الجمهورية التونسية
وزارة العدل وحقوق الإنسان
المعهد الأعلى للقضاء

"التجـــارة الإلكترونـية"

دورة دراسية

الخميس 27 فيفري 2003 بمقر المعهد

البرنـــامج

9.00 - كلمة الإفتتاح
- السيد حسن بن فـــلاح
المدير العام للمعهد الأعلى للقضاء

9.10 - التقرير التمهيدي
- السيد الناصر هلالي
قاضـي ناحيـة تـونـس

9.30 - الإطار القانوني للإمضاء والمصـادقة الإلكترونية
- السيد عبد المنعم كيوة
قاضـي ناحيـــة تـــونس

10.00 - استـراحـــــة

10.15 - الجوانب القانونية للحماية المعلوماتية – السيد ابراهيم نافع كاهية مدير
إدارة الشؤون القانونية و النزاعات
بوزارة تكنولوجيا الإتصال و النقل

10.45 - الجوانب التقنية للحماية المعلوماتية
– السيد نور الدين بودريقة
الرئيس المدير العام للوكالة
الوطنية للمصادقة الإلكترونية

11.15 – القوة الثبوتية للوثيقة الإلكترونية
– السيد بديع بن عباس القاضي
بالمحكمة الإبتدائية بصفاقس

11.45 – النقاش

13.00 – نهاية الأشغال

الجمهورية التونسيـــــــــة
وزارة العدل وحقوق الإنسان
المـــــعهد الأعلى للقضـــــاء

التجارة الإلكترونية

تقرير تمهيدي

إعداد الناصر الهلالي
حاكم ناحية تونس

شهد العالم ويشهد تطورا هائلا ومريعا مـــردد بالأســـاس تطـــور نظـــام المعلوماتية.

فالإعلامية تعد ابرز اكتشافات القرن العشرين حتى يكاد يقرن ويسمى بـــه فمنذ ظهور الإعلامية سنة 1962 شهدت جميع الميادين قفزة نوعية بعد إدماجـــها ضمن منظومتها.

سرعة الحصول على المعلومة مع وسائل الخزن الرهيبة واليـــة العمـــل بالحسوب وسهولته فتحت مجالات واسعة.

فقد اعتمدت على غزو الفضاء والصناعـــة والتجـــارة والإدارة والبنـــوك والبورصة والتنقل والطب وحتى الحروب (وانهم على علم باحث اقيـــم بأعمـــال مكافحة الإرهاب) وما زاد الأمر أهمية ابتكار نظام الترابط بين الكمبيوتـــر ممـــا احدث تكنولوجيا هائلة في ميدا الاتصالات وتناقل المعلومات حتى جعل أطـــراف العالم متقاربة وهو ما يعرف باسم "القرية الصغيرة".

كما احدث نقلة نوعية أن العلاقات فيما بين الدول والأفراد والمجموعـــات واحدث قواعد جدية في المعاملات غير معهودة.

ويبدوا انه لا داعي لمزيد التأكيد على أهمية ذلك لما يلمسه كل واحد منا في معاملاته اليومية من انعكاسات هامة باستعمال الإعلامية.

فتكاد تكون كل الإدارات تعتمد بصفة كلية على الإعلامية في علاقاتها فيما بينها أو مع المواطن خاصة بعد فرض اعتمادها.

ويجدر بنا في هذا المجال إعطاء لمحة وجيزة عن ظهور الانترنات .

فقد بدأت الانترنات بشبكة واحدة كان اسمها "اربانات" ARPANET.

تم تطويرها سنة 1979 ضمن تجارب الحكومة الأمريكية وتولت وكالة DARPA

بوزارة الدفاع الأمريكية ربط الباحثين بمراكز الحاسوب الآلي ثم تم ربط عدة شبكات وخلايا ضمن وحدة سميت DARBA INTERNET ثم تطورت وتوسعت إلى الجامعات والشركات سنة 1988 ثم تم ربط 12 المركز كانت خطوة أولى لولادة الانترنات الحالية أول من فكر في إنشاء هذه الشبكة باحثون في مؤسسة (CERN) وقد اخترع TIM BARNERS LEE سنة 1991 نظاما خاصا بنقل المعلومات أدى إلى ظهور ما يسمى (WORLD WIDE WEB W.W.W)

ثم بواسطة ربط ملايين المستخدمين عبر كامل بلدان العالم.

وأمام تزايد سرعة الاتصالات والمعاملات وتواجد كمية هائلة من المعلومات ولتسهيل التعامل معها وحسن دراستها تم فرض استعمال المعلوماتية والكمبيوتر في كامل المجالات وخاصة منها ميدان التجارة الذي تتوفر فيه كامل هذه الخصائص بشكل واضح وجلي .

فالحجم الكبير من المعطيات والمعاملات التي فرضها التعامل التجاري أوجب الالتجاء إلى فكرة التخلص من الحجم الكبير للوثائق المعتمدة فيه وهو ما عرف فيما بعد بالتجرد من الطابع المادي للوثائق DEMATERIALISATION وقد أدى ذلك إلى ابتكار بما يسمى بالوثيقة الإلكترونية.

لكن دخول هذه الوثيقة في المعاملات التجارية لم يكن بالسهولة والبساطة التي تميز ميدان الإعلامية والتجارة.

فلئن فتحت هذه الوثيقة مجالات واسعة للتعامل سواءا الدولية أو الداخلية فإنها واجهت اشكالات هامة قانونية وفنية وكذلك تجارية على مستوى حمايـــة المتعامل معها.

فبالنسبة للإشكاليات الفنية فبعد أن تمت معالجة العراقيل الفنية للاتصـــال عن بعد أوجب إيجاد حلول لتطويع هذه الطرق للمبادلات التجارية كما اتجـــهت الأبحاث إلى ابتكار طرق حماية من أنواع القرصنة الإلكترونية التي تزامنت مـــع أشكال الاتصال الحديثة .

الميدان التجاري يفترض معرفة هوية المتعاملين فيما بينهم وخاصة منها بالنسبة للعقود التجارية وهو ما أوجب ابتكار طرق للتعريف بهوية المتداخليـــن في مثل هذه المبادلات الإلكترونية وكذلك إثبات هويتهم وحماية محتوى المبادلات من أي تدخل وأيضا ضمان التواجد المسترسل لهذه الخدمات مما زاد في انتشار هذا النوع من التجارة "إذ شهدت التجارة الإلكترونية نمو ملحوظا إذ تطور حجـم المبادلات على الساحة العالمية من 57 مليار دولار سنة 1997 ليصـــل إلـــى 100 مليار دولار سنة 2003" وهو ما ورد بتقديم شروع قانون المبـــادلات والتجـــارة الإلكترونية ضمن مداولات مجلس النواب.

وقد شهدت التجارة الإلكترونية مفاهيم عديدة لكن بصفة كاملة تنقسم إلى ثلاثة أقسام :

1) المعاملات التجارية الإلكترونية المباشرة من تســـويق وخدمـــات ونشاطات وصفقات .
2) التجارة الإلكترونية بين المؤسسات والمستهلك وتتمثل في بيـــع المباشر للمستهلك وذلك بتمكينه من الدخول لاروقتها واقتناء حاجاته.
3) الإدارة الرقمية وتشمل الخدمات الإدارية من تصـــاريح وضرائـــب وفواتير والتوثيق والتسجيل والمكاتبات...

وأمام ما شهدته كل هذه المعاملات من قرصنة اتجه تعزيز ثقة المتدخلين وذلـــك بحماية الشبكات والمنظومات والمعطيات المعلوماتية باستخدام تقنيات أساسية.

- التعريف بمعلومات المتدخلين وإثباتها .

- الحفاظ على سلامة محتوى المبدلات والمراسلات والمعطيات .
- ضمان عدم إنكار المتدخل للمبادلة .
- ضمان التواجد المستمر للخدمات الإلكترونية .

كما يتطلب حماية المبادلات استعمال تقنيات متطورة بتطور المخاطر واكثر هذه التقنيات انتشارا وضمانا :

- التشفير : وهو استعمال مفتاح سرّي يغير شكل الكتابة يستحيل معه فهمها إلا باستعمال نفس المفتاح .
- الإمضاء الالكتورني وهو طريقة فنية تمكن من التعرف على صاحب المراسلة والتأكد من سلامة محتوى المبادلة .
- اعتماد منظومات حماية الشيكات والتي تتولى تحرير المبادلات وتحديد المخاطر والتعرف على الحركات المشبوهة والتصدي لها باستعمال طرق تقنية مجربة وفاعلة مثل العازل الناري.

ولمزيد إعطاء اكثر ضمانات ومصداقية للوثيقة الإلكترونية تم اعتماد نظام شهادات المصادقة الإلكترونية التي تمكن من إثبات هويات صاحب الشهادة وبالتالي ضمان المعاملة نفسها وهي تتنوع بتنوع الاستعمال وتسهر عليها هيئة تضمن التعريف بين المتداخلين وتأمين المبادلات وذلك باختيار المواصفات المتعلقة بشكل الشهادات والشروط التقنية للإمضاء والتدقيق في مدى مطابقة تعاطي النشاط ومراقبة تطابق إجراءات المصادقة .

وأمام عجز القواعد القديمة وقصورها على متابعة هذه التقنيات الحديثة فقد التجأت اغلب التشاريع إلى تنقيحها وإدخال قواعد قانونية تتماشى معها وذلك بالتنصيص صراحة باعتماد مثل هاته الوثائق الإلكترونية واعتبار مثل الكتب الخطيّ كما عدلت بعض القواعد الأخرى لتتماشى مع هذه التقنية إضافة إلى طرق حفظها واستعمالها وشروط التعامل معها والتوسط فيها وكذلك حماية المعطيات الشخصية كما رتبت جملة من العقوبات عند مخالفة هذه القواعد إضافة إلى سحب العقوبات الواردة بباب التدليس بالمجلة الجنائية على كل عملية تدليس وتغيير عمدا على وثيقة معلوماتية أو إلكترونية .

وكل هذه الإجراءات تمثل حماية قانونية للمبادلات اللاكترونية قد تعطي اكثر ثقة وأمانا في التعامل معها .

من جهة أخري فقد أعطت اغلب التشريعات التي بينت الوثيقة الإلكترونية القيمة الضرورية لها وذلك بإسناد القوة الثبوتيّة لها لكن إلى أي مدى تصل هذه القوة؟ فوسائل الاتصال وتقنيات المعلوماتية لا توفر ضمانات كافية كتلك التي يوفرهـــا الورق.

لقد اشترطت التشريعات لذلك ضمانات تكون قرينة على صدق محتوى الوثيقـــة وهي أن تكون محفوظة في شكلها النهائي وبطريقة موثـــوق فيـــها ومدعمـــة بإمضاء إلكتروني.

فالربط بين جدية الوثيقة وطريقة حفظها ضمانا لســـلامتها وديمومتـــها وذلـــك باعتبار طرق فنية تضمن الأمان والسرية والمصداقية مثل الميكرو فيلم والميكرو فيش وكل وسيلة إلكترونية أخرى .

وقد اعتبرت الوثيقة الإلكترونية بهذا الشكل كتب غير رسمي وبالتـــالي تنطبـــق عليه نفس قواعد الكتب الغير الرسمي الواردة بالفصل 449 م ا ج وما يليه.

وتظهر أهمية ذلك إذا علمنا مثل هذه الحجج تنقلب بصفة رسمية إذا اعترف بها الخصم أو ثبتت صحتها قانونا يبقى ان نتساءل أيهما يعتمد إذا تعارض الكتـــب الإلكتروني بالكتب الخطي فالمشرّع ساوى بينهما لكن واقعا قد لا يكـــون الأمـــر كذلك خاصة على مستوى فقه القضاء باعتبار أن الأمر ترك لاجتـــهاد القضـــاء المطلق وذلك اعتمادا على الفصل 460 من م ا ج التي تضمن أن الاعتراف بالخط أو الإمضاء لا يسقط الحق في معارضة الكتب ويبقى الاختلاق حول ثبوت تـــاريخ الكتب وهنا يأتي دور مكتب المصادقة الإلكترونية وتزود خدمات المصادقة إلا أن ذلك غير ممكن في المعاملات عبر الشبكات المفتوحة والخاصة منها المعـــاملات بين مستهلك عادي وبائع محترف.

وقد ساير المشرع التونسيّ هذه التطورات فبدأ بتنقيح قواعد التدليـــس ضمـــن المجلة الجنائية وذلك بتنقيح الفصول 172 و 199 مكرر و199 ثالثا منـــها بإدخـــال الوثيقة المعلوماتية او الإلكترونية ونظام البرمجيات والبيانات المعلوماتية ضمنها

ثم أتبعها بتنقيح م ا ج والفصول المتعلقة بالحجج والكتائب منها والتي أعطت مفهوما جديدا للحجة ثم جاء القانون عدد 83 لسنة 2000 المؤرخ في 9 اوت 2000 المتعلق بالمبادلات والتجارة الإلكترونية وألحقها بالأوامر والالتزامات المنظمة.

- الأمر عدد 2331 لسنة 2000 المؤرخ في 10 أكتوبر 2000 المتعلق بضبط التنظيم الإداري والمالي وطرق تسيير الوكالة الوطنية للمصاقة الإلكترونية.
- الأمر عدد 1660 لسنة 2001 المؤرخ في 17 جويلية 2001 المكلف بضبط إجراءات الحصول على ترخيص لممارسة نشاط مزود خدمات المصادقة الإلكترونية.
- قرار وزير تكنولوجيات الاتصال مؤرخ في 19 جويلية 2001 المتعلق بضبط المعطيات التقنية لشهادات المصادقة الإلكترونية والوثوق بها .
- قرار وزير تكنولوجيات الاتصال المؤرخ في 19 جويلية 2001 المتعلق بضبط المواصفات التقنية بمنظومة إحداث الإمضاء الإلكتروني .

وهذا التوجه لم يكن عشوائيا أو مسقطا بل كان نتيجة تفاعل الاقتصاد التونسي مع المستحدثات العلمية والأسواق الخارجية وهو ما نستنتجه من أجوبة السيد وزير التجارة في جلسة حوار مع مجلس النواب يوم 20 جوان 2000 الذي أكد خلاله انه في إطار المعاملات الخارجية سيتواصل الجهد من خلال الحملات التحسيسية وتنفيذ القرارات الرئاسية عند إشرافه على مجلس الوزراء المضيق الذي خصص لموضوع الاقتصاد اللامادي المنعقد يوم 19 ماي 1999 وقد تم اعتماد جملة من المبادئ الأساسية عند وضع مشروع هذا القانون.

- وهي توفيق الضمانات القانونية لتأمين المبادلات والتجارة الإلكترونية ودعم الثقة بين المتعاملين .
- إدراج الضمانات الإضافية الضرورية لحماية مصالح المتدخلين باعتبار الصبغة اللامادية للمبادلات .
- إخضاع هذا النوع إلى التشاريع المعمول بها.
- الحياد إزاء التكنولوجيات الممكن استعمالها.
- حماية المعطيات الشخصية المتبادلة.

- اعتماد نفس التمشي في المبادلات التجارية في خصوص العقوبات وهو ما جاء بالتقرير المشترك بين لجنة التشريع العام والتنظيم العام ولجنة التجهيز والخدمات ولجنة الفلاحة عند مناقشة القانون المتعلق بالمبادلات والتجارة الالكترونية.

وهو ما ورد أيضا بالتقرير حول التجارة الإلكترونية بتاريخ 15 مارس 1998 والذي قدم إلى وزارة الاقتصاد والمالية والصناعة التونسية في 8 جانفي 1998 والذي نشر عبر الانترنات وكان موضوع نقاش مفتوح لبيع الأشخاص والمؤسسات والجمعيات تبادلوا خلاله الآراء مما أثرى الافتراضات إلى حدود نهاية شهر فيفري والذي كان في إطار برنامج عمل الحكومة التونسية للدخول في مجتمع المعلوماتي .

ولا شكّ أن مثل هذه الملتقيات تعطي المجال لمثل هذه المقترحات لمزيد إثراء قواعد التدخل في ميدان التجارة الإلكترونية.

وزارة العدل وحقوق الانسان

المعهد الأعلى للقضاء

دورة دراسية حول التجارة الإلكترونية

27 فيفري 2003

عبد المنعم كيوة
قاض ناحية تونس
kiouaabdelmonem webmails.com

النصوص المرجعية :

1. القانون عدد 57 لسنة 2000 المؤرخ في 13 جوان 2000 المنقح والمتمم لبعض فصول من مجلة الالتزامات والعقود.
2. القانون عدد 83 لسنة 2000 المؤرخ في 9 أوت 2000 المتعلق بالمبادلات والتجارة الإلكترونية.
3. الأمر عدد 2331 لسنة 2000 المؤرخ في 10 أكتوبر 2000 المتعلق بالتنظيم الإداري والمالي وطرق تسيير الوكالة الوطنية للمصادقة الإلكترونية.
4. الأمر عدد 1667 لسنة 2001 المؤرخ في 17 جويلية 2001 المتعلق بالمصادقة على كراس الشروط الخاص بممارسة نشاط مزود خدمات المصادقة الإلكترونية.
5. الأمر عدد 1668 لسنة 2001 المؤرخ في 17 جويلية 2001 المتعلق بضبط إجراءات الحصول على ترخيص لممارسة نشاط مزود خدمات المصادقة الإلكترونية.
6. قرار من وزير تكنولوجيات الاتصال مؤرخ في 19 جويلية 2001 يتعلق بضبط المواصفات التقنية لمنظومة إحداث الامضاء الإلكتروني.
7. قرار من وزير تكنولوجيات الاتصال مؤرخ في 19 جويلية 2001 يتعلق بضبط المعطيات التقنية المتعلقة بشهادات المصادقة الإلكترونية والوثوق بها.
8. الأمر عدد 2727 لسنة 2001 مؤرخ في 20 نوفمبر 2001 يتعلق بضبط شروط وإجراءات استعمال وسائل أو خدمات التشفير عبر شبكات الإتصالات و تعاطي الأنشطة ذات العلاقة.

في الوقت الذي نشهد فيه تطورا مطردا للشبكات الإعلامية متعددة الوسائط المرتبطة بشبكة الانترنيت يطرح سؤال يثير الاهتمام يتعلق بالقواعد التي تحكم وتنظم المبادلات الدائرة في الفضاء الإلكتروني.

إن تطور المبادلات التجارية عن طريق استعمال الوسائل التكنولوجية الحديثة للاتصال مرتبط بوجود قواعد وآليات ضامنة لفعالية تلك المبادلات ، فلا يمكن أن توجد تجارة إلكترونية متطورة في غياب ضمانات تؤمن سلامتها وتطمئن مستعمليها.

والتأكيد على ضرورة توفير ضمانات ووسائل أمان وحماية في مجال المبادلات الإلكترونية مرده وجود عدة مخاطر محدقة بها يمكن حصرها في النقاط التالية :

1. عدم إمكان تحديد هوية الباعث.
2. تعرض المعلومات المتبادلة (رسالة البيانات) للتحريف والإتلاف.
3. إنكار حصول التبادل الإلكتروني للبيانات سواء من الباعث أو المبعوث إليه.
4. الاعتداء على سرية المعلومات والاطلاع عليها بدون وجه حق.
5. الاعتداء على حقوق التأليف.
6. المضايقة.[1]

والذي يهمنا في إطار هذه المداخلة هو البحث عن الحلول التي تمكننا من التعرف على هوية مصدر رسالة البيانات بحيث لا يمكن إنكار صدورها عنه من جهة (نسبة وثيقة إلى شخص معين **Imputabilité**) أو إنكار صدورها بغير الصيغة التي وردت بها إلى المبعوث إليه من جهة ثانية (ضمان عدم تحريف إرادة الباعث عن طريق ضمان سلامة محتوى الوثيقة المرسلة ***Intégrité***).

في المعاملات التقليدية القائمة على سند ورقي يقوم الإمضاء الخطي المتمثل في " وضع اسم أو علامة خاصة بيد العاقد نفسه مدمجة بالكتب المرسوم بها "[2] بالتعريف بهوية المتعامل والتحقق من تعبيره عن رضاه أو موافقته على مضمون الوثيقة أو حتى التأكد من توليه الاطلاع عليها.[3]

---

[1] في وقت مضى ومع بدايات اعتماد التبادل الإلكتروني للبيانات لم يكن بالامكان ايجاد حلول قانونية وتقنية لكل هذه الاشكاليات. واليوم ومع تطور الوسائل التكنولوجية للاتصال والأبحاث العلمية المتصلة بها أمكن ايجاد حلول لبعض الاشكاليات المطروحة في مجال حماية تبادل المعلومات إلكترونيا وتوفير الثقة والأمان للمتعاملين عبر الشبكات الإعلامية للاتصال المفتوحة للعموم ويمثل التشفير **Cryptage** أهم العناصر المركزية في نظام التأمين والحماية للمبادلات الإلكترونية فهو يمكن بنسبة عالية من تحقيق سرية وسلامة البيانات المتبادلة كما يمكن من تفادي إنكار حصول المعاملة أو المراسلة ويلعب دورا رئيسيا ومهما في التعريف بهوية مصدر رسالة البيانات إذ يقوم عليها ما يسمى بالامضاء الرقمي.

[2] الفصل 453 في فقرته الثانية من مجلة الالتزامات والعقود المضافة بموجب القانون عدد 57 لسنة 2000 المؤرخ في 13 جوان 2000.

[3] يتأكد اتصراف المتعاقد إلى قبول التصرف القانوني بعد إطلاعه على جميع بنوده باشتراط المشرع بالفصل 453 فقرة 1 من م إ ع أن يكون الإمضاء أسفل الكتب وهو ما يترتب عنه من كون إمضاء المتعاقد بأعلى الكتب لا عمل عليه. أنظر : يوسف بالعيوني : دراسة نقدية للإثبات في القانون المدني ، مذكرة للإحراز على شهادة الدراسات المعمقة في القانون الخاص ، كلية الحقوق والعلوم السياسية بتونس 1994 ص 194. غير أن

كما يمثل الوعاء الورقي للكتب بالنسبة للمتعاقدين ضمان مادي ضد كل تحريف أو تغيير لمحتواه بحيث أنه يمكن بالعين المجردة إدراك أنه سليم أو محرف فضلا على أنه يمكن الرجوع للاختبار للتأكد من ذلك.

لكن مع ظهور التبادل الإلكتروني للبيانات وانتشاره الواسع عبر الشبكات المفتوحة أصبح من الحتمي التفكير والبحث عن وسائل أخرى تقوم بوظائف الإمضاء التقليدي المعتمد على رسم خطي باعتبار أنه من غير الممكن تصور بقاء الإمضاء الخطي في المعاملات الإلكترونية إلا إذا أمكن حفره وجعله " رسما كمبيوتريا " لذلك يجري العمل اليوم بما يسمى بالإمضاء الإلكتروني. كما وجب البحث عن وسائل حماية الإرادة في التصرفات القانونية الدائرة في الفضاء الإلكتروني وذلك بضمان عدم تحريف محتوى الكتب الذي انصرفت إليه إرادة الممضي خصوصا أن تغيير محتوى وثيقة معلوماتية أمر ممكن ويسير.

وتأكيدا لذلك ينص الفصل 453 مكرر فقرة 2 من مجلة الالتزامات والعقود أن الوثيقة الإلكترونية تعد كتبا غير رسمي " إذا كانت محفوظة في شكلها النهائي بطريقة موثوق بها ومدعمة بإمضاء إلكتروني".[4]

ويستنتج من ذلك أن لكي يتم اعتماد الوثيقة الإلكترونية في الإثبات لابد من توفر شرطين اثنين هما:

أولا : أن تكون مدعمة بإمضاء إلكتروني وهو شرط بديهي لكل كتب خطي باعتبار أن الإمضاء هو الذي ننسب به الالتزام التعاقدي لشخص معين.

ثانيا : أن تكون محفوظة في شكل نهائي بطريقة موثوق بها تضمن عدم تحريفها سواء عمدا أو بدون عمد.[5] وهذا الشرط الخاص بالوثيقة الإلكترونية مرده المخاطر المحفوفة بسلامتها ولذلك لا بد من البحث عن الضمانات الكفيلة بحماية إرادة المتعاقدين عبر الوسائل الإلكترونية.

اشتراط تجسيم الموافقة بالامضاء أسفل الكتب بالفصل 453 فقرة 1 من م إ ع قد يتناقض مع ما جاء بالفقرة الثانية جديدة المضافة لنفس الفصل بالقول أن الامضاء الخطي مدمج بالكتب ؟

[4] وتضمن الفصل 1316-1 جديد من المجلة المدنية الفرنسية نفس المعنى حيث نص على ما يلي :

" L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier , sous réserve que puisse etre dument identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité ».

[5] يربط القانون النموذجي للأمم المتحدة حول التجارة الالكترونية (الفصل 9 فقرة 2) متبوعا في ذلك بالتشريعات الوطنية الصادرة في الغرض حجية الوثيقة الإلكترونية بالطرق والوسائل التقنية المتبعة في حفظها وضمان سلامتها

وتتفق جميع تشريعات العالم اليوم على اعتبار أن الإمضاء الإلكتروني والمصادقة الإلكترونية هما الوسيلتان المتوفرتان اليوم لضمان محيط إلكتروني آمن في التعامل عبر الشبكات المفتوحة. ولئن سنتناولهما في إطار هذه المداخلة بصورة منفصلة فإن ذلك لا يعني عدم وجود رابطة قوية بينهما كما سنتولى إبرازه في التحليل.

المبحث الأول
الإمضاء الإلكتروني

"...لا يمثل التوقيع بخط اليد سوى مرحلة من مراحل التطور في وسائل التصديق على التصرفات القانونية، وهو ليس الأداة الوحيدة أو المرحلة النهائية للتطور، بل يرتبط إلى حد بعيد بظاهرة الكتابة الورقية ... ولا يقف حاجزا أمام بروز أشكال جديدة ، فالهدف من الإمضاء يكمن في خلق حالة واقعية ظاهرة ومشاهدة ومعاينة ، فالتصديق تعبير مجرد عن حالة نفسية باطنية تتمثل في نقل القبول إلى رحاب العالم الخارجي المحسوس"[6].

وقد ظهر اليوم ما يسمى بالإمضاء الإلكتروني الذي أعتبر البديل للإمضاء الخطي جاء ليلائم المعاملات الإلكترونية [7] ويقوم بالوظائف المسندة إليه والمذكورة أعلاه.

الفقرة الأولى : مفهـــوم الامضاء الألكتروني :

يعرف المشرع التونسي الإمضاء الإلكتروني بمجلة الالتزامات والعقود في فصله 453 فقرة ثانية بأنه "منوال تعريف موثوق به يضمن صلة الإمضاء بالوثيقة الإلكترونية المرتبطة به "

وبصورة أدق يتمثل الإمضاء الإلكتروني في مجموعة بيانات إلكترونية (محدثة في شكل رموز رياضيـــة سرية) مصاحبة أو مرتبطة منطقيا بمجموعة بيانات إلكترونية أخرى (رسالة بيانات) تعرف بهـــوية صاحبهـــا يعبر عنه بمنوال تعريف.

يعرف الفصل الأول من القانون النموذجي للجنة الأمم المتحدة للقانون التجاري الدولي حول القواعد الموحدة للإمضاء الإلكتروني الذي جاء به ما يلي :

---

[6] يوسف بلعيوني : مرجع سابق ص 198.

[7] يخول الفصل 3 مكرر من المجلة الديوانية في فقرته الثانية تبليغ الوثائق ذات الصبغة الديوانية المحررة بواسطة الآلات الاعلامية إلى الديوانة بواسطة طرق إلكترونية أو طرق أخرى أوتوماتيكية ، وفي هذه الحالة إقتضى أن يتم تصديق هذه الوثائق بطرق أخرى غير الإمضاء الخطي.

(أ) "توقيع إلكتروني" يعني بيانات في شكل إلكتروني مدرجة في رسالة بيانات أو مضافة إليها أو مرتبطة بها منطقيا ، يجوز أن تستخدم لتعيين هوية الموقع بالنسبة إلى رسالة البيانات ، ولبيام موافقة الموقع على المعلومات الواردة في رسالة البيانات.[8]

وقد جاء بالفصل الثاني من توصية الاتحاد الأوروبي عدد 93 الصادرة بتاريخ 13 ديسمبر 1999 والمتعلقة بالإمضاء الإلكتروني تعريف الإمضاء الإلكتروني كما يلي :

" ... ***Une donnée sous forme électronique, qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification;*** »

وبين من التعاريف المذكورة أن مفهوم الإمضاء الإلكتروني ينبني على أولا على مفهوم وظيفي من جهة وتقني من جهة ثانية

1. المفهوم الوظيفي : المعادلة الوظيفية ***L'équivalence fonctionnelle*** بين الإمضاء الإلكتروني والإمضاء الخطي

يرى البعض أنه من الاعتباط إجراء مقارنة بين الإمضاء الخطي واستعمال تقنيات خاصة لتحديد هوية المتعامل إلكترونيا لكونهما أمران مختلفان اختلافا تاما ولو أنهما قد يحققان نفس الوظائف وهو يرون أنه لا يمكن بأي حال من الأحوال اعتبار تلك التقنيات إمضـــاء.

غير أنه يجري العمل اليوم على تسمية التقنيات المذكورة بـــ "الإمضاء الإلكتروني" لكونه يقوم بنفس وظائف الإمضاء الخطـــي بل إنه يتعداها ليشكل ضمانا لسلامة ***Intégrité*** الوثيقـــة الإلكترونية أو بالأحرى المعلومات المتبادلة إلكترونيا.

- وظائف الإمضاء التقليدية
- التعريف بهوية الممضي وهو في المجال الالكتروني مصدر رسالة البيانات

2. التأكد من موافقة الممضي على محتوى الوثيقة

- الوظائف الإضافية للإمضاء الإلكتروني : حماية الوثيقة الإلكترونية من التحريف والتغيير عن طريق اشتراط ارتباط الإمضاء بالوثيقة الالكترونية: التلازم بين الامضاء والوثيقة يضمن عدم تغيير محتوى الوثيقة.

تجدر الإشارة هنا إلى أن توصية الاتحاد الأوروبي تميّز في فصلها الثاني بين الإمضاء الإلكتروني " البسيط أو المجرد " ***Simple*** وبين الإمضاء الإلكتروني المدعم ***Renforcée*** أو المحمي ***Sécurisée*** .

---

[8] " *a) Le terme « signature électronique » désigne des données sous forme électronique contenues dans un message de données, ou jointes ou logiquement associées audit message et pouvant être utilisées pour identifier le signataire du message et indiquer qu'il approuve l'information qui est contenue ...* ».

والمقصود بالإمضاء الإلكتروني " المجرد " هو الإمضاء الذي يحقق الوظائف التقليدية للإمضاء وهي تحديد هوية صاحب الرسالة والتأكد من موافقته على مضمونها ، أما الإمضاء "المدعم" فهو الإمضاء الذي يكون فضلا عن ذلك محدثا ، بطريقة تضمن بقاءه تحت السيطرة المطلقة لصاحبه من جهة والمرتبط بالمعلومات المتبادلة بصورة تمكن من الكشف عن كل تحريف لها من جهة ثانية.

فقد جاء بالفصل 2 من توصية الاتحاد الأوروبي المذكورة تعريف الإمضاء المتقدم *Avancée* كما يلي :

« Aux fins de la présente directive , on entend par :
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 crée 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 ».

2. المفهوم التقني للإمضاء الإلكتروني

توجد عديد التقنيات تكيف على أنها إمضاء إلكتروني أبرزها :

1. الرمز السري *Code secret*

وهي التقنية المتداولة في المعاملات البنكية اليومية وتتمثل في خزن بعض المعلومات الشخصية للمتعامل بذاكرة حاسوب البنك مصدر البطاقة الذكية *Carte à puce* تولد بواسطة " دالة جبرية " رمزا سريا متكون من أربعة أرقام. وعند كل استعمال يتولى صاحب البطاقة إدخالها في آلة القراءة مع إضافة رمزه السري فإذا كان هذا الأخير صحيحا ومتطابقا مع البطاقة الخاصة بالمتعامل أمكن لهذه الأخيرة القيام بالوظيفة التي وضعت من أجلها كسحب الأموال والاطلاع على الحساب البنكي ... و تبعا لذلك لايمكن اعتبار الرمز السري إمضاء بالمعنى القانوني بمعزل عن البطاقة الذكية التي تمكن من استعماله.

2. الامضـــاء البيومتـــري *Signature Biométrique*

يقوم الامضاء البيومتري على تدوين أو خزن صفة جسدية للشخص المخول له الاستعمال بجهاز الكمبيوتر المتصرف أو المرتبط بالمنظومة المعلوماتية. والصفات المخزونة هي غالبا قزحية العين (IRIS) أو بصمة الابهـــام. و " تخزن الصورة بصفة رقمية ومضغوطة حتى لاتحوز مكانا كبيرا في الذاكرة الصلبة *Disque dur* للحاسوب أو في البطاقة الذكية ".

3. الامضاء الرقمي *Signature numérique* المبني على المفتاح الخاص (السري) *Clé privée* والمفتاح العلني *Clé publique*

تقتضي تقنية الامضاء الرقمي أن يكون لدى كل شخص مفتاحا سريا ومفتاحا علنيا ، فيتولى بواسطة مفتاحه السري التوقيع على الوثيقة المرسلة (وعندئذ تصبح رسالة مشفرة) ، ويتم تحديد هويته من قبل المرسل إليه عن طريق إعمال مفتاحه العلني (الباعث) فإذا إنكشف محتوى الوثيقة المرسلة للمبعوث إليه تيقن أن صاحب الوثيقة المرسلة هو صاحب ذلك المفتاح العلني المعلوم الهوية لديه ، بل يمكنه أيضا التيقن من أن الرسالة لم تحرف أثناء تراسلها بإجراء مقارنة بين النص المشفر من الباعث والمعاد تشفيره من المبعوث إليه بواسطة المفتاح العلني للباعث الأصلي.
غير أن هذه التقنية تمكن كل شخص من الاطلاع على محتوى الوثيقة المرسلة باعتبار أن المفتاح الذي يمكن من الكشف عنها وتحديد صاحبها هو مفتاح علني معلوم للجميع ولذلك تقترن تقنية الإمضاء الرقمي بتقنية التشفير المزدوج [9] الضامنة لسرية الوثيقة ، لكن لابد عندئذ من تدخل سلطة تصديق تضمن التعريف بالباعث (صاحب الشهادة) مع المبعوث إليه كما سيقع بيانه لاحقا.

3. خصـــائص الامضاء الألكتروني

يتميز الامضاء الألكتروني بثلاث خصائص أساسية وهي:
أولا – أنه شخصي أي أنه خاص بصاحبه وغير ممكن الاطلاع عليه من الغير لكنه ليس ذاتيا (شخصـــانيا) أي غير مرتبط بشخصية صاحبه بحيث يمكن تمكين الغير الموثوق فيه من استعماله عوضا عن صاحبه الحقيقي دون أن يتم التفطن لذلك من المبعوث اليه ، ويستثنى من ذلك طبعا الامضاء البيومتري لارتباطه المادي بجسد الممضي.

---

[9] يراجع في ذلك المثال عدد 3 الوارد بالصفحة 40.

ثانيا – أنه غير قابل للتقليـــد لأنه لايتخذ شكلا ماديا إذ هو مبني على لغة رياضية يصعـــب الكشف عن المعادلة القائم عليها خصوصا عندما يكون معتمدا فيها على تقنية تشفير ذات قدرة عالية بحيث أن الامضاء يصبح مندمجا في الوثيقة الألكترونية ذاتها ولا يمكن تمييزه عنها ، أو على صفة جسدية لشخص الممضي لا يمكن أن تماثل غيره من الأشخاص.

ثالثا – أنه إمضاء متغيـــر بتعدد المراسلات وهذه الخاصية يتميّز بها الامضاء الرقمي المبني على تقنية التشفير.

الفقرة الثانية : موثوقية الامضاء الألكـــتروني

جاء بالدليل القانوني للجنة الأمم المتحدة للقانون التجاري الدولي بشأن التحويلات الألكترونية للأموال الصادر سنة 1987 أن " التصديق هو تحديد رسالة ما بطريقة مادية أو إلكترونية أو بطريقة أخرى تتيح للمستلم التأكد من أنها واردة من المصدر المشار إليه ، وليس من المهم ما إذا كان التصديق يمكن أيضا أن يتيح للمستلم التأكد من أن الرسالة لم تتغيّر ، لا عمدا ولا بغير عمد. والتصديق على رسالة ما لايعني بالضرورة أن الرسالة بالصورة التي وردت بها كان مأذونا بها ، أو أن الشخص الذي أرسلها كان مأذونا له بأن يفعل ذلك ".

لتحديد موثوقية الإمضاء الإلكتروني لا بد من تحديد عناصر أو معايير تلك الموثوقية وطريقة اثباتها.

1. معايير موثوقية الإمضاء الإلكتروني

لتحديد عناصر موثوقية الامضاء الالكتروني يمكن الرجوع إلى القانون النموذجي للجنة الأمم المتحدة للقانون التجاري الدولي بشأن التوقيعات الإلكترونية (2001) والذي تضمن في فصله السادس ثالثا ما يلي :

3 – يعتبر التوقيع الإلكتروني موثوقا به لغرض الوفاء بالإشتراط المشار إليه في الفقرة 1 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

(ج) كان أي تغيير في التوقيع الإلكتروني ، يجرى بعد حدوث التوقيع، قابلا للإكتشاف ،

(د) كان الغرض من اشتراط التوقيع قانونا هو تأكيد سلامة المعلومات التي يتعلق بها التوقيع وكان أي تغيير يجرى في تلك المعلومات بعد وقت التوقيع قابلا للاكتشاف"

وبين من ذلك أن موثوقية الامضاء الالكتروني ما هو في الحقيقة إلا موثوقية المنوال التقني المستعمل.

وبين كذلك أن وظيفة الامضاء الالكتروني تتجاوز الوظائف التقليدية للامضاء لتضمن فضلا عن ذلك سلامة الوثيقة الممضاة.

2. إثبات موثوقية الإمضاء الإلكتروني

هنا لا بد من التمييز بين القرينة القانونية التي وضعها المشرع لموثوقية الإمضاء الإلكتروني التي تعفي الممضي من إثباتها و بين الموثوقية الواجبة الاثبات.

- الموثوقية المفترضة

ينص الفصل الخامس من قانون المبادلات والتجارة الالكترونية أنه " يمكن لكل من يرغب في إمضاء وثيقة إلكترونية احداث إمضائه الالكتروني بواسطة منظومة موثوق بها يتم ضبط مواصفاتها التقنية بقرار من الوزير المكلف بالاتصالات".

قبل صدور قرار وزير المواصلات المشار إليه ثار تساؤل هنا هل سيقع الاعتماد على الإمضاء الرقمي المبني على نظام المفتاحين : المفتاح العلني والمفتاح السري كما ذهب إلى ذلك المشرع الألماني والإيطالي أم على تقنية أخرى ؟

وللإجابة على ذلك يبدو أن الإتجاه ينحو بصورة لا تترك مجالا للشك نحو إعتماد الإمضاء المبني على تقنية التشفير (الامضاء الرقمي) ويستنتج ذلك من نص القانون المتعلق بالمبادلات والتجارة الألكترونية الذي تضمن في فصله الثاني تعريف منظومة إحداث الامضاء على أنها " مجموعة وحيدة من عناصر التشفير الشخصية أو مجموعة من المعدات المهيأة خصيصا لإحداث إمضاء إلكتروني".

كما تولى تعريف منظومة التدقيق في الامضاء على أنها " مجموعة من عناصر التشفير العمومية أو مجموعة من المعدات التي تمكن من التدقيق في الامضاء الألكتروني ".

كما تضمن الفصل 21 فقرة أخيرة أنه " لايمكن لصاحب الشهادة التي تم تعليقها أو إلغاؤها استعمال عناصر التشفير الشخصية للإمضاء موضوع الشهادة المعنية والتصديق على هذه العناصر من جديد لدى مزود خدمات مصادقة الكترونية آخر ".

كما تضمن الفصل 48 منه أنه " يعاقب كل من استعمل بصفة غير مشروعة عناصر تشفير شخصية متعلقة بإمضاء غيره بالسجن ...".

بعد كل هذا ماذا ترك القانون لقرار وزير المكلف بالاتصالات ؟ ألم تكن نية المشرع واضحة منذ البداية ؟ ثم ألا يشكل ذلك تعارضا مع المفهوم الواسع الذي جاء به مبدئيا الفصل 453 فقرة 2 من مجلة الالتزامات والعقود.

ويجدر الاشارة هنا أنه لاعتماد الإمضاء الرقمي أي ذلك المبني على تقنية التشفير يكون من الضروري تطوير النظام القانوني لاستعمال التشفير ليلائم تطور المبادلات الإلكترونية ويستجيب لمقتضيات حمايتها وهو ما تم فعلا بإصدار الأمر عدد 2727 المؤرخ في 20 نوفمبر 2001 المتعلق بضبط شروط وإجراءات استعمال وسائل أو خدمات التشفير عبر شبكات الاتصالات و تعاطي الأنشطة ذات العلاقة.

يميز الفصل الثالث من هذا الأمر بين صنفين من وسائل التشفير هما:

الصنف الأول : كل وسيلة تشفير تمكن فحسب من تشفير المعلومات الخاصة للتعريف بالمستعمل أو بالجهاز الطرفي عبر شبكات الاتصالات لضمان سرية هذه المعلومات.

الصنف الثاني : كل وسيلة تشفير تمكن من تشفير الوثائق الإلكترونية المتبادلة عبر شبكات الاتصالات أو إمضائها إلكترونيا.

وأعفى الفصل 13 من الأمر المذكور استعمال وسائل التشفير من الصنف الأول المصادق عليها أو وسائل التشفير من الصنف الثاني التي تعتمد العناصر الشخصية من الإمضاء المودعة لدى مزود خدمات المصادقة الإلكترونية المرخص له والذي يوفر خدمات التشفير من أي إجراء مسبق.

إن اللجوء إلى الإمضاء الرقمي يتطلب تدخل هيكل ضامن لقيام الصلة بين صاحب شهادة المصادقة الإلكترونية ومنظومة التدقيق في الإمضاء الخاصة به يسمى مزود خدمات المصادقة الإلكترونية موضوع المبحث الثاني من هذه المداخلة.

- الموثوقية المثبتة

يتحمل كل مستعمل لإمضاء آخر غير الإمضاء الرقمي عبئ إثبات موثوقية التقنية التي تولى اعتمادها في الإمضاء ويمكن الرجوع في ذلك للاختبار الفني.

المبحث الثاني

المصادقة الإلكترونية

يأخذ التصديق في مجال التبادل الألكتروني للمعلومات اليوم شكلا متقدما متمثلا في تكفل شخص خارج العلاقة لا فقط بضمان التعريف بهوية مصدر "رسالة البيانات" بصورة لا تدعو للشك وإنما أيضا ضمان صحتها وسلامة المعلومات الواردة بها من كل تحريف وذلك عن طريق تسليم شهادة مصادقة إلكترونية متضمنة مجموعة من البيانات الضرورية .

واللجوء إلى شخص مادي أو معنوي ، عمومي أو خاص ، للقيام بوظيفة المصادقة والذي يسميه القانون المذكور " مزود خدمات المصادقة القانونية " يعد اليوم أمرا ضروريا ولازما لضمان محيط إلكتروني آمن ومشجع للتعامل ولذلك خصص القانون عدد 83 لسنة 2000 المؤرخ في 9 أوت 2000 المتعلق بالمبادلات والتجارة الإلكترونية بابا مستقلا بخدمات المصادقة الألكترونية تضمن تحديدا لوظائف وواجبات ومسؤولية مزود خدمات المصادقة الألكترونية.

الفقرة الأولى : مفهوم ودور المصادقة الإلكترونية

لا يمكن إدراك مفهوم المصادقة الإلكترونية والدور الموكول لها كعنصر ثقة وأمان في المبادلات إلا من خلال النظر في الوظائف التي أسندها المشرع لشهادة المصادقة الإلكترونية من جهة والواجبات التي حملها على مزود خدمات المصادقة الإلكترونية من جهة ثانية.

1. وظائف شهادة المصادقة الإلكترونية

يعرف الفصل الثاني من القانون المتعلق بالمبادلات والتجارة الإلكترونية مزود خدمات المصادقة الإلكترونية بأنه " كل شخص طبيعي أو معنوي يحدث ويسلم ويتصرف في شهادات المصادقة ويسدي خدمات أخرى ذات علاقة بالإمضاء الإلكتروني ".

- يتبين من هذا التعريف أن المهمة الأساسية لمزود خدمات المصادقة الإلكترونية هي إصدار وتسليم وحفظ شهادات مصادقة وفق كراس شروط مصادق عليه بأمر تستجيب لمقتضيات السلامة والموثوقية.(الفصل 12 من قانون المبادلات والتجارة الإلكترونية)

لكن ما هو مفهوم شهادة المصادقة الالكترونية وإلى ماذا تهدف؟

يعرف الفصل الثاني من القانون المتعلق بالمبادلات والتجارة الإلكترونية شهادة المصادقة الإلكترونية بكونها " الوثيقة الإلكترونية المؤمنة بواسطة الإمضاء الألكتروني للشخص الذي أصدرها والذي يشهد من خلالها ، إثر المعاينة ، على صحة البيانات التي تتضمنها ".

ويميز الفصل السابع من كراس الشروط الخاص بممارسة نشاط مزود خدمات المصادقة الإلكترونية المصادق عليها بالأمر عدد 1667 لسنة 2001 المؤرخ في 17 جويلية 2001 بين ثلاث أنواع من الشهادات يمكن للمزود إصدارها بحسب الوظائف المسندة إليها وهي :

1. شهادة شخصية تمكن من تحديد هوية صاحب الشهادة وارتباطها بعناصر التدقيق في إمضائه.
2. شهادة موزع وأب تمكن من تحديد هوية الموزع والمصادقة على محتواه.
3. شهادة شبكة تمكن من تحديد هوية الشبكات الخاصة الافتراضية وتضمن سلامة جميع المبادلات التي تتم عبرها.

كما تضمن الفصل الرابع من من قرار وزير تكنولوجيات الاتصال المؤرخ في 19 جويلية 2001 المتعلق بضبط المعطيات التقنية المتعلقة بشهادات المصادقة الإلكترونية والوثوق بها تحديدا لمجال استعمال شهادات المصادقة وهو:

- التعريف بهوية صاحب الشهادة، ولذلك الغرض يتولى مزود خدمات المصادقة الإلكترونية جمع المعلومات ذات الصبغة الشخصية الضرورية لتسليم الشهادة مباشرة من الشخص المعني أو من الغير بعد موافقة ذلك الشخص الكتابية أو الإلكترونية. (الفصلين 16 و39 من قانون المبادلات والتجارة الإلكترونية).
- الإشهاد بحصول مبادلة وتحديد تاريخ وتوقيت حصولها ،
- القيام بعمليات التجارة الإلكترونية.

2. واجبـــات مزود خدمات المصادقة الألكترونية

- واجب توفير الأمان والموثوقية

- لتوفير بيئة إلكترونية آمنة وموثوقة يوجب المشرع على مزود خدمات المصادقة الالكترونية استعمال وسائل تقنية موثوق بها لإصدار وتسليم وحفظ الشهادات واتخاذ الوسائل اللازمة لحمايتها من التقليد والتدليس (الفصل 13 من قانون المبادلات والتجارة الإلكترونية).

- ولضمان الموثوقية في الامضاء الإلكتروني يوجب المشرع على مزود خدمات المصادقة الإلكترونية توفير الضمانات التالية :

- الصلة بين صاحب الشهادة ومنظومة التدقيق في الامضاء الخاصة به ،

- انفراد صاحب الشهادة بمسك منظومة إحداث إمضاء مطابقة للقانون ومتكاملة مع منظومة التدقيق في الامضاء المعرفة في الشهادة في تاريخ تسلمها.

(الفصل 18 من قانون المبادلات والتجارة الإلكترونية)

كم يلزمه قرار وزير تكنلوجيات الاتصال المؤرخ في 19 جويلية 2001 المتعلق بضبط المواصفات التقنية لمنظومة إحداث الامضاء الإلكتروني مزود خدمات المصادقة الإلكترونية للقيام بجملة من الاجراءات الكفيلة بتأمين استعمال منظومة إحداث الامضاء الالكتروني تتمثل في :

- مراقبة النفاذ إلى منظومة الإحداث المودعة لديه وتحديد هوية كل مستعمل لها ...(الفصل7)
- حفظ أزواج المفاتيح بواسطة كلمة سر وتقسم إلى عدة أجزاء ..(الفصل 8)
- التثبت من استجابة منظومات احداث المفاتيح لشروط السلامة ومطابقتها للمواصفات والمعايير الدولية في تأمين تكنلوجيا المعلومات.(الفصل 9)
- إخفاء المفتاح الخاص بعد كل استعمال (الفصل 10)

- واجب توفير معطيات كاملة وصحيحة بصورة مستمرة

الكمال والدقة

- توفير جميع البيانات التي أوجب القانون (الفصل 17 من قانون المبادلات والتجارة الإلكترونية) تضمينها بالشهادة وتتمثل بالخصوص في :
  - هوية صاحب الشهادة ،
  - هوية الشخص الذي أصدرها وإمضاءه الإلكتروني ،
  - عناصر التدقيق في إمضاء صاحب الشهادة ،
  - مدة صلوحية الشهادة ،
  - مجالات استعمال الشهادة.

ملاحظة :

يراجع بخصوص القائمة الكاملة للبيانات الوجوبية الفصل 3 من قرار وزير تكنلوجيات الاتصال المؤرخ في 19 جويلية 2001 المتعلق بضبط المعطيات التقنية المتعلقة بشهادات المصادقة الإلكترونية والوثوق بها.

- التقيد بالمواصفة الدولية X 509 الصادرة عن الاتحاد الدولي للإتصالات في إصدار شهادات المصادقة الإلكترونية.

الصحة

- ضمان صحة المعلومة المصادق عليها التي تضمنتها الشهادة في تاريخ تسليمها.(الفصل 18 من قانون المبادلات والتجارة الإلكترونية)
- تعليق العمل بشهادة المصادقة حالا بطلب من صاحبها أو عندما يتبين :
  1. أن الشهادة سلمت بالاعتماد على معلومات مغلوطة أو مزيفة ،
  2. أنه تم انتهاك منظومة إحداث الامضاء ،
  3. أن الشهادة استعملت بغرض التدليس ،
  4. أن المعلومات المضمنة بالشهادة قد تغيرت.

ويتولى إعلام صاحب الشهادة حالا بالتعليق وسببه. (الفصل 19 من قانون المبادلات والتجارة الإلكترونية)

- إلغـــاء شهادة المصادقة حالا في الحالات التالية :
  1. عند طلب صاحب الشهادة ،
  2. عند اعلامه بوفاة الشخص المادي أو انحلال الشخص المعنوي صاحب الشهادة ،
  3. عند القيام باختبارات دقيقة ، بعد تعليقها ، تبين أن المعلومات مغلوطة أو مزيفة أو أنها غير مطابقة للواقع أو أنه قد تم انتهاك منظومة احداث الامضاء أو الاستعمال المدلس للشهادة (الفصل 20 من قانون المبادلات والتجارة الإلكترونية)

<u>الإستمرارية</u>

مسك سجل إلكتروني لشهادات المصادقة على ذمة المستعملين مفتوح للإطلاع إلكترونيا بصفة مستمرة على المعلومات المدونة به وحمايته من كل تغيير غير مرخص فيه (الفصل 14 من قانون المبادلات والتجارة الإلكترونية).

يراجع كذلك الفصل 19 من كراس الشروط الذي يلزم المزود بوضع بنك معلومات مفتوح 24/24 ساعة كامل أيام الأسبوع متضمن لعدة معلومات.

- واجب المحافظة على السر المهني و حماية المعطيات الشخصية لصاحب الشهادة
- المحافـــظة على سرية المعلومات التي عهدت إليهم في إطار تعاطي نشاطاتهم (الفصل 15 من قانون المبادلات والتجارة الإلكترونية).
- الحصول على موافقة صاحب الشهادة المعني قبل معالجة المعطيات الشخصية الخاصة به. (الفصل 38 من قانون المبادلات والتجارة الإلكترونية)
- إعلام صاحب الشهادة بواسطة إشعار خاص بالاجراءات المتبعة من قبله في مجال حماية المعطيات الشخصية قبل معالجتها. (الفصل 41 من قانون المبادلات والتجارة الإلكترونية)

الفقرة الثانية : ضمانات حسن القيام بخدمات المصادقة الإلكترونية

يمكن تبين ضمانات حسن القيام بخدمات المصادقة الإلكترونية من خلال الشروط التي وضعها المشرع لممارسة وظيفة خدمات المصادقة وللجزاء الذي رتبه عند إخلال المزود بالواجبات المحمولة عليه وللنظام الذي وضعه للرقابة على أعماله.

1. شـــروط ممارسة نشاط مزود خدمات المصادقة الألكترونية

يتعين على كل شخص مادي أو معنوي يرغب في تعاطي نشاط مزود خدمات المصادقة الألكترونية الحصول على ترخيص مسبق من الوكالة التونسية للمصادقة الألكترونية (الفصل 11 فقرة 1).

وللحصول على هذا الترخيص يجب أن تتوفر في طالبه جملة من الشروط الذاتية والموضوعية تمثل ضمانا لحسن قيام مزود خدمات المصادقة بالوظائف المسندة إليه والتي يتوقف عليها تطور المبادلات والتجارة الإلكترونية.

- **الشـــروط الذاتية**

يجب أن تتوفر في طالب الترخيص الشروط التالية :

1. **أن يكون من ذوي الجنسية التونسية منذ خمسة أعوام على الأقل،**
2. **أن يكون مقيما بالتراب التونسي ،**
3. **أن يكون متمتعا بحقوقه المدنية والسياسية ونقي السوابق العدلية،**
4. **أن يكون متحصلا على شهادة جامعية معترف بها،**
5. **أن لا يتعاطى نشاطا مهنيا آخر.**

(الفصل 11 فقرة 2 من قانون المبادلات والتجارة الالكترونية)

ويضيف الفصل الثاني من كراس الشروط شرطا آخر وهو أن لا يكون طالب الترخيص في تعارض مع شروط ممارسة مهنة تجارية ...

- الشـــروط الموضوعية

– الموارد البشرية (الباب الثاني من كراس الشروط)

– الموارد المالية (الفصل الثاني من كراس الشروط)

1. تأمين المسؤولية المدنية والمهنية لتغطية الأضرار التي يمكن أن تلحق بالغير.
2. توفير رأس مال ...

– التجهيزات (الفصلين 17 و 18 من كراس الشروط)

1. وضع موزعات وأجهزة طرفية تمكن من النفاذ إلى الموزعات بمواقع مؤمنة ...
2. تجهيز المقر بشبكة كهربائية ونظام تكييف ...
3. تأمين حاويات الخزن ضد الحرارة و الرطوبة ...

2. مســـؤوليـــة مزود خدمات المصادقة الألكترونية

- **المســـؤولية المدنيـــة لمزود خدمات المصادقة الإلكترونية**

يعتبر مزود خدمات المصادقة الألكترونية مسؤولا عن :

- كل ضرر حصل لشخص وثق عن حسن نية في الضمانات الواجب عليه توفيرها للمتعاملين والمذكورة أعلاه.
- الضرر الحاصل لكل شخص نتيجة عدم تعليق أو إلغاء شهادة.

غير أنه لا يتحمل مسؤولية الأضرار الناتجة عن عدم احترام صاحب الشهادة لشروط استعمالها أو لشروط إحداث إمضائه الألكتروني (الفصل 22 من قانون المبادلات والتجارة الإلكترونية)

- **المسؤولية الجزائية لمزود خدمات المصادقة الإلكترونية**

إضافة إلى الجزاء الإداري المتمثل في سحب الترخيص منه وإيقاف نشاطه عند الإخلال بالواجبات المحمولة عليه والمذكورة أعلاه (الفصل 44 من قانون المبادلات والتجارة الإلكترونية) ، فإن مزود خدمات المصادقة الإلكترونية يمكن أن يكون محل تتبعات جزائية من أجل عدة جرائم إقتضاها القانون نوردها بصورة مختصرة صحبة العقوبات المقررة لها في الجدول التالي:

عدم احترام كراس الشروط المتعلقة بإصدار وتسليم وحفظ شهادات المصادقة.	الفصل 45.	خطية تتراوح بين ألف و عشرة آلاف دينار.
ممارسة نشاط مزود خدمات دون الحصول على ترخيص مسبق.	الفصل 46	السجن لمدة تتراوح بين شهرين و3 سنوات وبخطية تتراوح بين ألف وعشرة آلاف دينار.
معالجة معطيات شخصية بصاحب الشهادة بدون الحصول على موافقته.	الفصل 51	خطية تتراوح بين ألف و عشرة آلاف دينار.
جمع معلومات خاصة بصاحب الشهادة واستعمالها لغاية أخرى غير متعلقة بالمعاملة دون إعلام صاحب الشهادة وعدم معارضته.	الفصل 51	خطية تتراوح بين ألف و عشرة آلاف دينار.
إفشاء أو البحث أو المشاركة في إفشاء المعلومات التي عهدت إلى المزود أو أعوانه في إطار تعاطي نشاطهم في غياب ترخيص من صاحب الشهادة أو خارج الحالات التي نص عليها القانون.	الفصل 52 من القانون والفصل 254 من المجلة الجنائية.	السجن مدة ستة أشهر وخطية قدرها خمسمائة فرنك.

• ملاحظة : يقتضي الفصل 53 من القانون أنه يمكن للوزير المشرف على الوكالة الوطنية للمصادقة الألكترونية إجراء الصلح في المخالفات المنصوص عليها بالفصلين 49 و50.

4. مراقبة نشاط مزود خدمات المصادقة الألكترونية

- الهيكل المشرف على الرقابة : الوكالة الوطنية للمصادقة الإلكترونية

- أنواع الرقابة

- منح الترخيص بعد التثبت من توفر الشروط (الفصل 11 من قانون المبادلات والتجارة الإلكترونية)

- القيام بأعمال التدقيق (الفصلين 21 و22 من كراس الشروط).

- سحب الترخيص في صورة الاخلال بالالتزامات (الفصلين 10 و 11 من الأمر عدد 1668 لسنة 2001 المؤرخ في 17 جويلية 2001 المتعلق بضبط إجراءات الحصول على ترخيص لممارسة نشاط مزود خدمات المصادقة الإلكترونية)

الجوانب القانونية

للحماية المعلوماتية

- السيد ابراهيم نافع
كاهية مدير إدارة الشؤون القانونية
والنزاعات بوزارة تكنلوجيات الإتصال والنقل •••

المقدمة : اعتبارات تاريخية وقانونية

-> الإشكال : كيفية تأمين المراسلات

- الحلول المعتمدة : * دمغ المراسلة

* تشفير المراسلة

⇦ الحاجة، هذه التقنيات القديمة بقيت فاعلة حاليا ولم تتغير الا المراسلة (إلكترونية) نتيجة بروز وسائل اتصال حديثة.

...

-> الإشكال : هل أن مبدأ حرمة وسرية المراسلات يتلاءم والمتطلبات الأمنية.

* المعادلة تحدد الحلول المعتمدة.

* بصفة عامة لا يمكن للدولة أن تسمح باستعمال وسائل الاتصال، التي تضعها بصفة مباشرة أو غير مباشرة على ذمة العموم، للمساس بأمنها العام.

* إلى تاريخ قريب كانت مختلف المجتمعات تمنع استعمال وسائل الاتصال في غياب المراقبة.

* وسائل التشفير = سلاحا.

...

الباب الأول : اللا حماية الافتراضية

أولا : واقع اللاحماية

-> بينت الدراسات المتعلقة بالسلامة والسرية على شبكة الأنترنات بالنسبة لسنة 2000 :

* الخسائر : 600 دولار أمريكي/متضرر.
* 34 % من المبحرون استهدفوا لحوادث مرتبطة بالسلامة أو بسرية معطياتهم الشخصية.
* 87 % من الاحتيالات تمت بمواقع البيع بالمزاد العلني.

-> سجل FBI في الولايات المتحدة الأمريكية 17.672 حادث على شبكة الأنترنات.

ثانيا : الحاجة الملحة إلى الحماية المعلوماتية

* التعرف على الهوية.
* ضمان حرمة المراسلة
* السرية.
* مراقبة النفاذ.

ثالثا : تأمين الحماية المعلوماتية.

* إحداث الوثيقة
* إرسال الوثيقة
* خزن الوثيقة

⇦ تعتبر الحماية مقبولة إذا تم التعرف على الهوية بصفة دقيقة والتأكد من حرمة وسرية الوثيقة خلال مختلف مراحل حياتها.

رابعا : ضرورة إرساء مناخ الثقة في المعاملات الإلكترونية.

-> الإمضاء الإلكتروني : عنصر أساسي يضمن في الآن نفسه التعريف بهوية الممضي وحرمة الوثيقة.

-> الشهادة الإلكترونية : هي المفتاح العمومي للممضي مصحوبة بمعطيات أخرى غير قابلة للتدليس نتيجة تشفيرها بواسطة المفتاح الخاص.

-> مزود خدمات المصادقة الإلكترونية : يدقق ثم يضمن ملكية الممضي لمفتاحه العمومي.

-> الوكالة الوطنية للمصادقة الإلكترونية : المرجعية العليا في التسلسل الهرمي لخدمات المصادقة الإلكترونية.

...

الباب الثاني : عناصر الحماية المعلوماتية

-> على مستوى المعلومة :

* لا تتمتع المعلومة بحماية لذاتها فالحماية مرتبطة بالسند المادي (حقوق المؤلف، البراءات، سرية المراسلة).

-> على مستوى النظم :

* يمكن أن تكون الانتهاكات مادية مثل السرقة أو التدمير أو لا مادية مثل الاختراقات.

قانون عدد 89 لسنة 1999 المؤرخ في 2 أوت 1999 المتعلق بتنقيح وإتمام بعض أحكام المجلة الجنائية.

-> على مستوى الشبكات :

* حماية التجهيزات والخطوط من إتلافها وإفسادها.

مجلة الاتصالات الصادرة بالقانون عدد 1 لسنة 2001 المؤرخ في 15 جانفي 2001 كما تم إتمامها بالقانون عدد 46 لسنة 2002 المؤرخ في 7 ماي 2002.

-> على مستوى الأشخاص :

* الاستعمال غير المرخص فيه للمعطيات الشخصية، التحيل.

قانون عدد 33 لسنة 2000 المؤرخ في 9 أوت 2000 المتعلق بالمبادلات والتجارة الإلكترونية.

الباب الثالث - العنصر المحوري للحماية : التشفير

أولا : المفاهيم

* التشفير : استعمال رموز أو إشارات غير متداولة تصبح بمقتضاها المعلومات المرغوب تمريرها أو إرسالها غير قابلة للفهم من قبل الغير أو استعمال رموز أو إشارات لا يمكن الوصول إلى المعلومة بدونها.

* وسائل التشفير : مجموعة التجهيزات والبرمجيات التي تمكن من إنجاز أو فك التشفير.

* خدمات التشفير : الخدمات المتعلقة بالعناصر الشخصية المستعملة ضمن منظومات التشفير.

...

ثانيا- أنواع التشفير :

* مفتاح سري وحيد للتشفير المتوازي
* مفتحان خاص وعام للتشفير اللامتوازي.

ثالثا- التقنية المعتمدة : التشفير اللامتوازي.

* يحفظ المستعمل المفتاح الخاص ولا يستعمله الا بنفسه.
* يبقى المفتاح العمومي على ذمة الجميع ويستعمل من قبل كل شخص يرغب في ذلك.

-> يعتمد التشفير بالمفتاح العمومي على وسيط.

* يضع مزود الخدمة المفتاح العمومي على ذمة الجميع في شهادة إلكترونية.
* يشفر المصدر بواسطة المفتاح العمومي للمرسل إليه.
* يفك المرسل إليه الشفرة بواسطة مفتاحه الخاص.

رابعا – النظام القانوني للتشفير :

-> قبل سنة 2001

* الأمر عدد 501 لسنة 1997 المؤرخ في 14 مارس 1997 والمتعلق بالخدمات ذات القيمة المضافة للاتصالات.

* قرار وزير المواصلات المؤرخ في 9 ديسمبر 1997 والمتعلق بضبط شروط استعمال الشفرة في استغلال الخدمات ذات القيمة المضافة للاتصالات.

-> بعد سنة 2001 :

* مجلة الاتصالات الصادرة بالقانون عدد 1 لسنة 2001 المؤرخة في 15 جانفي 2001 كما تم إتمامها بالقانون عدد 46 لسنة 2002 المؤرخ في 7 ماي 2002.

الفصل 9 :

تضبط بمقتضى أمر شروط وإجراءات استعمال وسائل أو خدمات التشفير عبر شبكات الاتصالات وكذلك شروط تعاطي الأنشطة ذات العلاقة.

* الأمر عدد 2727 لسنة 2001 مؤرخ في 20 نوفمبر 2001 يتعلق بضبط شروط وإجراءات استعمال وسائل أو خدمات التشفير عبر شبكات الاتصالات وتعاطي الأنشطة ذات العلاقة.

...

-> مجال التطبيق :

* يهدف هذا الإطار إلى تسهيل وتعميم استعمالات التشفير على شبكات الاتصالات العمومية والخاصة مع تبسيط الإجراءات الإدارية المتعلقة بها.

-> أصناف وسائل التشفير :

* كل وسيلة تمكن فحسب من تشفير المعلومات الخاصة للتعريف بالمستعمل أو بالجهاز الطرفي عبر شبكات الاتصالات لضمان سرية هذه المعلومات.
* كل وسيلة تشفير تمكن من تشفير الوثائق الإلكترونية المتبادلة عبر شبكات الاتصال أو إمضائها إلكترونيا.

-> المصادقة على وسائل التشفير :

- المبدأ : جميع الوسائل خاضعة للمصادقة.

* الوكالة الوطنية للمصادقة الإلكترونية.

* مدة صلوحية المصادقة 3 سنوات.

* نشر قائمة في الوسائل المصادق عليها.

- الاستثناء : وسائل التشفير من الصنف الأول المتوفرة بالبرمجيات المتداولة.

* نشر قائمة في هذه الوسائل.

-> استعمال وسائل التشفير :

- دون إجراء مسبق :

* الوسائل من الصنف الأول.

* الوسائل من الصنف الثاني التي تعتمد العناصر الشخصية للإمضاء الإلكتروني المودعة لدى مزود خدمات المصادقة الإلكترونية.

- إيداع مفاتيح لدى الوكالة الوطنية للمصادقة الإلكترونية :

* الوسائل الأخرى من الصنف الثاني.

- تحجير الاستعمال :

* المحطات الراديوية الترفيهية أو التجهيزات الراديوية العاملة على قنوات النجدة والملاحة البحرية.

-> تعاطي الأنشطة في مجال التشفير :

- المبدأ :

* ترخيص من قبل وزير الدفاع الوطني بعد أخذ رأي لجنة التشفير.

- الاستثناء :

* مزودي خدمات المصادقة الإلكترونية.

الباب الرابع - المخالفات والعقوبات :

-> مجلة الاتصالات :

* الفصل 87 : يعاقب بالسجن لمدة تتراوح بين ستة أشهر وخمس سنوات وبخطية من ألف إلى خمسة آلاف دينار أو بإحدى هاتين العقوبتين كل من استعمل أو صنع أو استورد أو صدر أو حاز لأجل البيع أو التوزيع مجانا أو بمقابل أو عرض للبيع أو باع وسائل أو خدمات التشفير أو أدخل تغييرا عليها أو أتلفها دون مراعاة أحكام الأمر عدد 2727 لسنة 2001.

-> الأمر عدد 2727 لسنة 2001 :

- الفصول 17 و 18 و 19 :

* الإيقاف الفوري للعمل بالترخيص،

* سحب الترخيص مؤقتا لمدة لا تتجاوز 6 أشهر،

* سحب الترخيص نهائيا،

* حجز وسائل التشفير.

الخاتمة - التوجهات المستقبلية :

- الفصل 9 من الدستور : إعداد مشروع قانون حول حماية المعطيات الشخصية.

- المجلس الوزاري المضيق بتاريخ 31 جانفي 2003.

وضع مخطط وطني حول السلامة المعلوماتية.

* إحداث هيكل مكلف بالسلامة المعلوماتية.

* إقرار مبدأ التدقيق الدوري الإجباري على الهياكل العمومية والخاصة التي تستغل شبكات وأنظمة معلوماتية حساسة.

* المصادقة على الخبراء في مجال السلامة المعلوماتية.

وشكرا

التجارة الإلكترونية : الجوانب التقنية للحماية الرقميّة

نورالدين بودريقة
أستاذ في الاتصالات
المدير العام للوكالة الوطنية للمصادقة الإلكترونية

1. المقـــدمـــة

تعتـــبر حمايـــة المعطيات المعلوماتية والمبادلات الإلكترونية من العوامل الأساسية لإرساء ثقة المستهلك والمؤسسة لتطوير التجارة الإلكترونية.
إذ أنّ الصبغة اللامادية للمعطيات والمبادلات لا تتماشى ووسائل التصرّف التقليدية في حماية الأملاك والموارد.

وأمام الصبغة التحررية التي تتميز بها شبكات الاتصال الحالية إضافة إلى غـــياب تراتيب دولية تضفي على المبادلات صبغة قانونية لحمايتها، فسح المجال لـــتعدد المخالفـــات التي تشمل خاصّة النفاذ الممنوع للمعطيات ووسائل المراسلة وعملـــيات خـــزن المعطيات ومعاملات التجارة الإلكترونية والخدمات الإلكترونية بصفة عامة.

وتفاديـــا لهـــذه الـــنقائص وجب التأكد عند وضع منظومات المبادلات من الخاصـــيات التقنـــية للحماية المعتمدة وتمكين المتدخلين من وسائل الحماية التقنية الملائمة من خلال مجهود جماعي يتمّ بلورته.

2. التحولات الإلكترونية

أتت التحوّلات التكنولوجيّة التي يشهدها العالم إلى ظهور ثورة رقميّة نتيجة عولمـــة الاقتصاد وعولمة الاتصال التي حوّلت العالم إلى قرية كونية تقلّصت فيها المســـافات واختزل فيها الوقت وتتطوّرت فيها التقاليد والنماذج. ووصفت الثورة بالرّقمية لأنها كانت نتيجة تقارب
الـــنماذج الـــنظرية والتكنولوجيات الإلكترونية وأساليب المعالجة المعلوماتية التي اعتمدت كلّها مبدأ الرقم الثنائي.

كما اتسمت هذه الثورة الرقميّة بالملامح التالية :

1. اندمـــاج التكنولوجـــيات، حيث أصبح بإمكان الشبكات تمرير الحركة دون اعتبار نوعية الإشارة المنقولة (سواء كانت صورة أو صوتا أو معطيات) أو اعتبار نوع الخدمة المصاحبة لها .
2. تنامي ذكاء الشبكات، حيث أصبحت الشبكات قادرة على توفير أنماط جديدة من الخدمات مع سهولة الاستعمال وتدني كلفة إنجازها والارتباط بها.
3. تطـــوّر سعة الشبكات لكي تتمكّن من تلبية الحاجيات المتنامية للمستهلك في تبادل المعلومات بأنواعها والارتفاع المتواصل لعدد المستعملين وكذلك نمو حجم المعطيات المخزونة فوق الشبكة
4. تأميـــن استمرارية الاتصال باعتماد التكنولوجيات المتنقلة وتقنيات استشعار المستعملين
5. تنوع الخدمات وتحسن جودة تقديم هذه الخدمات إلى الحريف مع المحافظة على سرّية المعلومات المنقولة وضمان حماية المبادلات.

وشـــهدت الـــتحوّلات التكنولوجية انعكاسات اقتصادية أدّت إلى تغيير لنوعية العلاقات نذكر منها بالخصوص :

عولمـــة المبادلات : حيث أصبح من الصعب على أي مجتمع أن يتطوّر دون الانفتاح على العالم والتفاعل مع المحيط العالمي.
بـــروز أنمـــاط جديدة : من التعامل عن بعد باستعمال وسائل إلكترونية غير مادية اتسعت استعمالاتها لتشمل مختلف القطاعات والأنشطة الإقتصادية.
تنامـــي دور المعلومـــة : في دعم القدرة التنافسية للمؤسسة والاقتصاد عامة وأصبحت نشاطات المؤسسة بذلك مرتكزة حول الشبكات.
بـــروز مفاهـــيم جديدة : منها الاقتصاد اللاّمادي والإدارة الرقميّة والحضور اللاّمادي والخدمات عن بعد

وأصـــبح بذلـــك للمعلومـــة والارتباط بالشبكة دور يساهم كلّيا في تقدم المؤسسة ونجاحهـــا ويـــبرز قدراتهـــا التنافسيّة. هذا مما ساهم في بلورة تحوّلات اقتصادية عميقة وتحسين في المرد ودية الاقتصادية نذكر من أهمها:

الإنتاجية ونسق النمو : تساهم التطوّرات التكنولوجية بدور هام في دفع الإنتاجية من جهة وتحريك الطلب الدّاخلي

التشغيل والأجور : يجمع المختصّون على أن تكنولوجيات الاتصال بإمكانها خلق فرص عمل عديدة في البلدان المبدعة بالأخص

الكلفـــة : تشهد المجتمعات تقلص كلفة عديد الخدمات وارتفاع للمرابيح ظهر من خلال اعتماد التحولات التكنولوجية داخل أساليب الإنتاج بالمؤسسة

المعـــاملات الـــتجارية : تطـــوّر كبـــير تشهده التجارة الإلكترونية اليوم فاق كلّ الـــتّوقعات شملت 80% منها ما يسمى بالتجارة بين المؤسسات أو بين المؤسسات والإدارة.

3. التجارة الإلكترونية والإدارة الرقميّة:

شـــهدت الـــتجارة الإلكترونية مفاهيم مختلفة لعلّ أوسعها ذلك الذي يتعلّق بالتبادل الإلكتروني المرتبط بالأنشطة التجارية وهي تغطي العمليات التجارية التي تـــتمّ باســـتعمال الوثـــائق الإلكترونية كما نصّ عليها التعريف المستعمل بقانون التجارة والمبادلات الإلكترونية التونسي [1].

تنقســـم الـــتجارة الإلكترونـــية إلـــى ثلاثـــة أقسام، يشمل القسم الأول منه المعـــاملات التجارية الإلكترونية المباشرة بين المؤسسات، وهي أكثر انتشارا في الـــبلدان المصنّعة حيث تتسارع المؤسسات في استعمال التبادل الإلكتروني داخل كـــلّ نشـــاطاتها سواء كانت نشاطات تسويق للمنتوجات والخدمات أو النشاطات المـــتعلّقة بالصفقات التي تشمل التعاقد الإلكتروني والدفع الإلكتروني أو نشاطات الإنـــتاج والمناولة، ويرمي هذا التسارع إلى استعمال شبكات الاتصال والأنترنات كوســـيلة ناجعـــة لـــربح الوقـــت ودعم المنافسة وتحسين جودة التعامل وعرض الخدمات.

ويشـــمل القسم الثاني التجارة الإلكترونية بين المؤسسة والمستهلك ويتمثّل ذلـــك في البيع المباشر للمستهلك إذ يمكن لهذا الأخير دخول الأروقة التجارية أو الـــنفاذ إلـــى الخدمـــات الإلكترونـــية عبر الخط لاقتناء حاجياته من منتوجات أو خدمات. ويشهد هذا الصنف من التجارة الإلكترونية حركية كبيرة في بعض البلدان على غرار الولايات المتحدة الأمريكية، باعتبار ارتباطها بعادات المستهلك في هذه البلدان حيث تبلورت ثقافة رقميّة ساهمت في انتشارها عديد الاعتبارات منها تقاليد فـــي عمليا الشراء عن بعد (مثل البيع عبر المراسلة والبيع عبر القنوات التلفزية) وكذلك اعتماد مبدأ المخاطر (risk) ذات المستوى المقبول في التعامل التجاري.

وتشكلّ الإدارة الرقميّة القسم الثالث من التجارة الإلكترونية، ويشمل هذا الصنف عـــرض عديـــد الخدمات الإدارية باتجاه المؤسسة أو المواطن، ووضع موزعات تحـــتوي معطـــيات ذات قيمة مضافة، يمكن للمواطن النفاذ إليها. ونخصّ بالذكر الخدمات الإدارية التالية :

- الإدلاء بالضرائب واستخلاصها عن بعد
- استخلاص الفواتير عن بعد
- الحصول على وثائق إدارية أو معلومات عن بعد
- النفاذ إلى المكتبات الافتراضية

- التكوين الافتراضي

تبرز عديد الدراسات أن تطوّر التجارة الإلكترونية في عديد البلدان مرتبط ارتـباطا وثـيقا بتقلـيص الصـعوبات وتجاوز حواجز تعود أساسا إلى الطبيعة الافتراضية للمعاملات وتتعلق هذه الصعوبات والحواجز بالخصوص بـ :

- تعزيـز الإطـار القانوني حتى يتلاءم ومقتضيات التجارة الإلكترونية ليشمل حماية الملكية الرقميّة وإثبات الوثيقة الإلكترونية.
- تعزيز ثقة المتدخلين في المبادلات الإلكترونية (إدارة مؤسسة ومستهلك) وذلك بتأميـن وحمايـة المـبادلات المالية وحماية المستهلك وحماية المبادلات ذات الصبغة الشخصيّة.
- تعزيـز البنية الأساسية للإتصال وذلك لضمان ملاءمتها مع تطور المبادلات الإلكترونـية وذلـك بتوفير السعة الكافية والجودة المتطوّرة وتأمين المبادلات والمـنظومات المرتـبطة بالشبكات من المخاطر الإلكترونية مثل القرصنة أو التشويه أو انتحال الصفة أو التخريب
- نشر ثقافة المعلومات والاتصال لدى المتدخلين (إدارة ومؤسسة ومواطنا) وذلك بالتكويـن والتحسيس مع السهر على ملاءمة الاقتصاد "الرقمي" وذلك انطلاقا من المحيط الإجتماعي للمؤسسة والتقاليد الإجتماعية للمستهلك.

4. <u>في تعزيز ثقة المتدخلين</u> :

لقـد تنوعـت القرصـنة الإلكترونية وتنوعت الهجمات الإلكترونية حتى أصـبحت جـزءا لا يـتجزأ من مجال اختصاص لا بد من السيطرة عليه لحماية الشـبكات والمـنظومات ممّا استقطب اهتمام المسؤولين على الأجهزة الأمنية في الدّول المتقدمة.

وقد أظهرت التقارير التي أعدّتها عديد المصالح (مثل مصالح الأمن القومي بالولايـات المتّحدة الأمريكية، [2]) أنّ أكثر من ثلث المؤسسات تتعرّض شهريا إلى عمليات إندساس في أنظمتها أو مسّ لمعلوماتها لم يتمكن العديد منها من تحديد هويّـة المخـالف المـندس. كمـا أقرّت هذه الدّراسات بموجود نقائص للأنظمة المستعملة

وتتطلّب عملية تأمين المبادلات الإلكترونية عبر شبكات الاتصال وحماية المعطيات المعلوماتية استخدام تقنيات لتوفير خمسة خدمات أساسية هي :

1. الـتعريف بهويّـة الأطراف المتدخلة في المبادلات الإلكترونية أو في عمليات التعاقد الإلكتروني أو عمليات النفاذ عبر الشبكات إلى المعطيات المعلوماتية أو المنظومات المفتوحة للنفاذ إليها عبر الأنترنات.

2. إثـبات هويّـة المتدخلين وهي خدمة تضمن التثبت في صحّة الهويّة للمستهلك الذي يطلب النفاذ أو للموزع الذي يعرض خدمة أو متجرا افتراضيا أو أروقة تجاريـة. وتعـتمد هذه الخدمة استعمال عناصر إثبات مثل شهادات المصادقة الإلكترونية أو العناصر الحيوية (biometrics).
3. الحفـاظ علـى سـلامة محـتوى المبادلات والمراسلات والعقود الإلكترونية والمعطـيات المعلوماتية ومحتوى الموزعات ومخازن الأرشيف الإلكترونية. ويعـتمد الحفاظ على سلامة المحتوى تقنيات تعتمد التشفير الإلكتروني وبلورة سياسـات السـلامة الرقمية (security policies) التي ترمي إلى إيجاد قواعد سـلامة تضـمن الحفاظ على السلامة إذا ما تمّ اتباعها كليا عند كل نفاذ إلى المعلومات المحافظ عليها.
4. ضـمان عـدم إنكار أحد المتدخلين للمبادلة الإلكترونية الواحدة بعد إنجازها. ويشمل هذا عدم إنكار الرسالة الإلكترونية إثر إرسالها أو عدم إنكار الممضي لعقـد إلكتروني بعد إمضائه وتراسله أو عدم إنكار المرسل إلية تسلمه لرسالة إلكترونـية. ويعتمد ضمان عدم الإنكار تقنيات عديدة منها استعمال شهادات المصادقة الإلكترونية.
5. ضـمان الـتواجد المسترسـل (disponibility) للخدمات الإلكترونية الموجهة للأفـراد والجماعات. ويشمل هذا الضمان مثلا تواجد الموقع التجاري الفعلي طـيلة عمليات الشراء (وهي: إعداد الطلبية- الاستخلاص – نقل البضاعة – تسلم البضاعة – خدمة ما بعد البيع).

5. <u>في تقنيات حماية المبادلات</u> :

تتطلـب الحمايـة الإلكترونـية للمبادلات والمعطيات المعلوماتية استعمال تقنـيات متطوّرة لا بد من متابعة تطوّرها التكنولوجي ومراقبة قدراتها في الحماية مقارنـة بـتطور المخاطـر الإلكترونية بالتطوّر التكنولوجي للحواسيب. وتعتبر التقنيات التالية أكثر التقنيات انتشارا وضمانا لخاصيّات الحماية.

أ- مـنظومات التشـفير السري (secret crypto systems) : يتمثل التشفير بمفتاح سـري بين متداخلين اثنين في استعمال جملة من الأرقام كمفتاح وحيد (يمتلكه المتداخليـن لوحدهمـا) لتشفير المراسلة (أي تغييرها إلى شكل يستحيل تفهم محـتواه الأصـلي دون استعمال المفتاح)، ويتولى المرسل تشفير المبادلة أو الرسالة قبل إرسالها عبر شبكات الاتصال ويقوم الشخص الذي يتلقى الرسالة بفـتحها باسـتعمال نفـس المفـتاح السـري. ويستعمل التشفير وفك التشفير خوارزمـيات محـددة المواصـفات (مـثل مواصفات DES و AES) وقعت دراستها والتثبت في فاعلية حمايتها.

ب- منظومات التشفير بالمفتاح العمومي (Public crypto systems): تستوجب عملـيات التشفير هذه استعمال مفتاحين اثنين لكل متدخل يكون المفتاح الأول

خاصـــا بالمتدخل وسرّيا لا يمكن للمتداخلين الآخرين معرفته أو تكهنه، ويكون المفـــتاح الثاني عموميا ويمكن لكل متدخل معرفته (ثمّ استعماله) وذلك إمّا عن طـــريق النفاذ إلى موزع مؤمن للمفاتيح العمومي، أو عن طريق إرساله بصفة مؤمـــنة مـــن المرســـل إلى المرسل إليه، أو عن طريق وضعه داخل شهادة مصادقة إلكترونية يمضيها جهاز يؤمن ارتباط الشهادة بصاحب المفتاح. ويقع التشـــفير للمـــبادلات بأحد المفتاحين ويقع فك التشفير باستعمال المفتاح الآخر المرتـــبط بالمفـــتاح الأول، على أن يشفّر صاحب زوج المفاتيح مبادلاته التي يرسلها وأن يقع فك التشفير للمراسلات التي يتلقاها باستعمال المفتاح. الخاص وتشمل خوارزميات التشفير مواصفات مثل (RSA أو Elgamal).

ج-مـــنظومات الإمضـــاء : يقع الإمضاء الإلكتروني للمبادلات باستعمال عمليتين اثنين، أولها استخراج خاصّية تسمى بصفة المبادلة، وتضمن العملية الربط بين البصـــمة ومحتوى المبادلة بحيث يكون أي تغيير لحرف من حروف المحتوى سببا في تغيير البصمة (انظر المثال 1 الموالي). وتكون ثاني العمليات عملية تشـــفير البصمة من قبل الممضي باستعمال مفتاح خاص داخل منظومة تشفير للمفتاح العمومي.

النص 1 :

الوكالة الوطنية للمصادقة الإلكترونية تمنح شهادات المصادقة لمستعملي الشبكات

البصمة 1:

3f8a1de7b85cf0d2c2b553356482fa9ce4990bc5

النص 2 :

الوكالة الوطنية للمصادقة الإلكترونية تمنح شهادات المصادقة لمستعملي الشبكة

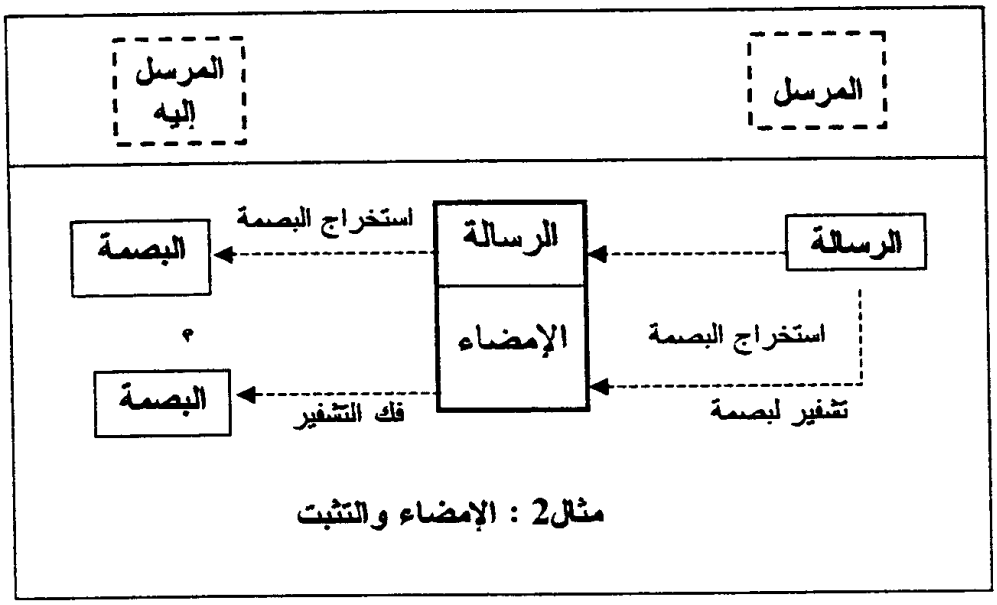
البصمة 2:

87de7ea1ad9e2a0dafc397eb4e24dccae950b44

مثال1 : ترابط البصمة بالمحتوى

ويتعين على المتدخل الذي أرسلت إليه المبادلة والإمضاء المصاحب لها أن يتثبت في الإمضاء المصاحب وذلك بحلّ الشفرة بواسطة المفتاح العمومي ومقارنة الحاصل بالبصمة التي يمكن للمرسل إليه استخراجها من نص المبادلة. وتمكّن هذه العملية المرسل إليه من القيام بما يلي:

1. التعرّف والتثبت على هويّة صاحب الإمضاء الذي بحوزته
2. التأكد من سلامة محتوى المبادلة التي وصلته



مثال2 : الإمضاء والتثبت

د – منظومات حماية الشبكات : تستعمل هذه المنظومات التحليل حركة المبادلات عبر وصلات الشبكات الدّاخليّة للمؤسسة وتحديد المخاطر التي قد تنجرّ عنها والتّصدي للحركات المشبوهة والتعرّف على عمليات النفاذ الممنوعة وذلك باستعمل تجهيزات مثل العازل الناري أو منظومات التعرّف على الإندساس (IDS) أو تقنيات مراقبة النفاذ إلى أنظمة استغلال الحواسيب أو بنوك المعطيات الدّاخلية.

وتعتبر هذه المنظومات ضرورية لحماية المعطيات المخزونة بالأروقة التجارية والتأكد من سلامة التصرّف فيها وتحيينها.

ونظرا للتطوّر السريع للمخاطر التي يمكن أن تؤثر في مردودية منظومات حماية الشبكات والمعطيات أو إبطال بعض الخدمات المعروضة للمستهلك (Denial of service) فوق الشبكة أو إهلاك الموارد أو المعطيات المتواجدة فوق الشبكة فإنّ المراقبة الدورية والتدقيق والتحيين من مستلزمات السلامة الرقميّة.

6. شهادات المصادقة وحماية المبادلات :

تمكّن شهادات المصادقة الإلكترونية من إثبات هويّة صاحب الشهادة. وهي تستعمل عند الإمضاء الإلكتروني من خلال الإستعمال الحقيقي للمفتاح الخاص المصاحب، ثمّ تستعمل عند التثبت في الإمضاء. وتتخذ هذه الشهادة شكلا مطابقا

للمواصـــفات العالمية (من اشهرها X.509 ، [3]). وتحتوي الشهادة خاصّة على مجموع المعلومات التالية :

- تعريف لصاحب الشهادة من خلال معلومات قد تشمل الاسم والعنوان الرسمي والعنوان الإلكتروني .
- المفتاح العمومي لصاحب الشهادة.
- اسم هيكل المصادقة الذي استصدر الشهادة وإمضاءه.
- تعريف لخاصيات الشهادة مثل الرقم التسلسي ونوع الشهادة.
- مدّة صلوحية الشهادة.

وتجمّع الشهادة التي يقع استصدار من قبل هيئة المصادقة (Certification authority) في قاعدة معطيات مؤمنة (LDAP) يقع النفاذ إليها للتثبت في صلوحيّة الشهادات.

وتنقســم شهادات المصادقة إلى عديد الأقسام حسب استعمالاتها نذكر منها شـــهادات موزع التي تمكن من إثبات هويّة البائع وتأمين المبادلات بين المشتري وموقـــع الـــواب الـــتجاري (مثل سريّة معلومات الاستخلاص) وشهادات البريد الإلكتروني التي تستعمل لإمضاء الرسائل الإلكترونية والتي تصاحب الرسائل عند بعـــثها كمـــا تتـــنوع هذه الشهادات حسب نوعية التثبت في الهويّة والمعلومات الشخصيّة المصاحبة عند استصدار الشهادة.

تسهر هيئة المصادقة خاصة على توفير الخدمات التالية :

- استصدار شهادات المصادقة وتجديدها(أو إبطالها) وتوزيعها إلى أصحابها
- الاحتفاظ بنسخ الشهادات في بنوك المعطيات التي تحدث للغرض
- إبطـــال صلوحية الشهادات عند فقدان أحد الشروط الأساسية لسلامة التعامل باستعمال الشهادات.

كمـــا يمكـــن أن توفـــر هذه الهيئة خدمات إضافية تعتمد تقنيات المصادقة والتشـــفير مثل عمليات التوقيت الإلكتروني للمبادلات، ويكون ذلك بإمضاء الهيكل لوثـــيقة تحتوي المبادلة وتوقيتها، أو خدمة الخزن المؤمّن للمعطيات المعلوماتية و المفاتيح الخاصّة (وتخزن هذه المفاتيح مشفرّة) عند الطلب.
تعتـــبر هيـــئة المصادقة عنصرا أساسيا لتركيز الثقة بين المتدخلين في المبادلات الإلكترونية ولحماية المعطيات المعلوماتية وترتّب هيئات المصادقة ما بينها حسب علاقتين اثنين :

- علاقة الاعتراف المتبادل للشهادات
- علاقة هيكلية تظبط مدى ترابط سياسة المصادقة المستعملة داخل كلّ هيئة.

ويعـــدّ بعـــث هيئة مصادقة من بين الوسائل التي تمكّن من التعريف بكافة المتدخليـــن في التجارة الإلكترونية وتأمين المبادلات بينهم، كما يساهم في تشجيع المســـتعملين لشبكة الأنترنات عبر العالم لاقتناء المنتوجات المعروضة في المواقع الـــتجارية، وذلـــك بتوفير شهادات مصادقة إلكترونية معترف بها دوليا من خلال علاقات الاعتراف المتبادل للشهادات بين هيئات المصادقة.

أمّـــا العلاقة الهيكليّة فإنها تساعد على إيجاد ارتباط قانوني بين الاختيارات التقنية في توفير خدمات المصادقة بين هيئات المصادقة كما أنّها تعمل على تطابق الإجراءات العملية للمصادقة والتثبّت في المعلومات الشخصيّة لطالبي الشهادات.

وتماشيا مع هذا التوجه العالمي للعلاقة الهيكليّة فإنّ نظام المصادقة التونسي أدرج دورين اثنين هما :

الـــدّور الأول : تقوم الوكالة الوطنية للمصادقة الإلكترونية بنشاط هيكل المصادقة الجذري وذلك بـــ :

- اختيار المواصفات المتعلقة بشكل الشهادات والشروط التقنية للإمضاء
- التدقـــيق في مدى مطابقة تعاطي النشاط المصادقة في التراتيب القانونية التي تنظم النشاط
- التصـــرّف في البنك الوطني لشهادات المصادقة والذي يجمّع جميع الشهادات التي يقع استصدارها في تونس
- مراقبة تطابق إجراءات المصادقة مع أدلّة الإجراءات المعتمدة وطنيا

الـــدّور الثانـــي : يقـــوم مزودو خدمات المصادقة الإلكترونية بنشاط استصدار الشـــهادات وتوفـــير خدمـــات ذات القيمة المضافة في المصادقة ويضمن المزود الاعتراف المتبادل للشهادات التي يستصدرها المزودون الآخرون.

7. الإشكاليات التقنية للحماية :

سلســـة التثبّـــت في شهادات المصادقة : يعتمد التثبّت في الإمضاء الإلكتروني اســـتعمال المفـــتاح العمومـــي للممضـــي فـــي فك تشفير البصمة، وتكون شهادة المصـــادقة، التـــي تضمن العلاقة بين المفتاح العمومي والممضي ممضاة من قبل هيئة مصادقة. وبذلك يرتبط مستوى إثبات الإمضاء بمستوى الاعتراف بهذه الهيئة أو بمســـتوى إثـــبات الإمضاء المقترن بشهادة المصادقة المذكورة. وبذلك يقترن التثبت في الإمضاء بتواجد سلسة من الشهادات في شكل:

(ش(1)، ش(2)،...، ش(هـــ))

تـــربط الشـــهادة الأولـــى (أي ش(1)) بين الممضي ومفتاحه العمومي وتربط الشـــهادة الثانـــية (أي ش(2)) بين المفتاح العمومي للهيئة التي أمضت الشهادة

الأولـــى والهيـــئة نفســـها وهكذا دواليك إلى حد الشهادة ش(هـــ) التي تمتاز عن الشهادات الأخرى بأنها ممضاة من قبل هيئة مصادقة معترف بها.

حماية مفاتيح التشفير وخزنها : يمكن استعمال المفاتيح الخاصة في إمضاء عقود إلكترونـــية قـــد تحفـــظ مدة تدوم عدة سنوات (15 سنة بالنسبة للقانون التونسي) وبذلـــك لا يمكن استعمال المفتاح العمومي المصاحب للوثيقة المخزونة طيلة مدّة الخزن القانوني. وتستعمل هيئات المصادقة أحد حلّين في خزن تلك المفاتيح. تبدأ الأولى بتجزئة المفتاح ثمّ خزن الأجزاء مشفرّة في حاويات مستقلّة.

أمّ الحـــل الثانـــي فإنـــه يشمل خزن العناصر المستعملة لاستخراج المفتاح بصـــفة مشـــفرة ومراقبة استعمال منظومة استخراج المفاتيح (من العناصر) طبقا لقواعد سلامة ثابتة.

الأرشـــيف الإلكترونـــي والـــتطوّر التكنولوجي للحماية : تعتمد عملية الأرشيف الإلكترونـــي خـــزن الوثائق الإلكترونية ممضاة لمدة قد تتجاوز عشرات السنين. وتكون التقنيات المستعملة خلال هذه العملية مرتبطة بمستوى التطوّر التكنولوجي ســـاعة الخزن. وقد تسفر التحولات التكنولوجيّة إلى إبراز خاصيات قد تستو جب التخلـــيّ عـــن تلك التقنيات المستعملة في التشفير والإمضاء عند الخزن أو تصبح إثـــرها ســـلامة الوثائق الإلكترونية المخزّنة غير مضمونة. ومن الحلول المتبعة لتلافي مثل هذه النقائص يمكن التعامل مع الأرشيف بصفة تضمن نقل محتواه عند كلّ اعتماد مواصفات أو العدول عن تكنولوجيات أثبتت العلوم قصر طاقاتها.

عمليات إعـــادة اســـتخراج المفاتيح : إنّ سلامة عمليات الإمضاء والتثبّت فيه مرتـــبطة ارتـــباطا وثيقا بسريّة المفتاح الخاص. كما أنّ تشفير المبادلات بالمفتاح العمومـــي يستوجب تواجد المفتاح لحل التشفير ساعة تلقي المبادلة أو بعد خزنها، وفي حالة ضياع المفتاح الخاص يضطرّ صاحب المفتاح إلى إعادة استخراجه في شكله الأصلي، وهي عمليّة لا يمكن إنجازها إلاّ إذا كانت عمليّة استخراج المفتاح لأول مـــرّة متبوعة بعملية خزن ما يلزم لإعادة الاستخراج. وهنا لا بدّ من حصرّ قانونـــي لـــدور المتدخل الثالث (trusted third party) الذي يمكن له توفير خدمة إعادة الاستخراج أو خزن الوثائق المشفرة لفائدة المستهلك.

8. <u>الخلاصـــة</u> :

يجمـــع المختصّون على أن حماية المعطيات والمبادلات الإلكترونية عامل أساســـي لإرساء ثقافة مجتمع المعلومات، وأنّ الجوانب التقنية لهذه الحماية تتطوّر بـــتطوّر الـــتحوّلات التكنولوجـــية. واعتبارا لهذه الخاصيّة فإنّ القواعد القانونية لمسايرة هذه التطوّرات لابد أن تأخذ بعين الاعتبار المبادئ التالية :

- الانفتاح التكنولوجي والسهر على عدم الانحياز إلى حلول أو مواصفات تقنية نابعة لمصنع أو لمجموعة تقنية.
- إبـــراز الخاصـــيات التـــي يجب توفيرها من خلال الحماية دون التطرق إلى الأساليب المستعملة والتي تتغير بتطوّر قدرات القرصنة.
- إيجاد الإطار الكامل الملائم للإثبات والبحث والتحري (Forensics).

9. المـــرجع :

[1] قـــانون عـــدد 83 مـــؤرخ فـــي 9 أوت 2000 يتعلق بالمبادلات والتجارة الإلكترونية

[2] Power R. (2002),2002 CSI/FBI (Computer Crime and Security Survey)

[3] X.509 - RFC 2459 (www.ietf.org/rfc/rfc2459.txt) جانفـــي 1999

القوة الثبوتيّة للوثيقة الإلكترونية

بديع بن عبّاس

قاضي بالمحكمة الإبتدائية بصفاقس

مقدمة :

يشهد العالم اليوم زخما معلوماتيا مذهلا وتناميا ملحوظا في مجال الإتصالات والإعلامية ، وتفاعلا لامتناه مع إشعاع التجارة الإلكترونية. وظهور الإقتصاد اللامادي وتوسعا كبيرا لمفهوم اللامادية في التعامل واتساعا كونيّا لرقعة المبادلات التجارية عبر شبكات مفتوحة قرّبت العالم من بعضه. وجعلت منه قرية صغيرة[1] يقع التخاطب فيها بسرعة فائقة ودون حاجة للتنقل من بلد لآخر[2] مما أدخل أعرافا وأنماطا جديدة من التعامل عن بعد لم تكن معروفة ولا حتى متوقّعة, مهدّت لبروز ما اعتبر بثورة ثالثة[3] اكتشاف الطباعة والثورة الصناعية[4] وميلاد عصر جديد هو عصر الهاتف الجوال وشبكات الأنترنات ومواقع الواب...[5] تم التحوّل فيه من التعامل المادي المباشر إلى الإتصال الامادي التي تختزل فيه المسافات وتختصر فيه الأبعاد وتنقل فيه المعلومة من مكان إلى آخر في زمن قياسي عير آلات ووسائل تقنيّة حديثة[6]، مما أعاد إلى الذاكرة قول بعض الفقهاء بأن من يساهم في تطور القانون ليس فلاسفته ولا رجاله، بل هم في الواقع المهندسون بفضل إختراعاتهم[7]. وهذا ما يفترض تفاعل القاعدة القانونية مع التقنيات

---

[1] محمّد الصالح بنحسين، "قواعد الإثبات والتقنيات المعلوماتية المستجدّة"، محاضرة إفتتاح السنة القضائية 2001/2000 بمحكمة الإستئناف بتونس، م.ق.ت عدد 8 لسنة 2000 ص. 29.

[2] علي كحلون، التجارة الإلكترونية، م.ق.ت. عدد 2 لسنة 2000 ص.11.

[3] - OLIVIER (F.) et BARBRY (E.), « des réseaux aux autorités de l'information : révolution technique ? Révolution Juridique ? », J.C.P, 1996, Ed. G.., n°19, p.179.
- Vivant (M.), « Cyber-monde, droit et droits des réseaux », J.C.P. 1996, Ed. G., n°43, p.401.

[4] BEN AHMED (M.), « L'informatique en Tunisie, De prometteuses respectives pour un développement harmonieux » ? L'économiste Maghrébin du 30/10 au 12/11/1996, n°169, p.19.

طارق الصيادي، التجارة الإلكترونية (على ضوء القانون عدد 83 لسنة 2000 المؤرخ في 9 أوت 2000)، محاضرة افتتاح السنة القضائية 2001/2000 بمحكمة الإستئناف المنستير، م.ق.ت. عدد 8 لسنة 2000 ص.123.

[5] طارق الصيادي، التجارة الإلكترونية (على ضوء القانون عدد 83 لسنة 2000 المؤرخ في 9 أوت 2000)، محاضرة افتتاح السنة القضائية 2001/2000 بمحكمة الإستئناف المنستير، م.ق.ت. عدد 8 لسنة 2000 ص.123.

[6] SANDOUAL (V.), Les autorités de l'information, Ed. HERMES, Paris 195, p.66.

[7] سامي الجربي، الإثبات الإلكتروني للتصرّف القانوني، مقال غير منشور ألقي بمدينة توزر سنة 2000.

والإكتشافات العلمية[8] من خلال تشريعات ترصد ظهورها وتطورها، وتجيز التعامل عن بعد وتنظّم مسالكه وتقنّن طرق ووسائل الإثبات فيه[9]. وبما أن أهم الإشكاليات التي تطرحها التصرفات التي تتم عبر شبكات المعلوماتية الحديثة وأهمها الأنترنات[10] على مستوى الإثبات تتعلّق بضرورة إستنباط شكليات إلكترونية تستجيب لموجبات الإثبات في ظل محيط يتسم بانعدام المادية وتجاوز الكتابة والإمضاء والحجج ذات السند الورقي. ونظرا للتلازم بين الجانب القانوني والجانب التقني، فقد سارعت عديد التشريعات إلى إرساء إطار قانوني جديد للإثبات مثل القانون الفرنسي عدد 230-2000 المؤرخ في 13 مارس 2000[11]. وكذلك القوانين الأوروبية الموحّدة بموجب التوصية عدد 93-1999 المؤرخة في 13 ديسمبر 1999[12] . ولم يتخلّف المشرع التونسي عن غيره من التشريعات، فقد أصدر القانون عدد 57 لسنة 2000 المؤرخ في 13 جوان 2000[13] لينقح الفصول الخاصة بالإثبات. وقد جاء هذا القانون بعد إرهاصات تشريعية عديدة[14] قبلت جزئيا إعتماد تقنيات الاتصال الحديثة في الإثبات وهيّأت تشريعنا لإستيعاب ما اصطلح على تسميته بالثورة الصناعية والإنخراط في هذا المسار العالمي الذي لم يكن مقتصرا على قطر دون آخر أو نظام دون آخر بل إتخذ بعد كونيا. كما سن المشرع التونسي القانوني عدد 83-2000 المؤرخ في 9 أوت 2000[15] "مستكملا المسار التحديثي في مجال حجيّة الشيء المعبّر عنه معلوماتيا"[16]. القانون التونسي يميّز بين الإثبات الحرّ للوقائع والمقيّد للتصرّفات القانونية. كما يقيّد القاضي من حيث وسيلة الإثبات المعتمدة لإثبات التصرّف القانوني ومن

---

8 REYNIS (B.), « Le droit à l'épreuve des nouvelles technologies », J.C.P. Notariale et immobilière des nouvelles technologies, n°36, 8 septembre 2000, p.1265.

9 BENSOUSAN (A.), Les télécoms et le droit, Mémento-guide, Ed. HERMES, Paris 1996, p.57.

10 - BREESE (P.) et KAIFMAN (G.), Guide juridique de l'Internet et du Commerce électronique, Ed. Librairie VUIBEST, 2000, p.16.
- DRISSI (I.), Les problèmes internationaux posés par l'Internet, Mémoire de D.E.A. en S.J.F., Université de droit, l'Economie et de gestion Tunis III, année Universitaire 1997-1998, p.3.

11 La Loi n°2000-230 du 13 mars 2000, portant adaptation du droit de la preuve aux technologies d'information et relative à la signature électronique, J.O. 62, 14 mars 2000, p.3369 et J.C.P. 2000, 151, 20259.

12 Directive n°1999/93 (C.E., 13 décembre 1999 : J.O.C.E., n°L.13, 19 janvier 2000.

13 القانون عدد 230-2000 المؤرخ في 13 جوان 2000، ر.ر.ج.ت عدد 48 المؤرخ في 16 جوان 2000، ص.1484.

14 نذكر مثلا " – الفصل 62 من مجلة الضريبة على دخل الأشخاص الطبيعي والشركات.
- الفصل 6 من مجلة التحكيم.
- الفصل 172-199 مكرر و 199 ثالثا من المجلة الجنائية التي تطرقت إلى الجريمة المعلوماتية.
- الفصل 410 ثالثا من المجلة التجارية المنقح في 1996/04/03 والفصول 294 فقرة أخيرة و373 من نفس المجلّة إثر تنقيح 20 جوان 2000.

15 القانون عدد 83-2000 المؤرخ في 9 أوت 2000 ر.ر.ج.ت. عدد64 المؤرخ في 11 أوت 2000. ص. 1887 وما بعد.

16 محمّد الصالح بنحسين، المقال السابق، ص.36.
Voir dans le même sens : MORENO (D.), « Le droit de la preuve à l'heure d'Internet », les petites affiches, 27 septembre 2000, n°193, p.7 et 8.

حيث حجيتها. "الإثبات الإلكتروني قد يكون شذب هذه القولة ولطّف من جحود هذا النظام بإدخال مرونة متّزنة على فحواه"[17] فأبقى على النصوص السابقة ويسّر قبول أحكام الإثبات الإلكتروني من خلال إدراجها في إطار النظرية العامة للإثبات. وهو إختبار يبدو الغاية منه هو إرساء سياسة إثباتية تبقى على النظام القانوني في أسسه وثوابته، دون مراجعته أو تشتيت نصوصه. فعرّف الوثيقة الإلكترونية بالفصل 453 (مكرر) من م.إ.ع. كما يلي:

"الوثيقة الإلكترونية هي الوثيقة المتكوّنة من مجموعة أحرف وأرقام أو أيّ إشارات رقمية أخرى بما في ذلك تلك المتبادلة عبر وسائل الإتصال تكون ذات محتوى يمكّن فهمه ومحفوظة على حامل إلكتروني يؤمن قراءتها والرجوع إليها عند الحاجة. تعتبر الوثيقة الإلكترونية كتبا غير رسمي إذا كانت محفوظة في شكلها النهائي بطريقة موثوق بها ومدعمة بإمضاء إلكتروني" الوثيقة الإلكترونية تطرح إشكالات هامة تتصل بقدرتها على منافسة الكتائب التقليدية وحول شروط صحتها و مدى حجيتها[18].

فكيف تكتسب الوثيقة الإلكترونية القوة الثبوتية، وإلى أي مدى يمكن الإحتجاج بها؟

لقد سن المشرع التونسي مجموعة من النصوص ليسّر بذلك قبول أحكام الإثبات الإلكتروني. فأحاط الوثيقة الإلكترونية بجملة من الضمانات الواجب توفرها لإكسائها بالقوة الثبوتية (**جزء أوّل**) وليجعل منها وسيلة إثبات تضاهي الوثيقة الورقية، غير أنها لا ترتقي أحيانا إلى مصافها (**جزء ثاني**).

<u>جزء أول</u> : ضمانات إكساء الوثيقة الإلكترونية بالقوة الثبوتيّة:

وسائل الإتصال الحديثة لا توفر ضمانات كافية كتلك التي يوفرها الورق، فهيا تعطي معلومات قدمت لها مما يجعل تلك المعلومات عرضة بطبيعتها للتغييرات والتبديلات[19]. لذلك إشترط المشرع التونسي ضمانات في الوثيقة الإلكترونية تمنحها

---

[17] سامي الجربي، المقال السابق، ص.3.

[18] BREBAN (Y.) et POTTIER (I.), « Sécurité, authentification et dématérialisation de la preuve dans les transactions électroniques (Premier Partie). La Problématique des échanges électroniques face à la preuve », Gaz. Pal., 1996 (1er semestre), Doctrine, p.276 et s.

[19] سامي الجربي، المقال السابق، ص. 11.

القدرة على الإقناع في الإثبات، ووضع قرينة تقوم على صدق محتوى الوثيقة الإلكترونية طالما كانت "محفوظة في شكلها النهائي بطريقة موثوق بها ومدعمة بإمضاء إلكتروني". فالمشرع التونسي ربط حينئذ بين التدوين الإلكتروني وصلته بمن أمضى عليه (أ) وضرورة حفظه (ب) للقول بالقوة الثبوتية للإلكترونية كوسيلة إثبات وإقناع للقاضي.

فرع 1 – الضمانات المتعلّقة بالإمضاء الا لكتروني

يعتبر الإمضاء الوسيلة التقليدية للتعبير عن الرضا فهو يحدد هويّة الممضي، كما يحدد علمه بمحتوى الوثيقة التي أمضى عليها[20]. فالإمضاء هو مبدئيا علامة شخصية[21] يضعها الشخص للتعبير عن رضاه والتدليل على موافقته بما احتوته الوثيقة الممضى عليها[22].وهذا التعريف ينطبق على التوقيع بخط اليد الذي يرتبط بالكتابة الورقية[23]، غير إنه لا يمثل سوى مرحلة من مراحل التطوّر في وسائل التصديق، ولا يقف حاجزا أمام بروز أشكال جديدة من الإمضاء[24]. ومع نمو التبادل غير المادي وتطوّره[25] ظهر الإمضاء الإلكتروني كبديل للإمضاء الخطي[26], فاقتضت أحكام الفقرة الثانية من الفصل 453 م.إ.ع (جديد) إثر تنقيحه في 13 جوان 2000 ما يلي.

"ويتمثل الإمضاء في وضع إسم أو علامة خاصة بخط يد العاقد نفسه مدمجة بالكتب المرسوم بها أو إذا كان إلكترونيا في استعمال منوال تعريف موثوق به يضمن صلة الإمضاء المذكور بالوثيقة الإلكترونية المرتبطة به"[27]. نستنتج أن المشرع التونسي كرّر بالفقرة الثانية للفصل 453 (جديد) نفس الشرط الوارد في نهاية الفصل 453 مكرر:

---

20 DAURIAC (I.), La signature, Thèse de Doctorat en droit, université PANTHEON-ASSAS (Paris II), 1997, p.365.

21 RAYNOUARD (A.), « Adaptation du droit de la preuve aux technologies de l'information et à la signature électronique ». DEFRENOIS, 30 mai 2000, n°10, p.606.

22 طارق الصيادي، التجارة الإكترونية (على ضوء القانون عدد 83 لسنة 2000 المؤرخ في 9 أوت 2000 م.ق.ت. عدد 8 لسنة 2000، ص. 123.

23 محمّد الصالح بنحسين، قواعد الإثبات والتقنيات المعلوماتية المستجدّة، م.ق.ت. عدد 8 لسنة 2000، ص. 38.

24 BEN SOUSSAN (A.), « Signature électronique et preuve : évolution ou révolution ? » in « Colloque de Deauville, organisé les 27 et 28 juin 2000 par l'association droit et commerce », Ed. R.J.C., 2001, p.44.

25 المنصف قرطاس، حجية الإمضاء الإلكتروني أمام القضاء، م.ق.ت عدد 2 لسنة 2000، ص.103.

26 BRULARD (Y.) et FERNANDEZ (P.), « Signature électronique : la réforme aura-t-elle accouché d'une « Souris » ? (Première Partie), les petites affiches, 25 octobres 2001, n°213, p.11.

27 أنظر مختلف التعريفات المتعلقة بالإمضاء الإلكتروني بمذكّرتنا السابق الإجماع إليها: ص.82 إلى 85.

فالكتب الإلكتروني لا يحصل على قوته الثبوتية ولا يكون موثوقا به إلا إذا تدعّم بإمضاء إلكتروني.

الصيغة التي تبناها المشرع التونسي، تماما مثل المشرع الفرنسي بالفصل 1316 فقرة 4 إثر تنقيح 13 مارس 2000[28] جاءت مرنة وقابلة لأن تستوعب كل تطور إعلامي أو إلكتروني دون حصره في صيغة جامدة أو حيز زمني ضيّق[29]. المشرع التونسي إشترط أن يكون الإمضاء موثوقا به حتى يقع ضمان حجيته وحجيّة الوثيقة الإلكترونية[30].

لكن ما هو المقصود بالإمضاء الموثوق به؟

الفصول 5،6، و 7 من قانون 9 أوت 2000 المتعلق بالمبادلات والتجارة الإلكترونية اشترط أن يكون الإمضاء الإلكتروني مندمجا في إطار منظومة موثوق بها تضبط مواصفاتها التقنية بنصوص ترتيبية.

لكن ما هو المقود بهذه المنظومة الموثوق بها؟

نظرا لأن التعامل الإلكتروني هو نشاط لا مادي تؤمنه شبكات مفتوحة، معرّض بطبيعته تلك إلى مخاطر القرصنة والتطفّل قصد الكشف عن أسرا ر المتعاملين وتحويل مقاصدهم[31]. لذلك تأتي منظومة الموثق بها في شكل تجهيزات وبرمجيات إعلامية وإجراءات عملية ومعادلات حسابية وكتابات رقمية لتؤمن سريّة المعلومات وسلامتها وضمان صحّتها وحمايتها من الإستعمالات غير المشروعة التي تفقد التعامل ضمان الأمن فيه[32].

ولم يقف تنوع التعامل الإعلامي عند هذا الحد بل تمادى في إقرار ضمانات أخرى للسرية الكاملة في التعامل من خلال نظام التشفير cryptographie[33] والتشفير نوعان[34] :

---

[28] L'article 1316-4 du code civil Français dispose que « la signature électronique doit consister en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle se rattache ».

[29] سامي الجربي، المقال السابق، ص.13.

[30] SEDALLIAN (V.), « Preuve et signature électronique », Juris-com. Net, 9 mai 2000, p.4.
- BEN SOUSSA (A.), « Signature électronique et preuve : évolution ou révolution ? », article précité, p.48.

[31] طارق الصيادي، المقال السابق، ص. 144.

[32] محمّد الصالح بنحسين، المقال السابق، ص.40.

[33] GOLIARD (F.), « Télécommunication et réglementation française du cryptage, Dalloz 1998, 11ème cahier, chrono, p.120.

[34] علي كحلون، التجارة الإلكترونية، م.ق.ت عدد لسنة 2000، ص. 47.

- التشفير الذي يعتمد على مفتاح واحد لتشفير المعلومة وتفكيكها cryptographie symétrique.
- التشفير الذي يعتمد على مفتاحين، واحد للتشفير وآخر للتفكيك cryptographie asmétrique.

فالتشفير هو وسيلة تقنيّة تمكّن من تحويل النص الإلكتروني إلى رموز مبهمة يعسر معرفة فحواها إلا من قبل المرسل اليه اعتمادا على طريقة فنية لتفكيك رموزها قصد إدرا ك مضمونها[35]. وهذه الظاهرة القديمة والتي كانت تقتصر على مجالا الإتصالات العسكريّة[36] لما توفر من متطلبات الأمن والسرية تم إعتمادها في ميدان التجارة الإلكترونية[37] واستلهمها المشرع التونسي في نطاق قانون 9 أوت 2000 الذي عرّفها في فصله الثاني كما يلي:

"1) استعمال رموز، أو إشارات، غير متداولة تصبح بمقتضاها المعلومات المرغوب بتمريرها غير قابلة للفهم من قبل الغير.2) أو إستعمال إشارات، رموز لا يمكن الوصول إلى المعلومة بدونها. ولتوفير الضمانات الكافية يمضي نفس الفصل ليقيم ضمانا آخر يتمثل في تصديق Authentification الإمضاء بواسطة الغير الذي يتولى ذلك الأمر Tiers certificateur [38]. وقد أوكل المشرع التونسي في نطاق قانون 9 أوت 2000 مهمة التصديق على الإمضاء الإلكتروني لهياكل مختصّة[39]، وحدد نفس القانون دور هذه الهياكل وعلاقتها بالمتعاملين على شبكة الأنترنات[40]. ومن الضمانات الأخرى ربط المشرع التونسي حجيّة الوثيقة الإلكترونية بمسألة الحفظ أو التوثيق الإلكتروني.

---

35 BEN SOUSSAN (A.), cryptologie et signature électronique, aspects juridiques, Ed. Hermes, Paris 1999, p.78.

36 محمّد الصالح بنحسين، المقال السابق، ص. 41.

37 OUDOT (J.M.), « La signature numérique », les petites affiches, 6 mai 1998, n°54, p.33.

38 CAPRIOLI (F.), « Sécurité et confiance dans le commerce électronique. Signature électronique et autorité de certification J.C.P. Ed. G. n°14, 1er avril 1998, p.586.

39 JACCARD (M.), « La distribution d'information en ligne et le commerce électronique. Le rôle, le statut et la responsabilité de l'autorité de certification dans la transmission de données signées numériquement » in « les contrats de distributions », contributions offertes au professeur François DESSEMENTET », Ed. CEDIDAC, 1998, p.410.

40 الفصول من 8 إلى10 من قانون 9 أوت 2000 يتعلق بالوكالة الوطنية للمصادقة الإلكترونية. والفصول من 11 إلى 24 تتعلق بخدمات المصادقة الإلكترونية.

فرع 2 : الضمانات المتعلّقة بالتوثيق الإلكتروني

لقد ربط المشرع التونسي بين حجيّة الوثيقة الإلكترونية ومسألة حفظها[41]، وحد د وظائف السند الإلكتروني أو الحامل الإلكتروني صلب الفصل 4 من قانون 9 أوت 2000 الذي نص على ما يلي:

" يعتمد قانونا حفظ الوثيقة الإلكترونية كما يعتمد حفظ الوثيقة الكتابية. ويلتزم المرسل إليه بحفظ هذه الوثيقة في الشكل الذي تسلمها به. ويتم حفظ الوثيقة الإلكترونية على حامل إلكتروني يمكّن من:

- الإطلاع على محتواها طيلة مدة صلاحيتها.
- حفظها في شكلها النهائي بصفة تضمن سلامة محتواها
- حفظ المعلومات الخاصّة لمصدرها ووجهتها وكذلك تاريخ ومكان إرسالها واستلامها".

المشرع التونسي استخدم عبارة حفظ الوثيقة conservation . وكان من الأجدر استخدام عبارة توثيق Archivage[42]، للاختلاف بين العبارتين، فالأولى تنصّب على الحقوق أمّا الثانية فيه تتعلّق بالسندات[43]. فنقول توثيق السند أو الحجّة وليس حفظه. والمقصود بالتوثيق هو حفظ معلومات لامادّية داخل برمجيّات معلوماتية يمكن الرجوع إليها وقت الحاجة[44]، ضمانا لسلامتها وديمومتها. فالإختلاف لا يتعلّق بالكتابة وإنما بفقدان السند الورقي وتعويضه بسند لامادي فرضته التقنيات المعلوماتية[45] لابد من توثيقه باعتماد وسائل فنّية تضمن الأمان والسرية والشرعية والمصداقية. وتتمثل هذه الوسائل الفنية أساسا في الأوعية ووسائل التوثيق الحديثة مثل الميكروفيلم، والميكروفيش، وكل وسيلة خزن إلكتروني، أو ضوئي أخرى، شرط أن توفر هذه الوسائل الفنية الضمانات لمطابقتها

---

[41] الأستاذ سامي الجربي، المقال السابق، ص. 14.

[42] CAPRIOLI (E.), « Variations sur le Thème du droit de l'archivage dans le commerce électronique (premier partie) », Les petites affiches, 18 août 1999, n°164, p.4.
Voir aussi : CAPRIOLI (E.), « Variations, sur le Thème du droit de l'archivage dans le commerce électronique (suite et fin) », les petites affiches, 19 août 1999, n°165, p.7 et s.

[43] BEN ABBES (B.), la formation du contra de vente sur internet, Mémoire de DEA faculté de droit de sfax 2001-2002 , p.107.

[44] BEN SOUSSAN (A.), cryptologie et signature électronique, aspects juridiques, op. cit., p.53.

[45] محمّد الصالح بنحسين، المقال السابق، ص.44.

لأصلها"[46]. وبهذه الطريقة حافظ المشرع التونسي على الحل الذي تبنّاه بالنسبة للنسخ وحجيتها، فتبنّى صيغة عامة لفسح المجال أمام الإجتهاد القضائي بحسب تطور الوسائل التقنيّة[47]. فالنصوص القديمة بمجلة الإلتزامات والعقود لم تكن تقر بالقوة الثبوتية للنسخ المأخوذة من الأصل إلا إذا شهد المأمورون العموميون بصحتها وبمطابقتها لأصولها. فالنص القديم كان مرتبطا بالسند الورقي، فإذا ما قدمت النسخة كان ضروريّا أن يتم تقريبها مع أصلها[48]. وهو حل لا يتماشى والتقنيات المعلوماتية الحديثة التي لا وجود لحجج أصلية لديها[49] إذا الأصل يتمثل في جملة المعلومات المخزّنة بذاكرة الحاسوب أو الحامل الألكتروني، وما المطبوعة المستخرجة منه إلاّ نسخة من تسجيل ، إذ يتم إنجازها وفق وسائل فنيّة توفّر كل الضمانات لمطابقتها لأصولها. وفي صورة عدم توفر هذه الشروط يتم عرضها على الإختبار لبيان صحّتها تطبيقا لأحكام الفصل 471 م.إ.ع (جديد)[50] وقد إعتبر فقه القضاء الفرنسي وأن للنسخ قوة ثبوتية تظاهي الأصول بشرط أن لا ينكر الأطراف مضمونها وذلك في قرار: Société Descamps/ la banque scalbert Dupont.المؤرخ في 2 ديسمبر 1997[51]. وهو نفس الحل الذي تبنته محكمة التعقيب الفرنسية في قرارها المؤرخ في 28 مارس 2000[52] S.A. LAZARD C/Mme Thurin-FUENTES. معتبرة وأن النسخة الإلكترونية المستخرجة من الحاسوب بعد حفظها وتوثيقها بطريقة موثوق بها يمكن الإحتجاج بها لتعذّر إحضار الأصل.

هذه هي الضمانات التي إشترطها المشرع التونسي لإكساء الوثيقة الإلكترونية بالقوة الثبوتية، وهي حفظها ضمانا لمصداقيتها وارتباطها الوثيق بالإمضاء وهوية الممضي. وكلما توفّرت هذه الضمانات إكتسبت الوثيقة الإلكترونية قيمة قانونية وأصبحت وسيلة إثبات مشكلة في عالم فرضي للإستدلال بها في العالم المادّي.

---

46 Les informations pouvaient « sur les disques durs respectifs des cocontractants ou sur d'autres instruments fiables comme les disquettes ZIP, les CD, etc… d'une façon sécurisé et pour une durée suffisante ». Ben Abbès (B.), mémoire précité, p.107.

47 محمّد صالح بن حسين، المقال السابق، ص. 47.

48 الأستاذ سامي الجربي، المرجع السابق، ص.15.

49 Hance (O.) et DIONNE-BALZ (S.), Business et droit d'Internet, Ed. BEST, 1996, p.224.

50 Ben Abbès (B.), Mémoire précité, p.104 et 105.

51 GRYNBAUM (L., Note sous cass. com. 2 décembre 1997, S.A Descamps C/S.A Banque scalbert Dupont, arrêt n°2431, J.C.P, Ed. G., n°25, 17 juin 1998, p.1107.

52 LEVENEUR (L.), note sous cass. civ., 1ère civ. 28 mars 2000, S.A. LAZARD c/Mme THURIN-FUENTES (Arrêt n°654 P), J.C.P. Ed. G., n°35, 30 août 2000, p.1555 et 1556.

جـــزء ثـــان : آثـــار إكســـاء الوثيقة الإلكترونيـــة بالقوة الثبوتية

أمام قصور الأحكام التقليدية للإثبات على تأطير الإثبات في المادة الإلكترونية، قبلت عديد التشريعات[53] الكتب الإلكتروني كوسيلة إثبات كلما توفرت فيه الضمانات التي يتحتّم على السند الإلكتروني توفيرها، من استبقاء لكل المؤشرات التي تثبت العمل القانوني. وقد اختارت أغلبها تطويع الأحكام المتعلقة بالإثبات وإقحام ظاهرة الإثبات الألكتروني في القانون، إلا أنها إختلفت حول القيمة الإثباتية للوثيقة الإلكترونية (أ) ومدى تحقق تعادل أو تنازل بينها وبين الوثيقة الخطية أو الورقيّة (ب).

فرع 1 – القيمة الإثباتية للوثيقة الإلكترونية :

على مستوى الفقه، وصف بعض الفقهاء[54] الوثيقة الإلكترونية كبداية حجة على معنى الفصل 477 م.إ.ع وهو وصف غير مستساغ لسببين على الأقل.

- السبب الأول : هو أن بداية الحجة بداية للإثبات، ولابد أن تتواصل مع سند إضافي يكمل الحجة بالوسائل غير المنقوصة فيصبح الجمع وسيلة إثبات كاملة[55].
- السبب الثاني: إعتبار الكتب الإلكتروني بداية حجة بالكتابة سوف يوهنه ويتعارض مع رغبة المشرع في الإرتقاء به إلى مصاف الحجج الكاملة[56].

لذلك فكّر جانب آخر من الفقه[57] في الإستثناءات الواردة بقانون الإثبات، وهي نوافذ تفتح على أسوار النظام القانوني المهيئ للكتب لكسر عزلته وذلك تطبيقا لأحكام الفصل 1348م مدنية فرنسية والفصل 478 م.إ.ع التي تأخذ بالوسائل الناقصة في الإثبات كلّما كان هناك تعذّر مادي أو معنوي في الحصول على كتب[58]. فالتعامل مع شبكة الإعلامية قد يؤدي إلى استحالة الحصول على كتب بسبب تعطّب البرمجيّة أو إنفساخ النص أو أيّ

---

53 HASSLER (T.), « La signature électronique ou la nouvelle frontière probatoire », R.J.C. 2000, p.194

54 HANCE (O.) et DIONNE –BALZ(s.), business et droit d'internet , EDITION BEST, 1996, p.221.

55 CATALA (P.), « le formalisme et les nouvelles technologies » Répertoire Defrénois, 2000, p.900..

56 الأستاذ سامي الجربي، المقال السابق، ص.5.

57 GAUTIER (P.), « De l'écrit électronique et des signatures qui s'y rattachent », J.C.P. Ed. G., n°24, p.1120.

58 الأستاذ سامي الجربي، المقال السابق، ص.5.

حادث عرضي آخر[59]. إلا أن هذا الرأي تم انتقاده لعدم إعتباره الوثيقة الإلكترونية كتبا بأتم معنى الكلمة[60]. المشرع التونسي ورغبة منه في تطبيع النظام القانوني مع المستحدثات والآليات التقنية في الإثبات إعتبر في إطار الفقرة الثانية من الفصل 453 مكرر إثر تنقيحه في 13 جوان 2000 وأن الوثيقة الإلكترونية "كتب غير رسمي" . فالوثيقة الإلكترونية إذا وبصريح الفصل 453 "كتب"[61] ,والنتيجة هو أن الوثيقة الإلكترونية باعتبارها كتبا فإنها لا تقبل أصلا إثبات خلاف ما جاء فيه باعتماد وسائل إثبات ناقصة، إذ لا يمكن إثبات عكس الكتابة إلا بالكتابة تطبيقا لأحكام الفصل 474 م.إ.ع.

المشرع الفرنسي لم يعط تكييفا معينا للوثيقة الإلكترونية واكتفى بالقول صلب الفصل 1316-1 أن الكتب الذي يكتسي صيغة إلكترونية يمكن قبوله في الإثبات مثل الكتب المرتكز على الورق... وأضاف الفصل 1316-3 أن الكتب ذا مرتكزالكتروني له نفس قوة الاثبات للكتب المرتكز على الورق. مما يجعل المجال مفتوحا في القانون الفرنسي لتكييف الوثيقة الإلكترونية كحجّة رسمية كلما توفرت شروط محددة[62]. أو كحجة غير رسمية إذا ما توفّرت شروطها[63] .

ويثير تعريف الحجة الرسمية الإلكترونية عدّة صعوبات:

تقليديا يقتضي قيام الحجة الرسمية تلقي التصريح من المأمور العمومي وذلك ليكون شاهدا على رضاء المتعاقد بمحتوى العقد، وهذا يفترض حضورا شخصيّا لدى المأمور العمومي. وقد تم تجاوز هذه الصعوبات على مستوى القانون الأمريكي الذي للغير المصادق Tiers certificateur دور الشاهد في الكتب الإلكتروني، ويصبح هذا الغير

---

59 « Les fichiers informatiques vulnérables aux atteintes physiques (détériorations de supports, effacements incidents) ainsi qu'aux atteintes logicielles (effacements volontaires) ou non, sabotage virus, piratage ». Voir Gautier (P.), article précité, p.1120.

60 CATLA (P.), article précité, p.900.

61 الفصل 453 مكرر م.إ.ع عرّف الكتب باعتباره "مجموعة أحرف وأرقام أو إشارات رقمية أخرى بما في ذلك تلك المتبادل عبر وسائل الإتصال تكون ذا محتوى يمكن فهمه ومحفوظة على حامل إلكتروني يؤمن قراءتها والرجوع إليها عند الحاجة".

62 GRYNBAUM (L.), « Loi du 13 mars 2000 : La consécration de l'écrit et de la preuve électroniques au prix de la chute de l'acte authentique », Revue communication –commerce électronique, Ed. Juris-classeur, Avril 2000, p.12.
Voir aussi CAPRIOLI (E.), « Ecrit et preuves électroniques dans la loi n°2000-230 du 13 mars 2000», J.C.P., Ed. E., n°2, 2000, p.6.

63 RAYNOUARD (A.), « Adaptation du droit de la preuve aux technologies de l'information et à la signature électronique », Défrénois, n°10, 30 mai 2000, p.6.

بمثابة عدل الإشهاد Notaire[64]. والملاحظ أن القانون التونسي يعترف بالحجة العادلة الإلكترونية كلما صدرت من الخارج، دون أن يخصص لها تنصيصا خاصا، مما يدعم الرأي القائل باستبعاد هذه الحجّة من مجلّة الإلتزامات والعقود[65]، إذ أن الكتب الإلكتروني لا يرقي تماما إلى مصاف الحجج الرسمية في القانون التونسي. أما بالنسبة للقانون الفرنسي فإن قبوله للحجة الرسمية الإلكترونية يعود أساسا إلى رؤية عملية للتوثيق الإلكتروني. فالإجتهاد القضائي قد أنشأ في فرنسا ومنذ قرار CREDICAS الصادرة في 8 نوفمبر 1989[66] ترادفا بين الكتب الإلكتروني والكتب الخطي, حيث إرتقت الإمضاءات الإلكترونية إلى إمضاءات عادية. ثم كان له تعريف للكتب يمكن أن يتشكل من كل سند موثوق به ويمكن نسبة محتواه إلى صاحبة بصفة متأكدة وغير معترض عليها، كالفاكس الذي يصلح لإثبات إحالة الدين[67]، أو النسخة المستخرجة من الحاسوب التي تصلح لإثبات الكفالة[68]. لكن هذا الترادف بين الكتب الإلكتروني، سواء كان حجة رسمية أم غير رسميّة، والكتب الخطى أو الورقي لا يمنع إمكانية التعارض بينهما في المحتوى، فيتنازع القادم الجديد مع القديم فكيف يتم فضّ هذا التنازع بين محتوى الكتبين؟

فرع 2 : تنازع الوثيقة الإلكترونية مع الوثيقة الورقيّة:

لم يتعرض المشرع التونسي إلى تنازع السندين[69] : السند الورقي والسند الإلكتروني. ولا يمكن أن يتنازع الكتب الرسمي مع الكتب الإلكتروني في القانون التونسي لسببين على الأقل:

السبب الأول : لأن الكتب الإلكتروني لا يرتقي في القانون التونسي إلى مصاف الكتائب الرسمية.

السبب الثاني: لأن الحجة الرسمية تغلب على الكتائب الخطية من حيث ضرورة رميها بالزور لإثبات عكس ما يحتويه[70] فلا يرفع حينئذ الكتب الإلكتروني إلى مقام الكتب الخطي

---

64 Ibid., n°29, p.611.

65 الأستاذ سامي الجربي، مقال سابق، ص.8.

66 GAVALDA (C.), note sous cass. civ. 1ère chambre, 8 novembre 1989 (Les arrêts CREDICAS), D. 1990, p.369 à 371.

67 GRYNBAUM (L.), Note précité, p.1107.

68 LEVENEUR (L.), Note précité, p.1555 et 1556.

69 RAYNOUARD (A.), article précité, n°19, p.604.

70 الأستاذ سامي الجربي، المقال السابق ص.7 مكرر.

الرسمي الذي لا يأتيه التفنيد إلا من كتب مثله. فإمكانية التنازع[71] تفترض الإحتجاج بكتائب متعارضة لها نفس الحجيّة. فالإشكال لا يطرح في القانون التونسي إلا في صورة تعارض كتب خطي غير رسمي مع كتب إلكتروني، إذ لا يمكن تصوّر تنازع بين كتب رسمي وكتب إلكتروني طالما وأن المشرع إعتبر هذا الأخير مجرد حجة غير رسمية. لكن هذا التنازع يمكن تصوره في القانون الفرنسي الذي يفسح المجال أمام إرتقاء الكتائب الإلكترونية إلى حجج رسمية[72]. فالفصل 1316-2 ساوى بين السندين الكتابي والدعامة الإلكترونية وأباح في حالة التعارض للقاضي سلطة الترجيح بينهما باعتماد جميع الوسائل ليقر بعلوية الكتب الذي يراه أقرب للحقيقة[73]. المشرع الفرنسي وضع حينئذ الكتب الخطى على قدم المساواة مع الكتب الإلكتروني[74] ليفتح في حالة الإختلاف والتعارض إعتماد الوسائل المنقوصة لتفسير الغموض أو التعارض الذي يعتري محتوى العقد. وهو موقف سبق أن تبنته محكمة التعقيب الفرنسية في عديد قراراتها[75] تطبيقا لأحكام الفصل 1341 من المجلة المدنية الفرنسية. ومكّن الفصل 2836 من مجلة الكيبيك من إثبات ضد ما يحتوي الكتب الإلكتروني بشتى وسائل الإثبات. وهو حل يجعل من الكتب في شكله الإلكتروني مجرد قرينة من القرائن الناقصة للإثبات[76]. أمّا بالنسبة للقانون التونسي فإن هذه الإمكانية لا تبدو متاحة إلا عند الغموض والتعارض تطبيقا لأحكام الفصل 474 م.إ.ع. إن المقصود بالتنازع بين الكتب الإلكتروني والكتب الورقي هو تنازع بين سندين، وليس بين وسيلتي إثبات[77]. ويتمتع قاضي الموضوع بسلطة تقديرية للترجيح بين أحد السندين أو الدعامتين. ويمكنه في هذا الصدد اللجوء إلى كل ما عسى أن ينجر عن ذلك من أعمال واختبارا ت, إذ يحق للقاضي أن يأذن بإجراء إختبار تطبيقي لأحكام الفصل 470 م.إ.ع كلما أنكر أحد أطراف الكتب إمضاءه، أو عندما ينكر الورثة إمضاء مورثهم. لكن هل

---

71 BEN ABBES (B.),mémoire précité, p.108.

72 Huet (J.), « Vers une consécration de la preuve et de la signature électronique », D. n°6/6971 du 10 février 2000 p.96 et R.J.L., n°4,2000 p.41.

73 SEDALLIAN (V.), article précité, p.2.

74 GRYNBAUM (L.), article précité, p.14

75 Cass. civ. 1er, 10 juin 1960, Bull. civ., I, n°316.
Cass. civ. 1er, 30 novembre 1964, Bull. civ., I, n°531.
Cass. civ. 1er, 10 février 1965, Bull. civ., I, n°128.

76 الأستاذ سامي الجربي، المقال السابق، ص.7.

77 CATALA (P.), « Le formalisme et les nouvelles technologies », article précité, p.904.

يمكن سحب هذه الإمكانية على الكتائب الخاصّة بمجرد الإقرار بالترادف بين الكتب الخطي والكتب الإلكتروني[78].

كما قد يتعارض تاريخ الكتب الإلكتروني مع تاريخ الكتب الخطي. فثبوت التاريخ في الحجج الرسمية يقع التمييز فيها بين أطراف الكتب والغير تطبيقا لمقتضيات الفصل 450 م.إ.ع و 1328 مجلة مدنية فرنسية. وقد حدد الفصل 450 الوقائع والأعمال التي تمكّن من ثبوت تاريخ الكتب تجاه الغير وإثبات علمه بها. وهي وقائع[79] لا تتماشى بطبيعتها مع خصائص الكتب اللامادي. ويبدو أن دور مزود خدمات المصادقة الإلكترونية هام من هذه الناحية وأن تقنية L'HORODATAGE كفيلة بتحقيق المعادلة بين الكتبين الإلكتروني والورقي من حيث ثبوت التاريخ. غير إن السلطات التي يتمتع بها القاضي[80] للترجيح بين إحدى الدعامتين الإلكترونية أو الورقية في حالة التنازع بينهما قد تحدّ منها الإتفاقات المتعلّقة بالإثبات التي يلجأ إليها أطراف العقد مسبّقا، والتي قد تقرّ بعلويّة وسيلة إثبات عن أخرى[81] ويجد هذا الحل أساسا له في القانون التونسي بالفصل 441 م.إ.ع[82] والفصل 1316-2 مجلة مدنية فرنسية إثر تنقيحه في 13 مارس 2000[83]. غير إن تطبيقه قد يطرح صعوبات عديدة بالنسبة لمعاملات تتم عبر شبكات مفتوحة كشبكة الأنترنات. وتزداد هذه الصعوبات تعقّدا وخطورة كلما أبرمت هذه الإتفاقات بين مستهلك consommateur وبائع محترف professionnel نظرا لطبيعة العلاقة التعاقدية الغير متكافئة بين الطرفين[84]. فحماية المستهلك في إطار التعامل الإلكتروني هي مسألة ذات أهمية بالغة وقد أسالت حبر عديد رجال القانون وتبنّتها منظمات الدفاع عن المستهلك عبر

---

78 CHARFEDDINE (M.K.), « L'écrit, une preuve à l'épreuve » in Mélange Jaques GHESTIN intitulé « Le contrat au début du XXIe siècle », L.G.D.J., 2001, p.231-232.

79 لا يكون تاريخ الكتب حجة على الغير إلا من التواريخ الآتية:
1- من يوم تسجيل الكتب بتونس أو بالبلاد الأجنبية
2- من يوم إيداع الكتب تحت يد المأمور العمومي
3- من يوم الوفاة أو من يوم العجز الثابت إذا كان الذي أمضى الحجة بصفة كونه عاقدا أو بصفة كونه شاهدا قد توفي أو عجز عن الكتابة عجزا بدنيا.

80 AMMAR (D.), « Preuve et ressemblance, contribution à l'étude de la preuve technologique », R.T.D. civ. 1993, p.499.

81 RYNOUARD (A.), article précité, n°20, p.605.

82 إقتضى الفصل 441 م.إ.ع ما يلي: "البيّنة بالكتابة تحصل من الحجج الرسمية وغير الرسمية... ويبقى للمجلس النظر فيما يستحق كل منها من الإعتبار بحسب الأحوال إلا إذا إقتضى القانون أو إشترط الفريقان بوجه صريح صورة مخصوصة".

83 L'article 1316-2 dispose « 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… ».

84 Conseil d'Etat, Internet et les réseaux numériques, étude adoptée par l'assemblée générale du Conseil d'Etat, 2 juillet 1998, Documentation française p.84. Disponible aussi sur http:///www.internet.gouv.Fr./.

العالم[85]. فمثل هذه المبادلات أو البيوعات فهي تتميّز بالعالمية universalité إذ يتم إبرامها عن بعد à distancé وعبر شبكات مفتوحةsur des réseaux ouverts وباللامادية immatérialité إذ لا تتجسد في شكل مادي ملموس ولا تترك أثرا كتابيا عند انعقادها. وبالافتراضية Virtualité إن تبرم وتنفّذ في عالم فرضي[86] ٪

حرر بصفاقس في 20فيفري 2003

---

85 O.C.D.E, les lignes directrices régissant la protection des consommateurs dans le contexte du Commerce Electronique, 2000.

86 LOUMI (A.), La protection des Consommateurs dans les transactions électroniques, Mémoire pour l'Obtention du Diplôme d'Etudes Approfondies en Droit des Affaires, Faculté de Droit de Sfax, année universitaire 2001-2002.