب تعليقها ، وفي هذه الجريمة نصبح أمام شخص لا يحق له قانونا القيام بهذه التصرفات إذ أنه لا يملك الصفة، ونظرا لما لهذا الفعل من خطورة فقد نص القانون البحريني على عقوبة الحبس لا زيد عن 10

[1] المستشار عبد الفتاح بيومي حجازي،المرجع السابق ،ص 497

سنوات وغرامة لا تتجاوز 100.000 دينار أو بإحدى هاتين العقوبتين بمجرد ثبوت قيام الشخص بهذه الأفعال.

الفرع الثالث : الجرائم الواقعة على التوقيع و الوسيط و المحرر الإلكتروني

أولا: استعمال توقيع أو وسيط أو محرر إلكتروني تالف ومزور وتزويره

لقد جرم هذه الأفعال المشرع المصري في المادة 23 فقرة ب و ج حين عاقب كل من: «...ب- أتلف أو عيب توقيعا أو وسيطا أو محررا إلكترونيا أو زور شيئا من ذلك بطريق الاصطناع أو التعديل أو التحوير أو بأي طريق أخر.

ج- استعمل توقيعا أو وسيطا أو محررا الكترونيا معيبا أو مزورا مع علمه بذلك .»

ومن خلال هاته المادة نستنتج أن هناك صورتين لهذه الجريمة

1- إتلاف وتزوير التوقيع أو الوسيط أو المحرر الإلكتروني : فالسلوك الإجرامي المتمثل في الإتلاف والتزوير يمكن أن ينصب إما على التوقيع أو الوسيط أو المحرر الإلكتروني.

وفعل الإتلاف يتحقق في حال ما إذا أصبح التوقيع أو المحرر أو الوسيط الإلكتروني غير صالح للقيام بمهامه كأن يقوم شخص بإدخال فيروس معلوماتي على التوقيع أو المحرر الإلكتروني فيفقد كل قيمة ويصبح غير صالح ،أو كأن يتم تحطيم الوسيط الإلكتروني المحفوظ فيه التوقيع أو المحرر الإلكتروني بشكل لا يمكن استرجاعه .

أما التعييب فالمقصود به أن التوقيع أو الوسيط أو المحرر الإلكتروني يفقد الصلاحية والقدرة على العمل ليس بشكل كامل إنما بصورة جزئية فقط كأن يصبح مشوها أو ناقصا أو غير واضح .

في حقيقة الأمر أنه لا يمكن تصور قيام هذه الجريمة على المحرر الإلكتروني دون أن يمس الوسيط الإلكتروني لأنها الدعامة التي تدون فيها هذه المحررات المذكرة المركزية للحاسب نفسه [1].

لقد أقر المشرع المصري إلى جانب ذلك جريمة تزوير المحرر أو التوقيع الإلكتروني، وقد أصاب في ذلك بما أنه قد أصبح للكتابة الإلكترونية نفس حجية الكتابة التقليدية وهو ما يرتب عنه ضرورة أن تكون لكلا النوعين نفس الحماية، وهو ما أدى إلى جعل جريمة التزوير تمتد كذلك إلى المحرر والتوقيع الإلكتروني .

يقصد بالتزوير التغيير في حقيقة المحرر بقصد الغش والاحتيال بتغيير مضمونه أو محتواه من أحد أطراف المحرر بالتعديل سواء بالإزالة أو الزيادة[2].

يمكن أن يتجسد تزوير التوقيع الإلكتروني في الفروض التالية:

-أن يكون التلاعب من جهة البنك بواسطة أحد موظفيه، على أساس عدم معرفة للرقم السري غير العميل والبنك.

-أن يفقد صاحب الحساب لبطاقة السحب ومعها شهادة المصادقة الإلكترونية[3] .

أما تزوير المحرر الإلكتروني فيمكن أن يتم ماديا عن طريق الاصطناع والتعديل، ويمكن أن يتم عن طريق التزوير المعني فقط أي بتعديل مضمونها دون اللجوء إلى التقليد والاصطناع.

---

[1] المستشار عبد الفتاح بيومي حجازي،المرجع السابق ،ص 543

[2] أ/قارة مولود ،المرجع السابق،ص 35

[3] أ/قارة مولود ،المرجع السابق،ص 36

2- استعمال توقيع أو وسيط أو محرر إلكتروني تالف أو مزور :

إن هذه الجريمة مرتبطة بالجريمة المذكورة أعلاه ، ففي حال ما إذا قام الشخص باستعمال الوسيط أو المحرر أو التوقيع الإلكتروني التالف فإن ذلك يمكن تشبيهه بحالة التزوير المفضوح إذ أنه عمليا لا يمكن استعمال أي من الأشكال المذكورة إذ لا يمكن استعمال شيء غير صالح .

في حال التعييب فإن المحرر والوسيط والتوقيع الإلكتروني لا يفقد كل قيمته ووظيفته بل جزءا منه ،وبالتالي فإن استعماله يمكن أن يؤدي إلى خداع بعض الناس، مثل ذلك المحرر الإلكتروني الذي لا يمكن تخزينه أو حفظه لعيب فني فيه وإن كان سليما وصحيحا إلا أنه لا يرتب أثار قانونية لأن المشرع يحظر ذلك [1] .

العقوبة المقرر للجريمتين لدى المشرع المصري هي الحبس والغرامة لا تقل عن 10.000جنيه أو بإحدى هاتين العقوبتين مع ترك السلطة التقديرية للقاضي في هذا الشأن، إلا أنه إذا ما وجدت عقوبة أشد سواء في قانون العقوبات أو قانون أخر فإنه تطبق هذه العقوبة .

ثانيا :جريمة فك الشفرة:

إن التشفير يعتبر وسيلة من الوسائل المقررة لحماية البيانات الواردة في التوقيع الإلكتروني بحيث لا يمكن للغير الإطلاع عليها، إلا أنه إذا ما تمكن شخص من فك هذه الشفرة فإنه يعتبر اعتداء وجب على المشرع أن يقرر له عقوبة جنائية.

وهو ما نص عليه المشرع المصري في الفصل العاشر من المشروع تحت عنوان «الجرائم والعقوبات» و المشرع التونسي في الفصل 48 :« يعاقب كل من استعمل بصفة

[1] المستشار عبد الفتاح بيومي حجازي،المرجع السابق ،ص 547

غير مشروعة عناصر تشفير شخصية متعلقة بإمضاء غيره بالسجن لمدة تتراوح بين 6 أشهر وعامين و بخطية تتراوح بين 1.000 و 10.000 دينار أو بإحدى هاتين العقوبتين».

الركن المادي لهذه الجريمة هو فض مفاتيح التشفير المتعلقة بالتوقيع الإلكتروني ،ومتى تحقق هذا الفعل من أحد الأشخاص حتى ولو لم يحقق من وراء هذا السلوك نتيجة معينة ،فإن الشخص يعتبر في نظر القانون جاني ويستحق العقاب ولا يهم إن كان هذا الفعل تم لمصلحته أو لمصلحة شخص أخر .

أما الركن المعنوي ،فإن القانون اشترط أن يتم هذا الفعل عمدا أي توافر عنصر العلم والإرادة .

بوجود الركن المادي والمعنوي فإن العقوبة المقررة لهذه الجريمة هي السجن من 6 أشهر إلى عامين و بخطية تتراوح بين 1.000 و 10.000 دينار أو بإحدى هاتين العقوبتين[1]، أما المشرع المصري فهي الحبس لمدة لا تقل عن السنة وغرامة لا تقل عن 3.000 جنيه.

نجد من خلال المقارنة بان المشرع التونسي كان أكثر صرامة من المشرع المصري حيث أن هذا الأخير لم تكن العقوبة تتجاوز السنة على أكثر تقدير بينما المشرع التونسي فقد جعلها عامين كحد أقصى ، وهو ما جعل بعض الفقهاء يرون أن العقوبات المقررة في القانون المصري ليست بالشدة التي لا بد وأن تقابل عمليات الغش التي قد تحدث في هذا المجال [2].

جرائم الشخص الاعتباري:

نلاحظ أن هذه العقوبات لا تنصب فقط على الشخص الطبيعي بل تشمل كذلك الشخص الاعتباري ،وهو ما أقرته مختلف التشريعات مثل المادة 33 من قانون إمارة دبي التي تنص:« إذا ارتكب أي شخص اعتباري مخالفة لأحكام هذا القانون أو اللوائح الصادرة

---

[1] بالنسبة للمشرع التونسي

[2] أمنير محمد الجنبيهي وأممدوح منير الجنبيهي ،المرجع السابق ،ص 125

بموجبه وثبت أن ذلك جاء نتيجة لتصرف أو إهمال أو موافقة أو تستر أي عضو مجلس إدارة أو مدير أو أي موظف آخر في ذلك الشخص الاعتباري أو أي شخص يبدو انه يتصرف بهذه الصفة، فإن ذلك الشخص والشخص الاعتباري يدانان بهذه المخالفة ويعاقبان تبعا لذلك.».

المادة 25 من القانون البحريني التي تنص :« مسئولية الشخص الاعتباري وموظفيه يسأل الشخص الاعتباري جنائيا ويعاقب بالغرامة التي لا تجاوز مائتي ألف دينار، إذا ارتكبت أي من الجرائم المنصوص عليها في هذا القانون باسمه أو لحسابه أو باستعمال إحدى وسائله ، وكان ذلك نتيجة تصرف أو إهمال جسيم أو موافقة أو تستر من أي عضو مجلس إدارة أو مدير أو أي مسئول آخر - في ذلك الشخص الاعتباري - أو ممن يتصرف بهذه الصفة . ويعد مرتكبا للجريمة كل من أسند إليه من هؤلاء الأشخاص الطبيعيين ارتكاب أي من الأفعال المذكورة، ويعاقب بالعقوبة المقررة لها طبقا لأحكام هذا القانون».

نلاحظ من خلال هاتين المادتين أنه لكي تقوم المسؤولية الجنائية للشخص الاعتباري سواء كان عام أو خاصا فإنه يجب أن تكون المخالفة أو الجريمة قد وقعت نتيجة لتصرف أو إهمال[1] أو موافقة أو تستر أي عضو مجلس إدارة أو مدير أو أي موظف آخر في ذلك الشخص الاعتباري أو أي شخص يبدو انه يتصرف بهذه الصفة، ولا يهم إن كان هذا الفعل المجرم قد تم لمصلحة هذا الشخص الاعتباري أو لمصلحة أي شخص أخر ،كما أنه لا يعفى هذا الشخص من المتابعة الجنائية إذا ما ثبت أن الجريمة قد تمت بالوسائل التي بحوزته .

تلحق العقوبة الجنائية في هذه الحالة الشخص الطبيعي الذي ارتكبها سواء كان عضو مجلس إدارة أو مدير أو أي موظف أخر في الشخص الاعتباري، ولا يهم في هذه الحالة نوع الجريمة المرتكبة بل يشترط في الفعل المعاقب عليه أن يشكل جناية ولم تحدد نوع العقوبة عند مشرع إمارة دبي إنما يجب أن تكون هذه العقوبة متفقة مع طبيعة الشخص المعنوي ،فلا

[1] القانون البحريني يشترط أن يكون الإهمال جسيما حتى تترتب المسؤولية الجنائية على عاتق الشخص الاعتباري

يمكن مثلا إقرار عقوبة الحبس أو السجن إنما يمكن أن تفرض الغرامة أو حتى حل الشخص المعنوي.

أخيرا فإنه يمكن للدعوى الجنائية أن تنقضي بالصلح وفق ما ينص عليه الفصل 53 من القانون التونسي [1] ، والمادة 35 من قانون إمارة دبي.

[1] يشترط المشرع التونسي لقيام الصلح دفع المبلغ المعين في الصلح مع حفظ الحقوق المدنية للأطراف المتضررة.

الخاتمة:

لقد اتضح لنا من خلال هذا البحث أنه لم تبقى هناك عوائق تذكر لإقرار المساواة بين الكتابة الإلكترونية والخطية وكذلك من إعمال التوقيع الإلكتروني وإعطائه نفس حجية التوقيع الخطي في مجال الإثبات، فالتطور السريع للتجارة الإلكترونية ألزم الدول ومزودي الخدمات على ضرورة أن يكون التوقيع الإلكتروني وسيلة أمنة وسريعة في إتمام العقود التي تتم عبر شبكة الانترنيت .

كما بينا في هذا البحث أن التوقيع الإلكتروني ما هو في حقيقة الأمر إلا امتداد للتوقيع الخطي ، فهو يهدف إلى التعبير عن رضا الموقع بما احتواه السند الإلكتروني ومنح هذه الوثيقة صفة الأصل، كما يسعى إلى الحفاظ على نزاهة وسلامة الوثيقة الإلكترونية من التعديل.

بل الأكثر من ذلك فإن مجال إعمال التوقيع الإلكتروني يشمل كل الأوراق التي يمكن أن توقع خطيا من ورقة رسمية أو عرفية، إلا في حالات معينة استثناها القانون وهذا نظرا لطبيعة المعاملة وخطورتها.

وقد برز مشكل الحفاظ على سلامة الوثيقة الإلكترونية بعد مرور مدة زمنية معينة، وهو ما حتم ظهور الأرشفة الإلكترونية توكل إما لمزود الخدمات أو لهيئة خاصة أخرى.

وكان تحديد هوية الموقع في التوقيع الإلكتروني عائقا كبيرا لإبرام الصفقات ، إلا أنه تم تجاوز هذا الإشكال بواسطة شهادة التصديق الإلكتروني التي تحدد هوية الموقع بشكل دقيق بحيث يجب أن تحتوي هذه الأخيرة على كل المعطيات المتعلقة بالموقع كالاسم واللقب و المهنة وحتى اسم الشهرة .

إضافة إلى ذلك يجب الاعتراف بشهادات التصديق الأجنبية باعتبار أن التوقيع الإلكتروني أصبحت أداة ذو طابع دولي لا تعترف بالحدود الوطنية، كما يجب إصدارها طرف مزود خدمات إما عن طريق التفويض الإرادي أو الترخيص.

ولزيادة الأمان القانوني فقد ألزم المشرع على الموقع والمرسل إليه أن يتخذوا خطوات معينة أثناء إعمال التوقيع الإلكتروني .

على هذا الأساس فإن على الجزائر أن تكون طرفا فعالا في التجارة الإلكترونية ولن يتسنى لنا ذلك إلا إذا كانت هناك قوانين خاصة متعلقة بالتوقيع الإلكتروني والتي يجب أن تبرز على الخصوص ما يلي :

- إعطاء تعريف لأهم المصطلحات المستعملة في هذا القانون مثل: التوقيع الإلكتروني، الوسيط الإلكتروني، المحرر الإلكتروني إلخ...

- شروط ومجال إعمال التوقيع الإلكتروني.

- المساواة بين الكتابة الخطية والإلكترونية وشروط صحتها

- توضيح المركز القانوني لمزودي الخدمات ،إذ يجب أن تبين الهيئة المانحة للترخيص والشروط الخاصة لمنح هذا الترخيص ، والتزامات مزود الخدمات ،وأخيرا تكريس المسؤولية المدنية لمزود الخدمات إن أخل بأحد التزاماته ،حتى يتسنى للأطراف المتضررة أخذ التعويض المناسب .

- وضع فصل خاص بشهادة التصديق الإلكتروني بحيث تبين فيها محتويات هذه الشهادة وحالات تعليقها وإلغائها، وضرورة الاعتراف بشهادات التصديق الأجنبية، وهذا نظرا لكون التعاقد عبر الانترنيت لا يعترف بالحدود .

- وضع قانون خاص بالجرائم المعلوماتية، وهو ما تسعى إليه وزارة العدل حاليا حيث تقوم بوضع مشروع قانون في هذا المجال.

- التأكيد على الحفاظ على المعلومات الشخصية للمشتركين لدى مقدمي خدمات التصديق.

- يمكن أن ينص القانون على إمكانية تولي مزود الخدمات القيام بمهام أخرى مثل الأرشفة الإلكترونية، ووضع تاريخ موحد ومنضبط للمحررات الإلكترونية، خصوصا عند تعدد أطراف الصفقة الإلكترونية وتواجدهم في أماكن مختلفة تتباين توقيتاتها[1].

- كما يمكن للمشرع الجزائري إما وضع قانونين أحدهما متعلق بالتجارة الإلكترونية والأخر بالتوقيع الإلكتروني، أو وضع قانون واحد يمزج فيه الاثنين معا.

لكن قبل ذلك يجب توفير عوامل النجاح لهذا القانون ومن أهمها:

-توسيع العمل بالإعلام الآلي ونشره عبر المجتمع، وهو ما تسعى إليه حاليا الدولة الجزائرية من خلال برنامج «أسرتك».

-توفير خدمة الانترنيت ذات البث العالي (ADSL) بأقل الأثمان، لأنها هي الوحيدة القادرة على منح السرعة اللازمة لإتمام وإبرام الصفقات على شبكة الانترنيت.

-توسيع شبكة الأنتريت لتشمل كل القطاعات الاقتصادية.

-تطوير المنظومة البنكية بشكل يسمح بإيجاد ما يعرف بالدفع الإلكتروني .

-تكوين القضاة على التعامل مع وسائل الإثبات الحديثة، وعدم التحفظ عليها أو النظر إليها نظرة الشك والريبة.

-يجب على القاضي حماية الطرف الضعيف في إطار العقود الإلكترونية، بحيث يلغي كل شرط تعسفي وترك السلطة التقديرية للقاضي في تقدير هذه الشروط

-إمكانية الاستعانة بالخبراء لتقدير مدى توافر الكتابة والتوقيع الإلكتروني للشروط المنصوص عليها قانونا .

-عدم التهاون في مجابهة الجريمة المعلوماتية وإقرار أقصى العقوبات لمرتكبيها، وهذا بالاستعانة بما ينص عليه القانون الحالي لغاية إصدار قانون خاص بالجريمة المعلوماتية.

---

[1] د-سعيد سيد قنديل،المرجع السابق ،ص 123

-الإسراع في إنشاء حكومة إلكترونية جزائرية، لتخفيف العبء على الإدارات وتسريع المعاملات الإدارية وتفادي البيروقراطية وإضاعة الوقت وراء السعي لاستصدار مختلف الوثائق .

-توفير شبكة معلوماتية تربط بين مختلف مزودي الخدمات.

تم بعون الله وحمده

ملحق رقم 1

J.O n° 62 du 14 mars 2000 page 3968

Lois

LOI no 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique (1)

NOR: JUSX9900020L

L'Assemblée nationale et le Sénat ont adopté,

Le Président de la République promulgue la loi dont la teneur suit :

Article 1er

I. - L'article 1316 du code civil devient l'article 1315-1.

II. - Les paragraphes 1er, 2, 3, 4 et 5 de la section 1 du chapitre VI du titre III du livre III du code civil deviennent respectivement les paragraphes 2, 3, 4, 5 et 6.

III. - Il est inséré, avant le paragraphe 2 de la section 1 du chapitre VI du titre III du livre III du code civil, un paragraphe 1er intitulé : « Dispositions générales », comprenant les articles 1316 à 1316-2 ainsi rédigés :

« Art. 1316. - La preuve littérale, ou preuve par écrit, résulte d'une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quels que soient leur support et leurs modalités de transmission.

« Art. 1316-1. - L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité.

« Art. 1316-2. - Lorsque la loi n'a pas fixé d'autres principes, et à défaut de convention valable entre les parties, le juge règle les conflits de preuve littérale en déterminant par tous moyens le titre le plus vraisemblable, quel qu'en soit le support. »

Article 2

L'article 1317 du code civil est complété par un alinéa ainsi rédigé :

« Il peut être dressé sur support électronique s'il est établi et conservé dans des conditions fixées par décret en Conseil d'Etat. »

Article 3

Après l'article 1316-2 du code civil, il est inséré un article 1316-3 ainsi rédigé :

« Art. 1316-3. - L'écrit sur support électronique a la même force probante que l'écrit sur support papier. »

Article 4

Après l'article 1316-3 du code civil, il est inséré un article 1316-4 ainsi rédigé :

« Art. 1316-4. - La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte.

« Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'Etat. »

Article 5

A l'article 1326 du code civil, les mots : « de sa main » sont remplacés par les mots : « par lui-même».

Article 6

La présente loi est applicable en Nouvelle-Calédonie, en Polynésie française, à Wallis-et-Futuna et dans la collectivité territoriale de Mayotte.

La présente loi sera exécutée comme loi de l'Etat.

Fait à Paris, le 13 mars 2000.

Jacques Chirac

Par le Président de la République :

Le Premier ministre,

Lionel Jospin

Le garde des sceaux, ministre de la justice,

Elisabeth Guigou

Le ministre de l'intérieur,

Jean-Pierre Chevènement

Le ministre de l'économie,

des finances et de l'industrie,

Christian Sautter

Le secrétaire d'Etat à l'outre-mer,

Jean-Jack Queyranne

Le secrétaire d'Etat à l'industrie,

Christian Pierret

(1) Loi no 2000-230.

- Directive communautaire :

Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques.

- Travaux préparatoires :

Sénat :

Projet de loi no 488 (1998-1999) ;

Rapport de M. Charles Jolibois, au nom de la commission des lois, no 203 (1999-2000) ;

Discussion et adoption le 8 février 2000.

Assemblée nationale :

Projet de loi, adopté par le Sénat, no 2158 ;

Rapport de M. Christian Paul, au nom de la commission des lois, no 2197 ;

Discussion et adoption le 29 février 2000.

J.O n° 77 du 31 mars 2001 page 5070

Textes généraux

Ministère de la justice

Décret no 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique

NOR: JUSC0120141D

Le Premier ministre,

Sur le rapport de la garde des sceaux, ministre de la justice,

Vu la directive 1999/93/CE du Parlement européen et du Conseil en date du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques ;

Vu le code civil, notamment ses articles 1316 à 1316-4 ;

Vu la loi no 90-1170 du 29 décembre 1990 modifiée sur la réglementation des télécommunications, notamment son article 28 ;

Le Conseil d'Etat (section de l'intérieur) entendu,

Décrète :

Art. 1er. - Au sens du présent décret, on entend par :

1. « Signature électronique » : une donnée qui résulte de l'usage d'un procédé répondant aux conditions définies à la première phrase du second alinéa de l'article 1316-4 du code civil ;

2. « Signature électronique sécurisée » : une signature électronique qui satisfait, en outre, aux exigences suivantes :

- être propre au signataire ;

- être créée par des moyens que le signataire puisse garder sous son contrôle exclusif ;

- garantir avec l'acte auquel elle s'attache un lien tel que toute modification ultérieure de l'acte soit détectable ;

3. « Signataire » : toute personne physique, agissant pour son propre compte ou pour celui de la personne physique ou morale qu'elle représente, qui met en oeuvre un dispositif de création de signature électronique ;

4. « Données de création de signature électronique » : les éléments propres au signataire, tels que des clés cryptographiques privées, utilisés par lui pour créer une signature électronique ;

5. « Dispositif de création de signature électronique » : un matériel ou un logiciel destiné à mettre en application les données de création de signature électronique ;

6. « Dispositif sécurisé de création de signature électronique » : un dispositif de création de signature électronique qui satisfait aux exigences définies au I de l'article 3 ;

7. « Données de vérification de signature électronique » : les éléments, tels que des clés cryptographiques publiques, utilisés pour vérifier la signature électronique ;

8. « Dispositif de vérification de signature électronique » : un matériel ou un logiciel destiné à mettre en application les données de vérification de signature électronique ;

9. « Certificat électronique » : un document sous forme électronique attestant du lien entre les données de vérification de signature électronique et un signataire ;

10. « Certificat électronique qualifié » : un certificat électronique répondant aux exigences définies à l'article 6 ;

11. « Prestataire de services de certification électronique » : toute personne qui délivre des certificats électroniques ou fournit d'autres services en matière de signature électronique ;

12. « Qualification des prestataires de services de certification électronique » : l'acte par lequel un tiers, dit organisme de qualification, atteste qu'un prestataire de services de certification électronique fournit des prestations conformes à des exigences particulières de qualité.

Art. 2. - La fiabilité d'un procédé de signature électronique est présumée jusqu'à preuve contraire lorsque ce procédé met en oeuvre une signature électronique sécurisée, établie grâce à un dispositif sécurisé de création de signature électronique et que la vérification de cette signature repose sur l'utilisation d'un certificat électronique qualifié.

Chapitre Ier

Des dispositifs sécurisés de création

de signature électronique

Art. 3. - Un dispositif de création de signature électronique ne peut être regardé comme sécurisé que s'il satisfait aux exigences définies au I et que s'il est certifié conforme à ces exigences dans les conditions prévues au II.

I. - Un dispositif sécurisé de création de signature électronique doit :

1. Garantir par des moyens techniques et des procédures appropriés que les données de création de signature électronique :

a) Ne peuvent être établies plus d'une fois et que leur confidentialité est assurée ;

b) Ne peuvent être trouvées par déduction et que la signature électronique est protégée contre toute falsification ;

c) Peuvent être protégées de manière satisfaisante par le signataire contre toute utilisation par des tiers.

2. N'entraîner aucune altération du contenu de l'acte à signer et ne pas faire obstacle à ce que le signataire en ait une connaissance exacte avant de le signer.

II. - Un dispositif sécurisé de création de signature électronique doit être certifié conforme aux exigences définies au I :

1o Soit par les services du Premier ministre chargés de la sécurité des systèmes d'information, après une évaluation réalisée, selon des règles définies par arrêté du Premier ministre, par des organismes agréés par ces services. La délivrance par ces services du certificat de conformité est rendue publique ;

2o Soit par un organisme désigné à cet effet par un Etat membre de la Communauté européenne.

Art. 4. - Le contrôle de la mise en oeuvre des procédures d'évaluation et de certification prévues au 1o du II de l'article 3 est assuré par un comité directeur de la certification, institué auprès du Premier ministre.

Un arrêté du Premier ministre précise les missions attribuées à ce comité, fixe sa composition, définit les procédures de certification et d'évaluation des dispositifs de création de signature électronique mentionnées à l'alinéa précédent ainsi que les procédures d'agrément des organismes d'évaluation. Il détermine, en outre, les obligations incombant à ces organismes et fixe les conditions dans lesquelles sont présentées et instruites les demandes de certification.

Chapitre II

Des dispositifs de vérification de signature électronique

Art. 5. - Un dispositif de vérification de signature électronique peut faire, après évaluation, l'objet d'une certification, selon les procédures définies par l'arrêté mentionné à l'article 4, s'il répond aux exigences suivantes :

a) Les données de vérification de signature électronique utilisées doivent être celles qui ont été portées à la connaissance de la personne qui met en oeuvre le dispositif et qui est dénommée « vérificateur » ;

b) Les conditions de vérification de la signature électronique doivent permettre de garantir l'exactitude de celle-ci et le résultat de cette vérification doit sans subir d'altération être porté à la connaissance du vérificateur ;

c) Le vérificateur doit pouvoir, si nécessaire, déterminer avec certitude le contenu des données signées ;

d) Les conditions et la durée de validité du certificat électronique utilisé lors de la vérification de la signature électronique doivent être vérifiées et le résultat de cette vérification doit sans subir d'altération être porté à la connaissance du vérificateur ;

e) L'identité du signataire doit sans subir d'altération être portée à la connaissance du vérificateur ;

f) Lorsqu'il est fait usage d'un pseudonyme, son utilisation doit être clairement portée à la connaissance du vérificateur ;

g) Toute modification ayant une incidence sur les conditions de vérification de la signature électronique doit pouvoir être détectée.

Chapitre III

Des certificats électroniques qualifiés

et des prestataires de services de certification électronique

Art. 6. - Un certificat électronique ne peut être regardé comme qualifié que s'il comporte les éléments énumérés au I et que s'il est délivré par un prestataire de services de certification électronique satisfaisant aux exigences fixées au II.

I. - Un certificat électronique qualifié doit comporter :

a) Une mention indiquant que ce certificat est délivré à titre de certificat électronique qualifié ;

b) L'identité du prestataire de services de certification électronique ainsi que l'Etat dans lequel il est établi ;

c) Le nom du signataire ou un pseudonyme, celui-ci devant alors être identifié comme tel ;

d) Le cas échéant, l'indication de la qualité du signataire en fonction de l'usage auquel le certificat électronique est destiné ;

e) Les données de vérification de signature électronique qui correspondent aux données de création de signature électronique ;

f) L'indication du début et de la fin de la période de validité du certificat électronique ;

g) Le code d'identité du certificat électronique ;

h) La signature électronique sécurisée du prestataire de services de certification électronique qui délivre le certificat électronique ;

i) Le cas échéant, les conditions d'utilisation du certificat électronique, notamment le montant maximum des transactions pour lesquelles ce certificat peut être utilisé.

II. - Un prestataire de services de certification électronique doit satisfaire aux exigences suivantes :

a) Faire preuve de la fiabilité des services de certification électronique qu'il fournit ;

b) Assurer le fonctionnement, au profit des personnes auxquelles le certificat électronique est délivré, d'un service d'annuaire recensant les certificats électroniques des personnes qui en font la demande ;

c) Assurer le fonctionnement d'un service permettant à la personne à qui le certificat électronique a été délivré de révoquer sans délai et avec certitude ce certificat ;

d) Veiller à ce que la date et l'heure de délivrance et de révocation d'un certificat électronique puissent être déterminées avec précision ;

e) Employer du personnel ayant les connaissances, l'expérience et les qualifications nécessaires à la fourniture de services de certification électronique ;

f) Appliquer des procédures de sécurité appropriées ;

g) Utiliser des systèmes et des produits garantissant la sécurité technique et cryptographique des fonctions qu'ils assurent ;

h) Prendre toute disposition propre à prévenir la falsification des certificats électroniques ;

i) Dans le cas où il fournit au signataire des données de création de signature électronique, garantir la confidentialité de ces données lors de leur création et s'abstenir de conserver ou de reproduire ces données ;

j) Veiller, dans le cas où sont fournies à la fois des données de création et des données de vérification de la signature électronique, à ce que les données de création correspondent aux données de vérification ;

k) Conserver, éventuellement sous forme électronique, toutes les informations relatives au certificat électronique qui pourraient s'avérer nécessaires pour faire la preuve en justice de la certification électronique.

l) Utiliser des systèmes de conservation des certificats électroniques garantissant que :

- l'introduction et la modification des données sont réservées aux seules personnes autorisées à cet effet par le prestataire ;

- l'accès du public à un certificat électronique ne peut avoir lieu sans le consentement préalable du titulaire du certificat ;

- toute modification de nature à compromettre la sécurité du système peut être détectée ;

m) Vérifier, d'une part, l'identité de la personne à laquelle un certificat électronique est délivré, en exigeant d'elle la présentation d'un document officiel d'identité, d'autre part, la qualité dont cette personne se prévaut et conserver les caractéristiques et références des documents présentés pour justifier de cette identité et de cette qualité ;

n) S'assurer au moment de la délivrance du certificat électronique :

- que les informations qu'il contient sont exactes ;

- que le signataire qui y est identifié détient les données de création de signature électronique correspondant aux données de vérification de signature électronique contenues dans le certificat ;

o) Avant la conclusion d'un contrat de prestation de services de certification électronique, informer par écrit la personne demandant la délivrance d'un certificat électronique :

- des modalités et des conditions d'utilisation du certificat ;

- du fait qu'il s'est soumis ou non au processus de qualification volontaire des prestataires de services de certification électronique mentionnée à l'article 7 ;

- des modalités de contestation et de règlement des litiges ;

p) Fournir aux personnes qui se fondent sur un certificat électronique les éléments de l'information prévue au o qui leur sont utiles.

Art. 7. - Les prestataires de services de certification électronique qui satisfont aux exigences fixées à l'article 6 peuvent demander à être reconnus comme qualifiés.

Cette qualification, qui vaut présomption de conformité auxdites exigences, est délivrée par les organismes ayant reçu à cet effet une accréditation délivrée par une instance désignée par arrêté du ministre chargé de l'industrie. Elle est précédée d'une évaluation réalisée par ces mêmes organismes selon des règles définies par arrêté du Premier ministre.

L'arrêté du ministre chargé de l'industrie prévu à l'alinéa précédent détermine la procédure d'accréditation des organismes et la procédure d'évaluation et de qualification des prestataires de services de certification électronique.

Art. 8. - Un certificat électronique délivré par un prestataire de services de certification électronique établi dans un Etat n'appartenant pas à la Communauté européenne a la même valeur juridique que celui délivré par un prestataire établi dans la Communauté, dès lors :

a) Que le prestataire satisfait aux exigences fixées au II de l'article 6 et a été accrédité, au sens de la directive du 13 décembre 1999 susvisée, dans un Etat membre ;

b) Ou que le certificat électronique délivré par le prestataire a été garanti par un prestataire établi dans la Communauté et satisfaisant aux exigences fixées au II de l'article 6 ;

c) Ou qu'un accord auquel la Communauté est partie l'a prévu.

Art. 9. - I. - Au titre de la déclaration de fourniture de prestations de cryptologie effectuée conformément aux dispositions de l'article 28 de la loi du 29 décembre 1990 susvisée, le prestataire de services de certification électronique doit, quand il entend délivrer des certificats électroniques qualifiés, l'indiquer.

II. - Le contrôle des prestataires visés au I est effectué par des organismes publics désignés par arrêté du Premier ministre et agissant sous l'autorité des services du Premier ministre chargés de la sécurité des systèmes d'information.

Ce contrôle porte sur le respect des exigences définies à l'article 6. Il peut être effectué d'office ou à l'occasion de toute réclamation mettant en cause l'activité d'un prestataire de services de certification électronique.

Lorsque le contrôle révèle qu'un prestataire n'a pas satisfait à ces exigences, les services du Premier ministre chargés de la sécurité des systèmes d'information assurent la publicité des résultats de ce contrôle et, dans le cas où le prestataire a été reconnu comme qualifié dans les conditions fixées à l'article 7, en informent l'organisme de qualification.

Les mesures prévues à l'alinéa précédent doivent faire l'objet, préalablement à leur adoption, d'une procédure contradictoire permettant au prestataire de présenter ses observations.

Chapitre IV

Dispositions diverses

Art. 10. - Le présent décret est applicable en Nouvelle-Calédonie, en Polynésie française, aux îles Wallis et Futuna et à Mayotte.

Art. 11. - Le ministre de l'économie, des finances et de l'industrie, la garde des sceaux, ministre de la justice, le ministre de l'intérieur, le secrétaire d'Etat à l'outre-mer et le secrétaire d'Etat à l'industrie sont chargés, chacun en ce qui le concerne, de l'exécution du présent décret, qui sera publié au Journal officiel de la République française.

Fait à Paris, le 30 mars 2001.

Lionel Jospin

Par le Premier ministre :

La garde des sceaux, ministre de la justice,

Marylise Lebranchu

Le ministre de l'économie,

des finances et de l'industrie,

Laurent Fabius

Le ministre de l'intérieur,

Daniel Vaillant

Le secrétaire d'Etat à l'outre-mer,

Christian Paul

Le secrétaire d'Etat à l'industrie,

Christian Pierret

J.O n° 92 du 19 avril 2002 page 6944
texte n° 1

Décrets, arrêtés, circulaires
Textes généraux
Premier ministre

Décret n° 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information

NOR: PRMX0100183D

Le Président de la République,

Sur le rapport du Premier ministre, du ministre de l'économie, des finances et de l'industrie et du ministre délégué à l'industrie, aux petites et moyennes entreprises, au commerce, à l'artisanat et à la consommation,

Vu la directive 98/34/CE du 22 juin 1998, modifiée par la directive 98/48/CE du 20 juillet 1998, prévoyant une procédure d'information dans le domaine des normes et réglementations techniques et des règles relatives aux services de la société de l'information ;

Vu le code de la consommation, notamment son article R. 115-6 ;

Vu le décret n° 97-34 du 15 janvier 1997, modifié par le décret n° 97-463 du 9 mai 1997 et par le décret n° 97-1205 du 19 décembre 1997, relatif à la déconcentration des décisions administratives individuelles ;

Vu le décret n° 97-1184 du 19 décembre 1997, modifié par le décret n° 2001-143 du 15 février 2001, pris pour l'application au Premier ministre du 1° de l'article 2 du décret n° 97-34 du 15 janvier 1997 relatif à la déconcentration des décisions administratives individuelles ;

Vu le décret n° 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique ;

Le Conseil d'Etat (section de l'intérieur) entendu ;

Le conseil des ministres entendu,

Décrète :

Article 1

La sécurité offerte par des produits ou des systèmes des technologies de l'information, au regard notamment de leur aptitude à assurer la disponibilité, l'intégrité ou la confidentialité de l'information traitée face aux menaces dues en particulier à la malveillance peut être certifiée dans les conditions prévues au présent décret.

Les administrations de l'Etat recourent, dans la mesure du possible et en fonction de leurs besoins de sécurité, à des produits ou des systèmes des technologies de l'information certifiés suivant la procédure prévue au présent décret.

Chapitre Ier

Procédure d'évaluation et de certification

Section 1

Evaluation

Article 2

Une évaluation en vue de la certification prévue à l'article 1er est effectuée à la demande d'un commanditaire qui adresse à la direction centrale de la sécurité des systèmes d'information un dossier d'évaluation. Le dossier comporte notamment la description du système de sécurité à évaluer, les dispositions prévues pour lui conférer sa pleine efficacité ainsi que le programme de travail prévisionnel permettant une évaluation.

Dès réception de ce dossier, la direction centrale de la sécurité des systèmes d'information si elle estime que les objectifs de sécurité ne sont pas définis de manière pertinente au regard des normes, prescriptions techniques ou règles de bonne pratique applicables au moment où commence l'évaluation, notifie au commanditaire qu'elle ne pourra pas en l'état du dossier procéder à la certification envisagée.

Article 3

Le commanditaire de l'évaluation choisit un ou plusieurs centres d'évaluation, agréés dans les conditions prévues au chapitre II, pour procéder à celle-ci. Avant le début des travaux, il détermine avec chacun de ces centres :

a) Le produit ou le système à évaluer ainsi que les objectifs de sécurité ;

b) Les conditions de protection de la confidentialité des informations qui seront traitées dans le cadre de l'évaluation ;

c) Le coût et les modalités de paiement de l'évaluation ;

d) Le programme de travail et les délais prévus pour l'évaluation.

Le commanditaire est tenu d'assurer la mise à la disposition des centres d'évaluation qu'il a choisis et de la direction centrale de la sécurité des systèmes d'information, si elle en fait la demande, de tous les éléments nécessaires au bon accomplissement de leurs travaux, le cas échéant après accord des fabricants concernés.

Article 4

Le commanditaire peut décider à tout moment de mettre fin à une évaluation.

Il est décidé entre les parties du dédommagement éventuellement dû au centre d'évaluation.

Article 5

La direction centrale de la sécurité des systèmes d'information veille à la bonne exécution des travaux

d'évaluation. Elle peut à tout moment demander à assister à ces travaux ou à obtenir des informations sur leur déroulement.

Article 6

Au terme des travaux d'évaluation, chaque centre remet un rapport d'évaluation au commanditaire et à la direction centrale de la sécurité des systèmes d'information. Ce rapport est un document confidentiel dont les informations sont couvertes par le secret industriel et commercial.

Section 2

Certification

Article 7

Le commanditaire et la direction centrale de la sécurité des systèmes d'information valident les rapports d'évaluation en liaison avec le centre d'évaluation intervenant. Lorsque l'ensemble des rapports prévus a été validé, la direction centrale de la sécurité des systèmes d'information élabore un rapport de certification dans un délai d'un mois. Ce rapport, qui précise les caractéristiques des objectifs de sécurité proposés, conclut soit à la délivrance d'un certificat, soit au refus de la certification.

Le rapport de certification peut comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Il est, au choix du commanditaire, communiqué ou non à des tiers ou rendu public.

Article 8

Le certificat est délivré par le Premier ministre.

Il atteste que l'exemplaire du produit ou du système soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Il atteste également que l'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises.

Article 9

La direction centrale de la sécurité des systèmes d'information peut passer, après avis du comité directeur de la certification, des accords de reconnaissance mutuelle avec des organismes étrangers homologues, ayant leur siège en dehors des Etats membres de la Communauté européenne.

Ces accords peuvent prévoir que les certificats délivrés par les organismes étrangers cosignataires, dans le cadre de procédures comparables à celle prévue au présent chapitre, sont reconnus comme ayant la même valeur que les certificats délivrés en application du présent décret. La reconnaissance mutuelle des certificats peut être limitée à un niveau d'assurance déterminé.

Sans préjudice des règles régissant la certification des dispositifs sécurisés de création de signature électronique mentionnées au 2° du II de l'article 3 du décret du 30 mars 2001 susvisé, le Premier ministre reconnaît aux certificats délivrés par les organismes ayant leur siège dans un Etat membre de la Communauté européenne, dans le cadre de procédures comparables présentant des garanties équivalentes, la même valeur qu'aux certificats délivrés en application du présent décret.

Chapitre II

Agrément des centres d'évaluation

Article 10

Les centres d'évaluation chargés de procéder à l'évaluation prévue au présent décret sont agréés dans les conditions fixées par le présent chapitre.

Article 11

I. - La demande d'agrément est formulée auprès de la direction centrale de la sécurité des systèmes d'information. Cette demande précise le domaine dans lequel l'organisme demandeur entend exercer son activité.

II. - L'organisme demandeur doit faire la preuve :

a) De sa conformité aux critères de qualité selon les règles et normes d'accréditation en vigueur ;

b) De son aptitude à appliquer les critères d'évaluation en vigueur et la méthodologie correspondante ainsi qu'à assurer la confidentialité requise par l'évaluation ;

c) De sa compétence technique à conduire une évaluation.

La conformité mentionnée au a et l'aptitude mentionnée au b sont attestées par une accréditation délivrée par une instance reconnue dans les conditions prévues à l'article R. 115-6 du code de la consommation ou délivrée par une instance étrangère équivalente.

La compétence technique mentionnée au c est appréciée par la direction centrale de la sécurité des systèmes d'information, notamment à partir des moyens, des ressources et de l'expérience du centre d'évaluation.

Article 12

L'agrément est délivré par le Premier ministre, après avis du comité directeur de la certification.

Il peut énoncer les obligations particulières auxquelles est soumis le centre d'évaluation.

Il est valable pour une durée de deux ans renouvelable.

Article 13

Lorsqu'un centre d'évaluation situé hors du territoire national ou d'un autre Etat membre de la Communauté européenne a déjà fait l'objet d'un agrément par les autorités de son pays d'installation dans le cadre d'une procédure homologue, le Premier ministre peut, après avis du comité directeur de la certification, le déclarer agréé au titre du présent décret. Cet agrément, qui est accordé pour une durée de deux ans renouvelable, peut être limité à un niveau d'assurance déterminé.

Lorsqu'un centre d'évaluation situé dans un Etat membre de la Communauté européenne a déjà fait l'objet d'un agrément par les autorités de cet Etat dans le cadre d'une procédure équivalente, le

Premier ministre, après avis du comité directeur de la certification, le déclare agréé au titre du présent décret.

Article 14

La direction centrale de la sécurité des systèmes d'information peut s'assurer à tout moment que les centres d'évaluation continuent à satisfaire aux critères au vu desquels ils ont été agréés.

Lorsqu'un centre ne satisfait plus aux exigences mentionnées à l'article 11 ou qu'il manque aux obligations fixées par la décision d'agrément, l'agrément peut être retiré par le Premier ministre, après avis du comité directeur de la certification. Le retrait ne peut être prononcé qu'après que le représentant du centre d'évaluation a été mis à même de faire valoir ses observations devant le comité directeur de la certification.

Chapitre III

Comité directeur de la certification

en sécurité des technologies de l'information

Article 15

Le comité directeur de la certification en sécurité des technologies de l'information a notamment pour mission :

a) De formuler des avis ou des propositions sur la politique de certification, sur les règles et normes utilisées pour les procédures d'évaluation et de certification et sur les guides techniques mis à la disposition du public ;

b) D'émettre un avis sur la délivrance et le retrait des agréments aux centres d'évaluation ;

c) D'examiner, à des fins de conciliation, tout litige relatif aux procédures d'évaluation organisées par le présent décret qui lui est soumis par les parties ;

d) D'émettre un avis sur les accords de reconnaissance mutuelle conclus avec des organismes étrangers en application de l'article 9.

La mission prévue au c ci-dessus peut être déléguée par le comité à l'un de ses membres, elle comporte obligatoirement l'audition des parties.

Article 16

Le comité directeur de la certification en sécurité des technologies de l'information est présidé par le secrétaire général de la défense nationale ou son représentant. Outre son président, il comprend :

a) Un représentant du ministre de la justice ;

b) Un représentant du ministre de l'intérieur ;

c) Un représentant du ministre des affaires étrangères ;

d) Un représentant du ministre de la défense ;

e) Un représentant du ministre chargé de l'industrie ;

f) Un représentant du ministre chargé de l'économie ;

g) Un représentant du ministre chargé de l'emploi ;

h) Un représentant du ministre chargé de la santé ;

i) Un représentant du ministre chargé de l'éducation nationale ;

j) Un représentant du ministre chargé de la communication ;

k) Un représentant du ministre chargé de la réforme de l'Etat ;

l) Un représentant du ministre chargé des transports ;

m) Un représentant du ministre chargé de la recherche.

Lorsque le comité directeur examine des questions concernant les dispositifs de création et de vérification de signature électronique, tels que définis à l'article 1er du décret du 30 mars 2001 susvisé, il comprend en outre douze personnalités qualifiées nommées pour trois ans par arrêté du Premier ministre.

Le secrétariat du comité directeur est assuré par la direction centrale de la sécurité des systèmes d'information.

Article 17

Le comité directeur se réunit sur convocation de son président qui en fixe l'ordre du jour.

Le président peut inviter tout expert ou personne qualifiée dont la participation aux débats lui paraît nécessaire.

Le comité rend compte de ses travaux au Premier ministre.

Article 18

La direction centrale de la sécurité des systèmes d'information fait annuellement rapport au comité directeur de la certification de l'activité qu'elle exerce dans le cadre de la mise en oeuvre du présent décret.

Chapitre IV

Dispositions diverses et transitoires

Article 19

Dans la partie « Sécurité et défense nationale » du paragraphe 2 de l'annexe au décret n° 97-1184 du 19 décembre 1997 susvisé, il est ajouté, à la suite du tableau relatif au décret n° 2001-143 du 15 février 2001, les mots et le tableau suivants :

« Décret n° 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.

Article 20

Le décret du 30 mars 2001 susvisé est ainsi modifié :

I. - Le 1° du II de l'article 3 est remplacé par les dispositions suivantes :

« 1° Soit par le Premier ministre, dans les conditions prévues par le décret n° 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information. La délivrance du certificat de conformité est rendue publique. »

II. - L'article 4 est remplacé par les dispositions suivantes :

« Art. 4. - La mise en oeuvre des procédures d'évaluation et de certification prévues au 1° du II de l'article 3 est assurée dans les conditions prévues par le décret n° 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information. »

III. - Au premier alinéa de l'article 5, les mots : « l'arrêté » sont remplacés par les mots : « le décret ».

IV. - Au deuxième alinéa de l'article 7, les mots : « selon des règles définies par arrêté du Premier ministre » sont supprimés.

V. - Au premier alinéa du II de l'article 9, les mots : « par des organismes publics désignés par arrêté du Premier ministre et agissant sous l'autorité des services du Premier ministre chargés de la sécurité des systèmes d'information » sont remplacés par les mots : « par la direction centrale de la sécurité des systèmes d'information ».

Article 21

Les certificats et les agréments des centres d'évaluation délivrés avant la date d'entrée en vigueur du présent décret, en application des dispositions de l'avis du Premier ministre relatif à la délivrance de certificats pour la sécurité offerte par les produits informatiques vis-à-vis de la malveillance, publié au Journal officiel de la République française du 1er septembre 1995, sont reconnus comme délivrés au titre du présent décret.

Article 22

Le présent décret est applicable :

a) En Nouvelle-Calédonie et en Polynésie française, en tant qu'il concerne la signature électronique ;

b) Dans les îles Wallis-et-Futuna et à Mayotte.

Article 23

Les dispositions du présent décret pourront être ultérieurement modifiées par décret, à l'exception :

a) Du premier alinéa des articles 8 et 12, du deuxième alinéa de l'article 14 et de l'article 19 dont la modification s'effectuera, le cas échéant, dans les conditions prévues à l'article 2 du décret du 15 janvier 1997 susvisé ;

b) De l'article 20.

Article 24

Le présent décret sera publié au Journal officiel de la République française.

Fait à Paris, le 18 avril 2002.

Jacques Chirac

Par le Président de la République :

Le Premier ministre,

Lionel Jospin

Le ministre de l'économie,

des finances et de l'industrie,

Laurent Fabius

La garde des sceaux, ministre de la justice,

Marylise Lebranchu

Le ministre de l'intérieur,

Daniel Vaillant

Le ministre délégué à l'industrie,

aux petites et moyennes entreprises,

au commerce, à l'artisanat

et à la consommation,

Christian Pierret

Le secrétaire d'Etat à l'outre-mer,

Christian Paul

ملحق رقم 2

قانون عدد 83 لسنة 2000 مؤرخ في 9 اوت 2000 يتعلق بالمبادلات والتجارة الالكترونية (1)

باسم الشعب بعد موافقة ، مجلس النواب يصدر رئيس الجمهورية التونسي القانون الاتي نصه :

الباب الأول

أحكام عامة

الفصل 1:

يضبط هذا القانون القواعد العامة المنظمة للمبادلات والتجارة الالكترونية.

وتخضع المبادلات والتجارة الالكترنية في ما لا يتعارض وأحكام هذا القانون الى التشريع والتراتيب الجاري بها العمل .

يجري على العقود الالكترونية نظام العقود الكتابية من حيث التعبير عن الارادة ومفعولها القانوني و صحتها و قابليتها للتنفيذ في ما لا يتعارض واحكام هذا القانون .

الفصل 2

يقصد في مفهوم هذا القانون ب:

-المبادلات الالكترونية : المبادلات التي تتم باستعمال الوثائق الالكترونية

-التجارة الالكترنية : العمليات التجارية التي تتم عبر المبادلات الالكترونية .

-شهادة المصادقة الالكترونية : الوثيقة الالكترونية المؤمنة بواسطة الامضاء الالكتروني للشخص الذي اصدرها والذي يشهد من خلالها اثر المعاينة ، على صحة البيانات التي تتضمنها .

-مزود خدمات المصادقة الالكترونية : كل شخص طبيعي او معنوي يحدث ويسلم ويتصرف في شهادات المصادقة ويسدي خدمات اخرى ذات علاقة بالامضاء الالكتروني

-التشفير : اما استعمال رموز او اشارات غير متداولة تصبح بمقتضاها المعلومات المرغوب تمريرها او ارسالها غير قابلة للفهم من قبل الغير او استعمال رموز او اشارات لا يمكن الوصول الى المعلومة بدون

-منظومة احداث الامضاء : مجموعة وحيدة من عناصر التشفير الشخصية او مجموعة من المعدات المهياة خصيصا لاحداث امضاء الكتروني.

-منظومة التدقيق في الامضاء : مجموعة من عناصر التشفير العمومية او مجموعة من المعدات التي

تمكن من التدقيق في الامضاء الالكتروني .

-وسيلة الدفع الاكتروني : الوسيلة التي تمكن صاحبها من القيام بعمليات الدفع المباشر عن بعد عبر الشبكات العمومية للاتصالات .

-منتوج : كل خدمة او منتوج طبيعي او فلاحي او حرفي او صناعي ، مادي او لا مادي.

الفصل 3

يخضع استعمال التشفير في المبادلات والتجارةالالكترونية عبر الشبكات العمومية للاتصالات الى التراتيب الجاري بها العمل في ميدان الخدمات ذات القيمة المضافة للاتصالات .

الباب الثاني : في الوثيقة الإلكترونية والإمضاء الإلكتروني

الفصل 4 :

يعتمد قانونا حفظ الوثيقة الالكترونية كما يعتمد حفظ الوثيقة الكتابية . ويلتزم المرسل بحفظ الوثيقة الالكترونية في الشكل المرسلة به ويلتزم المرسل اليه بحفظ هذه الوثيقة في الشكل الذي تسلمها به.

ويتم حفظ الوثيقة الالكترونية على حامل الكتروني يمكن من :

-الاطلاع على محتواها طيلة مدة صلوحيتها .

-حفظها في شكلها النهائي بصفة تضمن سلامة محتواها .

-حفظ المعلومات الخاصة بمصدرها ووجهتها وكذلك تاريخ ومكان ارسالها او استلامها

الفصل 5

يمكن لكل من يرغب في امضاء وثيقة الكترونية احداث امضائه الالكتروني بواسطة منظومة موثوق بها يتم ضبط مواصفاتها التقنية بقرار من الوزير المكلف بالاتصالات .

الفصل 6

يتعين على كل من يستعمل منظومة امضاء الكتروني :

-اتخاذ الاحتياطات الدنيا التي يتم ضبطها في القرار المنصوص عليه بالفصل 5 من هذا القانون لتفادي كل استعمال غير مشروع لعناصر التشفير او المعدات الشخصية المتعلقة بامضائه

-اعلام مزود خدمات المصادقة الاكترونية بكل استعمال غير مشروع لامضائه.

-الحرص على مصداقية كافة المعطيات التي صرح بها لمزود خدمات المصادقة الالكترونية ولكافة الاطراف التي طلب منها ان تثق في امضائه

الفصل 7

في صورة اخلاله بالالتزامات المنصوص عليها بالفصل 6 هن هذا القانون ، يتحمل صاحب الامضاء مسؤولية الاضرار اللاحقة بالغير الناتجة عن ذلك .

الباب الثالث : في الوكالة الوطنية للمصادقة الالكترونية

الفصل 8

احدثت مؤسسة عمومية لا تكتسي صبغة ادارية تتمتع بالشخصية المعنوية وبالاستقلال المالي اطلق عليها اسم (الوكالة الوطنية للمصادقة الالكترونية) و تخضع في علاقاتها مع الغير الى التشريع التجاري ومقراها بتونس العاصمة .

الفصل 9

تتولى هذه المؤسسة القيام خاصة بالمهام التالية :

-منح ترخيص تعاطي نشاط مزود خدمات المصادقة الالكترونية على كامل تراب الجمهورية التونسية .

-السهر على مراقبة احترام مزود خدمات المصادقة الالكترونية لاحكام هذا القانون ونصوصه التطبيقية .

-تحديد مواصفات منظومة احداث الامضاء و التدقيق .

-ابرام اتفاقيات الاعتراف المتبادل مع الاطراف الاجنبية .

-اصدار وتسليم وحفظ شهادات المصادقة الالكترونية الخاصة بالاعوان العموميين المؤهلين للقيام بالمبادلات الالكترونية ويمكن ان يتم ذلك مباشرة او عبر مزودي خدمات مصادقة الكترونية عموميين.

-المساهمة في انشطة البحث والتكوين والدراسة ذات العلاقة بالمبادلات والتجارة الالكترونية .

وبصفة عامة كل نشاط اخر يقع تكليفها به من قبل سلطة الاشراف وله علاقة بميدان تدخلها.

و هي تخضع لاشراف الوزارة المكلفة بالقطاع.

الفصل 10

يمكن ان تسند الى الوكالة الوطنية للمصادقة الالكترونية عن طريق التخصيص ممتلكات الدولة المنقولة وغير المنقولة الضرورية للقيام بمهامها . وفي صورة حل المؤسسة ترجع ممتلكاتها الى الدولة التي تتولى

تنفيذ التزاماتها وتعهداتها طبقا للتشريع الجاري به العمل .

الباب الرابع: في خدمات المصادقة الالكترونية

الفصل 11

يتعين على كل شخص طبيعي او معنوي يرغب في تعاطي نشاط مزود خدمات المصادقة الالكترونية الحصول على ترخيص مسبق من الوكالة الوطنية للمصادقة الالكترونية .

ويجب ان تتوافر في الشخص الطبيعي او الممثل القانوني للشخص المعنوي الراغب في الحصول على ترخيص التعاطي نشاط مزود خدمات المصادقة الالكترونية الشروط التالية :

-ان يكون من ذوي الجنسية التونسية منذ خمسة اعوام على الاقل .

-ان يكون مقيما بالبلاد التونسية .

بحقوقه المدنية والسياسية ونقي السوابق العدلية . -ان يكون متمتعا

-ان يكون متحصلا على الاقل على شهادة الاعدادية او ما يعادلها

- ان لا يتعاطى نشاطا مهنيا اخر

الفصل 12

يتولى كل مزود خدمات المصادقة الالكترونية اصدار وتصميم وحفظ الشهادات وفقا لكراس شروط تتم المصادقة عليه بامر ، وعند الاقتضاء تعليقها او الغاءها وفقا لاحكام هذا القانون.

ويتضمن كراس الشروط خاصة:

-كلفة دراسة ومتابعة ملفات مطالب الشهادات .

-آجال دراسة الملفات.

-الامكانيات المادية والمالية والبشرية التي يجب توفرها لتعاطي النشاط.

-شروط تأمين التفاعل المتبادل لانظمة المصادقة وربط سجلات شهادات المصادقة .

-القواعد المتعلقة بالاعلام والخاصة بخدماته والشهادات التي سلمها والتي يتعين على مزود خدمات المصادقة الالكترونية حفظها .

الفصل 13

يتعين على مزود خدمات المصادقة الالكترونية استعمال وسائل موثوق بها لاصدار وتسليم وحفظ

الشهادات و اتخاذ الوسائل اللازمة لحمايتها من التقليد والتدليس وفقا لكراس الشروط المنصوص عليه بالفصل 12 من هذا القانون .

الفصل 14

على كل مزود خدمات مصادقة الالكترونية مسك سجل الكتروني لشهادات المصادقة على ذمة المستعملين مفتوح للاطلاع الكترونيا بصفة مستمرة على المعلومات المدونة به .

ويتضمن سجل شهادات المصادقة من كل ، عند الاقتضاء ، تاريخ تعليق الشهادات او الغاؤها .

ويتعين حماية هذا السجل وشهادة المصادقة من كل تغيير غير مرخص فيه.

الفصل 15

يتعين على مزودي خدمات المصادقة الكترونية واعوانهم المحافظة على سرية المعلومات التي عهدت اليهم في اطار تعاطي انشطتهم باستثناء تلك التي رخص صاحب الشهادة كتابيا او الكترونيا في نشرها او اعلام بها او في الحالات التشريع الجاري به العمل .

الفصل 16

يتولى مزود خدمات المصادقة اللاكترونية ،عند طلب شهادة جمع المعلومات ذات الصبغة الشخصية مباشرة من الشخص المعني وله ان يتحصل عليها من الغير بعد الموافقة الكتابية او الالكترونية لهذا الشخص .

يحجر على مزود خدمات المصادقة الالكترونية جمع المعلومات التي لا تكون ضرورية لتسليم الشهادة .

ويحجر عليه استعمال المعلومات التي جمعها بغرض تسليم الشهادة خارج اطار انشطة المصادقة ، مالم يحصل كتابيا او الكترونيا على موافقة الشخص المعني .

الفصل 17

يصدر مزود خدمات المصادقة الالكترونية شهادات مصادقة تستجيب لمقتضات السلامة والوثوق بها .
وتضبط المعطيات التقنية المتعلقة بالشهادة و الوثوق بها بقرار من الوزير المكلف بالاتصالات .

وتتضمن هذه الشهادة بالخصوص :

- هوية صاحب الشهادة.

-هوية الشخص الذي اصدرها وامضاء الكتروني

-عناصر التدقيق في امضاء صاحب الشهادة.

-مدة صلاحية الشهادة

-مجالات استعمال الشهادة

الفصل 18

يضمن مزود خدمات المصادقة الالكترونية :

-صحة المعلومة المصادق عليها التي تضمنتها الشهادة في تاريخ تسليمها،

-الصلة بين صاحب الشهادة ومنظومة التدقيق في الامضاء الخاصة به،

-انفراد صاحب الشهادة بمسك منظومة احداث امضاء مطابقة لاحكام القرارا المنصوص عليه بالفصل 5 من هذا القانون ومتكاملة مع منظومة التدقيق في الامضاء المعروفة في الشهادة في تاريخ تسلمها .

وعند تسليم شهادة المطادقة الى شخص معنوي يتعين على مزود خدمات المصادقة الالكترونية التدقيق مسبقا في هوية الشخص الطبيعي الذي يتقدم اليه وصفة تمثيله للشخص المعنوي

الفصل 19

يتولى مزود خدمات المصادقة الالكترونية تعليق العمل بشهادة المصادقة حالا بطلب من صاحبها او عندما يتبين :

-ان الشهادة سلمت بالاعتماد على معلومات مغلوطة او مزيفة،

-انه تم انتهاك منظومة احداث الامضاء،

-ان الشهادة استعملت بغرض التدليس،

-ان المعلومات المضمنة بالشهادة قد تغيرت،

ويتولى مزود خدمات المصادقة الالكترونية اعلام صاحب الشهادة حالا بالتعليق وسببه

ويتم رفع هذا التعليق حالا اذا تبينت صحة المعلومات المدونة بالشهادة واستعمالها بصفة شرعية.

ويعارض صاحب الشهادة او الغير بقرار مزود الخدمات الخاص بتعليق الشهادة من تاريخ نشره بالسجل الالكتروني المنصوص عليه بالفصل 14 من هذا القانون.

الفصل 20

يلغي مزود خدمات المصادقة الالكترونية حالا الشهادة في الحالات التالية

-عند طلب صاحب الشهادة،

-عند اعلامه بوفاة الشخص الطبيعي او انحلال الشخص المعنوي صاحب الشهادة،

-عند القيام باختبارات دقيقة ، بعد تعليقها ، تبين ان المعلومات مغلوطة او مزيفة او انها غير مطابقة للواقع او انه قد تم انتهاك منظومة احداث الامضاء او الاستعمال المدلس للشهادة .

ويعارض صاحب الشهادة او الغير بقرار مزود الخدمات الخاص بالغاء الشهادة من تاريخ نشره بالسجل الالكتروني المنصوص عليه بالفصل 14 من هذا القانون

الفصل 21

يكون صاحب الشهادة المسؤول الوحيد عن سرية وسلامة منظومة احداث الامضاء التي يستعملها، وكل استعمال لهذه المنظومة يعتبر صادرا منه .

ويتعين على صاحب الشهادة اعلام مزود خدمات المصادقة الالكترونية بكل تغيير للمعلومات المضمنة بالشهادة .

لا يمكن لصاحب الشهادة التي تم تعليقها او الغاؤها استعمال عناصر التشفير الشخصية للامضاء موضوع الشهادة المعينة والمصادقة على هذه العناصر من جديد لدى مزود اخر لخدمات المصادقة الالكترونية

الفصل 22

يكون مزود خدمات المصادقة الالكترونية مسؤول عن كل ضرر حصل لكل شخص وثق عن حسن نية في الضمانات المنصوص عليها بالفصل 18 من هذا القانون .

ويكون مزود خدمات المصادقة الالكترونية مسؤولا عن الضرر الحاصل لكل شخص نتيجة عدم تعليق أو الغاء شهادة طبقا للفصلين 19 و 20 من هذا القانون .

ولا يكون مزود خدمات المصادقة الالكترونية مسؤولا عن الضرر الناتج عن عدم احترام صاحب الشهادة لشروط استعمالها او شروط احداث امضائه الالكتروني .

الفصل 23

تعتبر الشهادات المسلمة من مزود خدمات المصادقة الالكترونية الموجود ببلد اجنبي كشهادات مسلمة من مزود خدمات المصادقة الالكترونية موجود بالبلاد التونسية اذا تم الاعتراف بهذا الهيكل في اطار اتفاقية اعتراف متبادل تبرمها الوكالة الوطنية للمصادقة الالكترونية.

الفصل 24

يتعين على مزود خدمات المصادقة الالكترونية الراغب في ايقاف نشاطه اعلام الوكالة الوطنية للمصادقة الالكترونية قبل تاريخ الايقاف بثلاثة اشهر على الاقل

و يمكن لمزود خدمات المصادقة الالكترونية تحويل جزء او كل نشاطه الى مزود اخر ، ويتم هذا التحويل حسب الشروط التالية :

-اعلام اصحاب الشهادات الجاري بها العمل برغبته في تحويل الشهادات الى مزود اخر قبل شهر من التحويل المنتظر على الاقل،

-تحديد هوية مزود خدمات المصادقة الالكترونية الذي ستحول اليه الشهادات،

-اعلام اصحاب الشهادة بامكانية رفض التحويل المنتظر وكذلك اجال وطرق الرفض. وتلغى الشهادات اذا عبر اصحابها كتابيا او الكترونيا عن رفضهم في هذا الاجل

وفي حالة وفاة او افلاس او حل او تصفية مزود خدمات المصادقة الالكترونية يخضع ورثته او وكلاؤه او المصفون الى مقتضيات الفقرة الثانية من هذا الفصل في اجل لا يتجاوز ثلاثة اشهر .

وفي كل حالات ايقاف النشاط يتعين اتلاف المعطيات الشخصية التي بقيت تحت تصرف المزود وذلك بحضور ممثل عن الوكالة الوطنية للمصادقة الالكترونية

<u>الباب الخامس</u> : في المعاملات التجارية الالكترونية

الفصل 25 :

يجب على البائع في المعاملات التجارية الالكترونية ، ان يوفر للمستهلك بطريقة واضحة ومفهومة ، قبل ابرام العقد المعلومات التالية:

-هوية وعنوان وهاتف البائع او مسدي الخدمات،

-وصفا كاملا لمختلف مراحل انجاز المعاملة ،

-طبيعة وخاشيات وسعر المنتوج،

-كلفة تسليم المنتوج ومبلغ تأمينه والادعاءات المستوجبة،

-الفترة التي يكون خلالها المنتوج معروضا بالأسعار المحددة،

-شروط الضمانات التجارية والخدمة بعد البيع،

-طرق واجراءت الدفع، وعند الاقتضاء شروط القروض المقترحة ،

-طرق واجال التسليم وتنفيذ العقد ونتائج عدم انجاز الالتزامات ،

-امكانية العدول عن الشراء واجله،

-كيفية اقرار الطلبية،

-طرق ارجاع المنتوج او الابدال وارجاع المبلغ،

-كلفة استعمال تقنيات الاتصالات حين يتم احتسابها عل اساس مختلف عن التعريفات الجاري بها العمل ،

-شروط فسخ العقد اذا كان لمدة غير محدودة او تفوق السنة،

-المدة الدنيا للعقد ، في ما يخص العقود المتعلقة بتزويد المستهلك بمنتوج او خدمة خلال مدة طويلة او بصفة دورية،

يتعين توفير هذه المعلومات الكترونيا ووضعها على ذمة المستهلك للاطلاع عليها في جميع مراحل المعاملة

الفصل 26

يحجر على البائع تسليم منتوج مشروط بطلب دفع ، لم تصدر بشأنه طلبية من قبل المستهلك.

وفي حالة تسليم منتوج الى المستهلك لم تصدر بشأنه طلبية ، لا يمكن مطالبة هذا الاخير بسعره او كلفة تسليمه.

الفصل 27

يتعين على البائع ، قبل ابرام العقد تمكين المستهلك من المراجعة النهائية لجميع اختياراته وتمكينه من اقرار الطلبية او تغييرها حسب ارادته وكذلك الاطلاع على شهادة المصادقة الالكترونية المتعلقة بامضائه.

الفصل 28

ينشأ العقد الالكتروني بعنوان البائع وفي تاريخ موافقة هذا الاخير على الطلبية بواسطة وثيقة الكترونية ممضاة وموجهة للمستهلك ، مالم يتفق الطرفان على خلاف ذلك .

الفصل 29

يتعين على البائع ان يوفر للمستهلك عند الطلب خلال العشرة ايام الموالية لابرام العقد وثيقة كتابية او الكترونية تتضمن كافة المعطيات المتعلقة بعملية البيع .

الفصل 30

مع مراعاة مقتضيات الفصل 25 من هذا القانون ، يمكن للمستهلك العدول عن الشراء في اجل عشرة ايام عمل ، تحتسب :

-بالنسبة الى البضائع بداية من تاريخ تسلمها من قبل المستهلك،

-بالنسبة الى الخدمات بداية من تاريخ ابرام العقد،

ويتم الاعلام بالعدول بواسطة جميع الوسائل المنصوص عليها مسبقا في العقد .

في هذه الحالة ، يعين على البائع ارجاع المبلغ المدفوع الى المستهلك في اجل عشرة ايام عمل من تاريخ ارجاع البضاعة او العدول عن الخدمة.

ويتحمل المستهلك المصاريف الناجمة عن ارجاع البضاعة.

الفصل31

بقطع النظر عن جبر الضرر لفائدة المستهلك ، يمكن لهذا الاخير ارجاع المنتوج على حالته اذا كان غير مطابق للطلبية او اذا لم يحترم البائع اجال تسليمه وذلك في أجل عشرة ايام عمل تحتسب بداية من تاريخ التسليم.

في هذه الحالة ، يتعين على البائع ارجاع المبلغ المدفوع والمصاريف الناجمة عن ذلك الى المستهلك في أجل عشرة أيام عمل من تاريخ ارجاع المنتوج .

الفصل 32

مع مراعاة احكام الفصل 30 من هذا القانون وباستثناء حالات العيوب الظاهرة او الخفية، لا يمكن للمستهلك العدول عن الشراء في الحلات التالية :

-عندما يطلب المستهلك توفير الخدمة قبل انتهاء اجل العدول عن الشراء ويوفر البائع ذلك،

-اذا تم تزويد المستهلك بمنتوجات حسب خاصيات شخصية او تزويده بمنتوجات لا يمكن اعادة ارسالها او تكون قابلة للتلف او الفساد لانتهاء مدة صلوحيتها،

-عند قيام المستهلك بنزع الاختام عن التسجيلات السمعية او البصرية او البرمجيات والمعطيات الاعلامية المسلمة او نقلها آليا،

-شراء الصحف والمجلات

الفصل 33

اذا كانت عملية الشراء ناتجة كليا او جزئيا عن قرض ممنوح الى المستهلك من قبل البائع او الغير على اساس عقد مبرم بين البائع والغير ، فان عدول المستهلك عن الشراء يفسخ عقد القرض بدون تعويض.

الفصل 34

باستثناء حالات سوء الاستعمال يتحمل البائع ، في حالة البيع مع التجربة ، الاخطار التي قد يتعرض اليها المنتوج وذلك الى غاية انتهاء مدة تجربته ويعد لاغيا كل شرط للاعفاء من المسؤولية يكون مخالفا لاحكام هذا الفصل.

الفصل 35

يتعين على البائع ، في صورة عدم توفر المنتوج او الخدمة المطلوبة اعلام المستهلك بذلك في اجل اقصاه 24 ساعة قبل تاريخ التسليم المنصوص عليه في العقد وارجاع كامل المبلغ المدفوع الى صاحبه.

وباستثناء حالات القوة القاهرة يفسخ القعد اذا اخل البائع بالتزاماته ويسترجع المستهلك المبلغ المدفوع بقطع النظر عن جبر الضرر اللاحق به

الفصل 36

على البائع اثبات حصول الاعلام المسبق واقرار المعلومات واحترام الاجال وقبول المستهلك وكل اتفاق مخالف يعد باطلا .

الفصل 37

تخضع عمليات الدفع المتعلقة بالمبادلات والتجارة الالكترونية الى التشريع والترتيب الجاري بها العمل.

يجب على صاحب وسيلة الدفع الالكتروني اعلام مصدرها بضياعها او سرقتها او ضياع او سرقة الوسائل التي تمكن من استعمالها وكذلك كل استعمال مزيف لها.
يجب على مصدر وسيلة الدفع الالكتروني تحديد الوسائل الملائمة لهذا الاعلام في العقد المبرم مع صاحبها.

بقطع النظر عن حالات التدليس ، فان صاحب وسيلة الدفع الالكتروني :
-يتحمل، الى تاريخ اعلامه المصدر، نتائج ضياع او سرقة وسيلة الدفع او استعمالها المزيف من قبل الغير.
-لا يتحمل أي مسؤولية من استعمال وسيلة الدفع الالكتروني بعد اعلام المصدر.

واستعمال وسيلة الدفع الالكتروني دون تقديم الوسيلة وتحديد الهوية الكترونيا لا يلزم صاحبها.

الباب السادس: في حماية المعطيات الشخصية

الفصل 38

لايمكن لمزود خدمات المصادقة الالكترونية معالجة المعطيات الشخصية الا بعد موافقة صاحب المعني.

ويمكن اعتماد الاعلام الالكتروني بالموافقة اذا ضمن المزود :
-اعلام صاحب الشهادة بحقه في سحب الموافقة في كل وقت،
-امكانية تحديد هوية الاطراف المستعملة للمعطيات الشخصية،
-الاحتفاظ بحجة الموافقة التي لا يمكن تغييرها،

الفصل 39

باستثناء حالة موافقة صاحب الشهادة ، لا يمكن لمزود خدمات المصادقة الالكترونية او احد اعوانه جمع المعلومات الخاصة بصاحب الشهادة الا ما كان منها ضروريا لابرام العقد وتحديد محتواه و تنفيذ واعداد واصدار الفاتورة.

لا يمكن استعمال المعطيات المجمعة طبقا للفقرة الاولى من هذا الفصل لغير الغاية المذكورة اعلاه من قبل المزود او غيره الا اذا تم اعلام صاحب الشهادة بذلك ولم يعارضه.

الفصل 40

يمنع على مستعملي المعطيات الشخصية المجمعة طبقا للفصل 39 من هذا القانون ارسال الوثائق الالكترونية الى صاحب الشهادة الذي يرفض صراحة قبولها.

و يتعين على صاحب الشهادة اعلام الوكالة الوطنية للمصادقة الالكترونية باعتراضه بواسطة رسالة مضمونة الوصول مع اعلام بالبلوغ .

ويعتبر هذا الاعلام قرينة قاطعة على معرفة كل المزودين والغير لهذا الاعتراض.

الفصل 41

يتعين على مزود خدمات المصادقة الالكترونية ، قبل كل معالجة للمعلومات الشخصية ، اعلام صاحب الشهادة بواسطة اشعار خاص بالاجراءات المتبعة من قبله في مجال حماية المعطيات الشخصية.

ويتعين ان تمكن هذه الاجراءات صاحب الشهادة من الاطلاع آليا وبطريقة مبسطة على محتوى المعطيات.

ويجب ان تحدد هذه الاجراءات هوية المسؤول عن المعالجة وطبيعة المعطيات والغاية من المعالجة واصناف واماكن المعالجة ، وعند الاقتضاء كل معلومة ضرورية لضمان المعالجة الامنية للمعطيات .

الفصل 42

يمكن لصاحب الشهادة ، في كل وقت ، بطلب ممضى بخط اليد او الكترونيا النفاذ الى المعلومات الشخصية المتعلقة به وتعديلها . ويشمل حق النفاذ والتعديل الدخول على جميع المعطيات الشخصية المتعلقة بصاحب الشهادة.

ويتعين على المزود وضع الامكانيات التقنية اللازمة لتمكين صاحب الشهادة من ارسال مطلبه الممضى لتعديل المعلومات او فسخها بطريقة الكترونية .

الباب السابع : في المخالفات والعقوبات

الفصل 43

تتم معاينة المخالفات لاحكام هذا القانون من قبل اعوان الضابطة العدلية والاعوان المحلفين للوزارة المكلفة بالاتصالات والوكالة الوطنية للمصادقة الالكترونية واعوان المراقبة الاقتصادية وفق الشروط المنصوص عليها بالقانون عدد 64 لسنة 1991 المؤرخ في 29 جويلية 1991 المتعلق بالمنافسة والاسعار والنصوص المنقحة والمتممة له.

الفصل 44

يسحب الترخيص من مزود خدمات المصادقة الالكترونية ويتم ايقاف نشاطه ، اذا اخل بواجباته المنصوص عليها بهذا القانون او بنصوصه التطبيقية . وتتولى الوكالة الوطنية للمصادقة الالكترونية سحب الترخيص بعد سماع المزود المعني بالامر .

الفصل 45

علاوة على العقوبات المبنية بالفصل 44 من هذا القانون يعاقب كل مزود خدمات المصادقة الالكترونية لم يراع مقتضيات كراس الشروط المنصوص عليه بالفصل 12 من هذا القانون بخطية تتراوح بين 1.000 و 10.000 دينار .

الفصل 46

يعاقب كل من يمارس نشاط مزود خدمات المصادقة الالكترونية بدون الحصول على ترخيص مبق طبقا للفصل 11 من هذا القانون بالسجن لمدة تتراوح بين شهرين و 3 سنوات وبخطية تتراوح بين 1.000 و 10.000 دينار او باحدى هاتين العقوبتين .

الفصل 47

يعاقب كل من صرح عمدا بمعطيات خاطئة لمزود خدمات المصادقة الالكترونية ولكافة الاطراف التي طلب منها ان تثق بامضائه بالسجن لمدة تتراوح بين 6 اشهر وعامين وبخطية تتراوح بين 1.000 و 10.000 دينار او باحدى هاتين العقوبتين.

الفصل 48

يعاقب كل من استعمل بصفة غير مشروعة عناصر تشفير شخصية متعلقة بامضاء غيره بالسجن لمدة تتراوح بين 6 اشهر وعامين و بخطية تتراوح بين 1.000 و 10.000 دينار او بأحدى هاتين العقوبتين .

الفصل 49

يعاقب كل مخالف لاحكام الفصول 25و27 و 29 والفقرة الثانية من الفصل 31 والفصل 34 و الفقرة الاولى من الفصل 35 من هذا القانون بخطية تتراوح بين 5.00 و 5.000 دينار .

الفصل 50

يعاقب كل من استغل ضعف او جهل شخص في اطار عمليات البيع الالكتروني بدفعه للالتزام حاضرا او اجلا بأي شكل من الاشكال ، بخطية تتراوح بين 1.000 و 20.000 دينار ، وذلك اذا ثبت من ظروف الواقعة ان هذا الشخص غير قادر على تمييز ابعاد تعهداته او كشف الحيل والخدع المعتمدة بالالتزام او اذا ثبت انه كان تحت الضغط مع مراعاة احكام المجلة الجنائية .

الفصل 51

يعاقب كل من مخالف لاحكام الفصلين 38 و39 بخطية تتراوح بين 1000 و 10000 دينار.

الفصل 52

يعاقب طبقا لاحكام الفصل 254 من المجلة الجنائية مزود خدمات المصادقة الالكترونية واعوانه الذين يفشون او يحثون او يشاركون في افشاء المعلومات التي عهدت اليهم في اطار تعاطي نشاطاتهم باستثناء تلك التي رخص صاحب الشهادة كتابيا او الكترونيا في نشرها او الاعلام بها او في الحالات المنصوص عليها في التشريع الجاري به العمل .

الفصل53

مع حفظ الحقوق المدنية للمتضررين ، يمكن للوزير المكلف بالتجارة اجراء الصلح في المخالفات المنصوص عليها بالفصل 49 من هذا القانون و التي تتم معاينتها وفقا لاحكام هذا القانون .

مع حفظ الحقوق المدنية للمتضررين ، يمكن للوزير المشرف على الوكالة الوطنية للمصادقة الالكترونية اجراء الصلح في المخالفات المنصوص عليها بالفصل 45 من هذا القانون والتي تتم معايتنها وفقا لاحكام هذا القانون .

وتكون طرق واجراءات الصلح وفق النصوص القانونية الجاري بها العمل والمنظمة للمراقبة الاقتصادية وخاصة القانون عدد 64 لسنة 1991 المتعلق بالمنافسة و الاسعار و النصوص المنقحة و المتممة له ، بدون المساس بحقوق الغير .

تنقرض الدعوى العمومية بدفع المبلغ المعين في عقد الصلح .

ينشر هذا القانون بالرائد الرسمي للجمهورية التونسية وينفذ كقانون من قوانين الدولة .

تونس في 9 اوت 2000

ملحق رقم 3

نحن حمد بن عيسى آل خليفة ملك مملكة البحرين . بعد الإطلاع على الدستور ، وعلى قانون أصول المحاكمات الجزائية لعام 1966 وتعديلاته ، وعلى قانون المرافعات المدنية والتجارية الصادر بالمرسوم بقانون رقم (12) لسنة 1971 وتعديلاته ، وعلى المرسوم بقانون رقم (13) لسنة 1971 بشأن تنظيم القضاء وتعديلاته ، وعلى المرسوم بقانون رقم (14) لسنة 1971 بشأن التوثيق ، وعلى قانون إنشاء مؤسسة نقد البحرين الصادر بالمرسوم بقانون رقم (23) لسنة 1973 المعدل بالمرسوم بقانون رقم (14) لسنة1981 ، وعلى قانون العقوبات الصادر بالمرسوم بقانون رقم (15) لسنة 1976 وتعديلاته ، وعلى قانون التجارة الصادر بالمرسوم بقانون رقم (7) لسنة 1987 وتعديلاته ، وعلى قانون الإثبات في المواد المدنية والتجارية الصادر بالمرسوم بقانون رقم (14 (لسنة 1996 ، وعلى القانون المدني الصادر بالمرسوم بقانون رقم (19) لسنة 2001 ، وعلى قانون الشركات التجارية الصادر بالمرسوم بقانون رقم (21) لسنة 2001 ، وبناءً على عرض رئيس مجلس التنمية الاقتصادية ، وبعد موافقة مجلس الوزراء على ذلك ، رسمنا بالقانون الآتي :

مادة (1) : تعاريف في تطبيق أحكام هذا القانون تكون للكلمات والعبارات التالية ، المعاني المبينة قرين كل منها ما لم يقتض سياق النص خلاف ذلك :

- إلكتروني : تقنية استعمال وسائل كهربائية أو مغناطيسية أو كهرومغناطيسية أو بصرية أو بايومترية أو فوتونية أو أي شكل آخر من وسائل التقنية المشابهة .

- وكيل إلكتروني : برنامج حاسب أو أية وسيلة إلكترونية أخرى تستخدم لإجراء تصرف ما ، أو للاستجابة لسجلات أو تصرفات إلكترونية – كلياً أو جزئياً – بدون مراجعة أو تدخل من أي فرد في وقت التصرف أو الاستجابة له .

- السجل : المعلومات التي تدون على وسط ملموس ، أو تكون محفوظة على وسط إلكتروني أو على أي وسط آخر ، وتكون قابلة للاستخراج بشكل قابل للفهم .

- السجل الإلكتروني : السجل الذي يتم إنشاؤه أو إرساله أو تسلمه أو بثه أو حفظه بوسيلة إلكترونية.

- المنشئ : الشخص الذي يرسل ، أو يرسل نيابة عنه ، السجل الإلكتروني ، أو من يظهر من السجل الإلكتروني قيامه بإنشاء أو إرسال السجل الإلكتروني قبل حفظه - إن كان قد تم ذلك - ولا يشمل الشخص الذي يعمل وسيط شبكة بشأن هذا السجل .

- المرسل إليه: الشخص الذي يقصد المنشئ تسليم سجل إلكتروني إليه . ولا يشمل ذلك الشخص الذي يعمل وسيط شبكة بشأن هذا السجل .

- وسيط الشبكة: الشخص الذي يقوم نيابة عن شخص آخر بإرسال أو تسلم أو بث أو حفظ السجل

الإلكتروني ، أو يقوم بتقديم أية خدمات أخرى بشأن هذا السجل .

- المعلومات : البيانات والنصوص والصور والأشكال والأصوات والرموز وبرامج الحاسب والبرمجيات وقواعد البيانات والكلام و ما شابه ذلك .

- نظام المعلومات : نظام إلكتروني لإنشاء أو إرسال أو بث أو تسلم أو حفظ أو عرض أو تقديم المعلومات - .

التوقيع الإلكتروني : معلومات في شكل إلكتروني تكون موجودة في سجل إلكتروني أو مثبته أو مقترنة به منطقياً ، ويمكن للموقع استعمالها لإثبات هويته .

-الموقع : شخص حائز لأداة إنشاء توقيع قام بالتوقيع عن نفسه ، أو نيابة عن شخص يمثله . - أداة إنشاء توقيع : أداة تستخدم لإنشاء توقيع إلكتروني ، مثل برمجية مجهزة أو جهاز إلكتروني.

- بيانات إنشاء توقيع : بيانات فريدة تستعمل لإنشاء توقيع إلكتروني، كالرموز أو مفاتيح التشفير الخاصة.

- بيانات التحقق من توقيع : بيانات تستعمل للتحقق من صحة توقيع إلكتروني ، كالرموز أو مفاتيح التشفير العامة .

- شهادة معتمدة : سجل إلكتروني يتسم بأنه : أ - يربط بيانات تحقق من توقيع بشخص معين . ب- يثبت هوية ذلك الشخص . ج- يكون صادرا من قبل مزود خدمة شهادات معتمد . د -مستوفٍ للمعايير المتفق عليها بين الأطراف المعنية أو المنصوص عليها في القرارات التي تصدر استنادا لأحكام هذا القانون .

- مزود خدمة الشهادات : الشخص الذي يصدر شهادات إثبات الهوية لأغراض التوقيعات الإلكترونية أو الذي يقدم خدمات أخرى تتعلق بهذه التوقيعات .

- مزود خدمة شهادات معتمد : مزود خدمة شهادات يتم اعتماده لإصدار شهادات معتمدة طبقاً لأحكام المادتين (16) و(17) من هذا القانون. - نظام أمان : نظام يستخدم للتحقق من أن توقيعاً إلكترونياً أو سجلاً إلكترونياً يخص الشخص المعني ، أو يستخدم لكشف أية تغييرات أو أخطاء في محتوى سجل إلكتروني طرأت عليه منذ أن تم بثه من قبل المنشئ . - شخص : أي شخص طبيعي أو اعتباري أو جهة عامة . - فرد : أي شخص طبيعي.

- الوزارة : وزارة التجارة والصناعة .

- الوزير : وزير التجارة والصناعة .

مادة (2) : التطبيق 1- تسري أحكام هذا القانون على السجلات والتوقيعات الإلكترونية . 2- يستثني من أحكام هذا القانون ما يلي :- أ -كافة المسائل التي ينعقد الاختصاص بشأنها للمحاكم الشرعية طبقاً لأحكام

المرسوم بقانون رقم (13) لسنة 1971 بشأن تنظيم القضاء وتعديلاته . ب- مسائل الأحوال الشخصية لغير المسلمين مثل الزواج والطلاق والحضانة والتبني والميراث وإنشاء الوصايا وتعديلها . ج- المعاملات والتصرفات التي يشترط القانون للاعتداد بها أن تكون مثبتة في محررات رسمية . د - السندات القابلة للتداول . هـ - سندات الملكية ، فيما عدا تلك المنصوص عليها في المادة (20) من هذا القانون .

مادة (3): قبول التعامل الإلكتروني 1- لا يلزم هذا القانون أي شخص بإرسال أو تسلم أو استعمال سجل أو توقيع إلكتروني بدون موافقته على ذلك صراحة. وباستثناء الجهات العامة ، يجوز أن تكون الموافقة ضمناً من خلال السلوك الإيجابي . 2- لا يحظر هذا القانون على أي شخص يرغب في التعامل بشكل إلكتروني أن يضع شروطه المعقولة بشأن ما يكفل قبوله لتوقيع إلكتروني أو لسجلات إلكترونية .

مادة (4): شروط قبول الجهات العامة للتعامل الإلكتروني 1- يشترط لقبول الجهات العامة إرسال أو تسلم سجل أو توقيع في شكل إلكتروني ، أن يصدر قرار بذلك من الوزير المختص الذي يتولى الإشراف على تلك الجهة ، وينشر القرار في الجريدة الرسمية . ويحدد القرار نطاق ومجال قبول إرسال وتسلم السجلات والتوقيعات الإلكترونية . 2- تخضع الموافقة المشار إليها في البند السابق للاشتراطات الفنية التي يصدر بها قرار من وزير شئون رئاسة مجلس الوزراء خلال فترة لا تجاوز ستة أشهر من تاريخ العمل بأحكام هذا القانون ، وينشر القرار في الجريدة الرسمية . ويجوز أن تشتمل الاشتراطات على الآتي :- (أ (الأسلوب والصيغة – بما في ذلك معايير أنظمة المعلومات – التي يجب الالتزام بها في إنشاء و إرسال و بث و تسلم و حفظ السجلات الإلكترونية ، والأنظمة التي تستعمل لذلك . (ب) إذا كان مطلوباً استعمال توقيع إلكتروني لاعتماد سجل إلكتروني ، فإنه يلزم تحديد نوع التوقيع الإلكتروني المطلوب ، ومعايير نظام المعلومات المطلوب استعمالها ، وأسلوب وصيغة وضع التوقيع على السجل ، وأية اشتراطات أخرى يلزم توافرها للتحقق من صحة هذا التوقيع . (ج) أنظمة وإجراءات السيطرة المناسبة لحفظ وسلامة وأمان وخصوصية السجل الإلكتروني وقابليته للتدقيق وكيفية التخلص منه . (د) أية خصائص أخرى للسجلات الإلكترونية تعتبر ضرورية أو مناسبة في هذا الشأن . (هـ) أية اشتراطات بشأن الإقرار بتسلم السجلات الإلكترونية من قبل الجهات العامة . 3- لا تخل الأحكام السابقة بأي تشريع ينص صراحة على حظر استعمال الوسائل الإلكترونية ، أو يستلزم أن يكون استعمالها بطريقة معينة . 4 - لأغراض البند السابق ، فإن مجرد النص على أن تكون المعلومات أو المستندات ثابتة بالكتابة ، لا يعد حظرا لاستعمال الوسائل الإلكترونية .

مادة (5): حجية السجلات الإلكترونية في الإثبات 1 -للسجلات الإلكترونية ذات الحجية المقررة في الإثبات للمحررات العرفية ، ولا ينكر الأثر القانوني للمعلومات الواردة في السجلات الإلكترونية ، من

حيث صحتها وإمكان العمل بمقتضاها ، لمجرد ورودها – كلياً أو جزئياً – في شكل سجل إلكتروني أو الإشارة إليها في هذا السجل. 2- إذا أوجب القانون أن تكون المعلومات ثابتة بالكتابة ، أو رتب أثرا قانونيا على عدم الالتزام بذلك ، فإن ورود المعلومات في سجل إلكتروني يفي بمتطلبات هذا القانون ، بشرط أن تكون المعلومات قابلة للدخول عليها واستخراجها لاحقاً عن طريق البث أو الطباعة أو غير ذلك . 3- إذا أوجب القانون أن تكون المعلومات المقدمة إلى شخص آخر ثابتة بالكتابة ، فإن تقديمها في شكل سجل إلكتروني يفي بهذا الغرض إذا توافرت الشروط الآتية : أ- أن يتمكن المرسل إليه من الدخول على هذه المعلومات واستخراجها لاحقاً ، سواء عن طريق البث أو الطباعة أو غير ذلك . ب- أن يتمكن المرسل إليه من حفظ هذه المعلومات . 4- يراعى في تقدير حجية السجل الإلكتروني في الإثبات ، عند النزاع في سلامته ما يلي : أ) مدى الثقة في الطريقة التي تم بها إنشاء أو حفظ أو بث السجل الإلكتروني . ب) مدى الثقة في الطريقة التي تم بها توقيع السجل الإلكتروني . ج) مدى الثقة في الطريقة التي استعملت في المحافظة على سلامة المعلومات التي تضمنها السجل الإلكتروني . د) أية أمور أخرى ذات علاقة بسلامة السجل الإلكتروني.

مادة (6): التوقيع الإلكتروني 1- لا ينكر الأثر القانوني للتوقيع الإلكتروني ، من حيث صحته وإمكان العمل بموجبه ، لمجرد وروده – كلياً أو جزئياً – في شكل إلكتروني . 2- إذا أوجب القانون التوقيع على مستند ، أو رتب أثرا قانونيا على خلوه من التوقيع ، فإنه إذا استعمل سجل إلكتروني في هذا الشأن ، فإن التوقيع الإلكتروني عليه يفي بمتطلبات هذا القانون . 3- إذا عرض بصدد أية إجراءات قانونية توقيعَ إلكتروني مقرون بشهادة معتمدة ، قامت القرينة على صحة ما يأتي ما لم يثبت العكس أو يتفق الأطراف على خلاف ذلك : أ- أن التوقيع الإلكتروني على السجل الإلكتروني هو توقيع الشخص المسمى في الشهادة المعتمدة . ب- أن التوقيع الإلكتروني على السجل الإلكتروني قد وضع من قبل الشخص المسمى في الشهادة المعتمدة بغرض توقيع هذا السجل الإلكتروني . جـ- أن السجل الإلكتروني لم يطرأ عليه تغيير منذ وضع التوقيع الإلكتروني عليه . 4- إذا لم يتم وضع التوقيع الإلكتروني باستعمال شهادة معتمدة ، فإن قرينة الصحة المقررة بموجب أحكام البند السابق لا تلحق أياً من التوقيع أو السجل الإلكتروني .

مادة (7) : المستندات الأصلية 1- إذا أوجب القانون تقديم أو حفظ أصل أي مستند ، فإن تقديمه أو حفظه في شكل سجل إلكتروني يفي بهذا الغرض إذا تحققت الشروط الآتية : أ- توفر الضمان الكافي لسلامة المعلومات التي تضمنها السجل الإلكتروني منذ إنشائه في وضعه النهائي كسجل إلكتروني ، سواء كان أصل المعلومات واردا في شكل إلكتروني أو خطي . ب- في حالة الإلزام بتقديم أصل المستند إلى شخص معين ، فإنه يجب أن يكون السجل الإلكتروني قابلاً للدخول عليه واستخراجه وحفظه وعرضه بشكل قابل للفهم من قبل هذا الشخص . ج- موافقة الجهة العامة التي يخضع النشاط لإشرافها – إن وجدت – على أن

يتم الحفظ في شكل سجل إلكتروني واستيفاء أية اشتراطات تحددها هذه الجهة . 2- لأغراض البند /1) أ) من هذه المادة يراعى : أ- أن معيار تقييم سلامة المعلومات ، هو أن تظل هذه المعلومات التي تضمنها السجل الإلكتروني كاملة دون أن يطرأ عليها أي تغيير ، فيما عدا إضافة أي اعتماد أو تغيير يطرأ في السياق المعتاد للإنشاء أو المعالجة أو البث أو التسلم أو الحفظ أو العرض . ب- أن تقييم درجة الضمان يكون على ضوء الظروف التي أنشئ فيها السجل ، بما في ذلك الغرض من إنشائه .

المادة (8) : اشتراط تقديم نسخة واحدة أو أكثر من مستند إذا اشترط تقديم نسخة أو أكثر من مستند إلى شخص آخر ، وأجاز القانون أو اتفق الأطراف على استعمال سجل إلكتروني ، فإن تقديم نسخة واحدة من سجل إلكتروني بمضمون المستند يفي بهذا الشرط.

مادة (9): حفظ المستندات 1- إذا أوجب القانون حفظ أية مستندات أو سجلات أو معلومات تم إنشاؤها أو إرسالها أو تسلمها ، سواء في شكل إلكتروني أو ورقي ، فإن حفظها في شكل سجل إلكتروني يفي بهذا الغرض إذا توفرت الشروط الآتية: أ- أن يتم حفظ السجل الإلكتروني بالصيغة التي تم بها إنشاؤه أو إرساله أو تسلمه ، أو يتم حفظه في صيغة يثبت أنها تمثل بدقة المعلومات الأصلية التي تم إنشاؤها أو إرسالها أو تسلمها . ب- أن تكون المعلومات التي تضمنها السجل الإلكتروني الذي تم حفظه قابلة لأن يتم لاحقا الدخول عليها وعرضها واستخراجها بشكل قابل للفهم . ج- بيان المعلومات – إن وجدت – التي تحدد مصدر المستند والجهة المرسل إليها وتاريخ ووقت إرساله أو تسلمه ، وذلك إذا كان المستند المحفوظ قد أرسل أو تم تسلمه إلكترونياً. د- موافقة الجهة العامة التي يخضع النشاط لإشرافها – إن وجدت – على أن يتم الحفظ في شكل سجل إلكتروني واستيفاء أية اشتراطات تحددها هذه الجهة . 2- لا تسري الاشتراطات المنصوص عليها في البند السابق على أية معلومات تطرأ في السياق المعتاد للإنشاء أو المعالجة أو البث أو الإرسال أو الحفظ أو العرض . 3- يجوز لأي شخص استيفاء الشروط المشار إليها في البند (1) من هذه المادة من خلال الاستعانة بخدمات أي شخص آخر .

مادة (10) : إبرام العقود في سياق إبرام العقود يجوز التعبير ، كليا أو جزئيا ، عن الإيجاب والقبول وكافة الأمور المتعلقة بإبرام العقد والعمل بموجبه ، بما في ذلك أي تعديل أو عدول أو إبطال للإيجاب أو القبول ، عن طريق السجلات الإلكترونية ما لم يتفق الطرفان على غير ذلك.

مادة (11): إبداء النوايا أو التعبيرات المشابهة في العلاقة بين منشئ السجل الإلكتروني والمرسل إليه ، لا ينكر الأثر القانوني لإبداء النوايا - أو ما شابه ذلك من تعبيرات - أو صحته أو قابلية العمل بموجبه لمجرد أنه ورد في شكل سجل إلكتروني .

مادة (12) : دور الوكلاء الإلكترونيين في إبرام العقود 1- يجوز أن يتم إبرام العقود بين فرد ووكيل إلكتروني ، كما يجوز أن يتم ذلك بين وكلاء إلكترونيين . 2- تكون المعاملة الإلكترونية بين الفرد والوكيل

الإلكتروني قابلة للإبطال بناء على طلب الفرد إذا تحققت الشروط الآتية :- أ- وقوع الفرد في خطأ مادي في أي سجل إلكتروني أو في أية معلومات إلكترونية تم استعمالها في المعاملة أو كانت جزءا منها . ب- عدم إتاحة الوكيل الإلكتروني الفرصة للفرد لتلافي وقوع الخطأ أو تصحيحه . ج- قيام الفرد فور اكتشافه الخطأ بإبلاغ الطرف الآخر به دون إبطاء . د- قيام الفرد في حالة تسلمه لمقابل إثر الخطأ بإعادة هذا المقابل أو التصرف فيه طبقاً لما هو متفق عليه بين الطرفين أو بموجب تعليمات الطرف الآخر ، أو التصرف فيه بطريقة معقولة عند عدم وجود تعليمات ، وذلك كله ما لم تكن هناك منفعة مادية عادت على الفرد نتيجة لهذا التسلم . 3- تنصرف كلمة "الفرد" في هذه المادة إلى الفرد الذي يعمل لحساب نفسه ، أو لحساب شخص آخر سواء كان شخصاً طبيعياً أو اعتبارياً . 4- يسري الشرط الخاص بالإبلاغ ، المنصوص عليه في الفقرة (ج) من البند (2) من هذه المادة، في الحالة التي يكون فيها الطرف الآخر قد قدم للفرد البيانات اللازمة للاتصال بهذا الطرف.

مادة (13): الإسناد 1- ما لم يكن هناك اتفاق يقضي بغير ذلك بين منشئ السجل الإلكتروني والمرسل إليه ، فإن السجل الإلكتروني يسند إلى المنشئ إذا كان : أ- قد أرسل من المنشئ . ب- قد أرسل بناءً على موافقة صريحة أو ضمنية من قبل المنشئ ، أو من قبل وكيل عادي أو وكيل إلكتروني للمنشئ . ج- قد أرسل من شخص ، تمكّن من خلال علاقته بالمنشئ ، أو بأي وكيل له ، أن يصل إلى طريقة يستخدمها المنشئ للإشارة إلى أن السجل الإلكتروني خاص به ، وذلك ما لم يثبت المنشئ أن الوصول إلى الطريقة ليس راجعاً إلى إهماله . 2- يجوز إثبات الإسناد المشار إليه في البند السابق بكافة الطرق ، بما في ذلك إقامة الدليل على استعمال نظام أمان ، متفق عليه مسبقاً بين الطرفين أو معتمد بموجب قرار صدر تنفيذا لأحكام هذا القانون ، أو من خلال إثبات فاعلية أي نظام أمان استخدم لتحديد هوية من أسند إليه السجل الإلكتروني . 3- لا تخل أحكام هذه المادة بأي نص قانوني يتعلق بالوكالة أو بإبرام العقود .

مادة (14) : الإقرار بتسلم السجل الإلكتروني 1- إذا اتفق المنشئ مع المرسل إليه ، أو إذا طلب المنشئ من المرسل إليه ، عند أو قبل توجيه السجل الإلكتروني ، أن يرسل إقرارا بتسلم هذا السجل فإنه : أ - إذا لم يتضمن اتفاق المنشئ مع المرسل إليه أن يكون الإقرار بتسلم السجل الإلكتروني وفق شكل معين أو بطريقة معينة ، فإنه يجوز أن يتم الإقرار بتسلم هذا السجل عن طريق :- · أي إبلاغ من جانب المرسل إليه ، سواء كان بوسيلة أوتوماتيكية أو بأية وسيلة أخرى. · أي سلوك من جانب المرسل إليه يكفي لإعلام المنشئ بأن المرسل إليه قد تسلم السجل الإلكتروني . ب - إذا اشترط المنشئ أن يتلقى من المرسل إليه إقرارا بتسلم السجل الإلكتروني ، فإن للمنشئ أن يعتبر إرسال السجل الإلكتروني كأن لم يكن إلى أن يتم تسلم هذا الإقرار ، ما لم يتفق على خلاف ذلك . ج - إذا طلب المنشئ أن يتلقى إقرارا بتسلم السجل الإلكتروني من المرسل إليه دون أن يذكر أن السجل مشروط بتلقي هذا الإقرار خلال الوقت المحدد أو

المتفق عليه – أو خلال مدة معقولة إذا لم يتم تحديد وقت معين أو الاتفاق عليه – فإن للمنشئ أن يوجه إلى المرسل إليه إخطارا بأنه لم يتلق منه أي إقرار بالتسلم ، ويحدد له مدة معقولة يتعين خلالها تلقي هذا الإخطار ، فإن لم يرد الإقرار خلال هذه المدة ، جاز للمنشئ – بعد إخطار المرسل إليه – اعتبار إرسال السجل الإلكتروني كأن لم يكن، أو أن يتمسك بأية حقوق قد تكون له . 2 - في حالة تلقي المنشئ إقرارا بالتسلم من المرسل إليه ، فإنه يفترض – إلى أن يثبت العكس – تسلم المرسل إليه للسجل الإلكتروني ذي الصلة ، إلا أن هذا الافتراض لا يعني ضمناً تطابق السجل الإلكتروني الذي أرسل مع فحوى السجل الذي ورد . 3 - إذا تضمن الإقرار بالتسلم الذي تسلمه المنشئ أن السجل الإلكتروني ذا الصلة قد استوفى الاشتراطات الفنية ، سواء المتفق عليها أو المحددة في المعايير المعمول بها ، فإنه يفترض أن تلك الشروط قد تم استيفاؤها إلى أن يثبت العكس. 4- لا تنطبق أحكام هذه المادة إلا على إرسال السجل الإلكتروني أو تسلمه ، ولا يقصد بها معالجة أية آثار قانونية قد تترتب على السجل الإلكتروني أو على الإقرار بتسلمه .

مادة (15): وقت ومكان إرسال وتسلم السجلات الإلكترونية 1- ما لم يتفق المنشئ والمرسل إليه على غير ذلك ، يعتبر إرسال السجل الإلكتروني قد تم :- أ- وقت دخول هذا السجل في نظام للمعلومات لا يخضع لسيطرة المنشئ أو من أرسل السجل الإلكتروني نيابة عنه ، وذلك إذا كان كل من المنشئ والمرسل إليه لا يستخدم ذات نظام المعلومات. ب- وقت دخول هذا السجل حيز انتباه المرسل إليه وتمكنه من استخراجه ، وذلك إذا كان كل من المنشئ والمرسل إليه يستخدم ذات نظام المعلومات. 2- ما لم يتفق المنشئ والمرسل إليه على غير ذلك ، فإن وقت تسلم السجل الإلكتروني يحدد على النحو الآتي: - أ- إذا كان المرسل إليه قد عين نظام معلومات لغرض تسلم السجلات الإلكترونية ، فإن التسلم يعتبر قد تم: · وقت دخول السجل الإلكتروني نظام المعلومات المعين لهذا الغرض . · وقت دخول السجل الإلكتروني حيز انتباه المرسل إليه وتمكنه من استخراجه ، وذلك إذا أرسل السجل إلى نظام معلومات تابع للمرسل إليه غير النظام المعين لهذا الغرض . ب - إذا لم يعين المرسل إليه نظام معلومات ، فإن التسلم يقع وقت دخول السجل الإلكتروني نظام معلومات تابع للمرسل إليه . 3 - ما لم يتفق المنشئ والمرسل إليه على غير ذلك ، يعتبر السجل الإلكتروني مرسلاً من مقر عمل المنشئ ، ويعتبر مسلماً للمرسل إليه في مقر عمله . ولأغراض هذا البند فإنه : - أ- إذا كان للمنشئ أو المرسل إليه أكثر من مقر عمل ، فإنه يعتد بالمقر الأوثق علاقة بالمعاملة المعنية، أو مقر العمل الرئيسي إذا لم توجد معاملة تتعلق بالسجل . ب- إذا لم يكن للمنشئ أو المرسل إليه مقر عمل ، اعتبر محل الإقامة المعتاد للمنشئ أو المرسل إليه هو مقر عمل كل منهما . ج - لأغراض الفقرة السابقة ، يعتبر مقر إقامة الشخص الاعتباري هو المكان الذي أسس فيه.

مادة (16) : اعتماد مزودي خدمة الشهادات وإلغاء اعتمادهم -1 لمزود خدمة الشهادات أن يتقدم بطلب

بيانات إنشاء التوقيع ، وبيانات التحقق من صحة التوقيع تعملان بشكل متوافق ، وذلك إذا كان مزود خدمة الشهادات المعتمدة هو ذاته منشئ كل من البيانات المشار إليها . د- تسجيل أو نشر بيان بانتهاء أو إلغاء أو تعليق العمل بالشهادة المعتمدة ، طبقاً للقرارات التي تصدر في هذا الشأن تنفيذاً لأحكام هذا القانون . 2- تنتفي مسئولية مزود خدمة الشهادات المعتمد في أي من الحالات التالية : أ- إذا أثبت أنه لم يقع منه أي إهمال . ب- إذا كان الشخص الذي استند إلى الشهادة المعتمدة يعلم ، أو كان من شأنه أن يعلم بحسب المجرى العادي للأمور ، بأن الشهادة قد انتهى العمل بها أو ألغيت أو تم تعليق العمل بها ، أو أن اعتماد مزود خدمة الشهادات قد تم إلغاؤه . 3- لا يسأل مزود خدمة الشهادات المعتمد عن الأضرار الناشئة عن استعمال الشهادة المعتمدة خلافاً لما ورد بها من حدود وقيود – بما في ذلك القيود المتعلقة بقيمة المعاملات –إذا ما قام مزود الخدمة ببيان حدود وقيود استعمال هذه الشهادة على نحو يتحقق به علم الغير . ويستثني من ذلك حالة ما إذا كانت الأضرار ناشئة عن تغرير ، سواء تم عمدا أو نتيجة إهمال جسيم ، من مزود الخدمة .

مادة (19): مسئولية وسطاء الشبكات 1- لا يسأل وسيط الشبكة مدنياً أو جنائياً عن أية معلومات واردة في شكل سجلات إلكترونية - تخص الغير - إذا لم يكن هو مصدر هذه المعلومات واقتصر دوره على مجرد توفير إمكانية الدخول عليها ، وذلك إذا كانت المسئولية قائمة على :- أ - إنشاء أو نشر أو بث أو توزيع هذه المعلومات أو أية بيانات تتضمنها . ب- التعدي على أي حق من الحقوق الخاصة بتلك المعلومات . 2- يشترط لانتفاء مسئولية وسيط الشبكة استنادا إلى أحكام البند السابق ما يلي : أ- عدم علمه بأنه ينشأ عن هذه المعلومات أية مسئولية مدنية أو جنائية . ب- عدم علمه بأية وقائع أو ملابسات من شأنها أن تدل ، بحسب المجرى العادي للأمور ، على قيام مسئولية مدنية أو جنائية . ج- قيام وسيط الشبكة على الفور – في حالة علمه بما تقدم – بإزالة المعلومات من أي نظام للمعلومات تحت سيطرته ، ووقف توفير إمكانية الدخول على تلك المعلومات أو عرضها . 3- لا تفرض أحكام هذه المادة على وسيط الشبكة أي التزام قانوني بشأن مراقبة أية معلومات واردة في شكل سجلات إلكترونية تخص الغير – بغرض تحقق علم وسيط الشبكة بأن المعلومات ينشأ عنها مسئولية مدنية أو جنائية ، أو لتحقق علمه بأية وقائع أو ملابسات من شأنها أن تدل بحسب المجرى العادي للأمور على قيام هذه المسئولية – إذا اقتصر دور وسيط الشبكة على مجرد توفير إمكانية الدخول على هذه السجلات . 4- لا تخل أحكام هذه المادة بما يلي : أ- أية التزامات تنشأ عن أي عقد . ب -الالتزامات التي يفرضها أي تشريع بشأن تقديم خدمات الاتصالات اللاسلكية . ج -الالتزامات التي يفرضها أي تشريع آخر ، أو حكم قضائي واجب النفاذ ، بشأن تقييد أو منع أو إزالة أية معلومات واردة في شكل سجلات إلكترونية أو الحيلولة دون الدخول عليها . 5- في تطبيق أحكام هذه المادة يقصد بتوفير إمكانية الدخول على أية معلومات تخص الغير ، إتاحة الوسائل

إلى الوزارة للموافقة على اعتماده كمزود خدمة شهادات معتمد ، ويصدر قرار من الوزير بالموافقة على الاعتماد وإدراج مقدم الطلب في سجل " مزودي خدمة الشهادات المعتمدين " وذلك بعد التحقق من استيفاء الاشتراطات والمعايير المقررة في هذا الشأن ، بما في ذلك معايير التقييس الواجب استعمالها ، وينشر القرار في الجريدة الرسمية. ويستحق على الطلب وعلى منح الاعتماد رسم يصدر بتحديد فئاته قرار من الوزير بعد موافقة مجلس الوزراء . 2- للوزير إلغاء الاعتماد الممنوح لمزود خدمة الشهادات ، طبقاً لحكم البند السابق ، بقرار ينشر في الجريدة الرسمية ، وذلك إذا أصبح مزود الخدمة غير مستوفٍ للاشتراطات والمعايير المقررة . -3 يجب قبل إلغاء الاعتماد ، طبقاً لحكم البند السابق ، أن ترسل الوزارة إخطاراً كتابياً مسجلاً مصحوباً بعلم الوصول إلى مزود خدمة الشهادات المعتمد بشأن الإجراء المزمع اتخاذه حياله والأسباب المبررة لذلك. ولمزود الخدمة الاعتراض كتابة على ذلك خلال أربعة عشر يوماً من تاريخ تسلم الإخطار ، ويتم بحث أوجه الاعتراض والبت فيه خلال ثلاثين يوماً من تاريخ تقديمه. وفي جميع الأحوال ، يجب أن يصدر القرار بشأن قبول الاعتراض أو إلغاء الاعتماد - بحسب الأحوال - خلال خمسة وأربعين يوماً على الأكثر من تاريخ تسلم مزود الخدمة للإخطار المشار إليه . 4- يقصد بالاشتراطات والمعايير المقررة في هذه المادة ، تلك التي يصدر بها قرار من الوزير خلال فترة لا تجاوز أربعة أشهر من تاريخ العمل بأحكام هذا القانون . ولا يجوز أن تتضمن هذه المعايير اشتراط استعمال برمجيات أو أجهزة معينة . 4- يجوز إصدار الشهادات المعتمدة من قبل جهة حكومية يصدر بتسميتها للعمل كمزود لخدمة الشهادات المعتمدة وببيان المعايير التي يجب العمل بها وبالرسوم المستحقة على أداء خدماتها وبحالات الإعفاء منها قرار من مجلس الوزراء ، وينشر القرار في الجريدة الرسمية .

مادة (17) : اعتماد مزودي خدمة الشهادات الخارجيين وإلغاء اعتمادهم 1- للوزير بناءً على طلب من مزود خدمة الشهادات الذي يكون مقر نشاطه خارج مملكة البحرين أن يصدر قراراً باعتماد هذا المزود ، طبقاً للشروط والإجراءات المشار إليها في البند(1 (من المادة السابقة . 2- يراعى قبل منح الاعتماد طبقاً لحكم البند السابق ، أن يكون مزود خدمة الشهادات الخارجي مستوفياً للاشتراطات والمعايير المقررة لمزود خدمة الشهادات المعتمد . 3- للوزير إلغاء الاعتماد الممنوح لمزود خدمة الشهادات الخارجي بقرار ينشر في الجريدة الرسمية ، وذلك في الحالات وطبقاً للإجراءات والضمانات المنصوص عليها في البندين (2) و (3) من المادة السابقة .

مادة (18) : مسئولية مزودي خدمة الشهادات المعتمدين 1- يكون مزود خدمة الشهادات المعتمد مسئولاً قبل أي شخص استند بشكل معقول على شهادة أصدرها هذا المزود بشأن ما يلي : أ- دقة المعلومات الواردة بالشهادة المعتمدة وقت إصدارها . ب- ضمان أن الشخص المسمى في الشهادة المعتمدة كان وقت إصدارها حائزا لبيانات إنشاء التوقيع الإلكتروني ولبيانات التحقق من صحة هذا التوقيع . ج- ضمان أن

الفنية التي تمكن من الدخول على معلومات واردة في شكل سجلات إلكترونية تخص الغير ، أو بثها ، أو مجرد زيادة فاعلية البث ، ويشمل ذلك الحفظ التلقائي أو المرحلي أو المؤقت لهذه المعلومات بغرض إمكانية الدخول عليها . ويقصد بالغير فيما يخص وسيط الشبكة ، أي شخص ليس لوسيط الشبكة أية سيطرة فعلية عليه .

مادة (20): مستندات نقل البضائع 1- تسري أحكام هذه المادة بشأن أي إجراء يتعلق بعقد نقل البضائع ، بما في ذلك الآتي :- أ- الإخطار بعلامات أو عدد أو كمية أو وزن البضائع . ب- تحديد نوع البضائع أو قيمتها ، أو الإقرار بذلك . ج- إصدار إيصال بتسلم البضائع . د- إصدار تأكيد بأن البضائع قد تم تحميلها . هـ- إصدار تعليمات لناقل البضائع . و- المطالبة بتسليم البضائع . ز- الإذن بالإفراج عن البضائع . ح - الإخطار بفقد البضائع أو تلفها . ط- التعهد بتسليم البضائع إلى شخص معين أو إلى شخص مفوض بالمطالبة بالتسليم . ى- منح أو اكتساب أو نقل أو تداول أية حقوق بشأن البضائع ، أو التخلي أو التنازل عن أي من هذه الحقوق . ك- الإخطار بشروط عقد نقل البضائع . ل- الإخطار أو الإفادة بتنفيذ عقد نقل البضائع . م- اكتساب أو نقل الحقوق والالتزامات التي ينص عليها عقد نقل البضائع . 2- إذا تطلب القانون أن يتم أي إجراء مما نص عليه في البند السابق عن طريق مستند مكتوب ، فإن استيفاء ذلك من خلال استعمال سجل إلكتروني أو أكثر يفي بمتطلبات هذا القانون . 3- مع عدم الإخلال بنص البند السابق ، فإنه إذا اشترط القانون لمنح أي حق أو لإسناد أي التزام أن يتم من خلال استعمال أو تسليم مستند مكتوب ، فإن استيفاء ذلك من خلال استعمال سجل إلكتروني أو أكثر يفي بمتطلبات هذا القانون ، بشرط أن يتم إنشاء تلك السجلات بطريقة تضمن أن يكون الحق أو الالتزام مقصورا على الشخص المعني دون سواه . 4- يراعى بشأن تقدير مدى كفاءة طريقة إنشاء هذه السجلات في تحقيق الضمان المشار إليه في البند السابق ، الشروط التي اتفق عليها الأطراف ، وكافة الظروف والملابسات ، بما في ذلك الغرض الذي تم من أجله الإخطار بالحق أو الالتزام . 5- إذا استعمل سجل إلكتروني أو أكثر لأي من الإجراءات المنصوص عليها في الفقرتين (ي) أو(م) من البند(1) من هذه المادة ، فإنه لا يعتد بأي مستند خطي في هذا الشأن إلا إذا تحقق الشرطان الآتيان:- أ -العدول عن استعمال السجلات الإلكترونية بشأن ذلك الإجراء ، سواء تم ذلك بالاتفاق بين الأطراف المعنيين أو بإرادة أحدهم . ب- أن يتضمن المستند الخطي البديل ما يفيد العدول عن استعمال السجلات الإلكترونية في هذا الشأن . 6- لا يترتب على استبدال المستندات الخطية بسجلات إلكترونية ، على النحو المنصوص عليه في البند السابق ، التأثير على أي من حقوق أو التزامات الأطراف المعنيين . 7- لا يترتب على مجرد ورود عقد نقل البضائع في سجل إلكتروني أو أكثر ، أو ثبوته عن طريق سجل إلكتروني أو أكثر ، بدلاً من المستندات الورقية ، المساس بأحكام القوانين ذات العلاقة بعقد النقل وسريانها على هذا العقد .

مادة (21): تسجيل أسماء النطاق 1 - لوزير المواصلات أن يصدر قراراً بتنظيم تسجيل واستعمال اسم النطاق لمملكة البحرين (bh) والترخيص باستعماله أو حظر ذلك، بعد أخذ رأي وزير التجارة والصناعة وأي شخص يكون من المناسب استطلاع رأيه في هذا الشأن ، بما في ذلك مؤسسة الإنترنت للأسماء والأرقام المعينة . (Internet Corporation for Assigned Names and Numbers)

2 - يجوز أن يتضمن القرار الصادر بتنظيم تسجيل واستعمال إسم النطاق ما يلي -: أ- إنشاء مكتب لتسجيل إسم النطاق يتبع وزارة المواصلات . ب- البيانات التي يتضمنها طلب التسجيل . ج- مدة سريان التسجيل . د- الشروط والإجراءات والمدة المتعلقة بإعادة التسجيل . هـ- الشروط والإجراءات المتعلقة بمنح التسجيل . و- إجراءات التظلم من القرارات الصادرة من مكتب تسجيل إسم النطاق . ز - تحديد فئات الرسوم المستحقة على طلب التسجيل أو تجديده أو إعادة التسجيل ، وطريقة سداد هذه الرسوم ، بعد موافقة مجلس الوزراء . ح- أية مسائل أخرى متعلقة بالتسجيل . 3- يقصد باسم النطاق (bh) فيما يتعلق بتطبيق أحكام هذه المادة ، المستوى العلوي للنظام العالمي لاسم النطاق المعين لمملكة البحرين ، والذي يتكون من حرفين وفقا للمعيار الدولي أيزو 1- 3166 (رموز تمثيل أسماء البلدان وتقسيماتها الفرعية) الخاص بالمنظمة الدولية للتقييس .

مادة (22): الطعن في صحة السجلات والتوقيعات الإلكترونية 1- لصاحب المصلحة الطعن بالتزوير في السجلات الإلكترونية والتوقيع الإلكتروني عليها ، والطعن ببطلان استعمال هذا التوقيع ، إذا تم ذلك بدون تفويض من صاحب الحق ، أو لغير ذلك من أسباب البطلان المقررة قانوناً في شأن التوقيع الخطي .

2- تفصل المحكمة المختصة في الطعون المشار إليها في البند السابق ، أو الدفوع المتعلقة بشأنها، طبقاً للإجراءات وقواعد الإثبات المقررة قانوناً ، وبما يتفق وطبيعة السجلات والتوقيعات الإلكترونية وفقا للأحكام المنصوص عليها في هذا القانون .

مادة (23): سلطة التفتيش في حالة وجود دلائل كافية على استغلال أي محل في ارتكاب أي من الجرائم المنصوص عليها في هذا القانون ، فإنه يجوز إجراء تفتيش لهذا المحل وللمشتبه فيهم من الموجودين فيه ، وضبط الأشياء الموجودة فيه والتي يشتبه في صلتها بالجريمة ، وكل ما يفيد في كشف الحقيقة طبقاً للإجراءات والشروط المنصوص عليها في قانون أصول المحاكمات الجزائية لعام 1966 وتعديلاته . ويجوز الاستعانة أثناء التفتيش والضبط بموظفي وزارة التجارة والصناعة المختصين ، للاستفادة بخبرتهم الفنية في هذا الشأن .

مادة (24): العقوبات 1 - مع عدم الإخلال بأية عقوبة أشد ينص عليها أي قانون آخر ، يعاقب بالسجن مدة لا تزيد على عشر سنوات ، وبغرامة لا تجاوز مائة ألف دينار أو بإحدى هاتين العقوبتين كل من ارتكب عمدا فعلا من الأفعال الآتية : أ- نسخ أو حيازة أو إعادة تكوين أداة إنشاء توقيع إلكتروني لشخص

آخر أو الدخول على أداة إنشاء هذا التوقيع دون تفويض بذلك من هذا الشخص ، وبسوء نية . ب- تحريف أو تغيير أو استعمال أو إفشاء أداة إنشاء توقيع إلكتروني لشخص آخر دون تفويض منه بذلك ، أو بما يجاوز حدود هذا التفويض . ج- إنشاء أو نشر أو تحريف أو استعمال شهادة ، أو توقيع إلكتروني لغرض احتيالي أو لأي غرض غير مشروع . د- انتحال هوية شخص آخر ، أو الإدعاء زورا بأنه مفوض من قبله في طلب الحصول على شهادة أو قبولها ، أو طلب تعليق العمل بها أو إلغائها . هـ - نشر شهادة أو وضعها في متناول أي شخص ، يحتمل أن يعتمد عليها أو على توقيع إلكتروني وارد بها من خلال الاستناد لأية بيانات مدرجة بهذه الشهادة مثل الرموز أو كلمات السر أو الغوريثمات أو مفاتيح التشفير العامة أو أية بيانات تستعمل لأغراض التحقق من صحة التوقيع الإلكتروني ، إذا كان من ارتكب ذلك الفعل على علم بأي من الآتي :- ـ عدم إصدار الشهادة من قبل مزود خدمة الشهادات المدون في تلك الشهادة . ـ عدم قبول الشهادة من قبل صاحبها المدون بها . ـ إلغاء الشهادة أو وقف العمل بها ، بشرط ألا يكون نشر الشهادة أو وضعها في متناول الجمهور قد تم بغرض تمكين الغير من التحقق من صحة توقيع إلكتروني تم إنشاؤه قبل إلغاء الشهادة أو وقف العمل بها أو لغرض الإخطار بالإلغاء أو الوقف .

2 - مع عدم الإخلال بأية عقوبة أشد ينص عليها أي قانون آخر ، يعاقب بالحبس مدة لا تزيد على ثلاث سنوات ، وبغرامة لا تجاوز عشرة آلاف دينار أو بإحدى هاتين العقوبتين ، كل شخص منع عمدا أحد رجال الضبط القضائي أو المأذون بالاستعانة بهم في إجراء التفتيش ، أو حال دون قيام أي منهم بالأعمال المنصوص عليها في المادة (23) من هذا القانون .

مادة (25): مسئولية الشخص الاعتباري وموظفيه يسأل الشخص الاعتباري جنائيا ويعاقب بالغرامة التي لا تجاوز مائتي ألف دينار ، إذا ارتكبت أي من الجرائم المنصوص عليها في هذا القانون باسمه أو لحسابه أو باستعمال إحدى وسائله ، وكان ذلك نتيجة تصرف أو إهمال جسيم أو موافقة أو تستر من أي عضو مجلس إدارة أو مدير أو أي مسئول آخر - في ذلك الشخص الاعتباري - أو ممن يتصرف بهذه الصفة . ويعد مرتكبا للجريمة كل من أسند إليه من هؤلاء الأشخاص الطبيعيين ارتكاب أي من الأفعال المذكورة، ويعاقب بالعقوبة المقررة لها طبقا لأحكام هذا القانون .

مادة (26): القرارات يصدر الوزير – في غير المسائل التي عقد الاختصاص بشأنها لجهة أخرى – القرارات التنفيذية اللازمة لتنفيذ أحكام هذا القانون بما في ذلك ما يلي :- أ- تحديد الاشتراطات والمعايير المتعلقة باعتماد مزودي خدمة الشهادات لإصدار الشهادات المعتمدة . ب- تحديد فئات الرسوم المستحقة على الطلبات والخدمات المنصوص عليها في المادتين (16) و (17) من هذا القانون ، بعد موافقة مجلس الوزراء . ج -تنظيم كافة المسائل التي تدخل في اختصاصه طبقاً لأحكام هذا القانون . وتنشر هذه القرارات في الجريدة الرسمية .

مادة (27): نفاذ أحكام القانون على الوزراء - كل فيما يخصه - تنفيذ أحكام هذا القانون ، ويُعمل به من أول الشهر التالي لمضي ستين يوما من تاريخ نشره في الجريدة الرسمية . ملك مملكة البحرين حمد بن عيسى آل خليفة رئيس مجلس الوزراء خليفة بن سلمان آل خليفة صدر في قصر الدفاع : بتاريخ 7 رجب 423 هـ الموافق 14 سبتمبر 2002 م

ملحق رقم 4

النص الكامل لقانون امارة دبي الخاص بالمبادلات والتجارة الالكترونية:

أصدر الشيخ مكتوم بن راشد آل مكتوم نائب رئيس دولة الامارات رئيس مجلس الوزراء بصفته حاكماً لامارة دبي القانون رقم (2) لسنة 2002 بشأن المعاملات والتجارة الالكترونية والذي جاء في مقدمته انه تحقيقاً لتوجه حكومة دبي باحلال وسائل التقنية الحديثة في المعاملات والتبادل التجاري فقد قررنا اصدار هذا القانون الذي يتألف من (39) مادة ويسمى «قانون المعاملات والتجارة الالكترونية».

قانون رقم (2) لسنة 2002 بشأن المعاملات والتجارة الالكترونية نحن مكتوم بن راشد آل مكتوم حاكم دبي تحقيقاً لتوجه حكومة دبي باحلال وسائل التقنية الحديثة في المعاملات والتبادل التجاري، نقرر اصدار القانون الآتي:

الفصل الاول: تعريفات مادة (1) يسمى هذا القانون «قانون المعاملات والتجارة الالكترونية رقم (2) لسنة 2002 «مادة (2) يكون للكلمات والعبارات التالية المعاني المبينة ازاء كل منها ما لم يقتض سياق النص خلاف ذلك: الحكومة ـ حكومة دبي، وتشمل الدوائر الحكومية والمؤسسات والهيئات العامة التابعة لها.

الامارة ـ امارة دبي.

الرئيس ـ رئيس سلطة منطقة دبي الحرة للتكنولوجيا والتجارة الالكترونية والاعلام.

الكتروني ـ ما يتصل بالتكنولوجيا الحديثة وذو قدرات كهربائية او رقمية او مغناطيسية او لاسلكية او بصرية او كهرومغناطيسية او مؤتمتة او ضوئية او ما شابه ذلك.

المعلومات الالكترونية ـ معلومات ذات خصائص الكترونية في شكل نصوص او رموز او اصوات او رسوم او صور او برامج حاسب آلي او غيرها من قواعد البيانات.

نظام المعلومات الالكتروني ـ نظام الكتروني لانشاء او استخراج او ارسال او استلام او تخزين او عرض او معالجة المعلومات او الرسائل الكترونياً.

«سجل» او» مستند» الكتروني ـ سجل او مستند يتم انشاؤه او تخزينه او استخراجه او نسخه او ارسالة او ابلاغه او استلامه بوسيلة الكترونية، على وسيط ملموس او على اي وسيط الكتروني اخر، ويكون قابلاً للاسترجاع بشكل يمكن فهمه.

الحاسب الآلي ـ جهاز الكتروني يتعامل مع المعلومات والبيانات بتحليلها وبرمجتها واظهارها وحفظها

وارسالها واستلامها بواسطة برامج وانظمة معلومات الكترونية، ويمكن ان يعمل بشكل مستقل او بالاتصال مع اجهزة او انظمة الكترونية اخرى. المنشئ ـ الشخص الطبيعي او المعنوي الذي يقوم او يتم بالنيابة عنه ارسال الرسالة الالكترونية ايا كانت الحالة، ولا يعتبر منشأ الجهة التي تقوم بمهمة مزود خدمات فيما يتعلق بانتاج او معالجة او ارسال او حفظ تلك الرسالة الالكترونية وغير ذلك من الخدمات المتعلقة بها .

المرسل اليه ـ الشخص الطبيعي او المعنوي الذي قصد منشئ الرسالة توجيه رسالته اليه، ولا يعتبر مرسلا اليه الشخص الذي يقوم بتزويد الخدمات فيما يتعلق باستقبال او معالجة او حفظ المراسلات الالكترونية وغير ذلك من الخدمات المتعلقة بها.

برنامج الحاسب الآلي ـ مجموعة بيانات او تعليمات تستعمل بطريقة مباشرة او غير مباشرة في نظام معالجة معلومات الكترونية لغرض ايجاد او الوصول الى نتائج محددة.

الرسالة الالكترونية ـ معلومات الكترونية ترسل او تستلم بوسائل الكترونية ايا كانت وسيلة استخراجها في المكان المستلمة فيه.

المراسلة الالكترونية ـ ارسال واستلام الرسائل الالكترونية.

التوقيع الالكتروني ـ توقيع مكون من حروف او ارقام او رموز او صوت او نظام معالجة ذي شكل الكتروني وملحق او مرتبط منطقياً برسالة الكترونية وممهور بنية توثيق او اعتماد تلك الرسالة.

التوقيع الالكتروني المحمي ـ التوقيع الالكتروني المستوفي لشروط المادة (20) من هذا القانون.

الموقع ـ الشخص الطبيعي او المعنوي الحائز لاداة توقيع الكتروني خاصة به ويقوم بالتوقيع او يتم التوقيع بالنيابة عنه على الرسالة الالكترونية باستخدام هذه الاداة.

اداة التوقيع ـ جهاز او معلومات الكترونية معدة بشكل فريد لتعمل بشكل مستقل او بالاشتراك مع اجهزة ومعلومات الكترونية اخرى على وضع توقيع الكتروني لشخص معين، وتشمل هذه العملية اية انظمة او اجهزة تنتج او تلتقط معلومات فريدة مثل رموز او مناهج حسابية او حروف او ارقام او مفاتيح خصوصية او ارقام تعريف الشخصية او خواص شخصية.

الوسيط الالكتروني المؤتمن ـ برنامج او نظام الكتروني لحاسب آلي يمكن ان يتصرف او يستجيب لتصرف بشكل مستقل، كلياً او جزئياً، دون اشراف اي شخص طبيعي في الوقت الذي يتم فيه التصرف او الاستجابة له.

المعاملات الالكترونية المؤتمنة ـ معاملات يتم ابرامها او تنفيذها بشكل كلي او جزئي بواسطة وسائل او سجلات الكترونية، والتي لا تكون فيها هذه الاعمال او السجلات خاضعة لأية متابعة او مراجعة من قبل شخص طبيعي، كما في السياق العادي لانشاء وتنفيذ العقود والمعاملات.

مزود خدمات التصديق ـ اي شخص او جهة معتمدة او معترف بها تقوم باصدار شهادات تصديق الكترونية او اية خدمات او مهمات متعلقة بها وبالتواقيع الالكترونية والمنظمة بموجب احكام الفصل الخامس من هذا القانون.

شهادة المصادقة الالكترونية ـ شهادة يصدرها مزود خدمات التصديق يفيد فيها تأكيد هوية الشخص او الجهة الحائزة على اداة توقيع معينة، ويشار اليها في هذا القانون بـ «الشهادة».

اجراءات التوثيق المحكمة ـ الاجراءات التي تهدف الى التحقق من ان رسالة الالكترونية قد صدرت من شخص معين، والكشف عن اي خطأ او تعديل في محتويات او في نقل او تخزين رسالة الكترونية او سجل الكتروني خلال فترة زمنية محددة، ويشمل ذلك اي اجراء يستخدم مناهج حسابية او رموز او كلمات او ارقام تعريفية او تشفير او اجراءات للرد او لاقرار الاستلام وغيرها من وسائل اجراءات حماية المعلومات.

الطرف المعتمد ـ الشخص الذي يتصرف بالاعتماد على شهادة او توقيع الكتروني.

المعاملات الالكترونية ـ اي تعامل او عقد او اتفاقية يتم ابرامها او تنفيذها بشكل كلي او جزئي بواسطة المراسلات الالكترونية.

التجارة الالكترونية ـ المعاملات التجارية التي تتم بواسطة المراسلات الالكترونية .

مادة (3): يفسر هذا القانون طبقاً لما هو معقول في المعاملات والتجارة الالكترونية وبما يؤدي الى تحقيق الاهداف التالية: (1) تسهيل المراسلات الالكترونية بواسطة سجلات الكترونية يعول عليها.

(2) تسهيل وازالة اية عوائق امام التجارة الالكترونية والمعاملات الالكترونية الاخرى والتي قد تنتج عن الغموض المتعلق بمتطلبات الكتابة والتوقيع، ولتعزيز تطور البنية التحتية القانونية والتجارية لتطبيق التجارة الالكترونية بصورة مضمونة.

(3) تسهيل نقل المستندات الالكترونية الى الجهات والمؤسسات الحكومية وتعزيز توفير خدمات هذه الجهات والمؤسسات بكفاءة عن طريق مراسلات الكترونية يعول عليها.

(4 (التقليل من حالات تزوير المراسلات الالكترونية والتعديلات اللاحقة على تلك المراسلات ومن فرص الاحتيال في التجارة الالكترونية والمعاملات الالكترونية الاخرى .

(5) ارساء مبادئ موحدة للقواعد واللوائح والمعايير المتعلقة بتوثيق وسلامة المراسلات الالكترونية.

(6)تعزيز ثقة الجمهور في سلامة وصحة المعاملات والمراسلات والسجلات الالكترونية.

(7) تعزيز تطوير التجارة الالكترونية والمعاملات الاخرى على الصعيدين المحلي والعالمي وذلك عن طريق استخدام تواقيع الكترونية.

المادة (4): يراعى عند تطبيق احكام هذا القانون قواعد العُرف التجاري الدولي ذات العلاقة بالمعاملات والتجارة الالكترونية ودرجة التقدم في تقنية تبادلها.

مادة (5): (1) يسري هذا القانون على السجلات والتواقيع الالكترونية ذات العلاقة بالمعاملات والتجارة الالكترونية، ويستثنى من احكام هذا القانون ما يلي: (أ) المعاملات والأمور المتعلقة بالاحوال الشخصية كالزواج والطلاق والوصايا.

)ب) سندات ملكية الاموال غير المنقولة.

)ج) السندات القابلة للتداول.

(د) المعاملات التي تتعلق ببيع وشراء الاموال غير المنقولة والتصرف فيها وتأجيرها لمدد تزيد على عشر سنوات وتسجيل اية حقوق اخرى متعلقة بها.

(ه) اي مستند يتطلب القانون تصديقه امام الكاتب العدل.

(2) للرئيس بقرار يصدره ان يضيف اية معاملات او امور اخرى لما هو وارد في الفقرة (1) من هذه المادة، او ان يحذف منها او يعدل فيها.

مادة (6) :(1 (ليس في هذا القانون ما يتطلب من شخص ان يستخدم او يقبل معلومات بشكل الكتروني، الا انه يجوز استنتاج موافقة الشخص من سلوكه الايجابي.

(2) يجوز ان يتفق الاطراف الذين لهم علاقة بانشاء او ارسال او استلام او تخزين او معالجة اية سجلات الكترونية، على التعاقد بصورة مغايرة لأي من الاحكام الواردة في الفصل الثاني حتى الفصل الرابع من هذا القانون.

(3)استثناء من احكام الفقرة (1) السابقة، يجب ان يكون صريحاً قبول الحكومة بالتعامل الالكتروني في المعاملات التي تكون طرفاً فيها.

الفصل الثاني متطلبات المعاملات الالكترونية:

مادة (7) :(1) لاتفقد الرسالة الالكترونية أثرها القانوني أو قابليتها للتنفيذ لمجرد انها جاءت في شكل الكتروني.

(2)لاتفقد المعلومات التي تشير اليها الرسالة الالكترونية دون تفصيل أثرها القانوني أو قابليتها للتنفيذ، متى كان الاطلاع على تفاصيل تلك المعلومات متاحاً ضمن النظام الالكتروني الخاص بمرسلها، وتمت الاشارة الى كيفية الاطلاع عليها.

مادة (8): (1) اذا اشترط القانون حفظ مستند أو سجل أو معلومات لأي سبب، فان هذا الشرط يتحقق عندما يتم حفظ ذلك المستند أو السجل أو المعلومات في شكل سجل الكتروني، شريطة مراعاة ما يلي: (أ) حفظ السجل الالكتروني بالشكل الذي انشيء أو أرسل أو استلم به، أو بشكل يمكن من اثبات انه يمثل بدقة المعلومات التي انشئت أو أرسلت أو استلمت في الاصل.

(ب) بقاء المعلومات محفوظة على نحو يتيح استخدامها والرجوع اليها لاحقا.

)ج) حفظ المعلومات ان وجدت التي تمكن من استبانه منشأ الرسالة الالكترونة وجهة وصولها وتاريخ ووقت ارسالها واستلامها.

(2) لايمتد الالتزام بحفظ المستندات أو السجلات أو المعلومات وفقا للفقرة (1) - (ج) من هذه المادة الى أية معلومات تنشأ بصورة ضرورية وتلقائية للتمكين من ارسال أو استلام السجل.

(3)يجوز لأي شخص استيفاء المتطلبات المنصوص عليها في الفقرة (1) من هذه المادة بالاستعانة بخدمات أي شخص آخر، طالما التزم بالشروط المنصوص عليها في تلك الفقرة.

(4) ليس في هذه المادة ما يؤثر على ما يلي: (أ) أي قانون آخر ينص صراحة على الاحتفاظ بالمستندات أو السجلات أو المعلومات في شكل سجلات الكترونية وفق نظام معلومات الكتروني معين أو باتباع اجراءات معينة، أو الحفظ أو المراسلة عبر وسيط الكتروني.

(ب) حرية الحكومة في تحديد متطلبات اضافية للاحتفاظ بسجلات الكترونة تخضع لاختصاصها.

مادة (9): اذا اشترط القانون ان يكون خطياً أي بيان أو مستند أو سجل أو معاملة أو بينة أو نص على ترتيب نتائج معينة في غياب ذلك، فان المستند أو السجل الالكترون يستوفي هذا الشرط طالما تم الالتزام بأحكام الفقرة (1) من المادة السابقة.

مادة (10): (1) اذا اشترط القانون وجود توقيع على مستند أو نص على ترتيب نتائج معينة في غياب ذلك، فان التوقيع الالكتروني الذي يعول عليه في اطار المعنى الوارد في المادة (20) من هذا القانون يستوفي ذلك الشرط.

(2) يجوز لأي شخص ان يستخدم أي شكل من أشكال التوثيق الالكتروني، إلا اذا نص القانون بغير ذلك.

مادة (11): يكون المستند أو السجل الالكتروني أصلياً، عندما تستخدم بشأنه وسيلة: (1) توفر ما يعول عليه فنياً للتأكد من سلامة المعلومات الواردة في ذلك المستند أو السجل من الوقت الذي انشيء فيه للمرة

الأولى بشكله النهائي كمستند أو سجل الكتروني.

(2) وتسمح بعرض المعلومات المطلوب تقديمها متى طلب ذلك.

مادة (12): (1) لايحول دون قبول الرسالة الالكترونية أو التوقيع الالكتروني كدليل اثبات: (أ) لمجرد ان الرسالة أو التوقيع قد جاء في شكل الكتروني.

) ب) لمجرد ان الرسالة أو التوقيع ليس أصلياً أو في شكله الاصلي، وذلك اذا كانت هذه الرسالة أو التوقيع الالكتروني أفضل دليل يتوقع بدرجة معقولة ان يحصل عليه الشخص الذي يستشهد به.

(3) يكون للمعلومات الالكترونية ما تستحقه من حجية في الاثبات، وفي تقدير هذه الحجية يعطي الاعتبار لما يلي: (أ) مدى امكانية التعويل على الطريقة التي تم بها تنفيذ واحدة أو أكثر من عمليات الادخال أو الانشاء أو التجهيز أو التخزين أو التقديم أو الارسال.

)ب) مدى امكانية التعويل على الطريقة التي استخدمت في المحافظة على سلامة المعلومات.

(ج) مدى امكانية التعويل على مصدر المعلومات اذا كان معروفاً.

)د) مدى امكانية التعويل على الطريقة التي تم بها التأكد من هوية المنشيء، اذا كان ذلك ذا صلة.

(ه) أي عامل آخر يتصل بالموضوع.

(3)في غياب البينة المناقضة، يفترض ان التوقيع الالكتروني المحمي: (أ) يمكن التعويل عليه.

)ب) هو توقيع الشخص الذي تكون له صلة به.

)ج) قد وضعه ذلك الشخص بنية توقيع أو اعتماد الرسالة الالكترونية التي ألحقت أو اقترنت به بصورة منطقية.

(4) في غياب البينة المناقضة يفترض ان السجل الالكتروني المحمي: (أ) لم يتغير منذ ان انشيء.

) ب) معول عليه.

الفصل الثالث : المعاملات الالكترونية ـ انشاء العقود وصحتها

مادة (13): (1) لأغراض التعاقد يجوز التعبير عن الايجاب والقبول جزئياً أو كلياً بواسطة المراسلة الالكترونية.

(2) لايفقد العقد صحته أو قابليته للتنفيذ لمجرد انه تم بواسطة مراسلة الكترونية واحدة أو أكثر.

مادة (14) (1) يجوز ان يتم التعاقد بين وسائط الكترونية مؤتمتة متضمنة نظامي معلومات الكترونية أو أكثر تكون معدة ومبرمجة مسبقاً للقيام بمثل هذه المهمات، ويتم التعاقد صحيحاً ونافذاً ومنتجاً آثاره

القانونية على الرغم من عدم التدخل الشخصي أو المباشر لأي شخص طبيعي في عملية إبرام العقد في هذه الانظمة.

(2)كما يجوز ان يتم التعاقد بين نظام معلومات الكتروني مؤتمت يعود الى شخص طبيعي أو معنوي وبين شخص طبيعي اذا كان الأخير يعلم أو من المفترض ان يعلم ان ذلك النظام سيتولى مهمة إبرام العقد أو تنفيذه.

مادة (15): (1) تعتبر الرسالة الالكترونية صادرة عن المنشيء اذا كان المنشيء هو الذي أصدرها بنفسه.

(2)في العلاقة بين المنشيء والمرسل اليه، تعتبر الرسالة الالكترونية أنها صادرة عن المنشيء اذا أرسلت) :أ) من شخص له صلاحية التصرف نيابة عن المنشيء فيما يتعلق بالرسالة الالكترونية، أو.

(ب) من نظام معلومات مؤتمت ومبرمج للعمل تلقائياً من قبل المنشيء أو نيابة عنه.

(3)في العلاقة بين المنشيء والمرسل اليه، يحق للمرسل اليه ان يعتبر الرسالة الالكترونية قد صدرت عن المنشيء، وان يتصرف على أساس هذا الافتراض، اذا: (أ) طبق المرسل اليه تطبيقاً سليماً، اجراء سبق ان وافق عليه المنشيء من اجل التأكد من ان الرسالة الالكترونية قد صدرت عن المنشيء لهذا الغرض، أو (ب) كانت الرسالة الالكترونية، كما تسلمها المرسل اليه، ناتجة عن تصرفات شخص تمكن بحكم علاقته بالمنشيء أو بأي وكيل للمنشيء من الوصول الى طريقة يستخدمها المنشيء لاثبات ان الرسالة الالكترونية صادرة عنه.

(4) لا تسري احكام الفقرة (3) السابقة في الحالات التالية: (أ) اعتبارا من الوقت الذي تسلم فيه المرسل اليه اشعارا من المنشيء يفيد بأن الرسالة الالكترونية لم تصدر عنه، ويكون قد أتيح للمرسل اليه وقت للتصرف على هذا الأساس.

)ب) اذا عرف المرسل اليه أو كان يفترض فيه ان يعرف ان الرسالة الالكترونية لم تصدر عن المنشئ، وذلك اذا ما بذل عناية معقولة أو استخدام اي اجراء متفق عليه.

(ج) اذا كان من غير المعقول للمرسل اليه ان يعتبر الرسالة الالكترونية صادرة عن المنشيء أو ان يتصرف على أساس هذا الافتراض.

(5)عندما تكون الرسالة الالكترونية صادرة أو تعتبر أنها صادرة عن المنشيء أو عندما يكون من حق المرسل اليه ان يتصرف على أساس هذا الافتراض وفقاً للفقرات(1) ، (2)، (3)من هذه المادة، يحق عندئذ للمرسل اليه في اطار العلاقة بينه وبين المنشيء ان يعتبر ان الرسالة الالكترونية المستلمة هي الرسالة التي قصد المنشيء ان يرسلها، وأن يتصرف على هذا الاساس.

(6) يكون للمرسل اليه الحق في ان يعتبر كل رسالة الكترونية يستلمها على أنها رسالة مستقلة وان يتصرف على أساس هذا الافتراض وحده، ولاتنطبق الفقرة (7) من هذه المادة متى عرف المرسل اليه أو كان عليه ان يعرف، اذا بذل عناية معقولة أو استخدام اي اجراء متفق عليه، ان الرسالة الالكترونية كانت نسخة ثانية.

(7) لايكون للمرسل اليه الحق في الافتراضات والاستنتاجات الواردة في الفقرتين السابقتين (5)، (6)، متى عرف أو كان عليه ان يعرف اذا بذل عناية معقولة أو استخدام اجراء متفقاً عليه بأن البث أسفر عن أي خطأ في الرسالة الالكترونية كما استلمها.

مادة (16): (1) تنطبق الفقرات (2)، (3)،(4) ، من هذه المادة عندما يكون المنشيء قد طلب من المرسل اليه أو اتفق معه، عند أو قبل توجيه الرسالة الالكترونية، أو في تلك الرسالة، توجيه اقرار باستلامها.

(2) اذا لم يكن المنشيء قد اتفق مع المرسل اليه على ان يكون الاقرار بالاستلام وفق شكل معين أو بطريقة معينة، يجوز الاقرار بالاستلام عن طريق: (أ) أية رسالة من جانب المرسل اليه، سواء كانت بوسيلة الكترونية أو مؤتمتة أو بأية وسيلة اخرى، أو (ب) أي سلوك من جانب المرسل اليه، وذلك بما يكفي لاعلام المنشيء باستلام الرسالة الالكترونية.

(3) اذا كان المنشيء قد ذكر ان الرسالة الالكترونية مشروطة بتلقي إقرار بالاستلام، تعامل هذه الرسالة فيما يتعلق بترتيب حقوق أو التزامات قانونية بين المنشيء والمرسل اليه كأنها لم ترسل وذلك الى حين استلام المنشيء للإقرار .

(4) اذا لم يكن المنشيء قد ذكر ان الرسالة الالكترونية مشروطة بتلقي إقرار بالاستلام ولم يتلق المنشيء ذلك الاقرار في غضون الوقت المحدد أو المتفق عليه، أو في غضون مدة معقولة، اذا لم يكن قد تم تحديد وقت معين أو متفق عليه، فان للمنشيء: (أ) ان يوجه الى المرسل اليه اشعارا يذكر فيه انه لم يتلق أي إقرار بالاستلام ويحدد فيه وقتاً معقولاً يتعين في غضونه تلقي الاقرار.

) ب) اذا لم يرد الاقرار بالاستلام في غضون الوقت المحدد في الفقرة 4 (أ) السابقة، وبعد توجيه اشعار الى المرسل اليه، ان يعامل الرسالة الالكترونية وكأنها لم ترسل، أو ان يلجأ الى ممارسة أية حقوق اخرى قد تكون له.

(5) يفترض عندما يتلقى المنشيء إقرارا بالاستلام من المرسل اليه ان الأخير قد استلم الرسالة الالكترونية ذات الصلة، إلا اذا قدم دليلاً مناقضاً لذلك، ولا ينطوي هذا الافتراض ضمناً على ان الرسالة الالكترونية التي أرسلت من المنشيء تتطابق وفحوى الرسالة التي وردت اليه من المرسل اليه.

(6) عندما ينص الاقرار بالاستلام الذي يرد الى المنشيء على ان الرسالة الالكترونية ذات الصلة قد استوفت الشروط الفنية، سواء المتفق عليها أو المحددة في المعايير المعمول بها، فانه يفترض ما لم يثبت العكس، ان تلك الشروط قد استوفيت.

(7) باستثناء ما تعلق بارسال أو استلام الرسالة الالكترونية، فان هذه المادة لاتسري على الاثار القانونية التي قد تنتج عن الرسالة الالكترونية أو الاقرار بالاستلام.

مادة (17) :(1) ما لم يتفق المنشيء والمرسل اليه على خلاف ذلك: (أ) يقع ارسال الرسالة الالكترونية عندما تدخل الرسالة نظام معلومات لايخضع لسيطرة المنشيء أو الشخص الذي ارسل الرسالة نيابة عن المنشيء.

(ب (يتحدد وقت استلام الرسالة الالكترونية على النحو التالي: (1) اذا كان المرسل اليه قد عين نظام معلومات لغرض استلام الرسالة الالكترونية يتم الاستلام: (أ) وقت دخول الرسالة الالكترونية نظام المعلومات المعين، أو (ب) وقت استخراج المرسل اليه الرسالة الالكترونية اذا ارسلت الى نظام معلومات تابع له، ولكن ليس هو نظام المعلومات المعين لاستقبال الرسالة.

(2) اذا لم يعين المرسل اليه نظام معلومات، يقع الاستلام عندما تدخل الرسالة الالكترونية نظام معلومات تابع للمرسل اليه.

(2)تنطبق الفقرة (1) - (ب) من هذه المادة على الرغم من كون المكان الذي يوجد فيه نظام المعلومات يختلف عن المكان الذي يعتبر ان الرسالة الالكترونية استلمت فيه بموجب الفقرة (3) أدناه.

(3)ما لم يتفق المنشيء والمرسل اليه على خلاف ذلك، تعتبر الرسالة الالكترونية قد أرسلت من المكان الذي يقع فيه مقر عمل المنشيء وأنما استلمت في المكان الذي يقع فيه مقر عمل المرسل اليه.

(4 (لاغراض هذه المادة: (أ) اذا كان للمنشئ او المرسل اليه اكثر من مقر عمل واحد، يكون مقر العمل هو المقر الاوثق علاقة بالمعاملة المعنية، او مقر العمل الرئيسي اذا لم توجد مثل هذه المعاملة.

(ب) اذا لم يكن للمنشئ او المرسل اليه مقر عمل، يشار الى محل اقامته المعتاد.

(ج) «مقر الاقامة المعتاد»، فيما يتعلق بالشخص الاعتباري، يعني مقره الرئيسي او المقر الذي تأسس فيه.

مادة (18) (لا تنطبق المواد (15)، (16)، (17) من هذا القانون، على الحالات التي قد يحددها الرئيس بموجب قرار او لائحة او نظام يصدره.

الفصل الرابع : **السجلات والتوقيعات الالكترونية المحمية**

مادة (19) : (1) اذا تم بطريقة صحيحة تطبيق اجراءات توثيق محكمة، منصوص عليها في القانون او

معقولة تجارياً ومتفق عليها بين الطرفين، على سجل الكتروني للتحقق من انه لم يتم تغييره منذ وقت معين من الزمن، فإن هذا السجل يعامل كسجل الكتروني محمي منذ ذلك الوقت الى الوقت الذي تم فيه التحقق.

(2) لاغراض هذه المادة والمادة (20) من هذا القانون، ولتقرير ما اذا كانت اجراءات التوثيق المحكمة معقولة تجارياً، ينظر لتلك الاجراءات والظروف التجارية في وقت استخدامها بما في ذلك: (أ) طبيعة المعاملة.

(ب) معرفة ومهارة الاطراف.

)ج) حجم المعاملات المماثلة التي قام بها اي من الطرفين او كلاهما (د) وجود اجراءات بديلة.

)ه) تكلفة الاجراءات البديلة.

) و) الاجراءات المستخدمة عموماً لانواع مماثلة من المعاملات.

مادة (20 (1) (يعامل التوقيع على انه توقيع الكتروني محمي اذا كان من الممكن التحقق من خلال تطبيق اجراءات توثيق محكمة، منصوص عليها في هذا القانون او معقولة تجارياً ومتفق عليها بين الطرفين، من ان التوقيع الالكتروني كان في الوقت الذي تم فيه: (أ) ينفرد به الشخص الذي استخدمه.

(ب) ومن الممكن ان يثبت هوية ذلك الشخص.

)ج) وان يكون تحت سيطرته التامة سواء بالنسبة لانشائه او وسيلة استعماله وقت التوقيع.

)د) ويرتبط بالرسالة الالكترونية ذات الصلة به او بطريقة توفر تأكيداً يعول عليه حول سلامة التوقيع، بحيث اذا تم تغيير السجل الالكتروني فإن التوقيع الالكتروني يصبح غير محمي.

(2) على الرغم من احكام المادة (21 (من هذا القانون وما لم يثبت العكس، يعتبر الاعتماد على التوقيع الالكتروني المحمي معقولاً.

مادة (21) :(1) يحق للشخص ان يعتمد على التوقيع الالكتروني او الشهادة الالكترونية الى المدى الذي يكون فيه مثل ذلك الاعتماد معقولاً.

(2) عندما يكون التوقيع الالكتروني معززاً بشهادة، فإن الطرف الذي يعتمد على ذلك التوقيع يتحمل نتائج اخفاقه في اتخاذ الخطوات المعقولة اللازمة للتأكد من صحة ونفاذ الشهادة، وما اذا كانت معلقة او ملغاة ومن مراعاة اية قيود فيما يتعلق بتلك الشهادة.

(3) لتقرير ما اذا كان من المعقول لشخص ان يعتمد على توقيع او شهادة، يولي الاعتبار اذا كان ذلك مناسباً الى: (أ) طبيعة المعاملة المعنية والتي قصد تعزيزها بالتوقيع الالكتروني.

(ب) قيمة او اهمية المعاملة المعنية متى كان ذلك معروفاً.

(ج) ما اذا كان الشخص الذي اعتمد على التوقيع الالكتروني او الشهادة، قد اتخذ خطوات مناسبة ليقرر مدى امكانية الاعتماد على التوقيع الالكتروني او الشهادة.

(د) ما اذا كان الطرف الذي اعتمد على التوقيع الالكتروني قد اتخذ خطوات مناسبة للتحقق من ان التوقيع الالكتروني معزز بشهادة او كان من المتوقع ان يكون كذلك.

(ه) ما اذا كان الطرف الذي اعتمد على التوقيع او الشهادة، قد عرف او كان عليه ان يعرف ان التوقيع الالكتروني او الشهادة قد عدلت او الغيت.

)و) اية اتفاقية او سياق تعامل بين المنشئ والطرف الذي اعتمد على التوقيع الالكتروني او الشهادة، او اي عرف تجاري سائد.

)ز) اي عامل اخر ذي صلة.

(4)اذا كان الاعتماد على التوقيع الالكتروني او الشهادة غير معقول في ضوء الظروف المحيطة بالنظر للعوامل المذكورة في الفقرة (2) من هذه المادة، فإن الطرف الذي اعتمد على التوقيع الالكتروني او الشهادة يتحمل مخاطر عدم صحة ذلك التوقيع او تلك الشهادة.

مادة (22) :(1) يجب على الموقع: (أ) ان يمارس عناية معقولة لتفادي استخدام اداة توقيعه استخداماً غير مأذون.

(ب) ان يخطر الاشخاص المعنيين بدون تأخير غير مبرر، وذلك في حالة :ـ معرفة الموقع بأن اداة توقيعه تعرضت لما يثير الشبهة في درجة امانها.

ـ دلالة الظروف المعروفة لديه على احتمال كبير بأن تكون اداة التوقيع قد تعرضت لما يثير الشبهة في امانها.

(ج) ان يمارس عناية معقولة لضمان دقة واكتمال كل ما يقدمه من بيانات وتصريحات جوهرية ذات صلة بالشهادة طيلة فترة سريانها، وذلك في الحالات التي تستلزم فيها اداة التوقيع استخدام شهادة.

(2) يكون الموقع مسئولاً عن تقصيره في استيفاء متطلبات الفقرة (1)السابقة.

الفصل الخامس : الاحكام المتصلة بالشهادات وخدمات التصديق

مادة (23) (1) لأغراض هذا القانون يعين الرئيس بقرار يصدره، مراقباً لخدمات التصديق وعلى وجه الخصوص لاغراض ترخيص وتصديق ومراقبة انشطة مزودي خدمات التصديق والاشراف عليها،

وينشر هذا القرار في الجريدة الرسمية.

(2)يجوز للمراقب ان يفوض كتابة ايا من مسئولياته بموجب هذا الفصل لمن يراه.

(3)يعتبر المراقب او المفوض من قبله موظفاً عاماً.

(4) على المفوض ان يبرز عند ممارسته ايا من الصلاحيات المخولة له واستجابة لطلب الشخص الذي يتصرف تجاهه، ما يثبت الصلاحية التي خوله اياها المراقب.

مادة (24) :(1) على مزود خدمات التصديق: (أ) ان يتصرف وفقاً للبيانات التي يقدمها بخصوص ممارساته.

(ب) ان يمارس عناية معقولة لضمان دقة واكتمال كل ما يقدمه من بيانات جوهرية ذات صلة بالشهادة او مدرجة فيها طيلة سريانها.

)ج) ان يوفر وسائل يكون من المعقول الوصول اليها وتمكن الطرف الذي يعتمد على خدماته من التأكد مما يلي: 1 ـ هوية مزود خدمات التصديق.

2 ـ ان الشخص المعينة هويته في الشهادة لديه السيطرة في الوقت المعني على اداة التوقيع المشار اليها في الشهادة.

3ـ الطريقة المستخدمة في تعيين هوية الموقع.

4ـ وجود اية قيود على الغرض او القيمة التي يجوز ان تستخدم من اجلها اداة التوقيع.

5 ـ ما اذا كانت اداة التوقيع صحيحة ولم تتعرض لما يثير الشبهة .

6 ـ ما اذا كان للموقع وسيلة لاعطاء اشعار بموجب المادة (22) (1) ـ (أ(،) ب) من هذا القانون.

7ـ ما اذا كان هناك وسيلة مناسبة للابلاغ عن الالغاء.

)د) ان يوفر وسيلة للموقعين تمكنهم من تقديم اشعار بأن اداة التوقيع قد تعرضت لما يثير الشبهة، وان يضمن توفر خدمة الغاء التوقيع يمكن استخدامها في الوقت المناسب.

)ه) ان يستخدم في اداء خدماته نظماً واجراءات وموارد بشرية جديرة بالثقة.

(و) ان يكون مرخصاً من مدير عام السلطة اذا كان يعمل في الامارة.

(2) لتقرير ما اذا كانت اية نظم او اجراءات او موارد بشرية جديرة بالثقة لاغراض الفقرة (1) ـ (ه) السابقة، بتعيين ايلاء الاعتبار للعوامل التالية: (أ) الموارد المالية والبشرية بما في ذلك توافر الموجودات داخل منطقة الاختصاص.

(ب) مدى الثقة في اجهزة وبرامج الحاسب الآلي.

(ج) اجراءات معالجة واصدار الشهادات وطلبات الحصول على الشهادات والاحتفاظ بالسجلات.

(د) توفر المعلومات الخاصة بالموقعين المحددين في الشهادات، وكذلك توفير المعلومات للاطراف المعتمدة على خدمات التصديق.

) ه) انتظام ومدى مراجعة الحسابات من جانب جهة مستقلة.

)و) وجود اعلان من الحكومة او من جهة اعتماد، او من مزود خدمات التصديق بشأن وجود ما سبق ذكره او الالتزام به.

(ز) مدى خضوع مزود خدمات التصديق للاختصاص القضائى لمحاكم الامارة.

)ح) مدى التناقض بين القانون المطبق على اعمال مزود خدمات التصديق وقوانين الامارة.

(3) يجب ان تحدد الشهادة ما يلي: (أ) هوية مزود خدمات التصديق.

(ب) ان الشخص المعينة هويته في الشهادة لديه السيطرة في الوقت المعني على اداة التوقيع المشار اليها في الشهادة.

(ج) ان اداة التوقيع كانت سارية المفعول في او قبل تاريخ اصدار الشهادة.

(د) ما اذا كانت هناك اية قيود على الغرض او القيمة التي يجوز ان تستخدم من اجلها اداة التوقيع او الشهادة.

(ه) ما اذا كانت هناك اية قيود على نطاق او مدى المسئولية التي قبلها مزود خدمات التصديق تجاه اي شخص.

(4) اذا حدثت اية اضرار نتيجة لعدم صحة الشهادة او نتيجة لأي عيب فيها، يكون مزود خدمات التصديق مسئولا عن الخسائر التي يتكبدها: (أ) كل طرف تعاقد مع مزود خدمات التصديق حول تقديم الشهادة .

(ب) اي شخص اعتمد بصورة معقولة على الشهادة التي اصدرها مزود خدمات التصديق.

(5) لا يكون مزود خدمات التصديق مسئولاً عن اي ضرر: (أ) اذا ادرج في الشهادة بياناً يقيد نطاق ومدى مسئوليته تجاه اي شخص ذي صلة، ومدى ذلك القيد.

(ب) اذا اثبت بأنه لم يقترف أي خطأ او اهمال، او ان الضرر نشأ عن سبب اجنبي لا يد له فيه.

مادة (25) :يضع المراقب قواعد لتنظيم وترخيص عمل مزودي خدمات التصديق الذين يعملون في الامارة ويرفعها للرئيس لاعتمادها، بما في ذلك ما يلي: 1 ـ طلبات تراخيص او تجديد تراخيص مزودي خدمات التصديق وممثليهم المفوضين والامور المتعلقة بذلك.

2 ـ انشطة مزودي خدمات التصديق، ويشمل ذلك طريقة ومكان واسلوب الحصول على اعمالهم وجذب الجمهور لها.

3 ـ المعايير والقواعد التي يتعين على مزودي خدمات التصديق المحافظة عليها واتباعها في اعمالهم؛ 4 ـ تحديد المعايير المناسبة فيما يتعلق بمؤهلات وخبرة مقدمي خدمات الترخيص وتدريب موظفيهم.

5 ـ تحديد شروط ادارة الاعمال التي يقوم بها مزود خدمات التصديق.

6 ـ تحديد محتويات وتوزيع المواد والاعلانات المكتوبة او المطبوعة او المرئية والتي يجوز ان يوزعها او يستخدمها اي شخص فيما يتعلق بأية شهادة او مفتاح رقمي.

7 ـ تحديد شكل ومحتوى اية شهادة او مفتاح رقمي.

8 ـ تحديد التفاصيل التي يجب تدوينها في الحسابات التي يحتفظ بها مزودو خدمات التصديق.

9 ـ المؤهلات الواجب توافرها في مدقق حسابات مزودي خدمات التصديق.

10ـ وضع اللوائح اللازمة لتنظيم التفتيش والتدقيق في اعمال مزودي خدمات التصديق.

11 ـ شروط انشاء وتنظيم اي نظام الكتروني بواسطة مزود خدمات تصديق، سواء بمفرده او بالاشتراك مع مزودي خدمات تصديق آخرين، وفرض وتغيير تلك الشروط او القيود التي يراها المراقب ملائمة.

12ـ الطريقة التي يدير بها حامل الترخيص معاملاته مع عملائه، وكذلك عند تعارض مصالحه مع مصالحهم، وواجباته تجاههم فيما يتصل بالشهادات الرقمية.

13 ـ تحديد الرسوم التي يجب دفعها فيما يتصل بأي امر مطلوب بموجب احكام الفصل الخامس من هذا القانون واللوائح الصادرة بمقتضاه.

14ـ وضع اية نماذج لاغراض هذه المادة.

مادة (26): (1) لتقرير ما اذا كانت الشهادة او التوقيع الالكتروني نافذاً قانوناً، لا يتعين ايلاء الاعتبار إلى المكان الذي صدرت الشهادة او التوقيع الالكتروني.

(2) تعتبر الشهادات التي يصدرها مزودو خدمات التصديق الاجانب، كشهادات صادرة من مزودي خدمات التصديق الذين يعملون بموجب هذا القانون، اذا كانت ممارسات مزودي خدمات التصديق الاجانب ذات مستوى من الوثوق يوازي على الاقل المستوى الذي تتطلبه المادة (24) من مزودي خدمات التصديق العاملين بموجب هذا القانون، ومع الاخذ بالاعتبار المعايير الدولية المعترف بها.

(3)يجوز الاعتراف بالتوقيعات التي تستوفي شروط القوانين الخاصة بدولة اخرى، واعتبارها في مستوى التوقيعات الصادرة وفقاً لاحكام هذا القانون، اذا اشترطت قوانين الدولة الاخرى مستوى من الاعتماد على التوقيعات يوازي على الاقل المستوى الذي يشترطه هذا القانون لتلك التوقعات.

(4) يتعين في موضوع الاعتراف المنصوص عليه في الفقرتين (2)، (3) السابقتين، النظر إلى العوامل الواردة في الفقرة (2) من المادة (24) من هذا القانون.

(5) لتقرير ما اذا كان التوقيع الالكتروني او الشهادة نافذة قانوناً، يتعين ايلاء الاعتبار إلى اي اتفاق بين

الطرفين حول المعاملة التي يستخدم فيها ذلك التوقيع او الشهادة.

(6) على الرغم من احكام الفقرتين (2)، (3) السابقتين: (أ) يجوز للاطراف في المعاملات التجارية والمعاملات الاخرى ان يحددوا وجوب استخدام مزودي خدمات تصديق معينيين او فئة معينة منهم او فئة معينة من الشهادات فيما يتصل بالرسائل او التوقيعات الالكترونية المقدمة لهم.

(ب) وفي الحالات التي يتفق فيها الاطراف فيما بينهم على استخدام انواع معينة من التوقيعات الالكترونية او الشهادات فإن ذلك الاتفاق يعتبر كافياً لاغراض الاعتراف المتبادل بين الاختصاصات القضائية المختلفة للدول، شريطة الا يكون مثل هذا الاتفاق غير مشروع وفقاً لاحكام القوانين المطبقة في الامارة.

الفصل السادس الاستخدام الحكومي للسجلات والتوقيعات الالكترونية قبول الايداع والاصدار الالكتروني للمستندات.

(مادة 27): (1) على الرغم من وجود اي نص مخالف في اي قانون آخر، يجوز لاية دائرة او جهة تابعة للحكومة، في اداء المهمات المناطة بهم بحكم القانون، ان تقوم بما يلي: (أ) قبول ايداع او تقديم المستندات او انشائها او الاحتفاظ بها في شكل سجلات الكترونية.

(ب) اصدار أي اذن او ترخيص او قرار او موافقة في شكل سجلات الكترونية.

)ج) قبول الرسوم او اية مدفوعات اخرى في شكل الكتروني.

(د) طرح العطاءات واستلام المناقصات المتعلقة بالمشتريات الحكومية بطريقة الكترونية.

(2) اذا قررت اية دائرة او جهة تابعة للحكومة تنفيذ اي من المهام المذكورة في الفقرة (أ) من هذه المادة فيجوز لها عندئذ ان تحدد: (أ) الطريقة او الشكل الذي سيتم بواسطته انشاء او ايداع او حفظ او تقديم او اصدار تلك السجلات الالكترونية.

(ب) الطريقة والاسلوب والكيفية والاجراءات التي يتم بها طرح العطاءات واستلام المناقصات، وانجاز المشتريات الحكومية.

(ج) نوع التوقيع الالكتروني المطلوب بما في ذلك اشتراط ان يستخدم المرسل توقيعا رقمياً او توقيعاً الكترونياً محمياً آخر.

(د (الطريقة والشكل الذي سيتم بها تثبيت ذلك التوقيع على السجل الالكتروني والمعيار الذي يجب ان يتسوفيه مزود خدمات التصديق الذي يقدم له المستند للحفظ او الايداع.

(ه) عمليات واجراءات الرقابة المناسبة للتأكد من سلامة وامن وسرية السجلات الالكترونية او المدفوعات او الرسوم.

(و) اية خصائص او شروط او احكام اخرى محددة حالياً لارسال المستندات الورقية، اذا كان ذلك

مطلوباً فيما يتعلق بالسجلات الالكترونية الخاصة بالمدفوعات والرسوم.

الفصل السابع :العقوبات ـ نشر الشهادة

(مادة 28): لا يجوز لاي شخص ان ينشر شهادة تشير إلى مزود خدمات تصديق مدرج اسمه في الشهادة، اذا كان الشخص يعرف ان: (أ) مزود خدمات التصديق المدرج اسمه في الشهادة لم يصدر الشهادة.

(ب) الموقع المدرج اسمه في الشهادة لم يقبل الشهادة.

(ج) الشهادة قد الغيت او اوقفت، الا اذا كان ذلك النشر بغرض التحقق من توقيع الكتروني او رقمي تم استعماله قبل الايقاف او الالغاء.

مادة (29): يعاقب كل من أنشأ او نشر عن معرفة او وفر اية شهادة او بيانات غير صحيحة لاي غرض احتيالي او اي غرض آخر غير مشروع، بالحبس وبغرامة لا تجاوز 250.000 درهم او باحدى هاتين العقوبتين.

مادة (30): مع عدم الاخلال بأية عقوبة اشد ينص عليها اي قانون آخر، يعاقب كل من قدم متعمدا بيانات غير صحيحة عن هويته او تفويضة إلى مزود خدمات التصديق بغرض طلب استصدار او الغاء او ايقاف شهادة، بالحبس لمدة لا تزيد على ستة اشهر، وبغرامة لا تجاوز 100.000 درهم او باحدى هاتين العقوبتين.

مادة (31): (1) يعاقب كل شخص تمكن بموجب اية سلطات ممنوحة له في هذا القانون من الاطلاع على معلومات في سجلات او مستندات او مراسلات الكترونية، وافشى متعمدا ايا من هذه المعلومات، بالحبس وبغرامة لا تجاوز 100.000 درهم، او باحدى هاتين العقوبتين. وتكون العقوبة الغرامة التي لا تجاوز 100.000 درهم في حالة تسببه باهماله في افشاء هذه المعلومات.

(2) يستثنى من احكام الفقرة (أ) من هذه المادة حالات التصريح التي تتم لاغراض هذا القانون، او اية اجراءات جزائية حول جرم ارتكب بالمخالفة لاي قانون، او لاغراض الاوامر الصادرة عن اية سلطة قضائية.

مادة (32) مع عدم الاخلال باية عقوبة اشد ينص عليها اي قانون آخر، يعاقب كل من ارتكب فعلا يشكل

جريمة بموجب التشريعات النافذة، باستخدام وسيلة الكترونية، بالحبس لمدة لا تزيد على ستة اشهر، وبغرامة لا تتجاوز 100.000 درهم، او باحدى هاتين العقوبتين ويعاقب بالعقوبة الاشد اذا كانت العقوبات المقررة في تلك التشريعات تزيد على العقوبة المقررة في هذه المادة.

مادة (33) :اذا ارتكب اي شخص اعتباري مخالفة لاحكام هذا القانون او اللوائح الصادرة بموجبه وثبت ان ذلك جاء نتيجة لتصرف او اهمال او موافقة او تستر اي عضو مجلس ادارة او مدير او اي موظف آخر في ذلك الشخص الاعتباري او اي شخص يبدو انه يتصرف بهذه الصفة، فإن ذلك الشخص والشخص الاعتباري يدانان بهذه المخالفة ويعاقبان تبعا لذلك.

مادة (34): تحكم المحكمة ـ في حالة الادانة ـ بموجب احكام هذا القانون، بمصادرة الادوات التي استعملت في ارتكاب الجريمة.

مادة (35) :تنقضي الدعوى الجزائية في الجرائم التي ترتكب للمرة الاولى اذا تم الصلح بعد وقوع الجريمة وقبل الفصل فيها بحكم بات، واذا حدث ذلك بعد صيرورة الحكم باتا يوقف تنفيذه._ _

الفصل الثامن : **احكام متفرقة: ـ سلطة** الاستثناء

مادة (36): يجوز للرئيس ان يستثنى اي شخص او اية جهة من كل او بعض احكام هذا القانون او اية لوائح صادرة بموجبه، وذلك وفقاً للشروط والاحكام التي يراها مناسبة.

مادة (37) :يجوز للرئيس تشكيل محاكم او هيئات تحكيم خاصة للفصل في القضايا والمنازعات الناشئة عن تطبيق هذا القانون.

اللوائح

مادة (38) (يصدر الرئيس اللوائح التنفيذية اللازمة لتنفيذ هذا القانون.

بدء النفاذ

مادة (39) ينشر هذ القانون في الجريدة الرسمية، ويعمل به اعتبارا من تاريخ نشره.

مكتوم بن راشد آل مكتوم حاكم دبي

صدر في دبي بتاريخ 12 فبراير 2002م ـ الموافق 30 ذي القعدة 1422 ه

ملحق رقم 5

القسم الثاني

المسؤولية عن فعل الغير

المادة 40 : تعدل وتتمم المادة 134 من الأمر رقم 75-58 المؤرخ في 20 رمضان عام 1395 الموافق 26 سبتمبر سنة 1975 والمذكور أعلاه، وتحرر كما يأتي :

"*المادة 134 :* كل من يجب عليه قانونا أو اتفاقا رقابة شخص في حاجة إلى الرقابة بسبب قصره أو بسبب حالته العقلية أو الجسمية، يكون ملزما بتعويض الضرر الذي يحدثه ذلك الشخص للغير بفعله الضار.

ويستطيع المكلف بالرقابة أن يتخلص من المسؤولية إذا أثبت أنه قام بواجب الرقابة أو أثبت أن الضرر كان لابد من حدوثه ولو قام بهذا الواجب بما ينبغي من العناية".

المادة 41 : تعدل المادتان 136 و137 من الأمر رقم 75-58 المؤرخ في 20 رمضان عام 1395 الموافق 26 سبتمبر سنة 1975 والمذكور أعلاه، وتحرران كما يأتي :

"*المادة 136 :* يكون المتبوع مسؤولا عن الضرر الذي يحدثه تابعه بفعله الضار متى كان واقعا منه في حالة تأدية وظيفته أو بسببها أو بمناسبتها.

وتتحقق علاقة التبعية ولو لم يكن المتبوع حرا في اختيار تابعه متى كان هذا الأخير يعمل لحساب المتبوع".

"*المادة 137 :* للمتبوع حق الرجوع على تابعه في حالة ارتكابه خطأ جسيما".

المادة 42 : يتمم الأمر رقم 75-58 المؤرخ في 20 رمضان عام 1395 الموافق 26 سبتمبر سنة 1975 والمذكور أعلاه، بالمادتين 140 مكرر و140 مكرر1 وتحرران كما يأتي :

"*المادة 140 مكرر:* يكون المنتج مسؤولا عن الضرر الناتج عن عيب في منتوجه حتى ولو لم تربطه بالمتضرر علاقة تعاقدية.

يعتبر منتوجا كل مال منقول ولو كان متصلا بعقار، لاسيما المنتوج الزراعي والمنتوج الصناعي وتربية الحيوانات والصناعة الغذائية والصيد البري والبحري والطاقة الكهربائية".

"*المادة 140 مكرر1 :* إذا انعدم المسؤول عن الضرر الجسماني ولم تكن للمتضرر يد فيه، تتكفل الدولة بالتعويض عن هذا الضرر".

المادة 43 : يتمم الأمر رقم 75-58 المؤرخ في 20 رمضان عام 1395 الموافق 26 سبتمبر سنة 1975 والمذكور أعلاه، بالمادة 182 مكرر وتحرر كما يأتي :

"*المادة 182 مكرر:* يشمل التعويض عن الضرر المعنوي كل مساس بالحرية أو الشرف أو السمعة".

المادة 44 : يتمم الأمر رقم 75-58 المؤرخ في 20 رمضان عام 1395 الموافق 26 سبتمبر سنة 1975 والمذكور أعلاه، بالمادتين 323 مكرر و323 مكرر1 وتحرران كما يأتي :

"*المادة 323 مكرر:* ينتج الإثبات بالكتابة من تسلسل حروف أو أوصاف أو أرقام أو أية علامات أو رموز ذات معنى مفهوم، مهما كانت الوسيلة التي تتضمنها، وكذا طرق إرسالها".

"*المادة 323 مكرر1 :* يعتبر الإثبات بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة على الورق، بشرط إمكانية التأكد من هوية الشخص الذي أصدرها وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها".

المادة 45 : تعدل المادة 324 مكرر3 من الأمر رقم 75-58 المؤرخ في 20 رمضان عام 1395 الموافق 26 سبتمبر سنة 1975 والمذكور أعلاه، وتحرر كما يأتي :

"*المادة 324 مكرر3 :* يتلقى الضابط العمومي، تحت طائلة البطلان، العقود الاحتفائية، بحضور شاهدين".

المادة 46 : تعدل وتتمم المادة 327 من الأمر رقم 75-58 المؤرخ في 20 رمضان عام 1395 الموافق 26 سبتمبر سنة 1975 والمذكور أعلاه، وتحرر كما يأتي :

"*المادة 327 :* يعتبر العقد العرفي صادرا ممّن كتبه أو وقعه أو وضع عليه بصمة إصبعه ما لم ينكر صراحة ما هو منسوب إليه، أما ورثته أو خلفه فلا يطلب منهم الإنكار ويكفي أن يحلفوا يمينا بأنهم لا يعلمون أن الخط أو الإمضاء أو البصمة هو لمن تلقوا منه هذا الحق.

ويعتد بالتوقيع الإلكتروني وفق الشروط المذكورة في المادة 323 مكرر1 أعلاه".

ملحق رقم 6

قانون رقم 15 لسنة 2004
بتنظيم التوقيع الالكتروني
وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات

باسم الشعب
رئيس الجمهورية

قرر مجلس الشعب القانون الآتي نصه ، وقد أصدرناه:

مادة 1 - في تطبيق أحكام هذا القانون يقصد بالمصطلحات الآتية المعاني المبينة قرين كل منها:
(أ) الكتابة الالكترونية : كل حروف أو أرقام أو رموز أو أي علامات أخرى تثبت على دعامة الكترونية أو رقمية أو ضوئية أو أية وسيلة أخرى مشابهة وتعطي دلالة قابلة للإدراك.
(ب) المحرر الالكتروني : رسالة تتضمن معلومات تنشأ أو تدمج ، أو تخزن ، أو ترسل أو تستقبل كليا أو جزئيا بوسيلة الكترونية أو رقمية أو ضوئية أو بأية وسيلة أخرى مشابهة.
(ج) التوقيع الالكتروني : ما يوضع على محرر الكتروني ويتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها ويكون له طابع متفرد يسمح بتحديد شخص الموّقع ويميزه عن غيره.
(د) الوسيط الالكتروني: أداة أو أدوات أو أنظمة إنشاء التوقيع الالكتروني.
(هـ) الموقع : الشخص الحائز على بيانات إنشاء التوقيع ويوقع عن نفسه أو عمن ينيبه أو يمثله قانونا.
(و) شهادة التصديق الالكتروني: الشهادة التي تصدر من الجهة المرخص لها بالتصديق وتثبت الارتباط بين الموقع وبيانات إنشاء التوقيع.
(ز) الهيئة : هيئة تنمية صناعة تكنولوجيا المعلومات.
(ح) الوزارة المختصة: الوزارة المختصة بشئون الاتصالات والمعلومات.
(ط) الوزير المختص: الوزير المختص بشئون الاتصالات والمعلومات.
مادة 2- تنشأ هيئة عامة تسمى " هيئة تنمية صناعة تكنولوجيا المعلومات " تكون لها الشخصية الاعتبارية وتتبع الوزير المختص ، ويكون مقرها الرئيسي محافظة الجيزة ، ولها إنشاء فروع في جميع أنحاء جمهورية مصر العربية.

مادة 3 - تهدف الهيئة إلى تحقيق الأغراض الآتية:
(أ) تشجيع وتنمية صناعة تكنولوجيا المعلومات والاتصالات.
(ب) نقل التكنولوجيا المتقدمة للمعلومات وتحقيق الاستفادة منها.
(ج) زيادة فرص تصدير خدمات الاتصالات وتكنولوجيا المعلومات ومنتجاتها.
(د) الإسهام في تطوير وتنمية الجهات العاملة في مجال تكنولوجيا المعلومات والاتصالات.
(هـ) توجيه وتشجيع وتنمية الاستثمار في صناعة تكنولوجيا المعلومات والاتصالات.
(و) رعاية المصالح المشتركة لأنشطة تكنولوجيا المعلومات.
(ز) دعم البحوث والدراسات في مجال تكنولوجيا المعلومات والاتصالات وتشجيع الاستفادة بنتائجها.
(ح) تشجيع ودعم المشروعات الصغيرة والمتوسطة في مجال استخدام وتوظيف آليات المعاملات الالكترونية.
(ط) تنظيم نشاط خدمات التوقيع الالكتروني وغيرها من الأنشطة في مجال المعاملات الالكترونية وصناعة تكنولوجيا المعلومات.
مادة 4 - تباشر الهيئة الاختصاصات اللازمة لتحقيق أغراضها على الأخص ما يأتي :

(أ) إصدار وتجديد التراخيص اللازمة لمزاولة أنشطة خدمات التوقيع الالكتروني وغيرها من الأنشطة في مجال المعاملات الالكترونية وصناعة تكنولوجيا المعلومات ، وذلك وفقا لأحكام القوانين واللوائح المنظمة لها. (ب) تحديد معايير منظومة التوقيع الالكتروني بما يؤدي إلى ضبط مواصفاتها الفنية .
(ج) تلقي الشكاوى المتعلقة بأنشطة التوقيع الالكتروني والمعاملات الالكترونية وتكنولوجيا المعلومات واتخاذ ما يلزم في شأنها.
(د) تقييم الجهات العاملة في مجال أنشطة تكنولوجيا المعلومات وتحديد مستوياتها الفنية بحسب نتائج هذا التقييم .
(هـ) تقديم المشورة الفنية بشأن المنازعات التي تنشأ بين الأطراف المعنية بأنشطة التوقيع الالكتروني والمعاملات الالكترونية وتكنولوجيا المعلومات.
(و) تقديم المشورة الفنية إلى الجهات العاملة في أنشطة تكنولوجيا المعلومات ، وتدريب العاملين فيها.
(ز) إقامة المعارض والمؤتمرات والندوات المتخصصة في مجال تكنولوجيا المعلومات والاتصالات داخليا وخارجيا .
(ح) إنشاء الشركات التي تساعد في تنمية صناعة تكنولوجيا المعلومات والاتصالات أو المساهمة فيها.
(ط) إيداع وقيد و تسجيل النسخ الأصلية لبرامج الحاسب الآلي وقواعد البيانات ، التي تتقدم بها الجهات أو الأفراد الناشرون والطابعون والمنتجون لها للمحافظة على حقوق الملكية الفكرية وغيرها من الحقوق.

مادة 5 - يفرض لصالح الهيئة رسم بواقع واحد في المائة من إيرادات الخدمات والأعمال التي تقدمها المنشآت العاملة في مجال تكنولوجيا المعلومات والاتصالات تلتزم به هذه المنشآت ، يودع في حساب خاص للمساهمة في تنمية صناعة تكنولوجيا المعلومات والاتصالات ، ويصدر بتحديد هذه الخدمات والأعمال قرار من مجلس إدارة الهيئة .

كما يكون إصدار وتجديد التراخيص المنصوص عليها في البند(أ) من المادة (4) من هذا القانون بمقابل يصدر بتحديد فئاته وبقواعد وإجراءات اقتضائه قرار من مجلس إدارة الهيئة. مادة 6- تتكون موارد ومصادر تمويل الهيئة مما يأتي:
(أ) الإعتمادات التي تخصصها لها الدولة.
(ب) الرسم المنصوص عليه في الفقرة الأولى من المادة (5) من هذا القانون .
(ج) المقابل المنصوص عليه في الفقرة الثانية من المادة(5) البند (ج) من المادة (9) ، المادتين (19) ،(22) من هذا القانون.
(د) مقابل الخدمات الأخرى التي تؤديها الهيئة.
(هـ) الهبات والتبرعات والإعانات التي يقبلها مجلس إدارة الهيئة.
(و) القروض والمنح التي تعقد لصالح الهيئة.
(ز) عائد استثمار أموال الهيئة.
مادة 7 - تكون للهيئة موازنة مستقلة يجري إعدادها وفقا لقواعد إعداد موازنات الهيئات الإقتصادية، وتبدأ السنة المالية للهيئة مع بداية السنة المالية للدولة وتنتهي بانتهائها، ويكون للهيئة حساب خاص لدى البنك المركزي المصري تودع فيه مواردها ، ويجوز بموافقة وزير المالية فتح حساب للهيئة في احد البنوك.

ويرحل الفائض من موازنة الهيئة من سنة إلى أخرى . ويجوز بقرار من رئيس مجلس الوزراء بناء على عرض الوزير المختص بعد التشاور مع وزير المالية أن يؤول جزء من الفائض إلى الخزانة العامة

للدولة. مادة 8 - يتولى إدارة الهيئة مجلس إدارة يشكل بقرار من رئيس مجلس الوزراء برئاسة الوزير المختص وعضوية كل من :

(أ) الرئيس التنفيذي للهيئة .

(ب) مستشار من مجلس الدولة يختاره رئيس مجلس الدولة.

(ج)ممثل لوزارة الدفاع يختاره وزير الدفاع .

(د) ممثل لوزارة الداخلية يختاره وزير الداخلية.

(هـ) ممثل لوزارة المالية يختاره وزير المالية.

(و) ممثل لجهاز رئاسة الجمهورية يختاره رئيس ديوان رئيس الجمهورية.

(ز) ممثل لجهاز المخابرات العامة يختاره رئيس جهاز المخابرات العامة.

(ح) سبعة أعضاء من ذوي الخبرة يختارهم الوزير المختص.

تكون مدة عضوية مجلس الإدارة ثلاث سنوات قابلة للتجديد ، ويصدر بتحديد مكافأة العضوية قرار من رئيس مجلس الوزراء.

ولمجلس الإدارة أن يشكل من بين أعضائه لجنة أو أكثر يعهد إليها بصفة مؤقتة ببعض المهام ، وله أن يفوض رئيس مجلس الإدارة او الرئيس التنفيذي للهيئة في بعض اختصاصاته.

مادة 9 - مجلس إدارة الهيئة هو السلطة المسئولة عن شئونها وتصريف أمورها ، ويباشر اختصاصاته على الوجه المبين في هذا القانون، وله ان يتخذ ما يراه لازما من قرارات لتحقيق الأغراض التي أنشئت الهيئة من أجلها ، وله على الأخص ما يأتي:

(أ) وضع نظم وقواعد التوقيع الالكتروني والمعاملات الالكترونية طبقا لأحكام القوانين واللوائح المنظمة لها .

(ب) وضع القواعد الفنية و الإدارية والمالية و الضمانات الخاصة بإصدار التراخيص اللازمة لمزاولة أنشطة خدمات التوقيع الإلكتروني وغيرها من الأنشطة في مجال المعاملات الإلكترونية وتكنولوجيا المعلومات.

(ج) تحديد الخدمات التي تؤديها الهيئة للغير في مجال تكنولوجيا المعلومات والاتصالات ، ومقابل أداء هذه الخدمات.

(د) وضع القواعد التي تكفل احترام تقاليد المهنة في مجال المعاملات الإلكترونية و تكنولوجيا المعلومات والاتصالات.

(هـ) وضع اللوائح الداخلية المتعلقة بالشئون الفنية والمالية والإدارية ولوائح المشتريات والمخازن وغيرها من اللوائح المتعلقة بتنظيم نشاط الهيئة ، وذلك دون التقيد بالقواعد والنظم الحكومية.

(و) اعتماد مشروع الموازنة السنوية للهيئة .

(ز) وضع لائحة شئون العاملين بالهيئة المنظمة لتعيينهم وتحديد رواتبهم وبدلاتهم ومكافآتهم وترقياتهم وتأديبهم وإنهاء خدمتهم وسائر شئونهم الوظيفية ، وذلك مع مراعاة قواعد الكفاءة الإنتاجية وتوازن اقتصاديات الهيئة وبالتشاور مع المنظمة النقابية ذات الصلة ، ودون التقيد بقواعد ونظم العاملين المدنيين بالدولة.

(ح) وضع خطط وبرامج التدريب والتأهيل على صناعة تكنولوجيا المعلومات. ويصدر باللوائح والنظم المنصوص عليها في هذه المادة قرار من الوزير المختص.

مادة 10 - يجتمع مجلس الإدارة بدعوة من رئيسه مرة على الأقل كل شهر وكلما اقتضت الضرورة ذلك ، ويكون اجتماعه صحيحا بحضور أغلبية أعضائه وتصدر قراراته بأغلبية أصوات الحاضرين وعند التساوي يرجح الجانب الذي منه الرئيس.

وللمجلس أن يدعو لحضور جلساته من يرى الاستعانة بخبراتهم دون أن يكون لهم صوت معدود في

المداولات.

مادة 11 - للهيئة رئيس تنفيذي يصدر بتعيينه وتحديد معاملته المالية قرار من رئيس مجلس الوزراء بناء على اقتراح الوزير المختص .

ويمثل الرئيس التنفيذي الهيئة أمام القضاء وفي علاقتها بالغير ويكون مسئولا أمام مجلس الإدارة عن سير أعمال الهيئة فنيا وإداريا وماليا ، ويختص بما يأتي :

(أ) تنفيذ قرارات مجلس الإدارة .

(ب) إدارة الهيئة وتصريف شئونها والإشراف على سير العمل بها.

(ج) عرض تقارير دورية على مجلس الإدارة عن نشاط الهيئة وسير العمل بها ، وما تم إنجازه وفقا للخطط والبرامج الموضوعة ، وتحديد معوقات الأداء ، والحلول المقترحة لتفاديها.

(د) القيام بأية أعمال أو مهام يكلفه بها مجلس الإدارة.

(هـ) الاختصاصات الأخرى التي تحددها اللوائح الداخلية للهيئة .

مادة 12 - يحل الرئيس التنفيذي محل رئيس مجلس إدارة الهيئة حال غيابه .

مادة 13 - تلتزم جميع الجهات والشركات العاملة في مجال المعاملات الالكترونية وتكنولوجيا المعلومات بموافاة الهيئة بما تطلبه من تقارير أو إحصاءات أو معلومات تتصل بنشاط الهيئة.

مادة 14 - للتوقيع الالكتروني ، في نطاق المعاملات المدنية والتجارية والإدارية ، ذات الحجية المقررة للتوقيعات في أحكام قانون الإثبات في المواد المدنية والتجارية ، إذا روعي في إنشائه وإتمامه الشروط المنصوص عليها في هذا القانون والضوابط الفنية والتقنية التي تحددها اللائحة التنفيذية لهذا القانون .

مادة 15 - للكتابة الالكترونية وللمحررات الالكترونية ، في نطاق المعاملات المدنية والتجارية والإدارية، ذات الحجية المقررة للكتابة والمحررات الرسمية والعرفية في أحكام قانون الإثبات في المواد المدنية والتجارية ، متى استوفت الشروط المنصوص عليها في هذا القانون وفقا للضوابط الفنية والتقنية التي تحددها اللائحة التنفيذية لهذا القانون .

مادة 16 - الصورة المنسوخة على الورق من المحرر الالكتروني الرسمي حجة على الكافة بالقدر الذي تكون فيها مطابقة لأصل هذا المحرر ، وذلك مادام المحرر الالكتروني الرسمي والتوقيع الالكتروني موجودين على الدعامة الالكترونية.

مادة 17 - تسري في شأن إثبات صحة المحررات الالكترونية الرسمية والعرفية والتوقيع الالكتروني ، فيما لم يرد بشأنه نص في هذا القانون أو في لائحته التنفيذية الأحكام المنصوص عليها في قانون المرافعات المدنية والتجارية.

مادة 18 - يتمتع التوقيع الالكتروني والكتابة الالكترونية والمحررات الالكترونية بالحجية في الإثبات إذا ما توافرت فيها الشروط الآتية:

(أ) ارتباط التوقيع بالموقع وحده دون غيره.
(ب) سيطرة الموقع وحده دون غيره على الوسيط الإلكتروني.
(ج) إمكانية كشف أي تعديل أو تبديل في بيانات المحرر الالكتروني او التوقيع الإلكتروني .
وتحدد اللائحة التنفيذية لهذا القانون الضوابط الفنية والتقنية اللازمة لذلك.

مادة 19 - لا تجوز مزاولة نشاط إصدار شهادات التصديق الالكتروني الا بترخيص من الهيئة ، وذلك نظير مقابل يحدده مجلس إدارتها وفقا للإجراءات والقواعد والضمانات التي تقررها اللائحة التنفيذية لهذا القانون ودون التقيد بأحكام القانون رقم 129 لسنة 1947 بالتزامات المرافق العامة، مع مراعاة ما يأتي :
(أ) أن يتم اختيار المرخص له في إطار من المنافسة و العلانية.
(ب) أن يحدد مجلس إدارة الهيئة مدة الترخيص بحيث لاتزيد على تسعة وتسعين عاما.
(ج) أن تحدد وسائل الإشراف والمتابعة الفنية والمالية التي تكفل حسن سير المرفق بانتظام واطّراد.
و لا يجوز التوقف عن مزاولة النشاط المرخص به أو الاندماج في جهة أخرى أو التنازل عن الترخيص للغير إلا بعد الحصول على موافقة كتابية مسبقة من الهيئة.

مادة 20 - تحدد اللائحة التنفيذية لهذا القانون البيانات التي يجب أن تشتمل عليها شهادة التصديق الالكتروني.

مادة21 - بيانات التوقيع الالكتروني والوسائط الالكترونية والمعلومات التي تقدم إلى الجهة المرخص لها بإصدار شهادات التصديق الالكتروني سرية ، ولا يجوز لمن قدمت إليه أو اتصل بها بحكم عمله إفشاؤها للغير أو استخدامها في غير الغرض الذي قدمت من أجله.

مادة 22 - تختص الهيئة باعتماد الجهات الأجنبية المختصة بإصدار شهادات التصديق الالكتروني ، وذلك نظير المقابل الذي يحدده مجلس إدارة الهيئة ، وفي هذه الحالة تكون الشهادات التي تصدرها تلك الجهات ذات الحجية في الإثبات المقررة لما تصدره نظيراتها في الداخل من شهادات نظيرة ، وذلك كله وفقا للقواعد والإجراءات والضمانات التي تقرها اللائحة التنفيذية لهذا القانون.

مادة 23 - مع عدم الإخلال بأية عقوبة اشد منصوص عليها في قانون العقوبات أو في أي قانون آخر ، يعاقب بالحبس وبغرامة لاتقل عن عشرة آلاف جنيه ولا تجاوز مائة ألف جنيه أو بإحدى هاتين العقوبتين كل من :
(أ) أصدر شهادة تصديق الكتروني دون الحصول على ترخيص بمزاولة النشاط من الهيئة.
(ب) أتلف أو عيّب توقيعا أو وسيطا أو محررا الكترونيا ، أو زوّر شيئا من ذلك بطريق الاصطناع أو التعديل أو التحوير أو بأي طريق آخر .
(ج) استعمل توقيعا أو وسيطا أو محررا الكترونيا معيبا أو مزورا مع علمه بذلك.
(د) خالف أيّا من أحكام المادتين (19) ، (21) من هذا القانون .
(هـ) توصّل بأية وسيلة إلى الحصول بغير حق على توقيع أو وسيط أو محرر الكتروني او اخترق هذا الوسيط أو اعترضه أو عطله عن أداء وظيفته.
وتكون العقوبة على مخالفة المادة(13) من هذا القانون ، الغرامة التي لا تقل عن خمسة ألاف جنيه ولا تجاوز خمسين ألف جنيه.

وفي حالة العود تزاد بمقدار المثل المقررة ؛ العقوبة المقررة لهذه الجرائم في حديها الأدنى والأقصى .

وفي جميع الأحوال يحكم نشر حكم الإدانة في جريدتين يوميتين واسعتي الانتشار ، وعلى شبكات

المعلومات الالكترونية المفتوحة على نفقة المحكوم عليه.

مادة 24 - يعاقب المسئول عن الإدارة الفعلية للشخص الاعتباري المخالف بذات العقوبات المقررة عن الأفعال التي ترتكب بالمخالفة لأحكام هذا القانون ، إذا كان إخلاله بالواجبات التي تفرضها عليه تلك الإدارة قد أسهم في وقوع الجريمة مع علمه بذلك.

ويكون الشخص الاعتباري مسئولا بالتضامن عن الوفاء بما يحكم به من عقوبات مالية وتعويضات ، إذا كانت المخالفة قد ارتكبت من أحد العاملين به باسم ولصالح الشخص الاعتباري .

مادة25 - يكون للعاملين بالهيئة الذين يصدر بهم قرار من وزير العدل بالاتفاق مع الوزير المختص صفة مأموري الضبط القضائي بالنسبة إلى الجرائم التي تقع في حدود اختصاصهم بالمخالفة لأحكام هذا القانون . مادة 26 - مع عدم الإخلال بأحكام المادة (23) من هذا القانون ، يكون للهيئة ، إذا خالف المرخص له بإصدار شهادات تصديق الكتروني شروط الترخيص أو خالف أيا من أحكام المادة (19) من هذا القانون ، أن تلغي الترخيص ، كما يكون لها أن توقف سريانه حتى إزالة أسباب المخالفة وذلك كله وفقا للقواعد و الإجراءات التي تحددها اللائحة التنفيذية لهذا القانون .

مادة 27 - على كل من يباشر نشاط إصدار شهادات التصديق الالكتروني قبل تاريخ العمل بهذا القانون أن يوفق أوضاعه طبقا لأحكامه خلال مدة لا تجاوز ستة أشهر من تاريخ صدور لائحته التنفيذية ، وذلك وفقا للقواعد والإجراءات التي تنص عليها هذه اللائحة.

مادة 28 - لا تسري أحكام المادة (13) من هذا القانون على أجهزة رئاسة الجمهورية و القوات المسلحة و وزارة الداخلية وجهاز المخابرات العامة وهيئة الرقابة الإدارية.

مادة 29 - يصدر الوزير المختص اللائحة التنفيذية لهذا القانون خلال ستة أشهر من تاريخ نشره. مادة 30 - ينشر هذا القانون في الجريدة الرسمية ، ويعمل به اعتبارا من اليوم التالي لتاريخ نشره. يبصم هذا القانون بخاتم الدولة ، وينفذ كقانون من قوانينها. صدر برئاسة الجمهورية في غرة ربيع الأول سنة 1425 هـ (الموافق 21 إبريل سنة 2004 م) حسني مبارك

جمهورية مصر العربية

مشروع قانون لتنظيم التوقيع الإلكتروني

أ- مشروع قانون

قرار رئيس جمهورية مصر العربية

بمشروع قانون

باصدار قانون بتنظيم التوقيع الإلكتروني

رئيس الجمهورية

بعد الاطلاع على الدستور

وبعد موافقة مجلس الوزراء

قرر

مشروع القانون الآتي نصه يقدم إلى مجلس الشعب

المادة الأولى : يعمل في شأن تنظيم التوقيع الإلكتروني بالقانون المرافق، ويلغى كل حكم يتعارض مع أحكامه.

المادة الثانية: ينشر هذا القانون في الجريدة الرسمية ويعمل به من اليوم التالي لنقضاء ثلاثة أشهر من تاريخ نشره .

/ /2001

رئيس الجمهورية

محمد جسني مبارك

قانون بتنظيم التوقيعات الإلكترونية

أحكام عامة

تعريفات

مادة 1 : في تطبيق أحكام هذا القانون يقصد بالمصطلحات التية المعاني المبينة قرين كل منها :

1- كتابة إلكترونية :

كل حروف أو أرقام أو رموز أو أي علامات تثبت على دعامة إلكترونية أو رقمية أو ضوئية أو أي وسيلة أخرى مشابهة وتعطي دلالة قابلة للإدراك .

2- محرر إلكتروني:

رسالة بيانات تتضمن معلومات تنشأ أو تدمج أو تخزن أو ترسل أو تستقبل كليا أو جزئيا بوسيلة إلكترونية أو رقمية أو ضوئية أو بأي وسيلة أخرى مشابهة.

3- توقيع إلكتروني:

ما يوضع على محرر لإلكتروني ويتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها ويكون له طابع متفرد يسمح بتحديد شخص الموقع ويميزه عن غيره .

4- وسيط إلكتروني:

أداة أو أدوات أو أنظمة تكوين التوقيع الإلكتروني.

5- معاملة إلكترونية :

كل معاملة تتم باستخدام كتابة إلكترونية موقعة أو غير موقعة بهدف إحداث أثر قانوني معين .

6- الموقع:

الشخص الحائز على بيانات إنشاء التوقيع ويوقع عن نفسه أو عن من ينيبه أو يمثله قانونا.

7- شهادة التصديق الإلكتروني:

شهادة تبين العلاقة بين الموقع والمحرر الإلكتروني النسوب إليه وتحدد لائحة تنفيذية الشروط والأوضاع التي تصدر بها الشهادة.

8- المتعامل:

الشخص الطبيعي أو الإعتباري الذي يتعامل إستنادا إلى شهادة تصديق إلكتروني أو توقيع إلكتروني.

9- جهة الترخيص:

هيئة تنمية صناعة تكنلوجيا المعلومات ويشار إليها بالهيئة.

10- جهة التصديق:

الشخص الطبيعي أو الإعتباري المرخص له من جهة الترخيص باصدار شهادات تصديق إلكتروني أو تقديم أي خدمات متعلقة بالتوقيع الإلكتروني.

10- الوزارة المختصة :

وزارة الإتصال والمعلومات

نطاق تطبيق القانون

مادة 2: تسري أحكام هذا القانون على المعاملات المدنية والتجارية والإدارية المحررة والموقعة إلكترونيا في الأحوال والشروط و الأوضاع الواردة فيه وفي لائحته التنفيذية .

ولا تسري أحكام هذا القانون على الحالات التي يقتصر فيها تقديم خدمات التصديق الإلكتروني على الأغراض التعليمية أو التدريبية أو البحثية.

ويجوز بقرارار من الوزير المختص استثناء بعض المعاملات من تطبيق أحكام القانون عليها .

أحكام التوقيع الإلكتروني

مادة 3: يتمتع التوقيع الإلكتروني بذات الحجية المقررة للتوقيعات في مفهوم قانون الإثبات في المواد المدنية والتجارية متى تم طبقا للأوضاع وبالشروط المنصوص عليها ففي هذا القانون ولائحته التنفيذية.

مادة 4 : تتمتع الكتابة الإلكترونية بذات الحجية المقررة للكتابة في مفهوم قانون الإثبات في المواد المدنية والتجارية متى استوفت الشروط والضوابط الواردة في هذا القانون ولائحته التنفيذية.

وتحدد اللائحة التنفيذية ضوابط وشروط تمتع التوقيع الإلكتروني والكتابة الإلكترونية بالحجية في الإثبات بما يضمن توافر الأتي :

1- ارتباط التوقيع الإلكتروني بالموقع وحده دون غيره .
2- سيطرة الموقع وحده دون غيره على الوسيط الإلكتروني.
3- إمكانية اكتشاف أي تعديل أو تبديل في بيانات المحرر أو التوقيع الإلكتروني بعد وضعه على أي محرر.

مادة 5: يلتزم المتعامل بأن يتحقق من صحة التوقيع الإلكتروني المقدم له، وصلاحيته للإستخدام وصدوره من الموقع زذلط كله وفقا للشروط و الضوابط الواردة في القانون ولائحته التنفيذية.

مادة 6 : لا يجوز لجهة التصديق أو لجهة الترخيص أو الموقع الاحتجاج على المتعامل بالدفوع المبنية على علاقاته الشخصية بالأخر ما لم يثبت قصد المتعامل الإضرار بالمتعاملين الأخرين.

مادة 7: تعتبر المعاملة الإلكترونية قد اعقدت في الزمان والمكان الذي يصدر فيه القبول ما لم يتفق على غير ذلك.

التصديق الإلكتروني

مادة 8 : لا يجوز لأي شخص طبيعي أو اعتباري مزاولة خدمات التصديق الإلكتروني إلا بعد الحصول على ترخيص بذلك من جهة الترخيص وفقا للقواعد والإجراءات التي تحددها اللائحة التنفيذية.

مادة9: لا يجوز لمن يحصل على ترخيص بمنح شهادات التصديق الإلكتروني مباشرة العمل قبل الحصول على ضمان يغطي على مسئوليته قبل الموقع والغير طبقا للقواعد والمعايير التي تحددها جهة الترخيص.

مادة 10: تلتزم جهة التصديق بأن تضع في شهادة التصديق رقم الشهادة وتاريخها وفئتها ومدة صلاحيتها وبيان للضمان المنصوص عليه في المادة 9، فضلا عن بيانات الترخيص الصادر لها بمنح هذه الشهادة طبقا للائحة التنفيذية لهذا القانون.

كما تلتزم بالمحافظة على سرية البيانات والمعلومات التي تقدم بها طالب التوقيع الإلكتروني، وعدم إفشائها للغير أو استخدامها في غير الغرض الذي قدمت من أجله.

مادة 11: مع عدم الإخلال بأحكام الإتفاقيات الدولية النافذة في مصر ومبدأ المعاملة بالمثل: تعامل التراخيص الصادرة للمرخص لهم من جهات أجنبية معاملة التراخيص الوطنية بذات الشروط والضوابط الواردة في اللائحة التنفيذية، وبما يكفل توافر الضمانات الواردة في هذا القانون كحد أدنى. ولا يعتد بأي شهادات تصديق إلكتروني صادرة من جهات تصديق أجنبية إلا إذا كانت الجهة المصدرة لها معتمدة من جهة الترخيص طبقا لما تحدده اللائحة التنفيذية من أوضاع وشروط كلما كان القانون المصري واجب التطبيق.

الجرائم والعقوبات

مادة 12 : مع عدم الإخلال بأي عقوبة أشد وردت في أي قانون أخر يعاقب بالحبس مدة لا تقل عن ستة أشهر وبالغرامة التي لا تقل عن عشرين ألف جنيه ولا تجاوز مئة ألف جنيه أو باحدى هاتين العقوبتين كل من ارتكب فعلا أو أكثر مما يلي:

1- زور أو تلاعب في توقيع أو وسيط الكتروني سواء تم ذلك باصطناعه أو اتلافه أو تعييبه أو تعديله أو تحويره أو بأي طريقة أخرى تؤدي إلى تغيير الحقيقة في بياناته.
2- أفشى أو تواطأ مع الغير لإفشاء بيانات توقيع أو وسيط الكتروني أو بيانات أدلى بها المتعامل بتوقيع إلكتروني معتمد.
3- توصل بطريق الغش أو التدليس إلى الحصول على توقيع أو وسيط إلكتروني لا يحق الحصول عليه مستخدما في ذلك معلومات أو بيانات كاذبة أو خاطئة .

مادة 13 : مع عدم الإخلال بأي عقوبة أشد وردت في أي قانون أخر يعاقب بالحبس وبالغرامة التي لا تقل عن عشرة ألف جنيه ولا تتجاوز مئة ألف جنيه أو باحدى هاتين العقوبتين كل من ارتكب فعلا أو أكثر مما يلي:

1- إصدار شهادات تصديق إلكتروني للجمهور أو تقديم خدمات تتعلق بالتوقيعات الإلكترونية للجمهور قبل الحصول على ترخيص بذلك من جهة الترخيص.
2- عدم إخطار جهة الترخيص بأي تغيير في البيانات التي حصل بناء عليها على الترخيص بإصدار شهادات تصديق إلكتروني أو بتقديم خدمات تتعلق بالتوقيعات الإلكترونية للجمهور.

مادة 14: يعاقب بالغرامة التي لا تقل عن عشرين ألف جنيه كل من أصدر شهادة تصديق إلكتروني بالمخالفة لقواعد وأحكام هذا القانون ولائحته التنفيذية.

مادة 15 : تتعدد العقوبة المنصوص عليها في المواد 12 ، 13 ، 14 بتعدد التوقيعات أو الوسائط الإلكترونية.

وفي حالة العود تضاعف العقوبة المحكوم بها في حديها الأدنى والقصى.

وفي جميع الأحوال ينشر حكم الإدانة في جريدتين يوميتين على نفقة المحكوم عليه .

مادة 16: يعاقب بالغرامة التي لا تقل عن عشرة ألاف جنيه كل من تنازل للغير عن الترخيص الصادر إليه بمنح شهادات تصديق إلكتروني قبل الحصول على الموافقة بذلك من جهة الترخيص.

كما يعاقب بذات العقوبة أيضا كل من باشر منح شهادات تصديق إلكتروني قبل حصوله على الضمان المنصوص عليه في المادة 9 من هذا القانون.

مادة 17: لا تخل العقوبات الواردة في هذا القانون بحق جهة الترخيص في حظر مباشرة الشخص الطبيعي أو الاعتباري المخالف لأي عمل يتصل بالتوقيعات أو الوسائك الإلكترونية وفقا لهذا القانون، كما لها أن تقوم بوقف سريان الترخيص الصادر إليه مدة لا تزيد عن إثنى عشر شهرا، ولها أيضا أن تلغي هذا الترخيص كليا أو عدم تجديده مستقبلا.

احكام ختامية

مادة 18: يلتزم كل من يباشر نشاط تنطبق عليه أحكام هذا القانون بتوفيق أوضاعه في ميعاد غايته ستة أشهر من تاريخ صدور اللائحة التنفيذية.

مادة 19: مع عدم الإخلال بحقوق المتعاملين، يلتزم كل من يباشر نشاط التصديق الإلكتروني في مفهوم أحكام هذا القانون ويرغب في التوقف عن نشاطه أو عدم توفيق أوضاعه طبقا للمادة 18، بأن يسلم لجهة الترخيص ما لديه من بيانات أو معلومات خاصة بالتوقيعات الإلكترونية ليتم إتلافها بمعرفتها.

مادة 20: يصدر وزير العدل بالتنسيق مع الوزير المختص قرارا بمنح الضبطية القضائية لموظفي وزارته المعنيين بتطبيق أحكام هذا القانون.

ملحق رقم 7

DIRECTIVE 1999/93/CE DU PARLEMENT EUROPÉEN ET DU CONSEIL

du 13 décembre 1999

sur un cadre communautaire pour les signatures électroniques

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité instituant la Communauté européenne, et notamment son article 47, paragraphe 2, et ses articles 55 et 95,

vu la proposition de la Commission [1],

vu l'avis du Comité économique et social [2],

vu l'avis du Comité des régions [3],

statuant conformément à la procédure visée à l'article 251 du traité [4],

considérant ce qui suit:

(1) le 16 avril 1997, la Commission a présenté au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions une communication sur une initiative européenne dans le domaine du commerce électronique;

(2) le 8 octobre 1997, la Commission a présenté au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions une communication intitulée «Assurer la sécurité et la confiance dans la communication électronique — Vers un cadre européen pour les signatures numériques et le chiffrement»;

(3) le 1er décembre 1997, le Conseil a invité la Commission à présenter dès que possible une proposition de directive du Parlement européen et du Conseil sur les signatures numériques;

(4) les communications et le commerce électroniques nécessitent des «signatures électroniques» et des services connexes permettant d'authentifier les données; toute divergence dans les règles relatives à la reconnaissance juridique des signatures électroniques et à l'accréditation des «prestataires de service de certification» dans les États membres risque de constituer un sérieux obstacle à l'utilisation des communications électroniques et au commerce électronique; par ailleurs, l'établissement d'un cadre communautaire clair concernant les conditions applicables aux signatures électroniques contribuera à renforcer la confiance dans les nouvelles technologies et à en favoriser l'acceptation générale; la diversité des législations des États membres ne saurait entraver la libre circulation des marchandises et des services dans le marché intérieur;

(5) il convient de promouvoir l'interopérabilité des produits de signature électronique; conformément à l'article 14 du traité, le marché intérieur comporte un espace dans lequel la libre circulation des marchandises est assurée; des exigences essentielles spécifiques aux produits de signature électronique doivent être respectées afin d'assurer la libre circulation dans le marché intérieur et de susciter la confiance dans les signatures électroniques, sans préjudice du règlement (CE) n° 3381/94 du Conseil du 19 décembre 1994 instituant un régime communautaire de contrôle des exportations de biens à double usage [5] et de la décision 94/942/PESC du Conseil du 19 décembre 1994 relative à l'action commune adoptée par le Conseil, concernant le contrôle des exportations de biens à double usage [6];

(6) la présente directive n'harmonise pas la fourniture de services en ce qui concerne la confidentialité de l'information quand ils sont couverts par des dispositions nationales relatives à l'ordre public ou à la sécurité publique;

(7) le marché intérieur garantit la libre circulation des personnes et, dès lors, les citoyens et résidents de l'Union européenne ont de plus en plus souvent affaire aux autorités d'États membres autres que celui où ils résident; la disponibilité de communications électroniques pourrait être d'une grande utilité dans ce contexte;

(8) eu égard a la rapidité des progrès techniques et à la dimension mondiale d'Internet, il convient d'adopter une approche qui prenne en compte les diverses technologies et services permettant d'authentifier des données par la voie électronique;

(9) les signatures électroniques seront utilisées dans des circonstances et des applications très variées, ce qui entraînera l'apparition de toute une série de nouveaux services et produits liés à celles-ci ou les utilisant; il convient que la définition de ces produits et services ne soit pas limitée à la délivrance et à la gestion de certificats, mais couvre également tout autre service et produit utilisant des signatures électroniques ou connexe à celles-ci, tels les services d'enregistrement, les services horodateurs, les services d'annuaires, les services informatiques ou les services de consultation liée aux signatures électroniques;

(10) le marché intérieur permet aux prestataires de service de certification de développer leurs activités internationales en vue d'accroître leur compétitivité et d'offrir ainsi aux consommateurs et aux entreprises de nouvelles possibilités d'échanger des informations et de commercer en toute sécurité par voie électronique indépendamment des frontières; afin de favoriser la fourniture à l'échelle communautaire de services de certification sur des réseaux ouverts, il y a lieu que les prestataires de service de certification soient libres d'offrir leurs services sans autorisation préalable; on entend par «autorisation

[1] JO C 325 du 23.10.1998, p. 5.
[2] JO C 40 du 15.2.1999, p. 29.
[3] JO C 93 du 6.4.1999, p. 33.
[4] Avis du Parlement européen du 13 janvier 1999 (JO C 104 du 14.4.1999, p. 49), position commune du Conseil du 28 juin 1999 (JO C 243 du 27.8.1999, p. 33) et décision du Parlement européen du 27 octobre 1999 (non encore publiée au Journal officiel). Décision du Conseil du 30 novembre 1999.

[5] JO L 367 du 31.12.1994, p. 1. Règlement modifié par le règlement (CE) n° 837/95 (JO L 90 du 21.4.1995, p. 1).
[6] JO L 367 du 31.12.1994, p. 8. Décision modifiée en dernier lieu par la décision 1999/193/PESC (JO L 73 du 19.3.1999, p. 1).

préalable» non seulement toute autorisation à obtenir par le prestataire de service de certification au moyen d'une décision des autorités nationales avant d'être autorisé à fournir ses services de certification, mais aussi toute autre mesure ayant le même effet;

(11) les régimes volontaires d'accréditation visant à assurer un meilleur service fourni peuvent constituer pour les prestataires de service de certification le cadre propice à l'amélioration de leurs services afin d'atteindre le degré de confiance, de sécurité et de qualité exigés par l'évolution du marché; il est nécessaire que de tels régimes incitent à mettre au point des règles de bonne pratique entre prestataires de service de certification; il y a lieu que ces derniers restent libres de souscrire à ces régimes d'accréditation et d'en bénéficier;

(12) il convient de prévoir la possibilité que les services de certification soient fournis soit par une entité publique, soit par une personne morale ou physique, à condition qu'elle ait été établie conformément au droit national; il convient que les États membres n'interdisent pas aux prestataires de service de certification d'opérer en dehors des régimes d'accréditation volontaires; il y a lieu de veiller à ce que les régimes d'accréditation ne limitent pas la concurrence dans le secteur des services de certification;

(13) les États membres peuvent décider de la façon dont ils assurent le contrôle du respect des dispositions prévues par la présente directive; celle-ci n'exclut pas la mise en place de systèmes de contrôle faisant intervenir le secteur privé; la présente directive n'oblige pas les prestataires de services de certification à demander à être contrôlés dans le cadre de tout régime d'accréditation applicable;

(14) il est important de trouver un équilibre entre les besoins des particuliers et ceux des entreprises;

(15) l'annexe III couvre les exigences relatives aux dispositifs sécurisés de création de signature pour garantir les fonctionnalités des signatures électroniques avancées; elle ne couvre pas l'intégralité du cadre d'utilisation de ces dispositifs; pour le bon fonctionnement du marché intérieur, il est nécessaire que la Commission et les États membres agissent rapidement pour permettre la désignation des organismes chargés d'évaluer la conformité des dispositifs sécurisés de création de signature avec l'annexe III; les besoins du marché exigent que l'évaluation de conformité soit effectuée en temps opportun et de manière efficace;

(16) la présente directive favorise l'utilisation et la reconnaissance juridique des signatures électroniques dans la Communauté; un cadre réglementaire n'est pas nécessaire pour les signatures électroniques utilisées exclusivement à l'intérieur de systèmes résultant d'accords volontaires de droit privé entre un nombre défini de participants; il est nécessaire que la liberté des parties de convenir entre elles des modalités et conditions dans lesquelles elles acceptent les données signées électroniquement soit respectée dans les limites autorisées par le droit national; il convient de reconnaître l'efficacité juridique des signatures électroniques utilisées dans de tels systèmes et leur recevabilité comme preuves en justice;

(17) la présente directive ne vise pas à harmoniser les règles nationales concernant le droit des contrats, en particulier la formation et l'exécution des contrats, ou d'autres formalités de nature non contractuelle concernant les signatures; pour cette raison, il est nécessaire que les dispositions concernant les effets juridiques des signatures électroniques ne portent pas atteinte aux obligations d'ordre formel instituées par le droit national pour la conclusion de contrats ni aux règles déterminant le lieu où un contrat est conclu;

(18) le stockage et la copie de données afférentes à la création d'une signature risquent de compromettre la validité juridique des signatures électroniques;

(19) les signatures électroniques seront utilisées dans le secteur public au sein des administrations nationales et communautaires et dans les communications entre lesdites administrations ainsi qu'avec les citoyens et les opérateurs économiques, par exemple dans le cadre des marchés publics, de la fiscalité, de la sécurité sociale, de la santé et du système judiciaire;

(20) des critères harmonisés relatifs aux effets juridiques des signatures électroniques seront la garantie d'un cadre juridique cohérent dans la Communauté; les droits nationaux fixent des exigences différentes concernant la validité juridique des signatures manuscrites; les certificats peuvent être utilisés pour confirmer l'identité d'une personne qui signe électroniquement; les signatures électroniques avancées basées sur des certificats qualifiés visent à procurer un plus haut degré de sécurité; les signatures électroniques avancées qui sont basées sur des certificats qualifiés et qui sont créées par un dispositif sécurisé de création de signature ne peuvent être considérées comme étant équivalentes, sur un plan juridique, à des signatures manuscrites que si les exigences applicables aux signatures manuscrites ont été respectées;

(21) afin de contribuer à l'acceptation générale des méthodes d'authentification électronique, il est nécessaire de veiller à ce que les signatures électroniques puissent avoir force probante en justice dans tous les États membres; il convient que la reconnaissance juridique des signatures électroniques repose sur des critères objectifs et ne soit pas subordonnée à l'autorisation du prestataire de service de certification concerné; le droit national régit la délimitation des domaines juridiques dans lesquels des documents électroniques et des signatures électroniques peuvent être utilisés; la présente directive n'affecte en rien la capacité d'une juridiction nationale de statuer sur la conformité aux exigences de la présente directive ni les règles nationales relatives à la libre appréciation judiciaire des preuves;

(22) les prestataires de service de certification fournissant des services de certification au public sont soumis à la législation nationale en matière de responsabilité;

(23) le développement du commerce électronique international rend nécessaires des accords internationaux impliquant des pays tiers; afin de garantir l'interopérabilité globale, il pourrait être bénéfique de conclure avec des pays tiers des accords relatifs à des règles multilatérales en matière de reconnaissance mutuelle des services de certification;

(24) pour accroître la confiance des utilisateurs dans les communications et le commerce électroniques, il est nécessaire que les prestataires de service de certification respectent la législation sur la protection des données et qu'ils respectent la vie privée;

(25) il convient que les dispositions relatives à l'utilisation de pseudonymes dans des certificats n'empêchent pas les États membres de réclamer l'identification des personnes conformément au droit communautaire ou national;

(26) les mesures nécessaires pour la mise en œuvre de la présente directive sont arrêtées en conformité avec la décision 1999/468/CE du Conseil du 28 juin 1999 fixant les modalités de l'exercice des compétences d'exécution conférées à la Commission [1];

(27) il y a lieu que la Commission procède, deux ans après sa mise en œuvre, à un réexamen de la présente directive, entre autres pour s'assurer que l'évolution des technologies ou des modifications du contexte juridique n'ont pas engendré d'obstacles à la réalisation des objectifs qui y sont énoncés; il convient qu'elle examine les incidences des domaines techniques connexes et présente un rapport au Parlement européen et au Conseil à ce sujet;

(28) conformément aux principes de subsidiarité et de proportionnalité visés à l'article 5 du traité, l'objectif consistant à instituer un cadre juridique harmonisé pour la fourniture de signatures électroniques et de services connexes ne peut pas être réalisé de manière suffisante par les États membres et peut donc être mieux réalisé par la Communauté; la présente directive n'excède pas ce qui est nécessaire pour atteindre cet objectif,

ONT ARRÊTÉ LA PRÉSENTE DIRECTIVE:

Article premier

Champ d'application

L'objectif de la présente directive est de faciliter l'utilisation des signatures électroniques et de contribuer à leur reconnaissance juridique. Elle institue un cadre juridique pour les signatures électroniques et certains services de certification afin de garantir le bon fonctionnement du marché intérieur.

Elle ne couvre pas les aspects liés à la conclusion et à la validité des contrats ou d'autres obligations légales lorsque des exigences d'ordre formel sont prescrites par la législation nationale ou communautaire; elle ne porte pas non plus atteinte aux règles et limites régissant l'utilisation de documents qui figurent dans la législation nationale ou communautaire.

Article 2

Définitions

Aux fins de la présente directive, on entend par:

1) «signature électronique», une donnée sous forme électronique, qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification;

2) «signature électronique avancée» une signature électronique qui satisfait aux exigences suivantes:

   a) être liée uniquement au signataire;

   b) permettre d'identifier le signataire;

   c) être créée par des moyens que le signataire puisse garder sous son contrôle exclusif

   et

   d) être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable;

3) «signataire», toute personne qui détient un dispositif de création de signature et qui agit soit pour son propre compte, soit pour celui d'une entité ou personne physique ou morale qu'elle représente;

4) «données afférentes à la création de signature», des données uniques, telles que des codes ou des clés cryptographiques privées, que le signataire utilise pour créer une signature électronique;

5) «dispositif de création de signature», un dispositif logiciel ou matériel configuré pour mettre en application les données afférentes à la création de signature;

6) «dispositif sécurisé de création de signature», un dispositif de création de signature qui satisfait aux exigences prévues à l'annexe III;

7) «données afférentes à la vérification de signature», des données, telles que des codes ou des clés cryptographiques publiques, qui sont utilisées pour vérifier la signature électronique;

8) «dispositif de vérification de signature», un dispositif logiciel ou matériel configuré pour mettre en application les données afférentes à la vérification de signature;

9) «certificat», une attestation électronique qui lie des données afférentes à la vérification de signature à une personne et confirme l'identité de cette personne;

10) «certificat qualifié», un certificat qui satisfait aux exigences visées à l'annexe I et qui est fourni par un prestataire de service de certification satisfaisant aux exigences visées à l'annexe II;

11) «prestataire de service de certification», toute entité ou personne physique ou morale qui délivre des certificats ou fournit d'autres services liés aux signatures électroniques;

12) «produit de signature électronique», tout produit matériel ou logiciel, ou élément spécifique de ce produit destiné à être utilisé par un prestataire de service de certification pour la fourniture de services de signature électronique ou destiné à être utilisé pour la création ou la vérification de signatures électroniques;

13) «accréditation volontaire», toute autorisation indiquant les droits et obligations spécifiques à la fourniture de services de certification, accordée, sur demande du prestataire de service de certification concerné, par l'organisme public ou privé chargé d'élaborer ces droits et obligations et d'en contrôler le respect, lorsque le prestataire de service de certification n'est pas habilité à exercer les droits découlant de l'autorisation aussi longtemps qu'il n'a pas obtenu la décision de cet organisme.

[1] JO L 184 du 17.7.1999, p. 23.

Article 3

Accès au marché

1. Les États membres ne soumettent la fourniture des services de certification à aucune autorisation préalable.

2. Sans préjudice des dispositions du paragraphe 1, les États membres peuvent instaurer ou maintenir des régimes volontaires d'accréditation visant à améliorer le niveau du service de certification fourni. Tous les critères relatifs à ces régimes doivent être objectifs, transparents, proportionnés et non discriminatoires. Les États membres ne peuvent limiter le nombre de prestataires accrédités de service de certification pour des motifs relevant du champ d'application de la présente directive.

3. Chaque État membre veille à instaurer un système adéquat permettant de contrôler les prestataires de service de certification établis sur son territoire et délivrant des certificats qualifiés au public.

4. La conformité des dispositifs sécurisés de création de signature aux conditions posées à l'annexe III est déterminée par les organismes compétents, publics ou privés, désignés par les États membres. La Commission, suivant la procédure visée à l'article 9, énonce les critères auxquels les États membres doivent se référer pour déterminer si un organisme peut être désigné.

La conformité aux exigences de l'annexe III qui a été établie par les organismes visés au premier alinéa est reconnue par l'ensemble des États membres.

5. Conformément à la procédure visée à l'article 9, la Commission peut attribuer, et publier au *Journal officiel des Communautés européennes* des numéros de référence de normes généralement admises pour des produits de signature électronique. Lorsqu'un produit de signature électronique est conforme à ces normes, les États membres présument qu'il satisfait aux exigences visées à l'annexe II, point f), et à l'annexe III.

6. Les États membres et la Commission œuvrent ensemble pour promouvoir la mise au point et l'utilisation de dispositifs de vérification de signature, à la lumière des recommandations formulées, pour les vérifications sécurisées de signature, à l'annexe IV et dans l'intérêt du consommateur.

7. Les États membres peuvent soumettre l'usage des signatures électroniques dans le secteur public à des exigences supplémentaires éventuelles. Ces exigences doivent être objectives, transparentes, proportionnées et non discriminatoires et ne s'appliquer qu'aux caractéristiques spécifiques de l'application concernée. Ces exigences ne doivent pas constituer un obstacle aux services transfrontaliers pour les citoyens.

Article 4

Principes du marché intérieur

1. Chaque État membre applique les dispositions nationales qu'il adopte conformément à la présente directive aux prestataires de service de certification établis sur son territoire et aux services qu'ils fournissent. Les États membres ne peuvent imposer de restriction à la fourniture de services de certification provenant d'un autre État membre dans les domaines couverts par la présente directive.

2. Les États membres veillent à ce que les produits de signature électronique qui sont conformes à la présente directive puissent circuler librement dans le marché intérieur.

Article 5

Effets juridiques des signatures électroniques

1. Les États membres veillent à ce que les signatures électroniques avancées basées sur un certificat qualifié et créées par un dispositif sécurisé de création de signature:

a) répondent aux exigences légales d'une signature à l'égard de données électroniques de la même manière qu'une signature manuscrite répond à ces exigences à l'égard de données manuscrites ou imprimées sur papier

et

b) soient recevables comme preuves en justice.

2. Les États membres veillent à ce que l'efficacité juridique et la recevabilité comme preuve en justice ne soient pas refusées à une signature électronique au seul motif que:

— la signature se présente sous forme électronique

ou

— qu'elle ne repose pas sur un certificat qualifié

ou

— qu'elle ne repose pas sur un certificat qualifié délivré par un prestataire accrédité de service de certification

ou

— qu'elle n'est pas créée par un dispositif sécurisé de création de signature.

Article 6

Responsabilité

1. Les États membres veillent au moins à ce qu'un prestataire de service de certification qui délivre à l'intention du public un certificat présenté comme qualifié ou qui garantit au public un tel certificat soit responsable du préjudice causé à toute entité ou personne physique ou morale qui se fie raisonnablement à ce certificat pour ce qui est de:

a) l'exactitude de toutes les informations contenues dans le certificat qualifié à la date où il a été délivré et la présence, dans ce certificat, de toutes les données prescrites pour un certificat qualifié;

b) l'assurance que, au moment de la délivrance du certificat, le signataire identifié dans le certificat qualifié détenait les données afférentes à la création de signature correspondant aux données afférentes à la vérification de signature fournies ou identifiées dans le certificat;

c) l'assurance que les données afférentes à la création de signature et celles afférentes à la vérification de signature puissent être utilisées de façon complémentaire, dans le cas où le prestataire de service de certification génère ces deux types de données,

sauf si le prestataire de service de certification prouve qu'il n'a commis aucune négligence.

2. Les États membres veillent au moins à ce qu'un prestataire de service de certification qui a délivré à l'intention du public un certificat présenté comme qualifié soit responsable du préjudice causé à une entité ou personne physique ou morale qui se prévaut raisonnablement du certificat, pour avoir omis de faire enregistrer la révocation du certificat, sauf si le prestataire de service de certification prouve qu'il n'a commis aucune négligence.

3. Les États membres veillent à ce qu'un prestataire de service de certification puisse indiquer, dans un certificat qualifié, les limites fixées à son utilisation, à condition que ces limites soient discernables par des tiers. Le prestataire de service de certification ne doit pas être tenu responsable du préjudice résultant de l'usage abusif d'un certificat qualifié qui dépasse les limites fixées à son utilisation.

4. Les États membres veillent à ce qu'un prestataire de service de certification puisse indiquer, dans un certificat qualifié, la valeur limite des transactions pour lesquelles le certificat peut être utilisé, à condition que cette limite soit discernable par des tiers.

Le prestataire de service de certification n'est pas responsable des dommages qui résultent du dépassement de cette limite maximale.

5. Les dispositions des paragraphes 1 à 4 s'appliquent sans préjudice de la directive 93/13/CEE du Conseil du 5 avril 1993 concernant les clauses abusives dans les contrats conclus avec les consommateurs [1].

Article 7

Aspects internationaux

1. Les États membres veillent à ce que les certificats délivrés à titre de certificats qualifiés à l'intention du public par un prestataire de service de certification établi dans un pays tiers soient reconnus équivalents, sur le plan juridique, aux certificats délivrés par un prestataire de service de certification établi dans la Communauté:

a) si le prestataire de service de certification remplit les conditions visées dans la présente directive et a été accrédité dans le cadre d'un régime volontaire d'accréditation établi dans un État membre

ou

b) si un prestataire de service de certification établi dans la Communauté, qui satisfait aux exigences visées dans la présente directive, garantit le certificat

ou

c) si le certificat ou le prestataire de service de certification est reconnu en application d'un accord bilatéral ou multilatéral entre la Communauté et des pays tiers ou des organisations internationales.

2. Afin de faciliter les services de certification internationaux avec des pays tiers et la reconnaissance juridique des signatures électroniques avancées émanant de pays tiers, la Commission fait, le cas échéant, des propositions visant à la mise en œuvre effective de normes et d'accords internationaux applicables aux services de certification. En particulier et si besoin est, elle soumet des propositions au Conseil concernant des mandats appropriés de négociation d'accords bilatéraux et multilatéraux avec des pays tiers et des organisations internationales. Le Conseil statue à la majorité qualifiée.

3. Lorsque la Commission est informée de l'existence de difficultés rencontrées par des entreprises communautaires pour obtenir l'accès au marché de pays tiers, elle peut, au besoin, soumettre au Conseil des propositions en vue d'obtenir le mandat nécessaire pour négocier des droits comparables pour les entreprises communautaires dans ces pays tiers. Le Conseil statue à la majorité qualifiée.

Les mesures prises au titre du présent paragraphe ne portent pas atteinte aux obligations de la Communauté et des États membres qui découlent d'accords internationaux pertinents.

Article 8

Protection des données

1. Les États membres veillent à ce que les prestataires de service de certification et les organismes nationaux responsables de l'accréditation ou du contrôle satisfassent aux exigences prévues par la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données [2].

2. Les États membres veillent à ce qu'un prestataire de service de certification qui délivre des certificats à l'intention du public ne puisse recueillir des données personnelles que directement auprès de la personne concernée ou avec le consentement explicite de celle-ci et uniquement dans la mesure où cela est nécessaire à la délivrance et à la conservation du certificat. Les données ne peuvent être recueillies ni traitées à d'autres fins sans le consentement explicite de la personne intéressée.

3. Sans préjudice des effets juridiques donnés aux pseudonymes par la législation nationale, les États membres ne peuvent empêcher le prestataire de service de certification d'indiquer dans le certificat un pseudonyme au lieu du nom du signataire.

Article 9

Comité

1. La Commission est assistée par le «comité sur les signatures électroniques», ci-après dénommé «comité».

2. Dans le cas où il est fait référence au présent paragraphe, les articles 4 et 7 de la décision 1999/468/CE s'appliquent, dans le respect des dispositions de l'article 8 de celle-ci.

La période prévue à l'article 4, paragraphe 3, de la décision 1999/468/CE est fixée à trois mois.

3. Le comité adopte son règlement de procédure.

Article 10

Tâches du comité

Le comité clarifie les exigences visées dans les annexes de la présente directive, les critères visés à l'article 3, paragraphe 4, et les normes généralement reconnues pour les produits de signature électronique établies et publiées en application de l'article 3, paragraphe 5, conformément à la procédure visée à l'article 9, paragraphe 2.

[1] JO L 95 du 21.4.1993, p. 29.

[2] JO L 281 du 23.11.1995, p. 31.

Article 11

Notification

1. Les États membres communiquent à la Commission et aux autres États membres:

a) les informations sur les régimes volontaires d'accréditation au niveau national ainsi que toute exigence supplémentaire au titre de l'article 3, paragraphe 7;

b) les nom et adresse des organismes nationaux responsables de l'accréditation et du contrôle, ainsi que des organismes visés à l'article 3, paragraphe 4

et

c) les nom et adresse de tous les prestataires de service de certification nationaux accrédités.

2. Toute information fournie en vertu du paragraphe 1 et les changements concernant celle-ci sont communiqués par les États membres dans les meilleurs délais.

Article 12

Examen

1. La Commission procède à l'examen de la mise en œuvre de la présente directive et en rend compte au Parlement européen et au Conseil pour le 19 juillet 2003 au plus tard.

2. Cet examen doit permettre, entre autres, de déterminer s'il convient de modifier le champ d'application de la présente directive pour tenir compte de l'évolution des technologies, du marché et du contexte juridique. Le compte rendu d'examen doit notamment comporter une évaluation, fondée sur l'expérience acquise, des aspects relatifs à l'harmonisation. Le compte rendu est accompagné, le cas échéant, de propositions législatives.

Article 13

Mise en œuvre

1. Les États membres mettent en vigueur les dispositions législatives, réglementaires et administratives nécessaires pour se conformer à la présente directive avant le 19 juillet 2001. Ils en informent immédiatement la Commission.

Lorsque les États membres adoptent ces dispositions, celles-ci contiennent une référence à la présente directive ou sont accompagnées d'une telle référence lors de leur publication officielle. Les modalités de cette référence sont adoptées par les États membres.

2. Les États membres communiquent à la Commission le texte des dispositions essentielles de droit interne qu'ils adoptent dans le domaine régi par la présente directive.

Article 14

Entrée en vigueur

La présente directive entre en vigueur le jour de sa publication au *Journal officiel des Communautés européennes*.

Article 15

Destinataires

Les États membres sont destinataires de la présente directive.

Fait à Bruxelles, le 13 décembre 1999.

Par le Parlement européen	*Par le Conseil*
La présidente	*Le président*
N. FONTAINE	S. HASSI

ANNEXE I

Exigences concernant les certificats qualifiés

Tout certificat qualifié doit comporter:

a) une mention indiquant que le certificat est délivré à titre de certificat qualifié;

b) l'identification du prestataire de service de certification ainsi que le pays dans lequel il est établi;

c) le nom du signataire ou un pseudonyme qui est identifié comme tel;

d) la possibilité d'inclure, le cas échéant, une qualité spécifique du signataire, en fonction de l'usage auquel le certificat est destiné;

e) des données afférentes à la vérification de signature qui correspondent aux données pour la création de signature sous le contrôle du signataire;

f) l'indication du début et de la fin de la période de validité du certificat;

g) le code d'identité du certificat;

h) la signature électronique avancée du prestataire de service de certification qui délivre le certificat;

i) les limites à l'utilisation du certificat, le cas échéant et

j) les limites à la valeur des transactions pour lesquelles le certificat peut être utilisé, le cas échéant.

ANNEXE II

Exigences concernant les prestataires de service de certification délivrant des certificats qualifiés

Les prestataires de service de certification doivent:

a) faire la preuve qu'ils sont suffisamment fiables pour fournir des services de certification;

b) assurer le fonctionnement d'un service d'annuaire rapide et sûr et d'un service de révocation sûr et immédiat;

c) veiller à ce que la date et l'heure d'émission et de révocation d'un certificat puissent être déterminées avec précision;

d) vérifier, par des moyens appropriés et conformes au droit national, l'identité et, le cas échéant, les qualités spécifiques de la personne à laquelle un certificat qualifié est délivré;

e) employer du personnel ayant les connaissances spécifiques, l'expérience et les qualifications nécessaires à la fourniture des services et, en particulier, des compétences au niveau de la gestion, des connaissances spécialisées en technologie des signatures électroniques et une bonne pratique des procédures de sécurité appropriées; ils doivent également appliquer des procédures et méthodes administratives et de gestion qui soient adaptées et conformes à des normes reconnues;

f) utiliser des systèmes et des produits fiables qui sont protégés contre les modifications et qui assurent la sécurité technique et cryptographique des fonctions qu'ils assument;

g) prendre des mesures contre la contrefaçon des certificats et, dans les cas où le prestataire de service de certification génère des données afférentes à la création de signature, garantir la confidentialité au cours du processus de génération de ces données;

h) disposer des ressources financières suffisantes pour fonctionner conformément aux exigences prévues par la présente directive, en particulier pour endosser la responsabilité de dommages, en contractant, par exemple, une assurance appropriée;

i) enregistrer toutes les informations pertinentes concernant un certificat qualifié pendant le délai utile, en particulier pour pouvoir fournir une preuve de la certification en justice. Ces enregistrements peuvent être effectués par des moyens électroniques;

j) ne pas stocker ni copier les données afférentes à la création de signature de la personne à laquelle le prestataire de service de certification a fourni des services de gestion de clés;

k) avant d'établir une relation contractuelle avec une personne demandant un certificat à l'appui de sa signature électronique, informer cette personne par un moyen de communication durable des modalités et conditions précises d'utilisation des certificats, y compris des limites imposées à leur utilisation, de l'existence d'un régime volontaire d'accréditation et des procédures de réclamation et de règlement des litiges. Cette information, qui peut être transmise par voie électronique, doit être faite par écrit et dans une langue aisément compréhensible. Des éléments pertinents de cette information doivent également être mis à la disposition, sur demande, de tiers qui se prévalent du certificat;

l) utiliser des systèmes fiables pour stocker les certificats sous une forme vérifiable de sorte que:

— seules les personnes autorisées puissent introduire et modifier des données,

— l'information puisse être contrôlée quant à son authenticité,

— les certificats ne soient disponibles au public pour des recherches que dans les cas où le titulaire du certificat a donné son consentement et

— toute modification technique mettant en péril ces exigences de sécurité soit apparente pour l'opérateur.

ANNEXE III

Exigences pour les dispositifs sécurisés de création de signature électronique

1. Les dispositifs sécurisés de création de signature doivent au moins garantir, par les moyens techniques et procédures appropriés, que:

   a) les données utilisées pour la création de la signature ne puissent, pratiquement, se rencontrer qu'une seule fois et que leur confidentialité soit raisonnablement assurée;

   b) l'on puisse avoir l'assurance suffisante que les données utilisées pour la création de la signature ne puissent être trouvées par déduction et que la signature soit protégée contre toute falsification par les moyens techniques actuellement disponibles;

   c) les données utilisées pour la création de la signature puissent être protégées de manière fiable par le signataire légitime contre leur utilisation par d'autres.

2. Les dispositifs sécurisés de création de signature ne doivent pas modifier les données à signer ni empêcher que ces données soient soumises au signataire avant le processus de signature.

ANNEXE IV

Recommandations pour la vérification sécurisée de la signature

Durant le processus de vérification de la signature, il convient de veiller, avec une marge de sécurité suffisante, à ce que:

a) les données utilisées pour vérifier la signature correspondent aux données affichées à l'intention du vérificateur;

b) la signature soit vérifiée de manière sûre et que le résultat de cette vérification soit correctement affiché;

c) le vérificateur puisse, si nécessaire, déterminer de manière sûre le contenu des données signées;

d) l'authenticité et la validité du certificat requis lors de la vérification de la signature soient vérifiées de manière sûre;

e) le résultat de la vérification ainsi que l'identité du signataire soient correctement affichés;

f) l'utilisation d'un pseudonyme soit clairement indiquée et

g) tout changement ayant une influence sur la sécurité puisse être détecté.

ملحق رقم 8

قانون الأونيسترال النموذجى بشأن التوقيعات الإليكترونية باللغات الأصلية العربية والإنجليزية والفرنسية

(أ) النسخة العربية

قانون الأونيسترال النموذجى بشأن التوقيعات الإليكترونية ٢٠٠١ (١)

مادة ١- نطاق الإنطباق :

ينطبق هذا القانون حيثما تستخدم توقيعات إليكترونية فى سياق (٢) انشطة تجارية (٣) وهو لا يلغى أى قاعدة قانونية يكون القصد منها حماية المستهلكين .

---

(١) مقتطف من تقرير لجنة الأمم المتحدة للقانون التجارى الدولى عن أعمال دورتها الرابعة والثلاثين ، المعقودة فى فيينا .

(٢) تقترح اللجنة النص التالى للدول التى قد ترغب فى توسيع نطاق انطباق هذا القانون :

« ينطبق هذا القانون حيثما تستخدم توقيعات إليكترونية باستثناء الأحوال التالية (...) » .

(٣) ينبغى تفسير مصطلح « تجارى » واسعاً بحيث يشمل المسائل الناشئة عن جميع العلاقات ذات الطابع التجارى ، سواء أكانت تعاقدية أم غير تعاقدية . وتشمل العلاقات ذات الطابع التجارى المعاملات التالية ، على سبيل المثال لا الحصر : أى معاملة تجارية لتوريد أو تبادل البضائع أو الخدمات ، إتفاق التوزيع ، التمثيل التجارى أو الوكالة التجارية ، العمولة ، البيع الإيجارى ، تشييد المنشآت ، الخدمات الاستشارية ، الأعمال الهندسية ، منح الرخص ، الاستثمار ، التمويل ، الأعمال المصرفية ، التأمين ، اتفاق أو امتياز الاستغلال ، المشاريع المشتركة وغيرها من اشكال التعاون الصناعى او الأعمال ، نقل البضائع او الركاب جوا او بحرا او

مادة ٢- التعاريف :

لأغراض هذا القانون :

أ- « توقيع إليكتروني » يعني بيانات في شكل إليكتروني مدرجة في رسالة بيانات أو مضافة إليها أو مرتبطة بها منطقياً ، يجوز أن تستخدم لتعيين هوية الموقع بالنسبة إلى رسالة البيانات ، ولبيان موافقة الموقع على المعلومات الواردة في رسالة البيانات .

ب- « شهادة » تعني رسالة بيانات أو سجلاً آخر يؤكدان الارتباط بين الموقع وبيانات إنشاء التوقيع .

جـ- « رسالة بيانات » تعني معلومات يتم إنشاؤها أو إرسالها أو استلامها أو تخزينها بوسائل إليكترونية أو ضوئية أو بوسائل مشابهة ، بما في ذلك ، على سبيل المثال لا الحصر ، التبادل الإليكتروني للبيانات أو البريد الإليكتروني أو البرق أو التلكس أو النسخ البرقي .

د- « موقع » يعني شخصاً حائزاً على بيانات إنشاء توقيع ويتصرف إما بالأصالة عن نفسه وإما بالنيابة عن الشخص الذي يمثله .

هـ- « مقدم خدمات تصديق » يعني شخصاً يصدر الشهادات ويجوز أن يقدم خدمات أخرى ذات صلة بالتوقيعات الإليكترونية .

و- « طرف معول » يعني شخصاً يجوز ان يتصرف استناداً إلى شهادة أو إلى توقيع إليكتروني .

مادة ٣- المعاملة المكافئة لتكنولوجيا التوقيع :

لا يطبق أي من أحكام هذا القانون ، باستثناء المادة ٥ ، بما يشكل استبعاداً أو تقييداً أو حرماناً من مفعول قانوني لأي طريقة لإنشاء توقيع إليكتروني تفي بالاشتراطات المشار إليها في الفقرة ١ من المادة

مادة ٤- التفسير :

١- يولى الاعتبار في تفسير هذا القانون لمصدره الدولي وللحاجة إلى تشجيع توحيد تطبيقه ومراعاة حسن النية .

٢- المسائل المتعلقة بالأمور التي يحكمها هذا القانون ولا يسويها صراحة ، تسوى وفقاً للمبادئ العامة التي يستند إليها هذا القانون .

مادة ٥- التغيير بالاتفاق :

يجوز الاتفاق على الخروج على أحكام هذا القانون أو تغيير مفعولها ، ما لم يكن من شأن ذلك الإتفاق أن يكون غير صحيح أو غير ساري المفعول بمقتضى القانون المنطبق .

مادة ٦- الإمتثال لاشتراط التوقيع :

١- حيثما يشترط القانون وجود توقيع من شخص ، يعد ذلك الاشتراط مستوفى بالنسبة إلى رسالة البيانات إذا استخدم توقيع إليكتروني موثوق به بالقدر المناسب للغرض الذي انشئت أو أبلغت من أجله رسالة البيانات ، في ضوء كل الظروف ، بما في ذلك أي اتفاق ذي صلة .

٢- تنطبق الفقرة ١ سواء أكان الاشتراط المشار إليه فيها في شكل التزام أم كان القانون يكتفي بالنص على تبعات تترتب على عدم وجود توقيع .

٣- يعتبر التوقيع الإليكتروني موثوقاً به لغرض الوفاء بالاشتراط المشار إليه في الفقرة ١ إذا :

أ- كانت بيانات إنشاء التوقيع مرتبطة ، في السياق الذي تستخدم فيه ، بالموقع دون أي شخص آخر .

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

د- كان الغرض من اشتراط التوقيع قانوناً هو تأكيد سلامة المعلومات التى يتعلق بها التوقيع وكان أى تغيير يجرى فى تلك المعلومات بعد وقت التوقيع قابلاً للاكتشاف .

٤- لا تحد الفقرة ٣ من قدرة أى شخص :

أ- على القيام بأى طريقة أخرى بإثبات موثوقية التوقيع الإليكترونى ، لغرض الوفاء بالاشتراط المشار إليه فى الفقرة ١ ، أو

ب- على تقديم دليل على عدم موثوقية التوقيع الإليكترونى .

٥- لا تنطبق أحكام هذه المادة على ما يلى (...) .

مادة ٧- الوفاء بالمادة ٦ :

١- يجوز لـ (أى شخص أو جهاز أو سلطة تعينهم الدولة المشترعة جهة مختصة ، سواء أكانت عامة أم خاصة) تحديد التواقيع الإليكترونية التى تفى بأحكام المادة ٦ من هذا القانون .

٢- يتعين أن يكون أى تحديد يتم بمقتضى الفقرة ١ متسقاً مع المعايير المعترف بها .

٣- ليس فى هذه المادة ما يخل بسريان مفعول قواعد القانون الدولى الخاص .

مادة ٨- سلوك الموقع :

١- حيثما يمكن استخدام بيانات إنشاء التوقيع لإنشاء توقيع يكون له مفعول قانونى ، يتعين على كل موقع :

أ- أن يمارس عناية معقولة لإجتناب استخدام بيانات إنشاء توقيعه استخداماً غير مأذون به .

ب- أن يبادر ، دون تأخر لا مسوغ له ، إلى استخدام الوسائل التى يوفرها مقدم خدمات التصديق بمقتضى المادة ٩ من هذا القانون، أو على أى نحو آخر إلى بذل جهود معقولة ، لإشعار أى

التوقيع الإليكترونى أو أن يقدم خدمات تأييد التوقيع الإليكترونى ، وذلك فى حالة :

١- معرفة الموقع بأن بيانات إنشاء التوقيع تعرضت لما يثير الشبة، أو

٢- كون الظروف المعروفة لدى الموقع تؤدى إلى احتمال كبير بأن بيانات إنشاء التوقيع ربما تكون قد تعرضت لما يثير الشبهة .

جـ- أن يمارس ، فى حال استخدام شهادة لتأييد التوقيع الإليكترونى ، عناية معقولة لضمان دقة واكتمال كل ما يقدمه الموقع من تأكيدات مادية ذات صلة بالشهادة طيلة دورة سريانها ، أو يتوخى إدراجها فى الشهادة .

٢- يتحمل الموقع التبعات القانونية لتخلفه عن الوفاء باشتراطات الفقرة ١ .

مادة ٩- سلوك مقدم خدمات التصديق :

١- حيثما يوفر مقدم خدمات التصديق خدمات لتأييد توقيع إليكترونى يجوز استخدامه لاعطاء مفعول قانونى بصفته توقيعاً ، يتعين على مقدم خدمات التصديق المشار إليه :

أ- أن يتصرف وفقاً للتأكيدات التى يقدمها بخصوص سياساته وممارساته .

ب- أن يمارس عناية معقولة لضمان دقة واكتمال كل ما يقدمه من تأكيدات جوهرية ذات صلة بالشهادة طيلة دورة سريانها ، أو مدرجة فى الشهادة .

جـ- أن يوفر وسائل يكون الوصول إليها متيسراً بقدر معقول وتمكن الطرف المعول من التأكد ، من الشهادة مما يلى :

١- هوية مقدم خدمات التصديق .

٢- أن الموقع المعينة هويته فى الشهادة كان يسيطر على بيانات

مادة ٢- التعاريف :

لأغراض هذا القانون :

أ- « توقيع إليكترونى » يعنى بيانات فى شكل إليكترونى مدرجة فى رسالة بيانات أو مضافة إليها أو مرتبطة بها منطقياً ، يجوز أن تستخدم لتعيين هوية الموقع بالنسبة إلى رسالة البيانات ، ولبيان موافقة الموقع على المعلومات الواردة فى رسالة البيانات .

ب- « شهادة » تعنى رسالة بيانات أو سجلاً آخر يؤكدان الارتباط بين الموقع وبيانات إنشاء التوقيع .

جـ- « رسالة بيانات » تعنى معلومات يتم إنشاؤها أو إرسالها أو استلامها أو تخزينها بوسائل إليكترونية أو ضوئية أو بوسائل مشابهة ، بما فى ذلك ، على سبيل المثال لا الحصر ، التبادل الإليكترونى للبيانات أو البريد الإليكترونى أو البرق أو التلكس أو النسخ البرقى .

د- « موقع » يعنى شخصاً حائزاً على بيانات إنشاء توقيع ويتصرف إما بالأصالة عن نفسه وإما بالنيابة عن الشخص الذى يمثله .

هـ- « مقدم خدمات تصديق » يعنى شخصاً يصدر الشهادات ويجوز أن يقدم خدمات أخرى ذات صلة بالتوقيعات الإليكترونية .

و- « طرف معول » يعنى شخصاً يجوز أن يتصرف استناداً إلى شهادة أو إلى توقيع إليكترونى .

مادة ٣- المعاملة المكافئة لتكنولوجيا التوقيع :

لا يطبق أى من أحكام هذا القانون ، باستثناء المادة ٥ ، بما يشكل استبعاداً أو تقييداً أو حرماناً من مفعول قانونى لأى طريقة لإنشاء توقيع إليكترونى تفى بالإشتراطات المشار إليها فى الفقرة ١ من المادة

مادة ٤- التفسير :

١- يولى الاعتبار فى تفسير هذا القانون لمصدره الدولى وللحاجة إلى تشجيع توحيد تطبيقه ومراعاة حسن النية .

٢- المسائل المتعلقة بالأمور التى يحكمها هذا القانون ولا يسويها صراحة ، تسوى وفقاً للمبادئ العامة التى يستند إليها هذا القانون .

مادة ٥- التغيير بالاتفاق :

يجوز الاتفاق على الخروج على أحكام هذا القانون أو تغيير مفعولها ، ما لم يكن من شأن ذلك الإتفاق أن يكون غير صحيح أو غير سارى المفعول بمقتضى القانون المنطبق .

مادة ٦- الإمتثال لاشتراط التوقيع :

١- حيثما يشترط القانون وجود توقيع من شخص ، يعد ذلك الاشتراط مستوفى بالنسبة إلى رسالة البيانات إذا استخدم توقيع إليكترونى موثوق به بالقدر المناسب للغرض الذى انشئت او ابلغت من أجله رسالة البيانات ، فى ضوء كل الظروف ، بما فى ذلك اى اتفاق ذى صلة .

٢- تنطبق الفقرة ١ سواء اكان الاشتراط المشار إليه فيها فى شكل التزام ام كان القانون يكتفى بالنص على تبعات تترتب على عدم وجود توقيع .

٣- يعتبر التوقيع الإليكترونى موثوقًا به لغرض الوفاء بالاشتراط المشار إليه فى الفقرة ١ إذا :

أ- كانت بيانات إنشاء التوقيع مرتبطة ، فى السياق الذى تستخدم فيه ، بالموقع دون اى شخص آخر .

ب- كانت بيانات إنشاء التوقيع خاضعة ، وقت التوقيع ، لسيطرة الموقع دون اى شخص آخر .

٣- أن بيانات إنشاء التوقيع كانت صحيحة فى الوقت الذى أصدرت فيه الشهادة أو قبله .

د- أن يوفر وسائل يكون الوصول إليها متيسراً بقدر معقول وتمكن الطرف المعول من التأكد عند الاقتضاء ، من الشهادة أو من سواها ، مما يلى :

١- الطريقة المستخدمة فى تعيين هوية الموقع .

٢- وجود أى تقييد على الغرض أو القيمة التى يجوز أن تستخدم من أجلها بيانات إنشاء التوقيع أو أن تستخدم من أجلها الشهادة .

٣- أن بيانات إنشاء التوقيع صحيحة ولم تتعرض لما يثير الشبهة.

٤- وجود أى تقييد على نطاق أو مدى المسؤولية التى اشترطها مقدم خدمات التصديق .

٥- ما إذا كانت هناك وسائل متاحة للموقع لتقديم إشعار بمقتضى الفقرة ١ (ب) من المادة ٨ من هذا القانون .

٦- ما إذا كانت تتاح خدمة إلغاء آنية .

هـ- أن يوفر ، حيثما تقدم الخدمات بمقتضى الفقرة الفرعية (د) (٥) ، وسيلة للموقع لتقديم إشعار بمقتضى الفقرة ١ (ب) من المادة ٨ من هذا القانون ، وأن يضمن ، حيثما تقدم الخدمات بمقتضى الفقرة الفرعية (د) (٦) ، إتاحة خدمة إلغاء آنية .

و- أن يستخدم فى أداء خدماته نظماً وإجراءات وموارد بشرية جديرة بالثقة .

٢- يتحمل مقدم خدمات التصديق التبعات القانونية لتخلفه عن الوفاء باشتراطات الفقرة ١ .

مادة ١٠- الجدارة بالثقة :

لأغراض الفقرة ١ (و) من المادة ٩ من هذا القانون ، لدى تقرير ما إذا كانت أى نظم وإجراءات وموارد بشرية يستخدمها مقدم خدمات التصديق جديرة بالثقة ، أو مدى جدارتها بالثقة إيلاء الاعتبار للعوامل التالية :

أ- الموارد المالية والبشرية ، بما فى ذلك توافر الموجودات ، أو

ب- جودة نظم المعدات والبرمجيات ، أو

جـ- إجراءات تجهيز الشهادات وطلبات الحصول على الشهادات والإحتفاظ بالسجلات ، أو

د- إتاحة المعلومات للموقعين المعينة هويتهم فى الشهادات وللأطراف المعولة المحتملة ، أو

هـ- انتظام ومدى مراجعة الحسابات من جانب هيئة مستقلة ، أو

و- وجود إعلان من الدولة أو من هيئة اعتماد.أو من مقدم خدمات التصديق بخصوص الامتثال لما سبق ذكره أو بخصوص وجوده ، أو

ز- أى عامل آخر ذى صلة .

مادة ١١- سلوك الطرف المعول :

يتحمل الطرف المعول التبعات القانونية الناجمة عن تخلفه عن :

أ- اتخاذ خطوات معقولة للتحقق من موثوقية التوقيع الإليكترونى ، أو

ب- اتخاذ خطوات معقولة ، إذا كان التوقيع الإليكترونى مؤيداً بشهادة ، لأجل :

١- التحقق من صلاحية الشهادة أو وقفها أو إلغائها .

٢- مراعاة وجود أى تقييد بخصوص الشهادة .

مادة ١٢- الاعتراف بالشهادات والتوقيعات الإليكترونية الأجنبية :

١- لدى تقرير ما إذا كانت الشهادة أو التوقيع الإليكترونى سارى

أ- الموقع الجغرافى الذى تصدر فيه الشهادة أو ينشأ أو يستخدم فيه التوقيع الإليكترونى ، أو

ب- الموقع الجغرافى لمكان عمل المصدر أو الموقع .

٢- يكون للشهادة التى تصدر خارج (الدولة المشترعة) المفعول القانونى نفسه فى (الدولة المشترعة) الذى للشهادة التى تصدر فى (الدولة المشترعة) إذا كانت تتيح مستوى مكافئاً جوهرياً من الموثوقية.

٣- يكون للتوقيع الإليكترونى الذى ينشأ أو يستخدم خارج (الدولة المشرعة) المفعول القانونى نفسه فى (الدولة المشرعة) الذى للتوقيع الذى ينشأ أو يستخدم فى (الدولة المشرعة) إذا كان يتيح مستوى مكافئاً جوهرياً من الموثوقية .

٤- لدى تقرير ما إذا كانت الشهادة أو التوقيع الإليكترونى يتيحان مستوى مكافئاً جوهرياً من الموثوقية لأغراض الفقرة ٢ أو الفقرة ٣ ، يولى الاعتبار للمعايير الدولية المعترف بها ولأى عوامل أخرى ذات صلة .

٥- إذا اتفقت الأطراف فيما بينها ، برغم ما ورد فى الفقرات ٢ و٣ و٤ ، على استخدام أنواع معينة من التوقيعات الإليكترونية أو الشهادات ، يتعين الاعتراف بذلك الإتفاق باعتباره كافياً لأغراض الاعتراف عبر الحدود ، ما لم يكن من شأن ذلك الإتفاق أن يكون غير صحيح أو غير سارى المفعول بمقتضى القانون المنطبق .

*****

قائمة المراجع :

باللغة العربية

المراجع العامة :

1- د-جلال علي العدوي، الإثبات،منشأة المعارف بالاسكندرية-سنة1996

2-د/- سليمان مرقس- الوافي في شرح القانون المدني ، أصول الإثبات وإجراءاته في المواد المدنية.

3--د/عادل حسن علي: الإثبات في المواد المدنية ، مكتبة زهراء الشرق ، 1996

4-د/عباس العبودي : شرح أحكام قانون الإثبات ، دار الثقافة للنشر و التوزيع -1999

5-د/عبد الرزاق أحمد السنهوري : الوسيط في شرح القانون المدني الجديد الإثبات –آثار الالتزام ، الجزء الثاني –منشورات الحلبي الحقوقية بيروت لبنان، 2000 .

6-د- عبد الرزاق السنهوري –الوسيط في شرح القانون المدني الجديد ، نظرية الالتزام بوجه عام ،مصادر الالتزام ،المجلد الثاني ،منشورات الحلبي الحقوقية 2000

7-أ/عبد العزيز سليم : الإجراءات العملية في شرح قانون الإثبات ،1998

8-- د.الغوثي بن ملحة ، قواعد وطرق الإثبات ومباشرتها في النظام القانوني الجزائري، الطبعة الأولى، مطبوعات الديوان الجزائري للأشغال التربوية ،2001

9- المستشار محمد أحمد عابدين،حجية الورقة الرسمية والعرفية،دار الكتب القانونية،سنة1997

10- د-محمد حسن قاسم،الإثبات في المواد المدنية والتجارية،الدار الجامعية

المراجع الخاصة:

1- أ/إبراهيم السيد أحمد : قانون التجارة الإلكتروني والتوقيع الإلكتروني والملكية الفكرية والأدبية ،الدار الجامعية –2005

2-د/سعيد السيد قنديل : التوقيع الالكتروني ، دار الجامعة الجديدة للنشر –2004

3-د/عبد الفتاح بيومي حجازي : التوقيع الإلكتروني في النظم القانونية المقارنة ، دار الفكر الجامعي –2005

4- د/عبد الفتاح مراد : شرح قوانين التوقيع الإلكتروني في مصر والدول العربية ، شركة البهاء للبرمجيات والكمبيوتر والنشر الإلكتروني

5- أ/علي كحلون : الجوانب القانونية لقنوات الاتصال الحديثة والتجارة الإلكترونية دار إسهامات في أدبيات المؤسسة –2002

6- عمرو عيسى الفقي : وسائل الاتصال الحديثة وحجيتها في الإثبات ، المكتب الجامعي الحديث -2006

7- -أ/منير محمد الجنبيهي و أ/ممدوح محمد الجنبيهي : التوقيع الإلكتروني وحجيته في الإثبات ، دار الفكر الجامعي -2005

8- محمد الأمين الرومي،التعاقد الإلكتروني عبر الانترنيت ،دار المطبوعات الجامعية، الطبعة الأولى ، 2004

9-د/محمد حسين منصور :المسؤولية الإلكترونية ، دار الجامعة الجديدة للنشر -200

الرسائل الجامعية:

1- أ-بن شنات صالح ،الكتابة كدليل إثبات في المواد المدنية ، رسالة ماجستير في القانون الخاص ، جامعة السانيا وهران.

2- أ/قارة مولود ،التوقيع الإلكتروني كدليل إثبات في القانون الخاص،ماجستير في القانون الخاص ،جامعة فرحات عباس سطيف (الجزائر)،سنة 2004

المقالات:

-محمد بودالي، التوقيع الالكتروني،مجلة الإدارة عدد 26 سنة 2003 .

النصوص القانونية ومشاريع القوانين:

1- قانون التجارة الالكترونية البحريني ،الصادر بتاريخ 7 رجب 423 هـ الموافق 14 سبتمبر 2002 م.

2- قانون عدد 83 لسنة 2000 مؤرخ في 9 اوت 2000 يتعلق بالمبادلات والتجارة الالكترونية التونسي .

3- القانون رقم (2) لسنة 2002 بشأن المعاملات والتجارة الالكترونية بإمارة دبي .

4- قانون رقم 15 لسنة 2004 بتنظيم التوقيع الإلكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات .
5- مشروع قانون لتنظيم التوقيع الإلكتروني بجمهورية مصر العربية .
6- قانون الأونيسترال النموذجي بشأن التوقيعات الإلكترونية (النسخة العربية).
7- قانون رقم 05 – 10 المؤرخ في 20 جوان 2005 يعدل ويتمم المر رقم 75-58 المؤرخ في 26 سبتمبر 1975 والمتضمن القانون المدني المعدل والمتمم.
8- القانون رقم 06-02 المؤرخ في 20 فبراير2006 يتضمن تنظيم مهنة التوثيق.

باللغة الفرنسية:

المراجع الخاصة

الكتب:

1- Alain Bensoussan et Y ves le roux , Cryptologie et signature électronique aspects juridiques, Hermes Science Publication, Paris, 1999.
2- Arnaud-f .Fausse ;La signature électronique transaction et confiance sur internet,Dunod paris 2001.
3-Christan Féral-Schuhl ;Cyber droit,le droit a l'épreuve de l'internet ;3 em édition , Dalloz,Dunod .4
4-Delphine Majdanski ;la signature et les mentions manuscrites dans les contrats , presses universitaires de bordeaux,2003
5-Didier Gobert et étienne Montero , La signature dans les contrats et les paiements
6- Pierre bresse ,guide juridique de l'internet et du commerce électronique,entreprendre informatique,1998 .

7- Thierry Piette-coudol ;échanges électroniques Certification et sécurité , édition litec ,2001

الرسائل الجامعية

1-Julien esnault ;la signature électronique ;université de droit droit, d'économie et de science sociales paris II pantheo-assas ;publié sur signelec.com

2-Meme Mostefa-Kara Farida née Settouti, La preuve écrit en droit civil algérien , mémoire pour le diplôme de magistère en droit , université d'Alger , Institut des Sciences Juridiques et administratives, 1982.

3- Stéphane CAÏDI ; La preuve et la conservation de l'écrit dans la sociétéde l'information ; UNIVERSITÉ DE MONTRÉAL Faculté des études supérieures, Décembre 2002.

المقالات:

1- Anne lise Vilerrubla; Les apports de la signature électronique ;www.signelec.com.

2- Béatrice jaluzot ;Transposition de la derctive«signature électronique» :comparaison franco-allemande,Recueil Dalloz,2004,N0 40.

3- Eric caprioli,le juge électronique,www. juriscom.net,10janvier2000

4- Eric A.caprioli ,Régime juridique du prestataire de services de confiance au regard de la directive du 13 décembre 1999 ,www.caprioli-avocats.com, Date de la mise a jour : mai 2003.

5- Guenièvre Bordinat ; Introduction à la notion de signature électronique ; { HYPERLINK "http://www.signelec.com" }

6- Jérôme Huet, le code civil et les contrat électronique ; www.octoba.com .

7- Pascal Pascal Agosti ; Le régime jridiques des actes authentiques , www. caprioli-avocats.com.

8- Valérie Sédaillian ,Preuve et signature électronique,Juriscom .net,9 mai 2000

القوانين والمراسيم

1-LOI no 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique

2-Décret no 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique

3-Décret n° 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.

4- DIRECTIVE 1999/93/CE DU PARLEMENT EUROPÉEN ET DU CONSEIL du 13 décembre 1999 ;sur un cadre communautaire pour les signatures électroniques

قائمة المختصرات

المقدمة:.....1

الفصل الأول: طبيعة التوقيع الإلكتروني.....4

المبحث الأول : دور التوقيع في الإثبات..... 4

المطلب الأول : شروط ووظائف التوقيع 5

الفرع الأول شروط و محتوى التوقيع.....5

1- شروط الأخذ بالتوقيع 5

2- أنواع التوقيع.....6

3- محتويات التوقيع(تحديد هوية الموقع).....7

اللقب..... 7

الاسم 8

اسم الشهرة..... 9

الأحرف الأولى من الاسم واللقب..... 10

4-تحديد هوية الموقع في التوقيع الإلكتروني.....11

الفرع الثاني : وظائف التوقيع 13

أولا:التوقيع هو تعبير عن رضا الموقع بمحتوى السند الكتابي.....13

ثانيا : مراقبة مدى سلامة الوثيقة ونزاهتها..... 15

ثالثا : منح الوثيقة صفة« الأصل»..... 16

المطلب الثاني: نطاق حجية التوقيع في الإثبات 18

الفرع الأول : شروط الواقعة مراد إثباتها.....19

1- شروط بديهية.....19

2- شروط أساسية.....21

أ - أن تكون الواقعة متعلقة بالدعوى.....21

ب- أن تكون الواقعة منتجة في الدعوى 22

ج-أن تكون الواقعة جائزة الإثبات قانونا 23

الفرع الثاني :مجال إعمال التوقيع 24
1- التوقيع في الورقة العرفية 24
أولا:حجية التوقيع اتجاه المتعاقدين 24
ثانيا: حجية التوقيع اتجاه الغير.....25
2- التوقيع في الورقة الرسمية 26
المبحث الثاني: مكانة التوقيع الالكتروني في الإثبات.....29
المطلب الأول: ضرورة إعادة التعريف بالإثبات الخطي.....29
الفرع الأول:المساواة بين الكتابة الخطية والكتابة الإلكترونية......31
الفرع الثاني : تعريف التوقيع الالكتروني.....35
الفرع الثالث: أنواع التوقيع الإلكتروني.....39
أولا : نقل التوقيع الخطي بالماسح الضوئي(التوقيع بالقلم الإلكتروني) 39
ثانيا : التوقيع الكودي 40
ثالثا : التوقيع البيومتري 41
رابعا: التوقيع الرقمي 42
المطلب الثاني : مدى حجية التوقيع الإلكتروني 44
الفرع الأول:شروط صحة التوقيع الإلكتروني 45
أولا : يسمح بتحديد هوية الموقع 46
ثانيا :ارتباط التوقيع الإلكتروني بالموقع دون غيره. 47
ثالثا:سلامة مضمون الرسالة الإلكترونية التي ارتبط بها التوقيع 48
رابعا:إمكانية كشف أي تبديل أو تعديل في بيانات التوقيع الإلكتروني 48
الفرع الثاني:إشكالية حفظ التوقيع الإلكتروني وسلامته 49
أولا: سلامة الوثيقة الإلكترونية 49
ثانيا: سلامة التوقيع الإلكتروني 52
الفرع الثالث: مجال إعمال التوقيع الإلكتروني 54
أولا :التوقيع الإلكتروني في الورقة الرسمية 55

ثانيا:المعاملات المدنية و التجارية 58
أ - المعاملات التجارية 58
ب - المعاملات المدنية 59
1- حرية الإثبات في التصرفات التي لا تتجاوز حد معين 59
2- حالة المانع الأدبي أو المادي.....60
3-مبدأ الثبوت بالكتابة 61
الفصل الثاني: التوقيع الإلكتروني ومقتضيات الأمان القانوني 62
المبحث الأول:مقومات الأمان: التصديق.....62
المطلب الأول:مزود الخدمات(PSC)..... 63
الفرع الأول : شروط ممارسة عملية التصديق 64
أولا: منح الترخيص أو التفويض لمزاولة عملية التصديق.....65
1-التفويض الإرادي.....65
2-الترخيص.....67
أ- المشرع البحريني.....67
ب-مشرع إمارة دبي.....68
ج- المشرع المصري.....68
د- المشرع التونسي.....70
ثانيا: شروط أخرى.....70
1-بالنسبة للتعليمة الأوروبية وفرنسا.....70
2-بالنسبة للمشرع التونسي 71
3- بالنسبة للمشرع البحريني.....72
الفرع الثاني: التزامات مزود الخدمات.....72
1-التزامات مزود الخدمات في إمارة دبي وقانون الأونيسترال.....74
2-التزامات مزود الخدمات في مصر..... 75
3-التزامات مزود الخدمات في تونس..... 75

4-_التزامات مزود الخدمات في التعليمة الأوروبية و فرنسا.....76
الفرع الثالث : مسؤولية مزود الخدمات 78
أولا: مسؤولية مزود الخدمات تجاه الموقع.....80
ثانيا: مسؤولية مزود الخدمة تجاه المرسل إليه 82
ثالثا: الإعفاء من المسؤولية وتحديدها.....83
المطلب الثاني: شهادة التصديق الإلكتروني.....84
الفرع الأول: محتويات شهادة التصديق.....85
أ- تحديد هوية الموقع.....90
ب-هوية مزود الخدمات..... 91
ج- السيطرة على أداة التوقيع.....91
د-تحديد مجال استعمال الشهادة وصلاحيتها.....92
الفرع الثاني : الاعتراف بشهادة التصديق الأجنبية 93
الفرع الثالث: تعليق وإلغاء شهادة التصديق.....97
1-عند طلب صاحب الشهادة.....98
2-عند إعلامه بوفاة الشخص الطبيعي أو انحلال الشخص المعنوي
صاحب الشهادة.....99
3-الشهادة المحتوية على معلومات مغلوطة أو مزيفة.....100
4-تعليق الشهادة بسبب تغيير البيانات المتضمنة فيها.....100
المبحث الثاني: حماية التوقيع الإلكتروني 101
المطلب الأول: حماية التوقيع الإلكتروني أثناء استعماله.....102
الفرع الأول : التزامات ومسؤولية الموقع 102
الفرع الثاني: دور المرسل إليه في التوقيع الإلكتروني..... 106
المطلب الثاني: الحماية الجنائية للتوقيع الإلكتروني 109
الفرع الأول: المسؤولية الجنائية لمزود الخدمات 111
أولا: جريمة ممارسة نشاط مزود الخدمة من دون ترخيص 111

ثانيا:جريمة إفشاء الأسرار.....112
الفرع الثاني: الجرائم المتعلقة بشهادة التصديق.....114
أولا: جريمة نشر الشهادة بقصد الاحتيال 114
ثانيا : جريمة نشر الشهادة 116
ثالثا : جريمة تزييف الطلب وانتحال هوية شخص أخر.....117
1- جريمة تزييف الطلب.....117
2-انتحال هوية شخص أخر.....118
الفرع الثالث : الجرائم الواقعة على التوقيع و الوسيط و المحرر الإلكتروني....119
أولا: استعمال توقيع أو وسيط أو محرر إلكتروني تالف ومزور
وتزويره.....119
1- إتلاف وتزوير التوقيع أو الوسيط أو المحرر الإلكتروني..... 119
2-استعمال توقيع أو وسيط أو محرر إلكتروني تالف أو مزور..... 121
ثانيا : جريمة فك الشفرة.....121
ثالثا : جرائم الشخص الاعتباري.....122
الخاتمة.....125
الملحق رقم 1 129
الملحق رقم 2 147
الملحق رقم 3 163
الملحق رقم 4.....176
الملحق رقم 5 193
الملحق رقم 6 194
الملحق رقم 7 205
الملحق رقم 8.....219
قائمة المراجع
الفهرس