جـامعة مـولـود مـعمري تـيـزي وزو

كـلـية الـحقـوق و الـعلـوم السيـاسـية

مدرسة الدكتوراه للقـانون و العلوم السيـاسـية

# الـتوثيق في المعاملات الإلكترونية

# (د راسة مقا رنة)

مذكرة لنيــل شهـادة المـاجستيـر فـي القانـون

فـرع: القانـون الدولـي للأعمـال

من إعداد الطالــب:

دحـمـانـي سميــر

تحت إشـراف الأستــاذة:

د/ أولـد رابــح / إقلولـي صـافيـة

لـجنـة المنـاقشــة:

د/ جعفور محمد السعيد، أستاذ، جامعة مولود معمري، تيزي وزو.....رئيسا

د/ أولد رابح/إقلولي صافية، أستاذة، جامعة مولود معمري، تيزي وزو.....مشرفة و مقررة

د/ صبايحي ربيعة، أستاذة محاضرة (أ)، جامعة مولود معمري، تيزي وزو.....ممتحنة

تاريخ المناقشة: 2015/06/30.


أهدي عملي هذا إلى الوالدين الكريمين أطال اللّه في عمرهما وحفظهما من كلّ سوء ووفقني لأكون في مستوى تضحياتهما.

كلّ من شجعني في إنجاز هذه المذكرة وإلى كل طالب علم.

كلّ الأساتذة والمعلمين الذين أشرفوا على تعليمي عبر مختلف الأطوار التعليمية.

كما أهديه أيضا إلى جميع أفراد عائلتي وإلى أعزّ الناس والأصدقاء في حياتي.

**ســمير**


أتقدم بجزيل الشكر إلى الأستاذة المشرفة الدكتورة أولد رابح / إقلولي صافية، عرفانا وتقديرا على توجهاتها وملاحظاتها القيمة التي أنارت لي طريق البحث والتقصي.

كما لا أنسى أن أقدم شكري وامتناني لجميع أساتذتي المحترمين في كلية الحقوق والعلوم السياسية بجامعة مولود معمري بتيزي وزو.

**سمير**

# قائمة أهم المختصرات

**أولا- باللّغة العربية:**

ج ر: الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية.

ر. ر. ج. ت: الرائد الرسمي للجمهورية التونسية.

س.ض.ب.م: سلطة ضبط البريد والمواصلات السلكية واللاسلكية.

م.خ.ت.إ: مقدم أو مزود أو مؤدي خدمات التصديق أو المصادقة أو التوثيق الإلكتروني(ة).

هـ.ت.ص.ت.م: هيئة تنمية صناعة تكنولوجيا المعلومات.

هـ.ت.إ: هيئة تنظيم الإتصالات.

و.و.م.إ: الوكالة الوطنية للمصادقة الإلكترونية.

**ثانيا- باللّغة الفرنسية:**

ANSSI : **A**gence **N**ationale de la **S**écurité des **S**ystèmes d'**I**nformation.

ANCE : **A**gence **N**ationale de la **C**ertification **É**lectronique.

ARPT : **A**utorité de **R**égulation de la **P**oste et des **T**élécommunications.

AFNOR : **A**ssociation **F**rançaise de **N**ormalisation.

AC : **A**utorité de **C**ertification.

AE : **A**utorité d'**E**nregistrement.

AH: **A**utorité d'**H**orodatage.

Cass. Civ : **C**our de **C**assation (Chambre civile).

COFRAC: **C**omité **F**rançais d'**A**ccréditation.

CO: **C**ode des **O**bligations (Suisse).

CESTI: **C**entre d'**É**valuation de la **S**écurité des **T**echnologies d'**I**nformation.

CT : **C**ontremarque de **T**emps.

DPC : **D**éclaration de la **P**olitique de **C**ertification.

IGC : **I**nfrastructure de **G**estion de **C**lés.

ICP : **I**nfrastructure à **C**lés **P**ubliques.

J.O.R.F : **J**ournal **O**fficiel de la **R**épublique **F**rançaise.

J.O.C.E : **J**ournal **O**fficiel de la **C**ommunauté **E**uropéenne.

LCR : **L**iste des **C**ertificats **R**évoqués.

LFSCSE: **L**oi **F**édérale sur les **S**ervices de **C**ertification dans le domaine de la **S**ignature **É**lectronique.

MB: **M**oniteur **B**elge.

OSCSE : **O**rdonnance sur les **S**ervices de **C**ertification dans le domaine de la **S**ignature **É**lectronique (Suisse).

PC : **P**olitique de **C**ertification.

PSCE : **P**restataires de **S**ervice de **C**ertification **É**lectronique.

PSCO : **P**restataire de **S**ervices de **C**onfiance

SPS: **S**erveur de **P**aiement **S**écurisé.

SICE : **S**éminaire **I**nternational sur la **C**ertification **É**lectronique.

UIT: **U**nion **I**nternational des **T**elecommunications.

**ثالثا– باللغة الإنجليزية:**

BIT: **B**inary Dig**it**.

CPS: **C**ertificate **P**ractices **S**tatement.

DVD: **D**igital **V**ersatile **D**isc.

GPS: **G**lobal **P**ositioning **S**ystem.

HTTPS: **H**yper**t**ext **T**ransfer **P**rotocol **S**ecure.

ITIDA: **I**nformation **T**echnology **I**ndustry **D**evelopement **A**gency.

ISO: **I**nternational **O**rganization for **S**tandardization.

NCCUSL: **N**ational **C**onference of **C**ommissioners on **U**niform **S**tate **L**aws.

NSA: **N**ational **S**ecurity **A**gency.

PKI: **P**ublic **K**ey **I**nfrastructure.

TRA: **T**elecommunications **R**egulatory **A**uthority.

UETA: **U**niform **E**lectronic **T**ransactions **A**ct.

UNCITRAL: **U**nited **N**ations **C**ommission on **I**nternational **T**rade **L**aw

VPN: **V**irtual **P**rivate **N**etwork.

إنّ التطور المذهل في تكنولوجيات المعلومات والاتصالات أدّى بالعالم إلى الانصهار في عصر المعلومات أو ما يُعرف بالعصر الرقمي، الذي سيطرت فيه تكنولوجيا أو تقنية المعلومات(Information Technology) على جميع المعاملات الإلكترونية التي توسع نطاقها ليشمل قطاع الأعمال في شتى مجالاته الإقتصادية، بعدما أن انحصرت هذه المعاملات في مجال تقني مُحدّد تخدم أغراض شخصية متعلقة بالمستخدمون(User).

لقد تَوَلَّدَ عن ثورة الإتصالات وتكنولوجيا المعلومات مُصطلح جديد في معاملات التجارة العالمية ألا وهو الإقتصاد الرقمي، الذي يقوم على دعامتي التجارة الإلكترونية وتقنية المعلومات، التي سمحت للعديد من تقنيات ووسائل الإتصال الحديثة بفرض نفسها كحتمية أمام مُتطلبات ومُستجدات الوقت الراهن، كالعقود الإلكترونية، التسويق الإلكتروني، الحكومة الإلكترونية، التقاضي الإلكتروني، تقنية البريد الإلكتروني، النقود الرقمية، والتقنية العالية المعروفة بشبكة الإنترنيت التي بدورها جمعت بين تكنولوجيا الحاسوب بشتى أنواعها والأجهزة الإلكترونية المختلفة.

لذا تبقى شبكة الإنترنيت كأعظم تقنية إبتكرها الإنسان إلى حدِّ السَّاعة، لكونها تُمثل شريان حياة للكثير من رجال الأعمال الذين يستعينون بخدماتها المتعددة في مجال تبادل المعلومات والبيانات الإلكترونية، أثناء إبرامهم لمختلف الصفقات المرتبطة بنشاطاتهم الإقتصادية، فأصبح من المُمكن لهؤلاء تجنب مَشَقَّةَ السفر والانتقال من بلد إلى آخر قصد اللّقاء بشركائهم وعملائهم من أجل الترويج بمختلف المنتجات والخدمات، كما يُمكن للمُستهلك الحصول على كلّ ما يُريد من سلع وخدمات مع دفع ثمنها بوسائل إلكترونية في ظرفٍ وجيز دون التنقل إلى عين المكان، وما يقع على عاتقه سِوَى إقتناء جهاز الكمبيوتر أو الهاتف الذكي مع إشتراكه لدى أحد مُقدمي خدمة الإنترنيت[1].

---

1) - Pour accéder au réseau Internet, il faut impérativement réunir les trois conditions suivantes : → Un ordinateur géré par un système d'exploitation qui supporte le protocole de communication Internet (TCP/IP. TCP) « Transmission Control Protocol / Internet Protocol » se sont les deux protocoles de base…

إنّ جذور شبكة الإنترنيت مُنبثقة أصلا من شبكة الإتصالات المعروفة بالأربنات (ARPANET) التي اكتشفتها وكالة الأبحاث والمشاريع الأمريكية (ARPA, Advenced Research Project Agency) في عام 1960 بطلبٍ من وزارة الدفاع الأمريكية (Pentagon)، لأغراض عسكرية في زمن الحرب الباردة مع الإتحاد السوفياتي سابقاً (URSS)، عن طريق جمع شمل أكبر عدد ممكن من أجهزة الحاسوب من أجل إرسال تعليمات التصويب من مركز التَّحَكُمْ إلى قواعد الصواريخ لتفادي أيِّ هجوم نووي مُبَاغِتْ.

تم توسيع الشبكة(ARPANET) في السبعينيات إلى مختلف الجامعات والمعاهد والأكاديميات والشركات التجارية إلى أن تم تعويضها في التسعينيات بشبكة الإنترنيت(Internet)، بعدما أن توسع نطاقها بظهور الشبكة العنكبوتية العالمية(Web)[1] التي سمحت بخلق عالم الفضاء المصطنع(Cyber Espace) لتبادل المعطيات والمعلومات والبيانات بطريقة إلكترونية في جميع المجالات، وبالخصوص التجارة الإلكترونية أين عرفت فيها تقنيات إبرام العقد الإلكتروني انتشارا واسعا، الذي أصبح يُبرم بأشكال إلكترونية مُختلفة عن الأشكال المعروفة في العقد التقليدي، كما ظهرت تقنية التسويق الإلكتروني (Cyber

---

→ Une carte réseau ou un modem correctement installé, configuré et relié au réseau téléphonique ou d'un câble, «Une nouvelle technologie- appeler **WI-FI (Contraction de Wireless - Fidelity)** Signifiant en français (qualité sans fil). Permet également d'accéder à Internet. Toutes les données sont transmises par ondes radio d'un ordinateur à l'autre, sans modem ni ligne téléphonique. Ce type de connexion est très rapide, mais ne fonctionne que dans certaines zones.

→ Disposer d'un abonnement auprès d'un fournisseur d'accès (comme CERIST en Algérie).

Voir : **Djamel BENABDESSELAM.** Initiation à l'informatique, Edition Diffusion Communication OMEGA, Alger 1997, pp. 94, 95.

[1] – يُرمز إليها بمُصطلح(World Wide Web) أو بالإختصار(WWW)، تم إكتشافها من طرف المهندس البريطاني في الفيزياء والإعلام الآلي تيم برنر لي(TIM BERNERS-Lee) في 1989، التي تطورت بمساعدة المهندس البلجيكي في الإعلام الآلي روبرت كايو(ROBERT Cailliau) داخل المركز الأوروبي للأبحاث النووية(CERN) المتواجد على الحدود الفرنسية–السويسرية، وفي عام 1994 تم إنشاء تكتل تحت إسم (World Wide Web Consortium) أو ($W_3C$) الذي أحدث في عام 1998 معيار دولي معترف به(Extensible Markup Language) (XML)، في مجال إحداث التوقيعات الإلكترونية الموصوفة. لمزيد من المعلومات أنظر الموقع التالي: http://www.internet.gouve.fr/

(Marketing التي تعتمد على أساليب الإتصالات الإلكترونية الحديثة عبر الإنترنيت من أجل تحقيق الأهداف والغايات التسويقية بشكل أسرع من التسويق التقليدي، إذْ تسمح التقنية للمحترف الإقتصادي بترويج بضائعهم وخدماتهم بإستخدام مواقع الويب، الموزعة عبر شبكة الإنترنيت التي تسمح بعرضها عبر مختلف أسواق العالم في ظرف قصير وباستثمار أقل من رأس المال، ممّا يُتِيحُ للمستهلك إمكانية الإطلاع عليها في الوقت المناسب من أجل اتخاذ القرار الأخير في إبرام الصفقة التجارية إلكترونيا.

لذا يُمكن تشبيه التجارة الإلكترونية بسوق إلكتروني إفتراضي يتقابل فيه البائعون والموردون والوسطاء والمُستهلكون، بحيث تُقدم فيه السلع والخدمات في صورة رقمية أو إفتراضية ويتم دفع ثمنها بوسائل دفع إلكترونية حديثة (البطاقات الإلكترونية الذكية والنقود الرقمية أو الشيكات الإلكترونية الخ...) مُغايرة عن الطرق المعروفة تقليديا.

تُعتبر الثقة والأمان في مُقدمة الضمانات التي ينبغي توافرها في معاملات التجارة الإلكترونية وذلك بالنظر إلى المخاطر والعقبات والمشاكل القانونية المتولدة عن البيئة الإلكترونية الإفتراضية، التي تنصب حول إثبات الهوية وتحديد مدى صحة محتوى المحرر الإلكتروني ومن عدم تعرضه لأي تغيير أو تعديل أو تزوير فيه، الأمر الذي يستدعي الحاجة إلى البحث عن تقنية حديثة لتوثيق أو تصديق التصرفات الإلكترونية تعتمد على برامج(Logiciels)[1] وضعها المختصون، بهدف إحداث مُختلف الأساليب والتقنيات التي من شأنها أن تُساعد على توفير وتبادل ومعالجة واستعادة وتخزين مُختلف المعلومات والبيانات

1) - **Logiciel (en anglais Software)** : est un programme ou ensemble de programmes informatiques, assurant un traitement particulier de l'information, on peut distinguer deux grandes Familles de Logiciels : **Les Logiciels système et les Logiciels d'applications**.
**- Un Logiciel système :** contrôle le fonctionnement de l'ordinateur, jouant par conséquent le rôle de première interface entre l'homme et la machine. Il gère les travaux essentiels, mais souvent invisibles, relatifs à la maintenance des fichiers sur disque dur, à la gestion de l'écran, etc. Il constitue donc une partie d'un système d'exploitation. (Ordinateur de bureau, téléphone portable, récepteur GPS, lecteur DVD ou encore baladeur MP3, la liste des appareils contrôlés par des logiciels système est longue.)
**- Un Logiciel d'application :** concerne tous les autres logiciels. Ils permettent d'effectuer la multitude des tâches plus ou moins spécifiques pour lesquelles sont utilisés les ordinateurs : traitement de texte, gestion de base de données, comptabilité, programmation, utilisation de réseaux, jeux, etc. http://www.wikipédia.fr

المتعلقة بالتجارة الإلكترونية، إذْ يُعتبر البرنامج بالنسبة للحاسوب أو أيّة آلة تقنية آخرى بمثابة الرُّوح في جسد الإنسان، ومن ثمّة فإنّ عبقرية ذلك الجهاز لا تعود إلى الأجهزة المادية المكونة له(Matériel) وإنّما ترجع إلى عبقرية البرنامج الذي وُضع خصيصا لكي يجعل الحاسوب قادرا على تحقيق ما أُنيط به من أعمال ومُبتكرات، وبدونه تصبح الأجهزة المادية المُكَوِّنَة له مُجرد كُتل حديديّة وبلاستيكيّة بدون فائدة.

فبالرغم من التكلفة المالية الباهضة والجهد الإنساني الضخم من أجل إعداد برنامج واحد، سَاعَتْ مختلف دول العالم والمنظمات الدولية إلى الإستنجاد والإنتفاع بخدمات هذه البرامج، من خلال الإتفاق مع المُختصين في مجال البرمجيات(أفراد أو شركات مختصة) حول إعداد مُختلف النماذج المتعلقة بالعقود الإلكترونية، وتقنيات توثيق التصرفات الإلكترونية التي تعتمد على معدات وأنظمة أمن تكنولوجيا معلومات موثوق بها تضمن الحقوق القانونية لأطراف التعامل الإلكتروني، وتُقلّل من العوائق التقنية والقانونية التي من شأنها أن تُسهِّل أو تُمهّد الطريق لأصحاب الإختصاص[1] في اختراق الأنظمة المعلوماتية قصد التسلّل إلى البيانات الشخصية للأطراف، وانتحال صفتهم أو إستخدام البيانات بطريقة غير مشروعة من دون علمهم بذلك عن طريق تزوير توقيعاتهم الإلكترونية، بالإعتماد على

---

[1]– قد يُقصد بهم أشخاص ذي مُستوى عالٍ من العلم والمعرفة في تكنولوجيات الإتصال والمعلومات، كما قد يكون بعضم من صغار السّن أي من طلاب المدارس الثانوية وحتى الابتدائية، وهم:

أ– **القراصنة** (**Les Pirates**): هناك صنفان منهم: **الهواة** (**Hacker**)، هم الأشخاص الذين يسعون فقط للتسلية و لا يُشكلون خطورة على الإقتصاد وأنظمة المعلومات. أما **المحترفون** (**Crackers**): هم أشدّ خطورة من الصنف الأول لكونهم يُحدثون أضرار كبيرة، وذلك بقيامهم بأعمال التخريب والاقتحام الغير المشروعة وعادة ما يُشكلون نوادي لتبادل المعلومات بينهم.

ب– **المخادعون** (**Fraudeurs**): يتمثلون في الأخصائيين في المعلوماتية و من أصحاب الكفاءات الذين يتمتعون بقدرات فنية عالية، إذ تنصب مُعظم جرائمهم على شبكات تحويل الأموال و التلاعب بحسابات المصارف أو بطاقات الدفع الخ ...

ج– **الجواسيس** (**Espions**): يهدف هؤلاء إلى جمع المعلومات إمّا لِخِدْمَةِ مصالح دولهم أو لمصلحة بعض الأشخاص أو الشركات التي تتنافس فيما بينها. http://users.pandora.be/martin.melchior/

إحدى البرامج الخبيثة(Logiciels méchants ou malveillants)[1] التي تتخذ صُوَرْ عديدة حسب الأهداف المُسَطَّرَة لها، فقد يكون الغرض منها الخداع والاستيلاء على الأموال أو تدمير وإفساد بعض أو جُلّ البيانات والمعلومات المُرتبطة بمضمون التصرف الإلكتروني.

لذا إرتأت التشريعات الدولية والوطنية إلى إيجاد طرف ثالث مُستقل عن أطراف التعامل الإلكتروني، مُعتمد أو مرخص له من طرف الجهات الرسمية لمزاولة خدمات التصديق الإلكتروني المعتمدة وفقا للتشريع المعمول به، بحيث يُعول على خدماته من أجل تسهيل إجراءات إبرام مختلف الصفقات الإلكترونية والتَيَّقُن من إرادة كلٍّ طرف ومدى صحتها ونسبتها إلى من صُدرت منه، وبُعدها عن الغش والاحتيال، وكذلك التأكد من طبيعة التعاقد وسلامة البيانات الإلكترونية المتصلة بالمحرر الإلكتروني، من أيّ تعديل أو تغيير فيه مع ضمان تقنيات دفع واستلام المستحقات بطريقة إلكترونية آمنة عبر شبكة الإنترنيت من دون إنكارها في حالة النزاع.

---

[1] – من بين البرامج الخبيثة المعروفة نجد: – **برنامج حصان طروادة (Cheval de Troie):** (سُمي نسبة للحصان الخشبي الكبير الذي صنعه اليونانيون قصد غزو مدينة طروادة(**Troie**) إذ ضم بداخله مجموعة من الجنود قصد خداع جيش المدينة) هو برنامج مُخادع إذ يظهر كبرنامج عادي يؤدي بعض المهام المفيدة والمألوفة لمُستخدمه، لكن ظاهره يخفي غرض غير مشروع وهو تحقيق هدف حقيقي من وراء تشغيله، إذ يعتمد على الأوامر والتعليمات المتواجدة في داخله بطريقة خفية قصد محو البيانات من ذاكرة الحاسب الآلي، أو التهديد بذلك للابتزاز أو الإستيلاء على أموال مُستخدمه وذلك بتحريف البيانات المُدخلة أو المُخزنة، وعادة ما يتواجد هذا البرنامج في برامج الأعمال.

– **برامج الدودة (Les Vers)** التي تستغل فجوات نُظم التشغيل لتنتقل بكثرة كالبكتيريا من حاسب إلى آخر مُغطية شبكة بأكملها بهدف التخريب الفعلي للملفات والبرامج ونُظم التشغيل وبروتوكولات الإتصال.

– **القنابل المنطقية أو الموقوتة (Les Bombes logiques / à retardement):** هي برامج مُصممة بحيث تبقى ساكنة وغير فعالة أو مُكتشفة لمدة تصل من أشهر إلى سنوات بحسب البرنامج، ويبدأ هذا الآخير في مهامه الهدّامة بحلول المدة أو بتحقيق شروط منطقية قد حدّدها من قبل. لمزيد من المعلومات أنظر الموقع التالي: http://users.pandora.be/martin.melchior/

للتوثيق أو التصديق الإلكتروني أهمية إقتصادية وقانونية في ضبط تصرفات التجارة الإلكترونية، وإرساء مناخ ثقة أمن لمبادلاتها التي تعترضها مشاكل تتعلق بانتحال الهوية أو اختراق البيانات الإلكترونية، واستنكار عملية بيع أو تبادل أو دفع قيمة المستحقات عبر شبكة الإنترنيت، **فإلى أيّ مدى يُساهم التصديق الإلكتروني في توفير الثقة والأمان في المعاملات الإلكترونية؟ وما مدى حجيته في الإثبات؟**

للإيجابة على الإشكالية يقتضي الأمر التعرض إلى الإطار القانوني للتوثيق الإلكتروني الذي من خلاله[1]، نتعرض إلى إبراز مختلف المفاهيم القانونية له وفقا للتشريعات المقارنة مع تحديد أهمية التصديق الإلكتروني في بعث الثقة والأمان لدى أطراف التعامل الإلكتروني في إطار نماذج الثقة في التصديق الإلكتروني، وإبراز مدى جدارة الثقة في السياسة العامة المتبعة في تقديم خدمات التصديق الإلكتروني المتاحة من طرف جهات التصديق الإلكتروني الموثوق بها في مجال إحداث التوقيعات الإلكترونية الموصوفة، وإصدار أو إيقاف أو إلغاء شهادات التصديق الإلكتروني**(الفصل الأول)**، كما أنّ مقدم خدمة التصديق الإلكتروني الموثوق به تربطه علاقة قانونية وعقدية، بالأطراف المعولة على التوقيعات وشهادات التصديق الإلكتروني الموصوفة، بحيث يتحمل في إطارها كلّ طرف لمجموعة من الإلتزامات التي يترتب عنها تحمل المسؤولية عند الإخلال بها**(الفصل الثاني)**.

---

[1] – وفقا لقاموس المعاني يقصد بكلمة **التصديق: توثيق**، إقرار، إثبات، إبرام. أمّا كلمة التوثيق فتعني: إشهاد أو تزويد أو دعم بالوثائق. **تصديق** على حكم أو حساب أو تحويل أو توقيع أو عقد أو أمر. تسجيل، تمكين، تمتين. http://www.almaany.com/qdict.php?language=arabic

تُقابل كلمة التصديق أو التوثيق باللغة الفرنسية كلمة **Authentifier** ou **Certifier** التي تعني:

- **Certifier** : **1-** Affirmer, garantir, assurer quelque chose comme vrai ou valable. Certifier une nouvelle. Certifier un Chèque. **2-** Droit : **Authentifier**, légaliser, affirmer quelque chose ou la conformité d'une copie au document original, par l'autorité compétente (écrit officiel). Certifier un Procès- verbal. **3- (Certification)** : procédure d'authentification d'un acte.
- **Authentifier** : **1-** C**ertifier** la vérité, l'exactitude de quelque chose. **2-** Reconnaitre officiellement la conformité de quelque chose. Authentifier une signature.

**3-**(**Authentification**) : Processus par lequel un système informatique s'assure de l'identité de l'utilisateur. http://www.larousse.fr/dictionnaires/francais/ ou http://www.larousse.fr/dictionnaires/francais-arabe/

# الـفصل الأول

# الإطـار القـانونـي للتوثيـق الإلكتـرونـــي

# الفصل الأول

# الإطـار القـانوني للتوثيق الإلكتروني

بتطور وسائل الإتصالات وتقنية المعلومات أصبحت المعاملات الإلكترونية في المجال الإقتصادي تتم عن بُعد في بيئة إلكترونية إفتراضية بوساطة طرف ثالث مُسْتَقِلْ ومؤتمن به، الشيء الذي عَقَّدَ من إجراءات التوثيق التقليدية لمختلف التصرفات القانونية التي أصبحت لا تتأقلم مع طبيعة معاملات التجارة الإلكترونية التي تتسم بالسرعة في الأداء مع كسب الجهد والوقت في التنفيذ، كما أنّ الحاجة إلى تنظيم مبادلات التجارة الإلكترونية دفعت بمُختلف الدول والمنظمات الدولية والجهوية إلى إصدار تشريعات وتنظيمات قانونية خاصة بالمعاملات الإلكترونية، بهدف وضع مخططات تقديم خدمات تصديق إلكتروني وفقا لمُستويات أمنية معينة تسمح للدول المعنية بإتباع نموذج تصديق موثوق به في إطار مرافق المفاتيح العمومية، ولبيان ماهية التوثيق الإلكتروني نتطرق لمختلف التعريفات المقدمة في التشريعات الوطنية والتوجيهات الدولية(المبحث الأول)، وإلى إجراءات التوثيق الإلكتروني(المبحث الثاني).

## المبحث الأول

## مـاهية الـتوثيق الإلكتروني

بما أنّ عقود التجارة الإلكترونية يتم إبرامها عن بُعْدْ بوساطة إلكترونية دون تنقل لأطراف العلاقة العقدية إلى مكان الإبرام، فإنّ الحاجة إلى إثبات هوية وأهلية كلِّ طرف يستوجب البحث عن وسيلة قانونية تضمن حفظ حقوقهم، وسلامة وأمن التصرف الإلكتروني وبالتالي فإنّ التوقيع الإلكتروني لا يضمن لوحده تحديد هوية الأطراف المتعاقدة ولا سلامة مضمون العقد الإلكتروني، نظرا للمشاكل القانونية والتقنية التي قد يتعرض لها من جرّاء ظهور تقنيات حديثة متطورة في تزوير وتقليد التوقيعات الإلكترونية، ممّا يستدعى الأمر إلى ضرورة البحث عن طرف ثالث مُحايد ومُعتمد من طرف الدولة من أجل ضمان إجراءات توثيق المعاملات الإلكترونية بتقنيات مُؤمنة وموثوق بها، وإنطلاقا من ذلك نتطرق أولا إلى مفهوم التوثيق الإلكتروني في(المطلب الأول)، ثم إلى أهميته في(المطلب الثاني).

## المطلب الأول

## مفهوم التوثيق الإلكتروني

إنّ المخاطر والمشاكل القانونية والتقنية التي تعترض العقود الإلكترونية المُبرمة عبر شبكة الإنترنيت تؤدي إلى صعوبة التنبؤ في مصير العلاقة العقدية للأطراف، وذلك لغياب الوسائل والآليات التي من شأنها أن تضمن الثقة والأمان في تصرفاتهم الإلكترونية، الشيء الذي دفع بمُختلف دول العالم والمنظمات الدولية والجهوية، إلى تنظيم موضوع توثيق المعاملات الإلكترونية الذي يعتبر من بين مسائل الساعة المثيرة للإهتمام، ولتوضيح الطبيعة القانونية للتوثيق أو التصديق الإلكتروني يستوجب لنا التطرق أولاً إلى مفهوم التوثيق الإلكتروني عبر مختلف التشريعات والتوجيهات الدولية(الفرع الأول)، وفي التشريعات الوطنية الأجنبية(الفرع الثاني)، والتشريعات الوطنية العربية(الفرع الثالث)، وتعريف الفقه والقضاء له(الفرع الرابع).

### الفرع الأول

### مفهوم التوثيق الإلكتروني وفقا للتشريعات الدولية

أثار التوثيق أو التصديق الإلكتروني اهتمام مختلف التشريعات الدولية التي قامت بتنظيم كلّ المسائل المتعلقة بنشاطات التصديق الإلكتروني، التي تطرقت من خلالها إلى تعريف إجراءات التوثيق الإلكتروني المُعتمدة، التي يُشرف عليها مقدم خدمات تصديق إلكتروني محايد ومعتمد من طرف الجهات الرسمية لمزاولة نشاطاته، لِذا سنتعرض إلى تعريف التوثيق الإلكتروني من خلال لجنة القانون التجاري الدولي(الأونسيترال) التابعة لمنظمة الأمم المتحدة، والإتحاد الأوروبي كمنظمة إقليمية.

#### أولاً: قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية لعام 1996.

إنّ قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية إعتمدته لجنة القانون التجاري الدولي في دورتها التاسعة والعشرين، (أنشأتها الجمعية العامة للأمم المتحدة في دورتها

الواحدة والعشرون، بموجب قراراها رقم 2215(د-21) المؤرخ في 17 ديسمبر 1966 قصد تنسيق وتوحيد القانون التجاري الدولي)، كقانون دولي نموذجي[1] للدول الراغبة في إحداث أو تعزيز تشريعاتها المُنظمة لبدائل الأشكال الورقية للإتصال وتخزين المعلومات.

فبعد إطلاعنا على مواد هذا القانون لم نجد أيٌّ تعريف للتوقيع الإلكتروني بالرغم من إعترافه بحجية رسائل البيانات في الإثبات ومُساواته بين التوقيع الإلكتروني والتوقيع التقليدي من حيث القيمة القانونية، إلاّ أنّه نص بموجب المادة 1/07(أ)-(ب) منه على الشروط العامة الواجب توافرها حتّى تُعتبر رسائل البيانات مُوثقة بالشكل الذي يجعلها تتسم بالمِصداقية، لذا يجب أن تكون الطريقة المُستخدمة في تحديد هوية مُنشئ رسالة البيانات وتأكيد مُوافقته على مضمونها موثوقا فيها بالقدر المناسب الذي أُنشئت أو أُبلغت من أجله رسالة البيانات، ولتقدير درجة الثقة في التعويل على الطريقة الموثوق بها يُؤخذ بعين الإعتبار مُستوى التطور التِّقني للمعدّات التي يستخدمها الأطراف وطبيعة ونوع وحجم النشاط

---

[1] – إنّ المعاهدة الدولية والقانون النموذجي الدولي يختلفان من حيث القيمة القانونية، فالأولى عبارة عن إتفاق مبرم بين أشخاص القانون الدولي (الدول) وفقا للمادة 1/2 من اتفاقية فيّنا حول المعاهدات، المبرمة في 23 ماي 1969 والتي دخلت حيز التنفيذ عام 1980، فبمجرد إبداء أحد الدول رغبتها في مضمون المعاهدة سواءا بالتوقيع أو التصديق أو الانضمام سواءا بتحفظ أو بدونه، يجعلها تتحمل المسؤولية الدولية في حالة الإخلال بالتزاماتها كما أنّ أحكام المعاهدة يتم صياغتها ضمن تشريعاتها الداخلية (الدولة)، بينما القانون النموذجي الدولي ما هو إلاّ نموذج تشريعي مُقترح من طرف منظمة دولية أو إقليمية للدول من أجل مساعدتها على تحديث أو تعديل تشريعاتها وفقا لنصوص التشريع المقترح، وهذا ما يؤدي بالدول إلى قبول النموذج أم رفضه. (إنّ الاتفاقية الدولية يُمكن أن تُصاغ في شكل نموذجي مثل الاتفاقية النموذجية الدولية حول الدخل والثروة لمنظمة التعاون والتنمية الإقتصادية) (OCDE).

– قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية لعام 1999، مع دليل التشريع.
http://www.unicitral.org/pdf/Arabic/texts/selectcom/mt-elecsig/

– **ثروت عبد الحميد**، مدى حجية التوقيع الإلكتروني في الإثبات على ضوء القواعد التقليدية للإثبات، بحث مقدم في مؤتمر الأعمال المصرفية بين الشريعة والقانون، الذي نظمته جامعة الإمارات العربية المتحدة، بالتعاون مع غرفة التجارة الإلكترونية وصناعة دبي، في الفترة مابين 10 و12 ماي 2003. المجلد الأول، ص ص 417 – 423. http://www.unue.banque.com/imarat/arab/

التجاري، وظيفة الشروط الخاصة بالتوقيع، والامتثال لإجراءات التوثيق التي يضعها (م.خ.ت.إ) كوسيط محايد ومُؤتمن في توثيق رسائل البيانات، ونطاق التنوع الذي يُتيحه أي وسيط من إجراءات التوثيق والامتثال للأعراف والممارسات التجارية الخ...

لكي تتمتع رسالة البيانات بالحجية القانونية في الإثبات وفقا للمادتين 09 و10 من نفس القانون، يجب أن يولى الإعتبار لجدارة الطريقة التي أُستخدمت في إنشاء أو تخزين أو إبلاغ رسالة البيانات للتعويل عليها، وجدارة الطريقة المُستخدمة في تحديد هوية منشئ الرسالة أو أيّ عامل آخر متصل بالأمر، وكيفية المحافظة على سلامة المعلومات من أجل التعويل عليها، وفي كل الظروف لا يجب إنكار رسالة البيانات في الإثبات لشكلها الإلكتروني أو لعدم ورودها في شكلها الأصلي، كما حددت المادة 3/08(أ) من نفس القانون معيار تقدير سلامة المعلومات في حالة إضافة التصديق الإلكتروني إلى نهاية رسالة بيانات أصلية، فيَدُّلُ ذلك بالشهادة على مُطابقتها للأصل وعدم تعرضها لأي تغيير.

**ثانيًا: التوجيه الأوروبي بشأن التوقيعات الإلكترونية لعام 1999.**

إنّ حاجة دول الإتحاد الأوروبي إلى إطار قانوني خاص بالمعاملات الإلكترونية ينسق فيما بين تشريعاتها الداخلية، دفع ببرلمان الإتحاد إلى إقرار توجيه أوروبي رقم 93/99 في 13 ديسمبر 1999 بشأن التوقيعات الإلكترونية، بهدف تنظيم خدمات التصديق الإلكتروني المتعلقة بإحداث التوقيعات الإلكترونية الموصوفة مع الإعتراف القانوني لها، بحيث ميّز من خلال أحكامه(التوجيه) بين التوقيعات الإلكترونية على أساس مُستويات الأمان المُتطلبة فيها، فالأول يتعلق بالتوقيع الإلكتروني البسيط(Signature électronique simple) الذي عرفته المادة الثانية من التوجيه على أنّه:" **بيانات في شكل إلكتروني ترتبط أو تتصل منطقيا ببيانات إلكترونية آخرى، وتُستخدم كوسيلة توثيق.**"

أمّا الثاني يتعلق بالتوقيع الإلكتروني المُوصوف(Signature électronique qualifiée) المتمثل في التوقيع الإلكتروني المتقدم، الذي تمّ إحداثه على أساس شهادة تصديق إلكتروني موصوفة بموجب منظومة أمن إنشاء التوقيعات الإلكترونية، الموضوعة تحت سيطرة الموقع لوحده، بوساطة(م.خ.ت.إ) محايد ومؤهل في إطار نظام الإعتماد الاختياري، والذي يُقصد

به(م.خ.ت.إ) حسب المادة 11/02 من نفس التوجيه[1]:" **أي هيئة أو شخص طبيعي أو معنوي يقوم بإصدار الشهادات، ويتيح الخدمات الآخرى المتعلقة بالتوقيعات الإلكترونية.**"

فوفقا للمادة 02/5-6 من نفس التوجيه فإنّ منظومة أمن إحداث التوقيع الإلكتروني الموصوف، تحتوي على أيّ جهاز أو برنامج معلوماتي معد لتطبيق بيانات إحداث التوقيع الإلكتروني كالأرقام السرية، أو مفاتيح التشفير الخاصة المستعملة لإحداثه، والتي يجب أن تستجيب للمتطلبات المحددة في الملحق الثالث من التوجيه، كضمان إحداث بيانات التوقيع الإلكتروني في سريّة تامة لمرة واحدة فقط، مع عدم كشفها عن طريق عملية الإستنباط أو الإستنتاج(Déduction)، وأن لا تُغيّر من البيانات التي سيتم توقيعها أو تمنع إتاحتها للمُوقِّع قبل عملية التوقيع عليها، مع تمكين المُوقّع من حماية توقيعه بطريقة مؤمنة[2].

---

1) - Directive 1999/93/CE du parlement européen et du conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques. J.O.C.E, n° L 13, du 19 janvier 2000. http://www.ec.europa.eu ou http:// www.legifrance.gouve.fr/

- **Art.02/1-2** : «Signature électronique, une donnée sous forme électronique, qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification. »

- « Signature électronique avancée, une signature électronique qui satisfait aux exigences suivantes: **a)** être liée uniquement au signataire ;

**b)** permettre d'identifier le signataire ;

**c)** être créée par des moyens que le signataire puisse garder sous son contrôle exclusif ;

**d)** être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable. »

– **Art.02-11**: « toute entité ou personne physique ou morale qui délivre des certificats ou fournit d'autres services liés aux signatures électroniques. »

2) - **ANNEXE III** (Directive européenne n° 99/93 sur les signatures électroniques.)

« **1.** Les dispositifs sécurisés de création de signature doivent au moins garantir, par les moyens techniques et procédures appropriés, que :

**a)** les données utilisées pour la création de la signature ne puissent, pratiquement, se rencontrer qu'une seule fois et que leur confidentialité soit raisonnablement assurée;

**b)** l'on puisse avoir l'assurance suffisante que les données utilisées pour la création de la signature ne puissent être trouvées par déduction et que la signature soit protégée contre toute falsification par les moyens techniques actuellement disponibles;

**c)** les données utilisées pour la création de la signature puissent être protégées de manière fiable par le signataire légitime contre leur utilisation par d'autres.

**2.** Les dispositifs sécurisés de création de signature ne doivent pas modifier les données à signer ni empêcher que ces données soient soumises au signataire avant le processus de signature. »

أمّا منظومة فحص التوقيع الإلكتروني حسب المادة 02/7-8 من نفس التوجيه، تتمثل في أيّ جهاز أو برنامج معلوماتي معد لتطبيق بيانات فحص التوقيع الإلكتروني، كالأرقام السرية أو مفاتيح التشفير العمومية المُستعملة للتحقق من التوقيع الإلكتروني، والتي يجب أن تستجيب للمتطلبات المحددة في الملحق الرابع من نفس التوجيه، كضمان تحديد هوية المُوقِّع ومطابقة بيانات إحداث التوقيع الإلكتروني مع بيانات فحصه بوضوح، مع كشف أيّ تغيير أو تعديل فيها بطريقة آمنة، كما يجب على الطرف المعول على شهادة التصديق الإلكتروني الموصوفة التأكد مُسبقا من مِصداقية كلّ البيانات الواردة فيها[1].

إنطلاقا من ذلك ميّز المشرع الفيدرالي الأوروبي بموجب المادة 02/9-10 بين نوعين من الشهادات الإلكترونية، فالشهادة الإلكترونية البسيطة تربط بيانات فحص التوقيع الإلكتروني لشخص معين مع تأكيد هويته، أمّا الشهادة الإلكترونية الموصوفة يُقصد بها الشهادة الإلكترونية المُستوفية للمواصفات المحددة في الملحق الأول(Annexe I)، التي يُصدرها(م.خ.ت.إ) مُستوفيا للمتطلبات المحددة في الملحق الثاني(Annexe II)، وبالتالي يجب على الشهادة الإلكترونية الموصوفة أن تستجيب للمواصفات التقنية التي حدّدها الملحق الأول من التوجيه، كوجود بيان يؤكد بأنّها شهادة تصديق موصوفة(الفقرة a) مع تحديد هوية كلّ من(م.خ.ت.إ) مع بلد إقامته، وإسم المُوقِّع أو الإسم المستعار له وصفته في حالة إستعمال الشهادة لغرض معين(b-c-d)، وتأكيد مطابقة بيانات إحداث التوقيع الإلكتروني لبيانات فحصه، مع ذكر مدة صلاحية الشهادة ورمز تعريفها(e-f-g)، والتوقيع

---

1) - **ANNEX IV** (même directive): « Durant le processus de vérification de la signature, il convient de veiller, avec une marge de sécurité suffisante, à ce que:
**a)** les données utilisées pour vérifier la signature correspondent aux données affichées à l'intention du vérificateur;
**b)** la signature soit vérifiée de manière sûre et que le résultat de cette vérification soit correctement affiché;
**c)** le vérificateur puisse, si nécessaire, déterminer de manière sûre le contenu des données signées;
**d)** l'authenticité et la validité du certificat requis lors de la vérification de la signature soient vérifiées de manière sûre;
**e)** le résultat de la vérification ainsi que l'identité du signataire soient correctement affichés;
**f)** l'utilisation d'un pseudonyme soit clairement indiquée, et
**g)** tout changement ayant une influence sur la sécurité puisse être détecté. »

الإلكتروني الجذري لـ(م.خ.ت.إ) المُصدر للشهادة، وعند الإقتضاء يجب تحديد الشروط والقيمة التي تُستعمل من أجلها الشهادة(h-i-j).

**ثالثا: قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية لعام 2001.**

قامت لُجنة الأمم المتحدة للقانون التجاري الدولي في دورتها الرابعة والثلاثين بوضع قانون دولي نموذجي بشأن التوقيعات الإلكترونية لعام 2001، تدعيما وتعزيزا للمبادئ الجوهرية التي إستندت عليها المادة 07 من القانون الدولي النموذجي بشأن التجارة الإلكترونية لعام 1996، حول طرق التوثيق الإلكتروني والاعتراف القانوني بها، فيعني بالتوقيع الإلكتروني وفقا للمادة الثانية فقرة (أ) منه[1]: " **بيانات في شكل إلكتروني مدرجة في رسالة بيانات، أو مضافة إليها أو مرتبطة بها منطقيا، يجوز أن تُستخدم لتعيين هوية الموقع بالنسبة إلى رسالة البيانات، ولبيان هوية موافقة الموقع على المعلومات الواردة في رسالة البيانات.**"

أمّا (م.خ.ت.إ) حسب المادة 02/(هـ) من نفس القانون يتمثل في شخص يُصدر الشهادات ويجوز أن يُقدم خدمات آخرى ذات صلة بالتوقيعات الإلكترونية، التي تسمح للطرف المعول وفقا للفقرة(و) من نفس المادة(02) بأن يتصرف استنادا إلى شهادة التصديق الإلكتروني أو إلى التوقيع الإلكتروني، وبالتالي فإنّ الهدف الرئيسي لشهادة التصديق الإلكتروني وفقا للفقرة (ب) من نفس المادة ينصب حول الإعتراف بوجود صلة بين بيانات إنشاء التوقيع الإلكتروني والموقّع أو بيان وجود تلك الصلة أو تأكيد وجودها.

لتسهيل عملية التعويل على شهادة التصديق الإلكتروني يجب أن تحتوي هذه الآخيرة على مجموعة من البيانات، التي نص عليها قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية في المادة 09/ج- د، والمتعلقة بهوية كلّ من(م.خ.ت.إ) والمُوَقِّعْ الذي كان يتحكم في بيانات إنشاء التوقيع في وقت إصدار الشهادة، مع التأكيد بأنّ بيانات إحداث

---

[1] – قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية لعام 2001 مع دليله التشريعي. http://www.unicitral.org/pdf/Arabic/texts/selectcom/mt-elecsig/

التوقيع الإلكتروني كانت صحيحة في وقت أو قبل إصدار الشهادة ولم تتعرض لما يُثير الشبهة فيها، مع توضيح الطريقة المُستخدمة في تعيين هوية المُوَقِّع، وعند الضرورة يجب تحديد القيود المفروضة على القيمة التي تُستخدم من أجلها الشهادة أو على نطاق أو مدى المسؤولية التي اشترطها(م.خ.ت.إ) تجاه أيّ شخص.

تجدر الإشارة أنّه يُمكن لأيّ شخص التعويل على إحدى تقنيات طرق التوقيع الإلكتروني الآخرى في توثيق تصرفاتهم المتعلقة بالتجارة الإلكترونية، تفي بمُقتضيات قابلية التعويل الواردة في المادة 06 من نفس القانون، إذْ تقوم أيّة سلطة أو هيئة تُعينها الدولة لتقرير مدى صحة إستخدام هذه الطرق أو تشهد بطريقة آخرى على نوعيتها وفقا للمعايير الدولية المعترف بها[1]، فحسب الفقرتين الأولى والثالثة من نفس المادة 06/1-3، يعتبر التوقيع الإلكتروني موثوقا إذا كانت بيانات إنشاءه وقت التوقيع مُرتبطة بالموقع لوحده وتحت سيطرته، على النحو الذي يضمن كشف أيّ تغيير يمس بسلامة المعلومات المرفقة بالتوقيع الإلكتروني بعد وقت إحداثه.

من خلال ما سبق يتضح لنا أنّ أعضاء اللجنة عند صياغتهم للقانون النموذجي بشأن التوقيعات الإلكترونية، اتبعوا مبدأ الحياد التكنولوجي أو ما يُعرف بالحد الأدنى الذي لا يرتكز على نمط معين من التكنولوجيا المتعلقة بالتوثيق الإلكتروني، وذلك بهدف ترك الحرية للدول المُشترعة في إتباع النهج الأفضل في تقدير قابلية التعويل، على إحدى مُستويات الأمان في تكنولوجيا تقنيات التوثيق الإلكتروني في إطار مرافق المفاتيح العمومية الموثوق بها[2].

---

[1] – المادة 07 (قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية لعام 2001):

– "يجوز لأيٍّ ( شخص أو جهاز أو سُلطة تُعينهم الدولة المُشترعة جهة مُختصة، سواءا أكانت عامة أم خاصة) تحديد التواقيع الإلكترونية التي تفي بأحكام المادة الثانية(02) من هذا القانون.

– يتعين أن يكون أيّ تحديد يتم بمُقتضى الفقرة الأولى مُتسقا مع المعايير الدولية المُعترف بها.

– ليس في هذه المادة ما يخل بسريان مفعول قواعد القانون الدولي الخاص."

[2] – دليل تشريع قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية لعام 2001، ص 58.

## الفرع الثاني

## مفهوم التوثيق الإلكتروني وفقا للتشريعات الوطنية الأجنبية

تُعتبر القوانين الدولية النموذجية المتعلقة بالتجارة والتوقيعات الإلكترونية والتوجيه الأوروبي الخاص بالتوقيعات الإلكترونية، المراجع الأساسية التي إستندت عليها العديد من الدول الأجنبية في سنّ تشريعاتها الداخلية، وذلك بغض النظر عن شكل ونظام الدولة (موحدة كانت أم مُركبة)، والتي سنتطرق إليها على النحو التالي:

### أولا- في القانون الأمريكي:

تضم الولايات المُتحدة الأمريكية(كدولة مركبة) لمجموعة من الولايات الفيدرالية التي أعطت الأهميّة للمعاملات الإلكترونية وبالخصوص التجارة الإلكترونية، لذا فإنّ الحاجة إلى تنسيق وتوحيد قوانين هذه الولايات باتت من ضروريات الإقتصاد الرقمي الأمريكي.

### أ- القانون النموذجي الموحد بشأن المعاملات الإلكترونية لعام 1999.

في سنة 1999 وبمُبادرةٍ من الدولة الفيدرالية قامت اللجنة المفوضة بتوحيد قوانين الولايات الأمريكية في مؤتمر وطني(NCCUSL) أُنعقد في ولاية كولورادو(دانفر) بإعتماد القانون الموحد المتعلق بالمعاملات الإلكترونية(UETA)[1]، الذي يُعتبر كأول اجتهاد وطني في مجال خلق قواعد مُوَّحِدَة تهدف إلى تنظيم معاملات التجارة الإلكترونية وتحقيق الإنسجام والتوافق في تشريعات الولايات الفيدرالية، فالتوقيع الإلكتروني وفقا للجزء 08/02 منه يشتمل على كلّ صوت أو رمز أو عملية إلكترونية، مُرفقة أو مُرتبطة منطقيا بعقد أو سجّل آخر ومُنفذة أو مُتخذة من قِبل أحد الأشخاص بنيّة توقيع السّجل، في حين يُقصد بإجراءات أمن

---

1) - Uniform Electronic Transactions Act (1999), Drafted by the National Conference of Commissioners on Uniform State Laws, approved and recommended for enactment in all the states at its annual conference meeting in its one-hundred-and-eighth year in DENVER, COLORADO, july 23 – 30, 1999. http://www.law.upenn.edu/bll/ulc/uecicta/eta1299.htm http://www.nccusl.org/nccusl/uniformact_ factsheets/uniformacts-fs-ueta.asp

فحص التوقيع الإلكتروني بموجب الفقرة 14 منه[1]:" **الإجراءات المؤمنة المُستخدمة لغرض فحص التوقيع الإلكتروني ومدى نسبته لصاحبه، على نحو يسمح بكشف وتحديد التغييرات أو الأخطاء التي تمس بمعلومات السجل الإلكتروني المتصل بالتوقيع، ويشمل مُصطلح الإجراءات وجوب إستخدام خوارزميات أو الأرقام السرية الآخرى التي تُحدد الكلمات أو الأرقام، التشفير، أو الرّد أو إجراءات الإعتراف الآخرى.**"

فوفقا للجزء 09 من نفس القانون فإنّ صحة التوقيع الإلكتروني ونسبته لصاحبه مرهون بمدى جدارة الثقة في الطريقة التي أستخدمت في تحديد هوية المُوقِّع، مع الأخذ بعين الإعتبار أي عامل آخر متصل بإحداث توقيعه الإلكتروني، بالإضافة إلى ذلك نص الجزء 07 منه على عدم إنكار الأثر القانوني للسجل أو التوقيع الإلكترونيين لكونهما في شكل إلكتروني، والعقد الإلكتروني بسبب صياغته في محرر إلكتروني، وأيّ إشتراط قانوني في التوقيع والمحرر الكتابيين يكون بالمثل في التوقيع والمحرر الإلكترونيين[2]، وبالتالي فإنّ اللجنة(NCCUSL) اتبعت منهج الحد الأدنى الذي يمنح التكافؤ الوظيفي بين التوقيعات

---

1) – **Section 02.(8)-(14)** :"**Electronic signature** means an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record."

-"**Security procedure**: means a procedure employed for the purpose of verifying that an electronic signature, record, or performance is that of a specific person or for detecting changes or errors in the information in an electronic record. The term includes a procedure that requires the use of algorithms or other codes, identifying words or numbers, encryption, or callback or other acknowledgment procedures."

2) - **Section 07 :** "**(a)** A record or signature may not be denied legal effect or enforceability solely because it is in electronic form.

**(b)** A contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation.

**(c)** If a law requires a record to be in writing, an electronic record satisfies the law.

**(d)** If a law requires a signature, an electronic signature satisfies the law." **Source**: UNCITRAL Model Law on Electronic Commerce, Articles 5, 6, and 7.

- **Section 09:** "**(a)** An electronic record or electronic signature is attributable to a person if it was the act of the person. The act of the person may be shown in any manner, including a showing of the efficacy of any security procedure applied to determine the person to which the electronic record or electronic signature was attributable…

**(b)** The effect of an electronic record or electronic signature attributed to a person under subsection (a) is determined from the context and surrounding circumstances at the time of its creation, execution, or adoption, including the parties' agreement, if any, and otherwise as provided by law."

الإلكترونية والتوقيعات الكتابية، شريطة أن تهدف التكنولوجيات المُستخدمة في طرق التوثيق الإلكتروني إلى تحقيق مُستويات الأمان في وظائف محددة، وأن تُلبي مُتطلبات قابلية التعويل عليها في إثبات مُختلف التصرفات الإلكترونية أمام العدالة، كما ترك القانون النموذجي للولايات الفيدرالية مسألة تنظيم المرافق العمومية وفقا للقانون المعمول به.

**ب- القانون الفيدرالي المتعلق بالتوقيع الإلكتروني لعام 2000.**

في 30 جوان 2000 قام الكونجرس الأمريكي بإصدار قانون فيدرالي بشأن التوقيعات الإلكترونية في التجارة العالمية والمحلية(E-SIGN)[1]، لغرض تحقيق الإنسجام والتناسق في التشريعات الداخلية للولايات الفيدرالية التي اعتمدت مُسبقا القانون الموحد المتعلق بالمعاملات الإلكترونية لعام 1999، وبالتالي انتهج القانون الفيدرالي بدوره الحياد التكنولوجي من خلال تطبيقه لنفس تعريف التوقيع الإلكتروني الوارد في الجزء 08/02 من القانون الموحد المتعلق بالمعاملات الإلكترونية، في الجزء 5/106 من القانون المتعلق بالتوقيعات الإلكترونية(E-SIGN) من دون التطرق إلى الإجراءات المؤمنة، لذا عمل القانون الفيدرالي على منح نفس النظام القانوني المفروض على المحررات الورقية والتوقيعات اليدوية للمحررات والتوقيعات الإلكترونية، ولم يفرض أيّة شروط أو إجراءات معينة للاعتراف بصحة التوقيع الإلكتروني أو توثيقه في شهادة توثيق إلكتروني من طرف جهة معينة، ويُفسر البعض هذا الصمت بالقبول الضمني بالتوثيق الإلكتروني، ومن ثمّة ترك القانون الفيدرالي وفقا للجزء 102 منه الحرية للولايات الفيدرالية بسن قواعد تنظيمية حول التوثيق الإلكتروني[2].

---

1) - Public Law 106–229106th Congress June 30, 2000, Electronic Signatures in Global and National Commerce Act. http://www.fdic.govregulationscompliancemanualpdfX-3.1.pdf

2) - **Florence DARQUES et Laurence BIRNBAUM-SARCY**, La signature électronique Comparaison entre les législations française et américaine, pp. 2-5. Article publié sur: http://www .signelec.com/content/se/articles/comparaison_fr_us_html

**ثانيّا– في القانون الكندي:**

إنّ حتمية الإقتصاد الرقمي والطابع الفيدرالي لكندا كدولة اتحادية دفع بسلطاتها إلى التفكير في سنّ قوانين فيدرالية من أجل تنسيق وتوحيد تشريعات مقاطعاتها الفيدرالية المتعلقة بالمعاملات الإلكترونية، والتي سنتطرق إليها على النحو التالي:

**أ– القانون الموحد بشأن التجارة الإلكترونية لعام 2000.**

إنّ القانون الموحد بشأن التجارة الإلكترونية الذي أعدته لجنة توحيد القوانين الكندية في عام 1999 الذي دخل حيز التنفيذ في مارس 2000، جاء كنموذج قصد تنسيق وتوحيد قوانين المقاطعات الفيدرالية[1] مُستنبطا أحكامه من قانون الأونسيترال النموذجي المتعلق بالتجارة الإلكترونية لعام 1996، فبالرجوع إلى أحكام القانون الكندي نجد أنّه حثّ على إستخدام التوقيعات الإلكترونية المؤمنة في تأكيد مُختلف التصرفات الإلكترونية المتعلقة بالتجارة الإلكترونية، بحيث نص في الجزء 10 منه[2] أنّه في حالة إشتراط قوانين المقاطعات الفيدرالية لتوقيع إلكتروني يجب على السلطة المسئولة في كلّ مُقاطعة، الحرص بموجب التنظيم على ضمان موثوقية منظومات إحداث التوقيعات الإلكترونية، والحفاظ على سلامة المحررات الإلكترونية المُرتبطة بها وفقا لإجراءات توثيق مؤمنة، تضمن حفظ السجل الإلكتروني في شكله الإلكتروني الذي تم فيه إنشاءه أو إرساله أو استلامه على النحو الذي لا يمس بسلامة مضمونه، وأن يسمح نظام حفظ البيانات إتاحة المعلومات المتعلقة بالسجل الإلكتروني عند الحاجة إليها تبعا للظروف.

إنطلاقا من ذلك قامت مُقاطعة كيبك(Québec) بإصدار قانون متعلق بالإطار القانوني بتكنولوجيا المعلومات، الذي سمح بموجب الجزء 53 منه لـ(م.خ.ت.إ) طلب الإعتماد

---

1) - **Le canada** est en effet une fédération (monarchie constitutionnelle fédérale à régime parlementaire) de **dix provinces**, à savoir : Nouvelle Écosse, Nouveau Brunswick, Québec, Ontario, Manitoba, Colombie-Britannique, Île-du-Prince-Édouard, Alberta, Saskatchewan, Terre-Neuve, enfin les territoires du Nord-Ouest et du Yukon. http://www.a .gc.ca/main_e.html

2) - Loi uniforme sur le commerce électronique, Mars 2000. http : //www. ULCC Uniform Law Conference of Canada.

الاختياري وفقا لمُقتضيات الفقرة الثالثة من الجزء 69 منه، بحيث تقوم حكومة كيبك بإصدار نص تنظيمي يتعلق بخدمات التصديق الإلكتروني، تُحدد فيه الشروط والإجراءات المتعلقة بمنح وتجديد وإلغاء الإعتماد الاختياري والمصاريف المتعلقة به، كما ألزم الجزء 68 منه على وجوب مُطابقة معدات وأنظمة أمن تكنولوجيا المعلومات للمعايير المعمول بها قانونيا والمعترف بها دوليّا[1].

**ب- القانون الفيدرالي لحماية المعطيات الشخصية والمحررات الإلكترونية لعام 2000.**

إنّ الهدف من إصدار القانون الفيدرالي المتعلق بحماية المعطيات الشخصية والمحررات الإلكترونية[2]، يتعلق بتشجيع معاملات التجارة الإلكترونية مع حماية المعطيات الشخصية لكلّ طرف في التصرف الإلكتروني، بحيث ميّز بموجب المادة 31-1 من الجزء الثاني منه بين نوعين من التوقيعات الإلكترونية، فالأول يتعلق بالتوقيع الإلكتروني البسيط المُحدث بحرف أو بمجموعة من الحروف أو واحد أو أكثر من الأشكال والأعداد، أو الرموز في

---

1) – Loi concernant le Cadre Juridique des Technologies de l'Information. Disponible sur : http://www.canlii.ca/

- **Section 53** : « Le prestataire de services de certification peut adhérer à un régime d'accréditation volontaire. L'accréditation est accordée, eu égard aux exigences à satisfaire en vertu du paragraphe 3° de l'article 69, par une personne ou un organisme désigné par le gouvernement. Les mêmes critères sont appliqués quelle que soit l'origine territoriale du prestataire. L'accréditation fait présumer que les certificats délivrés par le prestataire répondent aux exigences de la présente loi. »

- **Section 68** : « Lorsque la présente loi exige qu'un procédé, une norme ou un standard techniques soit approuvé par un organisme reconnu, pour établir qu'il est susceptible de remplir une fonction spécifique, la reconnaissance peut en être faite par : La Commission électrotechnique internationale (CEI), l'Organisation internationale de normalisation (ISO) ou l'Union Internationale des Télécommunications (UIT) ; ou Le Conseil Canadien des Normes et ses organismes accrédités ; ou Le Bureau de Normalisation du Québec. La reconnaissance peut également inclure la référence à un procédé établi ou à la documentation élaborée par un groupement d'experts, dont l'Internet Engineering Task Force ou le $W_3C$. »

2) - Loi sur la Protection des Renseignements Personnels et les Documents Électroniques, LC 2000. Disponible sur : http://www.ulcc.cafrlois-uniformes-fr/

-**Art.31-1** : «**signature électronique** : Signature constituée d'une ou de plusieurs lettres, ou d'un ou de plusieurs caractères, nombres ou autres symboles sous forme numérique incorporée, jointe ou associée à un document électronique ».

«**signature électronique sécurisée** : Signature électronique qui résulte de l'application de toute technologie ou de tout procédé prévu par **règlement** pris en vertu du paragraphe 48(1). »

شكل رقمي مُتصلة بالمحرر الإلكتروني، أمّا الثاني يتعلق بالتوقيع الإلكتروني الموصوف المُحدث بإستعمال تكنولوجيات ومنظومات أمن المُحددة بموجب التنظيم.

**ثالثا- في القانون الفرنسي.**

تعتبر فرنسا من بين الدول العُضْوَة في الإتحاد الأوروبي إبتداءا من معاهدة ماستريخت(Maastricht) لعام 1992 بهولندا المنشئة له، والمُعَدَّلَة بموجب معاهدة أمستردام لعام 1999 ومعاهدة نيس لعام 2003 إلى غاية وقتنا الحاضر، وبالتالي فهي مُلتزمة بالتوجيهات الأوروبية داخل الإتحاد بالخصوص التوجيه الأوروبي رقم 93/99 الصادر في 13 ديسمبر1999 المتعلق بالتوقيعات الإلكترونية، تنفيذا لما نصت عليه المادة 13/1-2 من التوجيه[1] التي ألزمت الدول الأعضاء بإخضاع أحكامها التشريعية والتنظيمية والإدارية لأحكام التوجيه، وإدخالها حيّز التنفيذ قبل تاريخ 19 جويلية2001 مع إعلامها بذلك للجنة الأوروبية، ونحن نعلم أن التوجيه دخل حيّز التنفيذ من تاريخ صدوره في الجريدة الرسمية للإتحاد الأوروبي أي في 19 جانفي2000 وفقا للمادة (14) من نفس التوجيه.

إنطلاقا من ذلك أصدر المشرع الفرنسي القانون رقم 230/2000 الصادر بتاريخ 13 مارس2000، مُتضمنا تكييف قانون الإثبات بتكنولوجيا المعلومات والمتعلق بالتوقيع الإلكتروني، الذي من خلاله قام بتعديل مواد الإثبات التي نص عليها التقنين المدني الفرنسي، وذلك بمُساواته للمحرر الإلكتروني بالمحرر الكتابي من حيث الحجية القانونية في الإثبات، وتطبيقا لأحكام الفقرة الثانية من المادة 1316-4 من نفس التقنين (...**عندما يكون التوقيع إلكترونيّا يجب أن يستند إلى منظومة موثوق بها لتحديد الهوية تضمن ارتباطه**

---

1) – **Art. 13/ 1-2 :** (Directive européenne n° 1999/93 sur les signatures électroniques.)

« 1- Les États membres mettent en vigueur les dispositions législatives, réglementaires et administratives nécessaires pour se conformer à la présente directive avant le 19 juillet 2001. Ils en informent immédiatement la Commission. Lorsque les États membres adoptent ces dispositions, celles-ci contiennent une référence à la présente directive ou sont accompagnées d'une telle référence lors de leur publication officielle, les modalités de cette référence sont adoptées par les États membres.

2- Les États membres communiquent à la Commission le texte des dispositions essentielles de droit interne qu'ils adoptent dans le domaine régi par la présente directive. »

**بالتصرف المتصل به إلى غاية إثبات غير ذلك، فعندما يُحدث توقيع إلكتروني فإنّ هوية المُوقِّع مؤكدة، وسلامة المحرر مضمونة، وفقا لشروط تُحدد بموجب مرسوم بمجلس الدولة الفرنسي)**[1]، قام الوزير الأول(LIONEL Jospin) بعد إستشارة مجلس الدولة وجوباً بإصدار مرسوم تطبيقي رقم 2001-272 مؤرخ في 30 مارس2001 يتعلق بالتوقيع الإلكتروني، الذي تطرق من خلال أحكامه إلى تعريف منظومة أمن إحداث التوقيعات الإلكترونية الموثوق بها، التي تحتوي على أيّ جهاز أو برنامج معلوماتي معد لتطبيق بيانات إنشاء التوقيعات الإلكترونية(مفاتيح التشفير الخاصة بالموقع) وفقا للمتطلبات المحددة في المادة II -I/03 من المرسوم[2].

---

1) - Loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique. J.O.R.F, n° 62 du 14 mars 2000. http://www.legifrance.gouve.fr/

**Art.1316-4** : « […] Lorsqu'elle (la signature) est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé et présumé, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en conseil d'État. »

2) - Décret n° 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique. J.O.R.F, n° 0077 du 31 mars 2001. http://www.legifrance.gouve.fr/

- **Art.03** : « **I**- Un dispositif sécurisé de création de signature électronique doit :

**1.** Garantir par des moyens techniques et des procédures appropriés que les données de création de signature électronique :

**a)** Ne peuvent être établies plus d'une fois et que leur confidentialité est assurée ;

**b)** Ne peuvent être trouvées par déduction et que la signature électronique est protégée contre toute falsification;

**c)** Peuvent être protégées de manière satisfaisante par le signataire contre toute utilisation par des tiers.

**2.** N'entrainer aucune altération du contenu de l'acte à signer et ne pas faire obstacle à ce que le signataire en ait une connaissance exacte avant de le signer.

II - Un dispositif sécurisé de création de signature électronique doit être certifié conforme aux exigences définie au **I** : **1- Soit** par les services de premier ministre chargés de la sécurité des systèmes d'information, après une évaluation réalisée, selon des règles définie par arrêté de premier ministre, par des organismes agrées par ces services, la délivrance par ces services du certificat de conformité est rendue publique.

**2- Soit** par un organisme désigné à cet effet par un État membre de la communauté européenne. »

- **Art.1-2** « **Signature électronique sécurisée** : Une signature électronique qui satisfait, en outre, aux exigences suivantes : - être propre au signataire ; - être créée par des moyens que le

أمّا منظومة فحص التوقيع الإلكتروني فهي بدورها تحتوي على أيّ جهاز أو برنامج معلوماتي معد لتطبيق بيانات فحص التوقيع الإلكتروني(مفاتيح التشفير العمومية) وفقا للمتطلبات المحددة في المادة 05 من نفس المرسوم[1]، والتي يجب أن تضمن القَائِمْ بعملية الفحص تحديد هوية المُوقِّع ومطابقة بيانات إحداث توقيعه الإلكتروني مع بيانات فحصه مع كشف أيّ تعديل أو تغيير فيها بطريقة واضحة، كما يجب على الطرف المُعَوِّل على شهادة التصديق أن يتأكد من سلامة ومصداقية جميع البيانات الواردة فيها.

فعن طريق المنظومتين نتوصل إلى توقيع إلكتروني مؤمن تم إحداثه على أساس شهادة تصديق إلكتروني موصوفة، بموجب منظومة أمن إحداث التوقيعات الإلكترونية الموضوعة تحت سيطرة الموقع لوحده، بوساطة(م.خ.ت.إ) محايد ومؤهل في إطار مخطط الإعتماد الاختياري، والمتمثل(م.خ.ت.إ) وفقا لنص المادة 11/01 من نفس المرسوم، في أيّ شخص يُصدر شهادات إلكترونية أو يقوم بخدمات آخرى مُتعلقة بالتوقيع الإلكتروني.

---

signataire puisse garder sous son contrôle exclusif ; - garantir avec l'acte auquel elle s'attache un lien tel que toutes modifications ultérieure de l'acte soit détectable. »

- **Art.01-11** : « Prestataire de Service de Certification Électronique : toute personne qui délivre des certificats électronique ou fournit d'autres services en matière de signature électronique. »

1) **- Art.05** (Décret n° 2001-272…) : « Un dispositif de vérification de signature électronique peut faire, après évaluation, l'objet d'une certification, selon les procédures définies par l'arrêté mentionnée à l'article 04, s'il répond aux exigences suivantes : **a)** Les données de vérification de signature électronique utilisées doivent être celles qui ont été portées à la connaissance de la personne qui met en œuvre le dispositif et qu'est dénommé « vérificateur » ;

**b)** Les conditions de vérification de la signature électronique doivent permettre de garantir l'exactitude de celle-ci, et le résultat de cette vérification doit sans subir d'altération être portée à la connaissance du vérificateur ;

**c)** Ce dernier doit pouvoir, si nécessaire, déterminer avec certitude le contenu des données signées ;

**d)** Les conditions et la durée de validité du certificat électronique utilisée lors de la vérification de la signature électronique doivent être vérifiées et le résultat de cette vérification doit sans subir d'altération être porté à la connaissance du vérificateur ;

**e)** L'identité du signataire doit sans subir d'altération être porté à la connaissance du vérificateur ;

**f)** Lorsqu'il est fait usage d'un pseudonyme, son utilisation doit être clairement porté la connaissance du vérificateur ;

**g)** Toutes modifications ayant une incidence sur les conditions de vérification de signature électronique doit pouvoir être détectée. »

زيادة على ذلك ميّز المشرع الفرنسي بموجب المادة 10-9/01 بين نوعين من شهادات التصديق الإلكتروني، فالأولى تتعلق بالشهادة الإلكترونية البسيطة كوثيقة إلكترونية تُثبت الصلة بين بيانات فحص التوقيع الإلكتروني والمُوقّع، بينما الثانية تتعلق بشهادة التصديق الإلكتروني الموصوفة المستوفية للمتطلبات المُحددة في المادة l/06 من المرسوم، كالتأكيد بأنّها شهادة إلكترونية موصوفة(فقرة-a)، مع تحديد هوية كلّ من(م.خ.ت.إ) والموقع أو إسمه المستعار، وصفته في حالة إستعمال الشهادة لغرض معين(b-c-d)، وتأكيد مطابقة بيانات إحداث التوقيع الإلكتروني المطابقة لبيانات فحصه بوضوح، مع ذكر مدة صلاحية الشهادة ورمز تعريفها(e-f-g) والتوقيع الإلكتروني الجذري لـ(م.خ.ت.إ)، كما يجب توضيح الشروط والقيمة التي تُسْتَعْمَلُ من أجلها شهادة التصديق الإلكتروني(h-i).

**رابعا- القانون البلجيكي.**

مُراعاةً لأحكام المادة (2-1/13) من التوجيه الأوروبي رقم 93/99 المتعلق بالتوقيعات الإلكترونية، قام ملك بلجيكا(**Albert II**) بإصدار قانون 09 جويلية2001 يتضمن تحديد القواعد المتعلقة بالإطار القانوني للتوقيعات الإلكترونية وبخدمات التصديق[1]، بحيث تطرق من خلال المادة 10/02 منه إلى(م.خ.ت.إ) بصفته كطرف مستقل يشرف على إجراءات التوثيق الإلكتروني المعتمدة، الذي يكون في هيئة شخص طبيعي أو معنوي يقوم بإصدار الشهادات أو الخدمات الأخرى المتعلقة بالتوقيعات الإلكترونية، في حين ميّز المشرع البلجيكي بموجب المادة 4-3/02 من نفس القانون، بين نوعين من الشهادات الإلكترونية فالأولى تتعلق بالشهادة الإلكترونية البسيطة التي تربط بيانات التحقق من التوقيع الإلكتروني

---

1) – La Belgique est une **monarchie constitutionnelle**, représentative, héréditaire et parlementaire, La succession au trône est déterminée par primogéniture, La Constitution belge a été promulguée le 7 février 1831 et révisée en 1893, 1921, 1970, 1971, 1980, 1989 et 1993. Répondant à des tensions entre les régions **francophones** et **néerlandophones**, les réformes intervenues depuis 1970 ont transformé la Belgique en un **État fédéral communautaire** et **régional** à la fois, depuis la **révision constitutionnelle de 1993** (entrée en vigueur le 1er janvier 1995), la plupart des pouvoirs gouvernementaux essentiels appartiennent aux trois régions que sont la **Région flamande**, **la Région wallonne** et **Bruxelles-Capitale**.
http://www.monde-diplomatique.fr/index/pays/belgique.
- **Loi du 9 Juillet 2001**, fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification. MB n° 2699 du 29.09.2001.www.moniteur.be

لشخص طبيعي أو معنوي مع تأكيد هويته، أمّا الثانية تتعلق بالشهادة الإلكترونية الموصوفة المُستوفية للمتطلبات المحددة في الملحق الأول من القانون الملكي التي يُصدرها(م.خ.ت.إ) معتمد(مُستوفيا للشروط المحددة في الملحق الثاني منه).

إنطلاقا من ذلك فإنّ التوقيع الإلكتروني البسيط وفقا للمادة 1/02 من نفس القانون يحتوي على بيانات إلكترونية مرتبطة مع البيانات الإلكترونية الآخرى لإستعمالها كوسيلة توثيق، أمّا التوقيع الإلكتروني الموصوف يتمثل في التوقيع الإلكتروني المتقدم الذي تم إحداثه على أساس شهادة تصديق إلكتروني موصوفة، بموجب منظومة أمن إحداث التوقيعات الإلكترونية[1] الموضوعة تحت سيطرة الموقع لوحده، بوساطة(م.خ.ت.إ) محايد ومؤهل من طرف الجهات الرسمية لمزاولة نشاطاته.

لذا يجب على منظومة أمن إحداث التوقيع الإلكتروني أن تضمن سرية وعدم إستعمال بيانات إنشاءه من الناحية العملية لأكثر من مرّة واحدة، مع عدم إمكانية الكشف عنها عن طريق الإستنباط، وأن لا تُغير من البيانات التي سيتم توقيعها أو تمنع عملية التوقيع عليها مع تمكين المُوقّع من حماية توقيعه بطريقة آمنة، كما يجب على الطرف المعول إتباع

---

[1] - **Art.7** (Loi du 9 Juillet 2001…): « 1- Les exigences relatives aux dispositifs sécurisés de création de signature électronique sont reprises à l'annexe III de la présente loi. La conformité des dispositifs sécurisés de création de signature électronique par rapport aux exigences visées à l'annexe III de la présente loi est attestée par des organismes compétents désignés par **l'Administration** et dont la liste est communiquée à la Commission Européenne. Le **Roi** détermine les conditions auxquelles doivent répondre les organismes visés au paragraphe précèdent. La conformité établie par un organisme désigné par un autre État membre de l'Espace économique européen est reconnue en Belgique. »

– **Art.02** (loi du 09 juillet 2001…): 1- « **signature électronique** : une donnée sous forme électronique jointe ou liée logiquement à d'autres données électroniques et servant de méthode d'authentification. »

2- « **signature électronique avancée** : une donnée électronique, jointe ou liée logiquement à d'autres données électroniques, servant de méthode d'authentification et satisfaisant aux exigences suivantes : **a)** être liée uniquement au signataire;

**b)** permettre l'identification du signataire;

**c)** être créée par des moyens que le signataire puisse garder sous son contrôle exclusif;

**d)** être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectée. »

الخطوات المعقولة لتقدير قابلية التعويل على التوقيع الإلكتروني الموصوف التي حثّ عليها المشرع البلجيكي بموجب الملحق الرابع من القانون الملكي.

**خامسا- القانون الفيدرالي السويسري لعام 2003.**

أصدرت الجمعية الفيدرالية التابعة لِلْكُنْفِيدِرَالِيَّة السويسرية[1] قانون التوقيع الإلكتروني- (SCSE) في 19 ديسمبر 2003 الذي دخل حيّز التنفيذ في 01 جانفي2005[2]، بهدف تنظيم كل المسائل المتعلقة بخدمات التصديق الإلكتروني المعتمدة، التي يُشرف عليها وفقا للمادة 02/(g) والمادة 08 منه(م.خ.ت.إ) معترف به من طرف هيئة الإعتماد السويسرية لمزاولة الخدمات المتعلقة بإحداث التوقيعات الإلكترونية الموصوفة، في حين ميّز المشرع الفيدرالي فيما بين التوقيع الإلكتروني البسيط (Signature électronique simple) والتوقيع الإلكتروني الموصوف (Signature électronique qualifiée)، بحيث عرّف في المادة الثانية فقرة(a) منه التوقيع الإلكتروني البسيط على أنّه:" **بيانات إلكترونية مُرفقة أو مُرتبطة منطقيا ببيانات إلكترونية آخرى والتي تُستخدم للتحقق من مصداقيتها.**"

أمّا التوقيع الإلكتروني الموصوف حسب الفقرة(c) من نفس المادة(c/02) يتمثل في التوقيع الإلكتروني المتقدم، المُحدث بموجب منظومة أمن إنشاء التوقيعات الإلكترونية المستوفية للمواصفات المحددة في المادة 2-1/06 من القانون، والمعزز بشهادة تصديق إلكتروني موصوفة سارية المفعول، تحتوي على البيانات المحددة بموجب المادة 2-1/07 من نفس القانون، كالرقم التسلسلي لشهادة التصديق الإلكتروني الموصوفة، واسم المُوقّع أو

---

1) - **La Suisse** est un **État fédéral** depuis **1848**, son pouvoir est réparti entre la Confédération (État central), les 26 cantons (États fédéraux) et les 2495 communes (Etat au 1/1/2012). Chacun de ces niveaux dispose d'un pouvoir législatif (édicter des lois) et exécutif (les faire exécuter). La Confédération et les cantons ont en outre un pouvoir judiciaire (ensemble de tribunaux) qui se charge de les faire respecter. **La confédération**, est une association égalitaire entre des **États indépendants** qui acceptent de coopérer dans un certain nombre de domaines, sans renoncer à leur **souveraineté**. http://www.admin.ch/org/polit/

2) - Loi fédérale sur les services de certification dans le domaine de la signature électronique (Loi sur la signature électronique, SCSE) du 19 décembre 2003. http://www.admin.chopcfrclassified-compilation20011277index.html

الاسم المستعار له وصفته في حالة تمثيل الشخص المعنوي، مع ذكر اسم وبلد إقامة المزود المعترف به مع توقيعه الإلكتروني الجذري ومدة صلاحية الشهادة، كما يجب عند الإقتضاء تحديد الغرض والقيمة التي تُسْتَعْمَل من أجلها الشهادة[1].

زيادة على ذلك يجب على منظومة أمن إحداث التوقيعات الإلكترونية وفقا للمادة 2/06 من نفس القانون، أن تضمن سريّة إستعمال المفتاح الخاص بالتوقيع الإلكتروني لمرة واحدة فقط مع عدم إمكانية كشفه عن طريق عملية الإستنباط(Déduction)، وأن تُمكّن المُوقِّع من حماية توقيعه بطريقة آمنة، كما يجب على منظومة فحص التوقيع الإلكتروني أن تستجيب للمتطلبات المحددة بموجب الفقرة الثالثة من نفس المادة(3/06)، كضمان تحديد هوية المُوقِّع ومطابقة بيانات إحداث توقيعه الإلكتروني مع بيانات فحصه بوضوح، مع كشف أيّ تغيير أو تعديل في البيانات الإلكترونية بعد التوقيع عليها، كما يجب على الطرف المعول التأكد مُسبقا من مصداقية كلّ البيانات الواردة في الشهادة الإلكترونية.

## الفرع الثالث

## مفهوم التوثيق الإلكتروني في التشريعات الوطنية العربية

إنّ تأثير تقنيات المعلومات الحديثة على جميع المعاملات الإقتصادية دفعت بالدول العربية إلى إحداث أو تغيير منظوماتها التشريعية وفقا للقوانين الدولية النموذجية المُنَظِمَة للمعاملات الإلكترونية، وتشريعات الدول الغربية السَبَّاقَة في تنظيم معاملات التجارة الإلكترونية، والتي سنتطرق إليها على النحو التالي:

---

1) – Art 02 (LFSCSE 2003):

**a)**- « **Signature électronique**: données électroniques jointes ou liées logiquement à d'autres données électroniques et qui servent à vérifier leur authenticité. »

**(c)**- « **Signature électronique qualifiée**: signature électronique avancée fondée sur un dispositif sécurisé de création de signature au sens de l'art. 6, al. 1 et 2, et sur un certificat qualifié valable au moment de sa création. »

**g**)- « **Fournisseur de services de certification (fournisseur):** organisme qui certifie des données dans un environnement électronique et qui délivre à cette fin des certificats numériques. »

**أولا- القانون التونسي.**

تطرق المشرع التونسي من خلال الفصل الثاني من القانون عدد 83-2000 المتعلق بالمبادلات والتجارة الإلكترونية[1]، إلى منظومة إحداث التوقيع الإلكتروني التي تحتوي على مجموعة من عناصر التشفير الشخصية أو المعدات المهيأة خصيصا لإحداث التوقيع الإلكتروني بصاحبه، ومنظومة فحص التوقيع الإلكتروني التي تحتوي بدورها على مجموعة من عناصر التشفير العمومية أو المعدات التي تُمكّن من فحص التوقيع الإلكتروني، بحيث يشرف على المنظومتين(م.خ.ت.إ) يكون في هيئة أيّ شخص طبيعي أو معنوي يُحْدِثْ ويُسَلِّمْ ويَتَصَرَّفْ في شهادة المُصادقة، ويقوم بخدمات أخرى ذات صلة بالتوقيع الإلكتروني في حين يُقصد بشهادة التصديق الإلكتروني حسب نفس الفصل:" **الوثيقة الإلكترونية المؤمنة بواسطة الإمضاء الإلكتروني للشخص الذي أصدرها والذي يشهد من خلالها أثر المعاينة على صحة البيانات التي تضمنتها**".

تطبيقا لأحكام الفصل 17 من نفس القانون أصدر وزير تكنولوجيا الإتصال القرار المؤرخ في 19 جويلية2001 المتعلق بضبط المعطيات التقنية المتعلقة بشهادات المصادقة الإلكترونية والوثوق بها[2]، الذي حدّد في الفصل الثالث منه البيانات الإلزامية التي يجب أن تحتويها شهادة المصادقة الإلكترونية، كدرجتها مع الرمز الوحيد المعرف بها، وذكر هوية كلّ من المزود المُصدر لها وعنوانه مع المعرف الوحيد له، وهوية الشخص الطبيعي صاحب الشهادة أو الاسم الاجتماعي بالنسبة للشخص المعنوي صاحب الشهادة، أو اسم المجال وهوية المتصرف بالنسبة للموزعات واسم المجال، وهوية المتصرف بالنسبة للشبكات مع ذكر

---

[1] – قانون عدد 83 لسنة 2000 مُؤرخ في 9 أوت 2000 يتعلق بالمبادلات والتجارة الإلكترونية، المنشور في ر.ر.ج.ت عدد 64، الصادر في 9 أوت 2000. http://www.legislation.tn

[2] – قرار وزير تكنولوجيا الإتصال التونسي المؤرخ في 19 جويلية 2001 يتعلق بضبط المواصفات التقنية لمنظومة إحداث الإمضاء الإلكتروني، و القرار الثاني الصادر منه في نفس التاريخ والسنة يتعلق بضبط المعطيات التقنية المتعلقة بشهادات المصادقة و الوثوق بها، المنشورين في ر.ر.ج.ت عدد 60، الصادر في 19 جويلية 2001. http://www.legislation.tn

المعرف الوحيد لصاحب الشهادة، كما يجب ذكر مدة صلاحية الشهادة، مع تحديد منظومة التدقيق في توقيع كلّ من المُوقِّع ومزود الخدمة، كما يُمكن أن تتضمن كذلك الشهادة الإلكترونية البيانات الإختيارية المنصوص عليها في المواصفة الدولية (X509).

**ثانيّا- القانون الأردني.**

قام المشرع الأردني بإصدار قانون المعاملات الإلكترونية رقم 2001/85 الصادر في 11 ديسمبر 2001 لغرض تنظيم المعاملات المدنية والتجارية الإلكترونية، بحيث سوى بموجب المادة 07 منه[1] بين المحررات الإلكترونية والمحررات الكتابية من حيث القيمة القانونية في الإثبات، وحثّ(المشرع) كذلك أطراف التعامل الإلكتروني على إتباع إجراءات توثيق معتمدة ومُتفق عليها من طرفهم، تُشرف عليها جهات توثيق إلكتروني مُرخص لها بمزاولة نشاطاتها بالرغم من عدم تعريفه لها(الجهات)، إذ تنص المادة 02 من نفس القانون على أنّ إجراءات التوثيق المعتمدة تتمثل في:" **تلك الإجراءات المتبعة للتحقق من أنّ التوقيع الإلكتروني أو السجل الإلكتروني قد تم تنفيذه من شخص معين، أو لتتبع التغيرات والأخطاء التي حدثت في سجل إلكتروني بعد إنشائه، بما في ذلك إستخدام وسائل التحليل للتعرف على الرموز والكلمات والأرقام وفك التشفير والاستعادة العكسية وأيّ وسيلة أو إجراءات آخرى تُحقق الغرض المطلوب.**"

فالتوقيع الإلكتروني الموثق حسب المادتين 31 و32 من نفس القانون هو الذي ينفرد بصاحبه وكافيا للتعريف بهويته، بحيث يتم إنشاءه بوسائل خاصة به وتحت سيطرته على النحو الذي يضمن كشف أيّ تغيير في البيانات المرفقة به، فيكون السجل الإلكتروني موثوقا به ومتمتعا بالحجية الكاملة في الإثبات، إذا حمل توقيع إلكتروني موثق وفقا لإجراءات مُعتمدة ومُطابقة لرمز التعريف المبيّن في شهادة توثيق صادرة من جهة توثيق مُعتمدة ومُرخص لها بمزاولة العمل من طرف الدولة، أو جهة توثيق أجنبية مُرخصة ومُعترف بها أو

---

[1] – قانون المعاملات الأردني رقم 2001/85 المؤرخ في 11 ديسمبر 2001، الصادر في الجريدة الرسمية للمملكة الأردنية رقم 6010، في 31 ديسمبر 2001.
http://www.lob.gov.jouilawsindex.jsp

قد تكون هذه الجهة دائرة حكومية أو مؤسسة أو هيئة مُفوضة قانونا لذلك، فشهادة التوثيق الإلكتروني وفقا للمادة 02 من نفس القانون تعني:" **الشهادة التي تُصدر عن جهة مختصة مُرخصة أو معتمدة لإثبات نسبة توقيع إلكتروني إلى شخص معين استنادا إلى إجراءات توثيق معتمدة.**"

**ثالثا- القانون المصري.**

إنّ المشرع المصري لم يَعْتَرِفْ بالقيمة القانونية في الإثبات للمحررات الإلكترونية إلاّ بعد صدور قانون رقم 2004/15 الصادر في 22 أفريل 2004، المتعلق بتنظيم التوقيع الإلكتروني وبإنشاء(هـ.ت.ص.ت.م)[1]، فوفقا للمواد 14 و15 و18 منه يتضح لنا أنّه في حالة إستيفاء كلٍّ من التوقيع الإلكتروني، الكتابة الإلكترونية والمحررات الإلكترونية المُعتمدة عليها في نطاق المعاملات المدنية والتجارية والإدارية، للضوابط الفنية والتقنية التي يُحددها فيما بعد القرار المتضمن اللائحة التنفيذية، تكون لها نفس الحجية القانونية في الإثبات المقررة للكتابة والمحرّرات الرسمية والعرفية التي نص عليها قانون الإثبات في المواد المدنية والتجارية.

لذا ترك المشرع المصري مسألة تنظيم إجراءات التوثيق الإلكتروني المعتمدة للوائح التنظيمية للحكومة التي سمحت للوزير المُكَلَّفْ بالإتصالات وتكنولوجيا المعلومات، بإصدار قرار رقم 2005/109 مؤرخ في 15 ماي 2005 يتضمن إصدار اللاّئحة التنفيذية لقانون التوقيع الإلكتروني وبإنشاء(هـ.ت.ص.ت.م)[2]، بحيث تطرق من خلال المادة 19/01 إلى منظومة إنشاء التوقيع الإلكتروني التي تحتوي على مجموعة من الوسائط الإلكترونية

---

[1] – قانون رقم 2004/15 المتعلق بتنظيم التوقيع الإلكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات، المنشور في الجريدة الرسمية عدد 17، الصادر في 22 أفريل 2004. http://www.ragylaw.com~rplfegimagesfile/

[2] – قرار رقم 2005/109، المؤرخ في 15 ماي 2005، المتعلق بإصدار اللائحة التنفيذية لقانون التوقيع الإلكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات، المنشور بالوقائع المصرية عدد 115 الصادر في 25 ماي 2005. http://www.arablaw.org

والبرامج الحاسوبية، التي بواسطتها يتم التوقيع إلكترونيا على المحرر الإلكتروني بإستخدام بيانات إحداث التوقيع الإلكتروني وشهادة التصديق الإلكتروني، التي يتم بواسطتها وضع وتثبيت المحرر المُوَقَّع إلكترونيا على دعامة إلكترونية، وفقا للضوابط الفنية والتقنية المحددة بموجب المادة 03/6-7 من اللائحة، والتي تُشرف عليها جهات تصديق إلكتروني مرخص لها بإصدار شهادة التصديق الإلكتروني وتقديم خدمات تتعلق بالتوقيع الإلكتروني، في حين يكمن الدور الرئيسي لشهادة التصديق الإلكتروني في إثبات ارتباط بيانات إنشاء التوقيع الإلكتروني لصاحبه، والتي يجب أن تتضمن(الشهادة) على البيانات الواردة في المادة 20 من اللائحة التنفيذية.

فالتوقيع الإلكتروني المُصدق وفقا للمادة 09 من اللائحة التنفيذية هو الذي استند إلى منظومة أمن خاصة بإنشاء بيانات التوقيع الإلكتروني على النحو المُحدد في المواد (2-3-4) من اللائحة التنفيذية، والمُعزز بشهادة تصديق إلكتروني سارية المفعول صادرة من جهة تصديق إلكتروني مُعتمدة أو مرخص لها من طرف(هـ.ت.ص.ت.م)، والجدير بالذكر أنّ المشرع المصري فرّق بموجب المادتين 06 و07 من اللائحة بين نوعين من منظومة الفحص، فالأولى تتعلق بفحص بيانات إحداث التوقيع الإلكتروني التي يترتب عنها إصدار شهادة فحص بياناته، والثانية تتعلق بفحص التوقيع الإلكتروني الذي يتم وفقه إصدار شهادة فحص التوقيع الإلكتروني، فمنطقيا يترتب عن صدور شهادة فحص التوقيع الإلكتروني بالتبعية صحة بيانات إنشاءه، فمن الأفضل الاكتفاء بخدمة فحص التوقيع الإلكتروني[1].

**رابعا- قانون الإمارات العربية المتحدة.**

أصدرت الإمارات العربية المتحدة كدولة فيدرالية لقانون إتحادي رقم 2006/01 بشأن المعاملات والتجارة الإلكترونية، يهدف إلى إرساء مبادئ مُوَحِّدَة للقواعد واللوائح والمعايير المُتعلقة بتوثيق وسلامة المراسلات الإلكترونية، وحماية حقوق المتعاملين إلكترونيا مع تحديد

[1] – **محمد محمد سادات**، حجية المحرّرات الموقعة إلكترونيًّا في الإثبات (دراسة مقارنة)، دار الجامعة الجديدة، مصر، 2011، ص ص 129، 130.

إلتزاماتهم وتشجيع وتسهيل المعاملات والمراسلات الإلكترونية، بما فيها التجارة الإلكترونية مع تعزيز الثقة فيها وسلامتها من العراقيل المحلية والدولية عن طريق إستخدام توقيعات إلكترونية مَحْمِيَّة، بحيث تطرق من خلال المادة الأولى منه[1] إلى تعريف إجراءات التوثيق المُحكمة على أنّها:" **الإجراءات التي تهدف إلى التحقق من أنّ رسالة إلكترونية قد صدرت من أو إلى شخص معيّن، والكشف عن أيّ خطأ أو تعديل في مُحتويات أو إرسال أو تخزين رسالة إلكترونية أو سجل إلكتروني خلال فترة زمنية مُحددة، ويشمل ذلك أيّ إجراء يستخدم مناهج حسابية أو رموز أو كلمات أو أرقام تعريفية أو تشفير أو إجراءات للرد لإقرار الاستلام أو غيرها من وسائل إجراءات حماية المعلومات.**"

إنطلاقا من ذلك فإنّ إجراءات التوثيق المحكمة يُشرف عليها(م.خ.ت.إ) مرخص له من طرف هيئة تنظيم الإتصالات(TRA) بصفتها كمُراقِب على أنشطة خدمات التصديق الإلكتروني[2]، والذي(م.خ.ت.إ) يكون في هيئة أيّ شخص أو جهة مُعتمدة أو مُعترف بها تقوم بإصدار شهادات تصديق إلكتروني أو أية خدمات أو مُهِمَات متعلقة بها، وبالتوقيعات الإلكترونية المنظمة بموجب أحكام هذا القانون، وبالتالي فإنّ الهدف من إصدار شهادة التصديق الإلكتروني يتمثل في تأكيد هوية الشخص أو الجهة الحائزة على أداة إحداث التوقيع الإلكتروني، والتي يجب أن تحتوي على البيانات الواردة في المادة 3/21 من القانون الإتحادي، كهوية(م.خ.ت.إ) مع التأكيد بأنّ الشخص المُعينة هويته في الشهادة قد سيطر على أداة التوقيع المُشار إليها فيها، والتي يجب أن تكون(الأداة) سارية المفعول في أو قبل تاريخ إصدار الشهادة، مع توضيح ما إذا كانت هناك أية قيود على الغرض أو القيمة التي

---

[1] – القانون الإتحادي لدولة الإمارات العربية المتحدة رقم 2006/1 بشأن المعاملات والتجارة الإلكترونية الصادر بتاريخ 30 جانفي 2006. http://sbusiness.abudhabi.aeegovPoolPortal/

- **Les Émirats arabes** sont une **fédération de sept émirats** (Abou Dabi, Dubaï, Sharjah, Ajman, Umm al-Qaïwain, Fujaïrah et Ras al-Khaïmah), chaque émirat est gouverné par un **émir** dont le pouvoir est **héréditaire** et **absolu**, les sept émirs forment le Conseil suprême, qui constitue la plus haute instance du gouvernement fédéral. http://www.wikipédia.fr

[2] – قرار مجلس الوزراء رقم 291/8 مؤرخ في 15 أكتوبر 2006، بشأن تعيين الهيئة العامة لتنظيم قطاع الاتصالات كمراقب لخدمات التصديق الإلكتروني. http://www.government.ae

يجوز أن تُستخدم من أجلها أداة التوقيع أو الشهادة، أو ما إذا كانت هناك أيّة قيود على المسؤولية التي قبِلها(م.خ.ت.إ) تجاه أيِّ شخص.

فوفقا للمادة 1/17 من نفس القانون يكون التوقيع الإلكتروني محميًّا إذا انفرد به الشخص الذي استخدمه مع إمكانية إثبات هويته، وأن تكون بيانات إنشاءه أو وسيلة استعماله تحت سيطرته التّامة وقت التوقيع، على النحو الذي يضمن ارتباطه بالرسالة الإلكترونية المتصلة به بطريقة تُوفر تأكيدًا يُعتمد عليه حول سلامة التوقيع، بحيث إذا تم تغيير السجل الإلكتروني فإنّ التوقيع الإلكتروني يصبح غير محمي.

**خامسا- القانون العمّاني.**

قام سلطان عمّان بإصدار قانون رقم 2008/69 مؤرخ في 17 ماي 2008 يتعلق بالمعاملات الإلكترونية، الذي تطرق من خلال المادة الأولى منه إلى تعريف إجراءات التوثيق الإلكتروني على أنها:" **الإجراءات التي تهدف إلى التحقق من أنّ رسالة إلكترونية قد صدرت من شخص معين، والكشف عن أيّ خطأ أو تعديل في مُحتويات أو في إرسال أو تخزين رسالة إلكترونية أو سجل إلكتروني من خلال فترة زمنية محددة، بحيث يشمل ذلك كل إجراء يستخدم معادلات رياضية أو رموزا أو كلمات أو أرقاما تعريفية أو تشفيرا إجراءات للرد أو لإقرار التسلم أو غيرها من وسائل حماية المعلومات المماثلة.**"

أمّا(م.خ.ت.إ) الذي يُشرف على هذه الإجراءات يكون في هيئة أيِّ شخص أو جهة مُعتمدة أو مُرخص لها تقوم بإصدار شهادات تصديق إلكتروني، (تُؤكد الإرتباط بين المُوقِّع وبيانات التوقيع الإلكتروني) أو أيّة خدمات آخرى مُتعلقة بها وبالتوقيعات الإلكترونية، في حين يجب على شهادة التصديق الإلكتروني أن تحتوي على البيانات التي حددتها المادة 33 من نفس القانون[1]، كهوية(م.خ.ت.إ) مع التأكيد بأنّ المُوقّع يُسيطر في تاريخ إصدار

[1] – المرسوم السلطاني رقم 69-2008 مؤرخ في 17 ماي 2008، المتعلق بإصدار قانون المعاملات الإلكترونية، ج ر عدد 864، الصادر في 17 ماي 2008.http://www.omanlegal.org/law

الشهادة على أداة إنشاء توقيعه، كما يجب تحديد أية قيود على القيمة التي يجوز إستخدام الشهادة فيها، أو على نطاق المسؤولية التي قبلها(م.خ.ت.إ) تجاه أيّ شخص.

**سادسا- القانون الجزائري.**

بعد إعتراف المشرع الجزائري بالكتابة والتوقيع الإلكترونيين في الإثبات على إثْرِ تعديله لأحكام التقنين المدني، قام بإصدار قانون رقم 15-04 مؤرخ في 01 فيفري 2015 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين[1]، الذي تطرق من خلال المادة 4/02 منه إلى منظومة أمن إحداث التوقيع الإلكتروني، المتمثلة في أيّ جهاز أو برنامج معلوماتي معّد لتطبيق بيانات إنشاء التوقيع الإلكتروني الفريدة، كالرموز أو مفاتيح التشفير الخاصة التي يستعملها المُوقِّع في إحداث توقيعه الإلكتروني، والتي يجب أن تضمن وفقا للمادة 11 من نفس القانون سرية وأحادية البيانات المستخدمة في إحداث التوقيع الإلكتروني مع عدم اكتشافها عن طريق عملية الإستنتاج، وأن لا تُغير من البيانات التي ستُوقع أو تمنع

---

[1] – قانون رقم 15-04 مؤرخ في 01 فيفري 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، ج ر عدد 06 الصادر في 10 فيفري 2015.

– المادة 323 مكرر1 والمادة 2/327 من الأمر رقم 75-58 المؤرخ في 26 سبتمبر 1975 المتضمن القانون المدني، المعدل والمتمم.

– تجدر الإشارة أنّ المشرع الجزائري تطرق إلى بعض المسائل المتعلقة بالتوثيق الإلكتروني في المرسوم التنفيذي رقم 07-162 المؤرخ 2007/05/30 المتعلق بنظام الإستغلال المُطبق على كلّ نوع من أنواع الشبكات بما فيها اللاّسلكية الكهربائية وعلى مُختلف خدمات المواصلات السلكية واللاسلكية، ج ر عدد 37 الصادر في07 جويلية2007، المعدل والمتمم للمرسوم التنفيذي رقم 01-123 المؤرخ في 2001/05/09، ج ر عدد 27 الصادر في 2001/05/13، وذلك قبل صدور القانون رقم 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، بحيث عرف بموجب المادة 03 مكرر من المرسوم كلّ من التوقيع الإلكتروني المؤمن ولم يُعرّف التوقيع الإلكتروني البسيط، ولا التوقيع الإلكتروني الموصوف، كما أنّه لم يحدد المواصفات المتعلقة بمنظومة أمن إحداث التوقيعات الإلكترونية ولا منظومة فحصها الموثوق بها، ولم يعرف كذلك شهادة التصديق الإلكتروني الموصوفة ولم يحدد بياناتها، الخ...

من عرضها للموقِّع قبل عملية التوقيع عليها، وأن تُمكّن المُوقّع من حماية توقيعه بطريقة مؤمنة.

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

إنطلاقا من ذلك ميّز المشرع الجزائري بين التوقيعات الإلكترونية وفقا لمستويات أمان معينة، فالتوقيع الإلكتروني البسيط (Signature électronique simple) وفقا للمادة 02 منه يحتوي على بيانات إلكترونية مرفقة أو مرتبطة منطقيا بالبيانات الإلكترونية الآخرى لإستعمالها كوسيلة توثيق، بينما التوقيع الإلكتروني الموصوف (Signature électronique qualifiée) وفقا للمادة 07 من نفس القانون يعني التوقيع الإلكتروني المؤمن الذي تم إحداثه على أساس شهادة تصديق إلكتروني موصوفة، بموجب آلية أمن إنشاء التوقيعات الإلكترونية الموضوعة تحت سيطرة المُوقِّع لوحده، بوساطة جهة توثيق إلكتروني مرخص لها من طرف الجهات الرسمية لمزاولة نشاطاتها.

بالإضافة إلى ذلك ميّز المشرع الجزائري بموجب المادة 12-11/02 من نفس القانون بين نوعين من سلطات التصديق الإلكتروني بحسب القطاع(الخاص أو العام) الذي تُمَارَسْ فيه خدمات التصديق، فـ(م.خ.ت.إ) يُقصد به كلّ شخص طبيعي أو معنوي يقوم بمنح شهادات تصديق إلكتروني موصوفة، وقد يقدم خدمات أخرى في مجال التصديق الإلكتروني، أمّا "الطرف الثالث الموثوق" يتمثل في هيئة شخص معنوي يقوم بمنح شهادات تصديق إلكتروني موصوفة، وقد يقدم خدمات آخرى متعلقة بالتصديق الإلكتروني لفائدة المتدخلين في الفرع الحكومي، كالمؤسسات والإدارات العمومية والهيئات العمومية المحددة في التشريع المعمول به، والمؤسسات الوطنية المستقلة وسلطات الضبط، والمتدخلون في

المبادلات ما بين البنوك، وكذا كلّ شخص أو كيان ينتمي إلى الفرع الحكومي بحكم طبيعته أو مهامه[1].

كما أنّ شهادة التصديق الإلكتروني حسب المشرع تنقسم إلى نوعين، فالأولى يُقصد بها الشهادة الإلكترونية البسيطة المتمثلة وفقا للمادة 7/02 من نفس القانون، في وثيقة إلكترونية تثبت الصلة بين بيانات التحقق من التوقيع الإلكتروني والموقّع، أمّا شهادة التصديق الإلكتروني الموصوفة وفقا للمادة 15 من نفس القانون، تتمثل في شهادة التصديق الإلكتروني التي يُصدرها الطرف الثالث الموثوق أو(م.خ.ت.إ)، للموقّع دون سواه وفقا للمواصفات المحددة في الفقرة الثالثة من نفس المادة(3/15).

فمن خلال إستعراضنا لكلّ ما سبق نصل إلى أنّ التشريعات الدولية والوطنية المُنظمة للمعاملات الإلكترونية، اعتمدت على مُستويات معينة من الأمان في اختيار التكنولوجيا المناسبة للتوثيق الإلكتروني، فبإستثناء قوانين الأونسيترال النموذجية المتعلقة بالتجارة الإلكترونية والتوقيعات الإلكترونية وكذا التشريعات الإتحادية، التي التزمت الحياد التكنولوجي في إشتراط مُستويات مُعينة من الأمان والثقة إزاء طرق التوثيق الإلكتروني، فإنّ التوجيه الأوروبي المتعلق بالتوقيع الإلكتروني وتشريعات دول أعضاءه وتشريعات الدول العربية، قد أخذت بنهج المُستويين أو الشقين الذي حُظيت فيه طرق التوثيق الإلكتروني(التوقيعات الإلكترونية البسيطة) بحد أدنى معيّن من المفعول القانوني من جهة، ومن جهة آخرى منحت بعض طرق التوثيق الإلكتروني ذات مُستويات أمان عالية مفعولا قانونيا أكبر(التوقيعات الإلكترونية الموصوفة)، مما يتيح المجال لاستيعاب مُختلف التطورات التكنولوجية المستقبلية.

[1] – المادة 13/02 من قانون رقم 15-04، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين.

## الفرع الرابع

## المفهوم الفقهي والقضائي للتوثيق الإلكتروني

ركز الفقه لدى تعريفه للتوثيق الإلكتروني على جهات التصديق الإلكتروني بصفتها كأطراف ثالثة محايدة تشرف على إتاحة إجراءات التوثيق الإلكتروني المعتمدة، كما أنّ للقضاء دور كبير في إثبات القيمة القانونية لإجراءات التصديق الإلكتروني الموثوق بها.

**أولا: التعريف الفقهي للتوثيق الإلكتروني.**

هناك من الفقهاء الذين عرّفوا جهات التصديق الإلكتروني على أنّها[1]:" **كلّ جهة أو مُنظمة عامة أو خاصة تستخرج شهادة إلكترونية، وهذه الشهادة تُؤمن صلاحية الموقع أو حجية توقيعه وتُؤكد هوية الموقع وتُمكنه من معرفة المفتاح العام.**"

أمّا الجانب الآخر من الفقه عرفها على أنّها[2]:" **شركات أو أفراد أو جهات مُستقلة ومُحايدة تقوم بدور الوسيط بين المتعاملين لتوثيق معاملاتهم الإلكترونية، فتُعد طرفا ثالثا مُحايداً.**"

كما عرّفها الفقهاء الآخرون على أنّها[3]:" **هيئة عامة أو خاصة، تعمل على ملء الحاجة إلى وجود طرف ثالث موثوق في التجارة الإلكترونية، بأن يصدر شهادات تثبت صحة حقيقة معينة متعلقة بموضوع التبادل الإلكتروني، كتأكيد نسبة التوقيع الإلكتروني إلى شخص معين، وتأكيد نسبة المفتاح العام المُستخدم إلى صاحبه.**"

---

[1] – **خالد مصطفى فهمي**، النظام القانوني للتوقيع الإلكتروني في ضوء الاتفاقيات الدولية والتشريعات العربية، دار الجامعة الجديدة، الإسكندرية، 2007، ص 148.

[2] – **إبراهيم خالد ممدوح**، التوقيع الإلكتروني، دار الجامعية، الإسكندرية، 2010، ص 172.

[3] – **علاء محمد عيد نصيرات**، حجية التوقيع الإلكتروني في الإثبات (دراسة مقارنة)، الطبعة الأولى، عمّان، دار الثقافة للنشر والتوزيع، 2005، ص ص 145، 146.

من خلال التعريفات السابقة يتضح لنا أنّ جهات التصديق الإلكتروني يمكن أن تكون في هيئة شخص طبيعي أو معنوي محايد ومؤتمن به، يشرف على خدمات إصدار شهادات توثيق التوقيعات الإلكترونية في إطار نماذج الثقة المتبعة في التصديق الإلكتروني.

**ثانيًا: المفهوم القضائي للتوثيق الإلكتروني.**

اعترفت محكمة النقض الفرنسية بالتوقيع الإلكتروني في صورة رقم سرّي مُرفق في بطاقة الدفع المُمَغنطة كوسيلة في الإثبات، في قراريها الصادرين في 08 نوفمبر 1989 حول قضية(Crédicas)[1]، التي أسستهما وفقا للمادتين 1134 و1341 من التقنين المدني الفرنسي حول الإثبات اللتان تُعتبران كقواعد مُكملة غير آمرة، الشيء الذي دفع بالقضاة والفقهاء إلى الإعتراف إجماعا حول إمكانية أطراف العلاقة العقدية الإتفاق حول وسيلة إثبات معينة[2]، وإنطلاقا من ذلك قررت محكمة النقض في تقريرها السنوي لعام 1989 أنّ التوقيع المعلوماتي(Signature informatique) الذي تم وفقا للإجراءات الحديثة، يُقدم الضمان والثقة التي يُوفرها التوقيع الخطي ما لم يفوقه بكثير، حيث أنّ الرقم السري للبطاقة البنكية لا يعرفها إلاّ صاحبها[3].

لكن محكمة النقض الفرنسية لم تبقى عند هذا الحدّ، بل ذهبت بعيدا في مسألة الإعتراف بالتوقيع الإلكتروني الموثق في الإثبات، وذلك في قرارها الصادر في 30 سبتمبر 2010[4] أين ألغت قرار محكمة الإستئناف ديجون(Dijon) الصادر في 02 ديسمبر 2008، بحيث

---

1) - **Cass. Civ, 1ère chambre**, du 8 novembre 1989, pourvoi n° 86-16196. Bulletin 1989, I, N° 342.
- **Cass. Civ, 1ère chambre**, du 8 novembre 1989, pourvoi n° 86-16197. Bulletin 1989, I, N° 342. http://www.legifrance.gouve.fr

2) – **Art. 1316-2** du code civil Français **: «** lorsque la loi n'a pas fixé d'autres principes, et à défaut de convention valable entre les parties, le juge règle les conflits de preuve littérale en déterminant par tous les moyens, le titre le plus vraisemblable, quelqu'en soit le support **.»**

3) – **Alain BENSOUSSAN et Charles COPIN**, Le livre blanc de la signature électronique, pp. 33, 34. Article disponible sur : http://www.alain-bensoussan.com

4) - **Cass. Civ, 1ère chambre**, du 30 septembre 2010, pourvoi n° 09-68555. Bulletin 2010, I, n° 178. http://www.legifrance.gouve.fr

أسست قرار النقض وفقا للمواد 1315، 1316-1، 1316-4، 1324 من التقنين المدني الفرنسي، التي أكدّت فيه أنّ التوقيع الإلكتروني الموثق المُحدث وفقا لمنظومة أمن إحداث التوقيعات الإلكترونية، والمعزز بشهادة تصديق إلكتروني موصوفة صادرة من جهات توثيق إلكتروني مُعتمدة يضفيه الحجية القانونية في الإثبات، ومن ثمة فإنّ محكمة الإستئناف قد أغفلت في قرارها أحكام المواد 1315، 1316-1، 1316-4، 1324 من التقنين المدني الفرنسي المتعلقة بالتوقيع الإلكتروني الموصوف، كما أنّ محكمة الإستئناف لم تُراعي في قرارها أحكام المادة 287 من تقنين الإجراءات المدنية الفرنسية، التي تلزم القضاة في حالة ما إذا أنكر أحد الأطراف الإعتراف بالكتابة أو التوقيع الإلكترونيين، بالتحقق من مدى إستيفاء كلّ من الكتابة والتوقيع الإلكترونيين للشروط التي نصت عليها أحكام المادتين 1316-1 و1316-4 من التقنين المدني الفرنسي[1].

فمن خلال القرارات السابقة لمحكمة النقض الفرنسية نفهم أنّ القضاء الفرنسي اعترف بالتوقيع الإلكتروني الموصوف الذي تم إحداثه وفقا لمنظومة أمن إنشاء التوقيعات الإلكترونية، بوساطة(م.خ.ت.إ) معتمد في إطار مخطط الإعتماد الاختياري، كما منحته الأولوية من حيث القيمة القانونية في الإثبات بالمقارنة مع التوقيع الإلكتروني البسيط.

إنطلاقا من كلّ ما سبق من تعريفات يُمكننا تعريف التوثيق الإلكتروني[2]على أنّه:" **وسيلة فنيّة آمنة للتحقق من صحة التوقيع أو المحرر الإلكتروني، بحيث يتم نسبته إلى شخص أو كيان مُعيّن بوساطة جهة محايدة موثوق بها، يُطلق عليها إسم مقدم خدمات التصديق الإلكتروني أو الطرف الثالث الموثوق به.**"

---

1) - **Art. 287** du Code de procédure civile français dispose : « [...] Si la dénégation ou le refus de reconnaissance porte sur un écrit ou une signature électronique, le juge vérifie si les conditions, mises par les articles **1316-1 et 1316-4** du code civil à la validité de l'écrit ou de la signature électroniques, sont satisfaites. » http://www.legifrance.gouve.

2) – **أسامة بن غانم العبيدي**، "التصديق الإلكتروني وتطبيقاته في النظام السعودي"، المجلة القضائية، الرياض، عدد 04، 1433هـ، ص 179. http://adl.moj.gov.sa/Alqadaeya

## المطلب الثاني

## أهمية التصديق الإلكتروني

تكمن أهمية التصديق الإلكتروني من خلال الجوانب الأمنية للمعاملات الإلكترونية(الفرع الأول)، وفي شهادات التصديق الإلكتروني التي تُصدرها جهات التوثيق الإلكتروني المعتمدة(الفرع الثاني)، والتي تستوجب الإعتراف القانوني بالشهادات الأجنبية(الفرع الثالث) في إطار نماذج الثقة المتبعة في التصديق الإلكتروني(الفرع الرابع).

### الفرع الأول

### الجوانب الأمنية للتصديق الإلكتروني

تضمن عملية التصديق الإلكتروني ثلاثة جوانب أمنية رئيسية لضمان تبادل المعلومات عبر شبكة الإنترنيت والمتمثلة في:

**أولا- تحديد هوية أطراف المعاملة الإلكترونية: (Identification+Authentification)**

إنّ الغرض من التوثيق يتمثل في تأكيد وإثبات صحة واقعة أو تصرف قانوني معين بعد التحقق منه(ها)، بجميع الوسائل والإمكانيات المتاحة للقائم بعملية الفحص باعتباره كطرف محايد ومعتمد أو مرخص له من طرف الجهات الرسمية في الدولة، لمزاولة خدمات التصديق على المحررات(كتابية أم إلكترونية) مما يضفيها القيمة القانونية في الإثبات أمام العدالة.

إنطلاقا من ذلك فإنّ إعتماد أطراف العلاقة الإلكترونية على آليات التشفير لوحدها في تبادل معطياتهم الإلكترونية في بيئة إلكترونية إفتراضية، لا تضمن كشف وتحديد وإثبات هوية كلٍّ منهم، مما تدفع بهم الحاجة إلى حتمية التعويل على خدمات طرف ثالث محايد وموثوق به، يقوم بعد التحقق من هويتهم وصفاتهم الخ...، بجميع الوسائل المتاحة له في إطار عقد تقديم خدمة التصديق الإلكتروني، بإتاحتهم لمعدات وأنظمة أمن تكنولوجيا معلومات موضوعة تحت سيطرتهم، التي من خلالها تُتِيح منظومة أمن إحداث التوقيع

الإلكتروني أثناء مراحل إحداثه، لزوج مفاتيح التشفير الخاص والعام الذي يُعول عليهما برنامج الحاسوب في عملية تشفير قيمة الهاش الأصلية الأحادية الاتجاه[1]، المتعلقة ببيانات الرسالة الإلكترونية على النحو الذي لا يُمكن كشفها عن طريق عملية الإستنباط أو الإستنتاج(Déduction)، ولتأكيد ارتباط التوقيع الإلكتروني بهوية صاحبه تقوم جهة التوثيق الإلكتروني المعتمدة بتعزيزه بشهادة تصديق إلكتروني موصوفة، التي تُعتبر بمثابة وثيقة إثبات هوية الموقع (بطاقة التعريف الوطنية أو جواز السفر)[2].

**ثانيا– ضمان سلامة وسرية محتوى البيانات المتداولة: (Intégrité-Confidentialité)**

إنّ ضمان سلامة وسرية بيانات الرسالة الإلكترونية يعتبر من بين الأهداف الرئيسية التي يسعى أطراف التصرف الإلكتروني إلى تحقيقها، لذا يجب عليهم الإستعانة بأدوات إنشاء توقيعات إلكترونية مؤمنة تضمن في سرية تامة أُحادية اتجاه بيانات إنشاء التوقيع لمرة واحدة فقط، على نحو تُمكِّن من كشف أيّ تغيير أو تعديل يمس بمُحتوى البيانات

---

[1] – عبارة عن منهج يُعتمد عليه في عملية إنشاء التوقيعات الإلكترونية والتثبت من صحتها، إذْ يعمل على إنشاء تمثيل رقمي معين أو بصمة على شكل قيمة أو نتيجة هاش، بمقياس طوله أصغر من الرسالة الإلكترونية ولكنه مُقترنا ومحصورا بها، وكلّ تغيير في الرسالة ينتج عنه قيمة هاش مُختلفة عند إستخدام وظيفة الهاش نفسها. لمزيد من التفاصيل أنظر دليل تشريع قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية لعام 2001، ص ص 28، 29.

[2] - **Marc LACOURSIÈRE et Édith VÉZINA**, « La sécurité des opérations bancaires par Internet », 41 R.J.T. 89. 2007, pp. 98, 99. Disponible sur : www.themis.umontreal.ca

– **إبراهيم الدسوقي أبو الليل**، توثيق التعاملات الإلكترونية ومسئولية جهة التوثيق تجاه الغير المضرور، المجلد الخامس. ص ص 1828، 1829. **نجوى أبو هيبة**، التوقيع الإلكتروني (تعريفه–مدى حجيته في الإثبات)، المجلد الأول. ص ص 449، 450. بحثان مقدمان في مؤتمر الأعمال المصرفية بين الشريعة والقانون، الذي نظمته كلية الشريعة والقانون في جامعة الإمارات العربية المتحدة، بالتعاون مع غرفة التجارة الإلكترونية وصناعة دبي، في 10 و12 ماي 2003. http://slconf.uaeu.ac.aearabic_prev_conf2003.asp

– **سعيد السيد قنديل**، التوقيع الإلكتروني: ماهيته– صوره– حجيته في الإثبات بين التداول والإقتباس، الطبعة الثانية، دار الجامعة الجديدة للنشر، الإسكندرية، 2006، ص ص 74، 75.

الإلكترونية بعد التوقيع عليها، لذا يقوم صاحب الرسالة الإلكترونية الأصلية قبل توقيعها بإعدادها عن طريق تعيين أو تحديد كافة المعلومات المتصلة بها، قصد السماح لدالة البعثرة (الهاش) المعينة في حاسوبه بإحتساب قيمة الهاش الأصلية المقتصرة على الرسالة، من أجل تشفيرها بإحدى خوارزميات المفتاح العام وتحويلها إلى توقيع إلكتروني بإستعمال المفتاح الخاص للمُوَقِّعْ.

فبواسطة شهادة التصديق الإلكتروني يباشر برنامج حاسوب مُتَلَقِّي الرسالة الإلكترونية الأصلية لعملية فحص مدى مطابقة بيانات فحص التوقيع الإلكتروني لبيانات إحداثه، عن طريق إعادة احتساب قيمة هاش جديدة لغرض التأكد من مُطابقتها لنتيجة الهاش الأصلية التي تم تحويلها لتوقيع إلكتروني موصوف، فإذا توصل الحاسوب إلى تحصيل نفس قيمة الهاش فيعني عدم تعرض البيانات الإلكترونية الموقعة لما يثير الشبهة فيها[1].

**ثالثا– ضمان عدم إنكار رسالة البيانات المتداولة: (Non-Répudiation)**

تُعتبر العقود المبرمة عن طريق الويب الأكثر إشاعةً واستخداما في مجال إبرام مُختلف صفقات التجارة الإلكترونية عبر الإنترنيت، التي من خلالها يتبادل أطراف العقد الإلكتروني الوثائق والبيانات في بيئة إلكترونية إفتراضية مملوءة بالمخاطر[2]، الشيء الذي يدفعهم إلى الإستعانة بخدمات(م.خ.ت.إ) محايد ومعتمد يقوم بتأمين المواقع الإلكترونية، مع تزويد

---

1) - **Thierry-PIETTE COUDOl**, La signature électronique (Introduction technique et juridique à la signature électronique sécurisée, preuve et écrit électronique), Edition Litec, Paris, 2001, pp. 26, 61.
- **Garance MATHIAS et Jean-Michel SAHUT**. le paiement : enjeu du e – commerce, p. 227. Article disponible sur : http://piae.univ-larochelle.frimg/

2)– **يونس عرب**، قانون تقنية المعلومات والتجارة العالمية، ص ص57، 58، 82. ونفس المؤلف، العقود الإلكترونية– أنظمة الدفع والسداد الإلكتروني، ص ص 112–114. مقالان منشوران على الموقع التالي: http://www.arablaw.org

– **مناني فرح**، أدلة الإثبات الحديثة في القانون، دار الهدى للطباعة والنشر، الجزائر، 2008، ص ص 87، 145. **نفس المؤلف**، العقد الإلكتروني وسيلة إثبات حديثة في القانون المدني الجزائري، دار الهدى للطباعة والنشر، الجزائر، 2009، ص ص 196، 197.

توقيعاتهم بشهادات تصديق إلكتروني موصوفة تضمن سلامة وصحة البيانات الإلكترونية المتداولة في وقت أو قبل إصدارها مع عدم إنكارها، لذا يجب على المرسل والمرسل إليه الإلتزام بحفظ الشهادة في شكلها الإلكتروني على أيّ حامل إلكتروني بطريقة مؤمنة، مع احتفاظ (م.خ.ت.إ) بشكلها النهائي في نظام حفظ مؤمن خاص بها يسمح بالرجوع إليها عند الحاجة.

## الفرع الثاني

## أنواع شهادات التصديق الإلكتروني

إنّ(م.خ.ت.إ) يُصدرون شهادات تصديق إلكتروني بِحَسَبِ الأغراض التي تُستعمل من أجلها في إطار المعاملات الإلكترونية، لذا قامت مُختلف التشريعات الوطنية بتصنيف شهادات التصديق الإلكتروني التي يُمكن لـ(م.خ.ت.إ) إصدارها في مجال المعاملات الإلكترونية، إلى أربعة أصناف وفقا لمستويات معينة من الأمان والمتمثلة في:

### 1- شهادة الإمضاء الإلكتروني: (Certificat de signature)

تسمى كذلك بالشهادة الشخصية[1] ويُقصد بها شهادة توثيق التوقيع الإلكتروني التي تربط هوية صاحب الشهادة بمفتاح عمومي، إذ يُعول عليها المُوقِّع في إثبات هويته وتأكيد صحة ونسبة بيانات إحداث توقيعه الإلكتروني، كما يُعول الطرف المُستقبل للرسالة الإلكترونية على الشهادة من أجل التعرف على هوية كلٍّ من المُوَقِّعْ و(م.خ.ت.إ) المُصدر لها، والتأكد من وجود صلة بين بيانات إنشاء التوقيع الإلكتروني وصاحبه، فعن طريقها يقوم برنامج الحاسوب إعادة احتساب قيمة هاش جديدة من أجل مطابقتها لقيمة الهاش

[1] – الفصل 07 في الباب الثالث من الأمر عدد 1667- 2001 المؤرخ في 17 جويلية 2001، يتعلق بالمصادقة على كرّاس الشروط الخاص بممارسة نشاط مزود خدمات المصادقة الإلكترونية، منشور في (ر.ر.ج.ت) عدد 60، الصادر في 27 جويلية 2001.

المستخدمة في إحداث التوقيع الإلكتروني للمرسل، فإذا توصل إلى تحصيل قيمة هاش مُطابقة لقيمة الهاش الأصلية فيعني عدم تعرض البيانات الإلكترونية لما يُثير الشبهة فيها.

### 2- شهادة مُوزع ويب: (Certificat serveur -Web)

تُسمى كذلك بشهادة التصديق الجذرية التي تُصدرها سلطة التصديق الرئيسية الأعلى درجة على مُستوى مرفق المفاتيح العمومية، إذ تمكن من تحديد هوية مُوزع الويب والتصديق على مُحتواه، عن طريق إتفاق سلطة التصديق الإلكتروني مع الخادم أو موزع ويب(serveur) حول قبول والاعتراف بشهادة التصديق الرئيسية لها، التي تربط هوية الموزع بمفتاح عمومي يسمح بتبادل البيانات الإلكترونية بين الموزع وعملائه في إطار مناخ ثقة آمن، إذ يقوم المتعامل الإلكتروني بتثبيت(Installer) الشهادة على برنامج حاسوبه من أجل تأمين عمليات البيع والشراء أو التبادل أو الدفع الإلكتروني، عبر موقع تجاري من دون إطلاق الموزع أو الخادم لرسائل تحذير على جهاز الحاسوب[1].

### 3- شهادة الشبكة: (Certificats VPN)

تُمكن هذه الشهادة من تحديد هوية الشبكات الخاصة الإفتراضية وتضمن سلامة جميع المبادلات التي تتم عبرها، عن طريق ربط المعلومات المتعلقة ببعض المواقع على شبكة معينة (محولات routeurs، جدران نارية firewalls، مركزات concentrateurs...) بالمفتاح العمومي، ويتم استخدام هذه الشهادة لضمان سلامة المبادلات بين منظمة وفروعها الموزعة

---

1) - Plusieurs **autorités de certification** ont conclu des ententes avec les principaux **navigateurs** Internet afin que leurs **certificats racines** y soient installés par défaut, le logiciel d'exploitation Windows XP contient 107 certificats racines pré-installés provenant de **22 autorités de certification**, lorsqu'un **certificat racine est installé par défaut**, le terminal de l'usager le reconnaît et n'affiche aucune **alerte de sécurité**. Le seul indice que ce dernier vient d'entrer en communication sécurisée est l'apparition de l'icône de sécurité dans le bas de l'écran. Lorsqu'un usager doit franchir les étapes d'installation d'un certificat racine, il acquiert une certaine connaissance des **engagements** pris par l'autorité de certification envers les utilisateurs qui acceptent de faire **confiance** à ses certificats. **Marc LACOURSIÈRE et ÉDITHE Vézina**, op.cit., pp. 126, 127.

**- Louise MARTEL et René ST-GERMAIN**, « la Certification de Conformité des Sites Web », HEC Montréal / Gestion, 2002/5 Vol. 27, pp. 91, 92. http://www.cairn.info/revue-gestion-2002-5-page-91.htm

جغرافيا عبر مسالك مؤمنة في شبكة الاتصالات، كما تسمح (الشهادة) بإقامة علاقة ثقة بين المحترف والمُستهلك في إطار مناخ آمن عبر شبكة الإنترنيت.

**4- شهادة إمضاء الرمز: (Certificat de signature de code)**

تسمح بالإمضاء على أيّ برنامج أو نص أو برمجية لضمان تعريفه بتوقيع صاحبه، كما تمكن من حمايته ضد مخاطر القرصنة.

## الفرع الثالث

## الإعتراف بشهادات التصديق الأجنبية

من بين العقبات الرئيسية التي تعرقل إستخدام تقنيات التوثيق الإلكتروني عبر الحدود نجد عدم قابليتها للتشغيل فيما بين مرافق المفاتيح العمومية، وذلك من جرّاء التنازع أو التباين في المعايير وعدم الاتساق في تنفيذها، لذا قامت مختلف التشريعات الدولية والجهوية والوطنية بتنظيم المسائل المتعلقة بالإعتراف بالتوقيعات وشهادات التصديق الإلكتروني الصادرة من جهات أجنبية مُعتمدة، والتي سنتطرق إليها على النحو التالي:

**أولا- في التشريعات الدولية.**

**1- قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية لعام 2001:**

أرست أحكام المادة 1/12(أ)،(ب) من قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية لعام 2001، مبدأ أساسي للاعتراف بالشهادات والتوقيعات الأجنبية المتمثل في عدم الأخذ بعين الإعتبار الموقع الجغرافي، الذي تمت فيه عملية إصدار الشهادة أو أنشأ وأستُخدم فيه التوقيع الإلكتروني، أو المَوْقِعْ المُرتبط بمكان عمل المُصْدِرْ أو المُوَقِّعْ، وإلى جانب هذا المبدأ وضعت الفقرات الثانية والثالثة والرابعة من نفس المادة(12/2-3-4) معيار عام يرتكز على الحد الأدنى للتكافؤ التقني للشهادات الأجنبية، الذي يعتمد على اختبار تقييم قابلية التعويل عليها وفقا للشروط الموثوق بها في كلّ دولة، كما يجب أن يُطبق المعيار دون الأخذ بعين الإعتبار لطبيعة مُخطط التصديق الإلكتروني المُطبق في الدولة

التي صُدرت منها الشهادة أو التوقيع الإلكتروني، قصد التقليل من التنقلات التي تُشكل عبئ على(م.خ.ت.إ) الذين يضطرون في كلّ مهام إلى الحصول على التراخيص من كلّ دولة.

بالإضافة إلى ذلك فإنّ(م.خ.ت.إ) يصدر شهادات تصديق ذات مُستويات مُتفاوتة من قابلية التعويل عليها وفقا للغرض الذي تُستخدم فيه كلّ شهادة، كما أنّ مفعولها القانوني يتفاوت على المستوى الداخلي أو الخارجي لكلّ دولة، لذا ينبغي الأخذ بعين الإعتبار أثناء اختبار تقييم قابلية التعويل على الشهادات الأجنبية، مُستوى التكافؤ في الرتب على أساس الشهادات المُتشابهة وظيفيا، في حين يمكن لسلطات التصديق الرئيسية وفقا للفقرة الخامسة من نفس المادة(5/12) أن تقوم بإبرام إتفاقات الثقة أو الإعتراف المتبادل عبر الحدود بشأن إستخدام أنواع معينة من التوقيعات الإلكترونية أو شهادات التصديق، من دون إخضاعها لاختبار التكافؤ الجوهري لقابلية التعويل[1].

## 2- التوجيه الأوروبي رقم 99- 93 المتعلق بالتوقيع الإلكتروني:

نصت المادة 1/07 من التوجيه الأوروبي رقم 93/99 المتعلق بالتوقيعات الإلكترونية على ثلاثة حالات للاعتراف بشهادات التصديق الإلكتروني الصادرة من طرف(م.خ.ت.إ) المقيم خارج نطاق الإتحاد الأوروبي[2]، فالحالة الأولى تتمثل في قيام(م.خ.ت.إ) معتمد مقيم في دولة عضوة في الإتحاد، بضمان شهادة التصديق الأجنبية الصادرة من(م.خ.ت.إ) أجنبي في إطار اتفاقية التصديق المتبادل، وأمّا الحالة الثانية تتعلق في حصول(م.خ.ت.إ) الأجنبي على إعتماد اختياري في دولة عضوة في الإتحاد، والحالة الأخيرة تتعلق بتواجد إتفاق ثنائي أو مُتعدد الأطراف بين الإتحاد الأوروبي والبلدان الآخرى أو منظمات دولية حول الإعتراف بشهادات التصديق أو(م.خ.ت.إ).

---

[1] – راجع المادة 12 من قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية لعام 2001 مع دليله التشريعي، ص ص 85-88.

[2] - Directive 1999/93/CE du Parlement Européen et du Conseil sur un cadre communautaire pour les signatures électroniques. http://www.ec.europa.eu

**ثانيا– في التشريعات الوطنية الأجنبية.**

**أ– القانون الفرنسي:**

كرّس المشرع الفرنسي الأحكام الواردة في المادة 1/07 من التوجيه الأوروبي رقم 99–93 المتعلق بالتوقيعات الإلكترونية، في المادة الثامنة(08) من المرسوم رقم 2001–272 المؤرخ في 30 مارس 2001 المتعلق بالتوقيع الإلكتروني، التي نظمت حالات الإعتراف بشهادات التصديق الإلكتروني الأجنبية الصادرة من(م.خ.ت.إ) الغير المُقيمين في نطاق الإتحاد الأوروبي، فالحالة الأولى تتمثل في إستيفاء(م.خ.ت.إ) الأجنبي للشروط الواردة في الفقرة الثانية من المادة السادسة(06/II) من نفس المرسوم، وأن يتحصل على الإعتماد الاختياري من أيّة دولة عضوة في الإتحاد الأوروبي، وأمّا الحالة الثانية تتمثل في أن يضمن(م.خ.ت.إ) المعتمد المقيم في نطاق الإتحاد الأوروبي، شهادة التصديق الصادرة من(م.خ.ت.إ) الأجنبي في إطار اتفاقية التصديق المتبادل، والحالة الأخيرة تتمثل في أن يتم الإعتراف بالشهادات الأجنبية في إطار إتفاق يكون الإتحاد الأوروبي عضوا فيه.

**ب– القانون الفيدرالي السويسري:**

كلّف المشرع الفيدرالي السويسري بموجب المادة 1/19 من قانون التوقيع الإلكتروني لعام 2003(SCSE) المجلس الفيدرالي السويسري، بمهمة إبرام إتفاقيات دولية حول الإعتراف بشهادات التصديق الإلكتروني الموصوفة التي يُصدرها(م.خ.ت.إ) الأجانب، الذين تتوافر فيهم الشروط المنصوص عليها في المادة 1/3 من نفس القانون، وتُضيف الفقرة الثانية من نفس المادة[1] حالة ما إذا تم الإعتراف بهم من طرف مراكز إعتراف أجانب يُمكن

---

[1] –**Art.03/2** (LFSCSE du 19 décembre 2003) :- « [...] Lorsqu'un fournisseur étranger a déjà obtenu une reconnaissance de la part d'un organisme de reconnaissance étranger, l'organisme de reconnaissance suisse peut le reconnaître s'il est prouvé que:
**a)-** la reconnaissance a été octroyée selon le droit étranger;
**b)-** les règles du droit étranger applicables à l'octroi de la reconnaissance sont équivalentes à celles du droit suisse;
**c)-** l'organisme de reconnaissance étranger possède des qualifications équivalentes à celles qui sont exigées d'un organisme de reconnaissance suisse;

لمراكز الإعتراف السويسرية أن تعترف بخدماتهم إذا أثبتوا أنّ الإعتراف بخدماتهم تم وفقا لأحكام قانون أجنبي مُماثل لأحكام القانون السويسري، وأنّ مراكز الإعتراف الأجنبية تتمتع بنفس المؤهلات المفروضة على مراكز الإعتراف السويسرية مع ضمان التعاون فيما بينها من أجل رقابة نشاطات(م.خ.ت.إ) الأجانب في سويسرا.

**ثالثا- التشريعات الوطنية العربية:**

**أ- القانون التونسي:**

نص المشرع التونسي في الفصل 23 من القانون رقم 83-2000 بشأن المبادلات والتجارة الإلكترونية، على اعتبار الشهادات المُسَلَّمَة من(م.خ.ت.إ) مقيم في بلد أجنبي كشهادات مُسلّمة من(م.خ.ت.إ) تونسي، إذا تم الإعتراف بهذا الهيكل في إطار اتفاقية إعتراف مُتبادل أبرمتها(و.و.م.إ)، وهذا ما أكدّه نص الفصل 14 من الأمر عدد 1667-2001 المتعلق بالمصادقة على كراس الشروط الخاص بممارسة نشاط (م.خ.م.إ):" **يلتزم مزودي خدمات المصادقة الإلكترونية بقبول جميع الشهادات الصادرة عن مُزودي خدمات مصادقة إلكترونية مُتواجد ببلد أجنبي، تم الإعتراف به في إطار اتفاقية إعتراف مُتبادل تُبرمها الوكالة الوطنية للمصادقة الإلكترونية. تَمُدُّ الوكالة الوطنية المزودين بقائمة الاتفاقيات المبرمة في الغرض وتتعهد بتحيينها كلما أبرمت اتفاقية جديدة.**"

**ب- القانون المصري:**

نص المشرع المصري بموجب أحكام المادة 21 من اللائحة التنفيذية المتعلقة بالتوقيع الإلكتروني على الحالات التي تسمح بالإعتراف بشهادات التصديق الأجنبية، والتي من خلالها يمكن لـ(هـ.ت.ص.ت.م) أن تعترف تلقائيا بنفسها، بشهادات التصديق الإلكتروني الصادرة من جهات توثيق إلكتروني أجنبية مرخص لها في مصر بمُزاولة نشاط إصدار شهادات التصديق الإلكتروني، أو في حالة ما إذا كانت الجهة الأجنبية ضمن الجهات التي

---

**d)-** l'organisme de reconnaissance étranger garantit sa collaboration à l'organisme de reconnaissance suisse pour la surveillance du fournisseur en Suisse. » http://www.admin.chopcfrclassified-compilation20011277index.html

وافقت دولة مصر بموجب اتفاقية دولية، أو في حالة إبرام(هـ.ت.ص.ت.م) لاتفاقية الإعتراف المتبادل مع جهة الترخيص الأجنبية المثيلة لها في هرم مرفق المفاتيح العمومية.

**ج- القانون الجزائري:**

كلّف المشرع الجزائري بموجب المادة 3/18 من القانون رقم 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين،"السلطة الوطنية للتصديق الإلكتروني" بمهمة إبرام إتفاقيات الإعتراف المتبادل مع سلطات التصديق الأجنبية المثيلة لها[1]، لغرض ضمان قابلية التشغيل البيني من الناحية التقنية لشهادات التصديق الأجنبية والتوافق في السياسة العامة المنظمة لها بين نطاقات المرافق العمومية المعنية، وهذا ما أكدته نص المادة 63 من نفس القانون:" **تكون لشهادات التصديق الإلكتروني التي يمنحها مؤدي خدمات التصديق الإلكتروني المقيم في بلد أجنبي، نفس قيمة الشهادات الممنوحة من طرف مؤدي خدمات التصديق الإلكتروني المقيم في الجزائر، بشرط أن يكون مؤدي الخدمات الأجنبي هذا، قد تصرف في إطار اتفاقية الإعتراف المتبادل أبرمتها السلطة.**"

إنّ الإعتراف بشهادات التصديق الأجنبية من الناحية العملية تتجسد في إطار إتفاقيات الإعتراف المتبادل فيما بين جهات التصديق الإلكتروني الرئيسية على مُستوى أعلى في هرم مرافق المفاتيح العمومية(PKI-IGC-ICP)، وليس فيما بين(م.خ.ت.إ) بمُفردهم على مُستوى أدنى في هرم مرفق المفاتيح العمومية في نطاق معين، بحيث تَنْصَبُّ إتفاقات التصديق المتبادل على تقييم عملية إعتماد مرفق المفاتيح العمومية الآخر، مع تحديد أصناف شهادات

---

[1] – تجدر الإشارة أنّ المادة 03 مكرر1 من المرسوم التنفيذي رقم 07-162 المتعلق بنظام الإستغلال المطبق على كل نوع من الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية، كلفت (س.ض.ب.م) بمهمة إبرام إتفاقيات الإعتراف المتبادل لشهادات التصديق الأجنبية، وذلك قبل إصدار القانون رقم 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، الذي كلّف السلطة الوطنية للتصديق الإلكتروني بهذه المهمة بإعتبارها كسلطة تصديق رئيسية في مرفق المفاتيح العمومية في الجزائر، وليس(س.ض.ب.م) التي تأتي في مرتبة أدنى منها من حيث سلم تدرج سلطات التصديق الإلكتروني.

التصديق التي يُصدرها (م.خ.ت.إ) المعترف بهم تلقائيا من طرف كلّ مرفق، والتي تسمح لزبائنهم باستخدامها لتحقيق أغراض معينة تتعلق بالمعاملات الإلكترونية، كما أنّ الإعتراف المتبادل يستوجب من الناحية التقنية على البرامج التطبيقية للحاسوب، أن تكون قادرة على معالجة الشهادات الأجنبية، والدخول إلى النظام الدليلي الحاسوبي(service d'annuaire) لمنطقة مرفق المفاتيح العمومية الأجنبي من أجل التأكد من صحة وضعية الشهادة.

لذا يُمكن لوكالة(ANCE) كسلطة تصديق إلكتروني رئيسية في تونس، أن تُبرم إتفاقات الإعتراف المتبادل مع جهات تصديق جذرية مثيلة لها في نطاقات هرمية أعلى على مستوى مرافق المفاتيح العمومية، كالشركة الأمريكية(Verisign) وهيئة(ITIDA) في مصر والسلطة الوطنية للتصديق الإلكتروني في الجزائر، لغرض الإعتراف بشهادات التصديق التي يُصدرها (م.خ.ت.إ) التابعين لكل مرفق، بحيث تقوم كلّ جهة تصديق على حِدَا بإصدار شهادة تصديق متقاطعة(Certificat Croisé) التي تسمح لها بالتوقيع على المفتاح العام، التابع لجهة التصديق الإلكتروني المثيلة لها في المرفق الأخر، التي تقوم بدورها بإصدار شهادة تصديق متقاطعة تُوقّع من خلالها على المفتاح العام التابع للجهة الأولى، وتتم نفس العملية بالنسبة لجهات التصديق الأخرى في إطار التصديق المتبادل فيما بين مرافق المفاتيح العمومية.

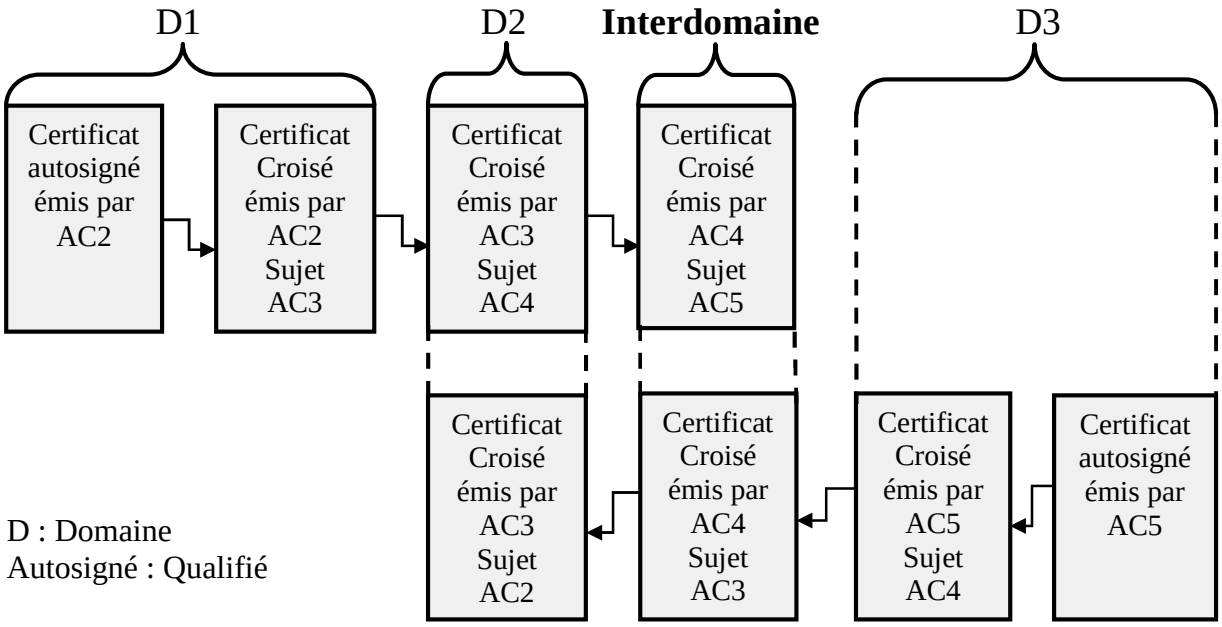
في حين يُبيِّن زوج الشهادات المُصدرة من طرفهم(Cross-Certificat) علاقة الثقة المتبادلة فيما بين سلطات التصديق الرئيسية، بالشكل الذي يُؤدي إلى الاندماج الكلّي أو الجزئي لنطاقات مرافق المفاتيح العمومية ضمن نطاق أكبر حجماً، وخلق تكافؤ وتوازن في السياسات العامة المتبعة في خدمات التصديق الإلكتروني[1].

---

1) - **Arnaud-F.FAUSSE**, op.cit., p. 128.

– عرفت المادة 01 من قرار وزير الاقتصاد الإماراتي شهادة المصادقة المتبادلة على أنّها:" شهادات المصادقة الإلكترونية التي تُصدّق بين اثنان أو أكثر من(م.خ.ت.إ) في عملية تبادلية لبعضهم البعض ويتم تطبيق الاستخدام التبادلي لها وتصدر عن أيّ منهم."

**نموذج للتصديق الإلكتروني المتبادل فيما بين مرافق المفاتيح العمومية. الشكل رقم (01)**




**المصدر:** من إعداد الطالب اعتمادا على: **-Arnaud-F. FAUSSE,** La signature électronique, transaction et confiance sur Internet, DUNOD, Paris, 2001, p.129.

## الفرع الرابع

## النماذج التنظيمية لإصدار شهادات التصديق الإلكتروني

إنّ تقدير قابلية التعويل على شهادات التصديق الإلكتروني مرهون بمدى قوة المفتاح العمومي المُستخدم في إصدارها، في إطار نماذج الثقة المعمول بها في التصديق الإلكتروني لذا توجد أربعة (04) نماذج تنظيمية لإصدار شهادات التصديق الإلكتروني والمتمثلة في:

### أولا- مرفق المفاتيح العمومية الهرمي: (Hierarchy PKI)

يستند هذا النموذج(PKI) إلى مُستويات هرمية مُختلفة من السلطة، التي من خلالها يخضع كلّ(م.خ.ت.إ) لسلطة تصديق رئيسية(Root Authority) في مرتبة أعلى يكون مفتاحها الجذري كنقطة محورية لكلّ الشهادات والمفاتيح الفرعية المربوطة به، وتُصدّق (السلطة الرئيسية) على تكنولوجيا وممارسات جميع الأطراف المرخص لها بإصدار أزواج مفاتيح التشفير أو شهادات تصديق تتعلق باستخدام تلك الأزواج من المفاتيح، كما تسجل

سلطات التصديق التابعة لها[1]، بالإضافة إلى ذلك تكون للسلطة الرئيسية سلطات تصديق مختلفة(AC) في مرتبة أدنى منها، تُصَدِّقْ على أن المفتاح العام لأحد المستعملين يناظر بالفعل المفتاح الخاص لذلك المستعمل(أي لم يتعرض لما يثير الشبهة فيه)، وسلطات تسجيل محلية مختلفة(AE) على مستوى أدنى من مستوى سلطات التصديق، تتولى مهام تلقي الطلبات من المستعملين للحصول على أزواج مفاتيح التشفير(الترميز) أو على شهادات التصديق المتعلقة باستخدام تلك الأزواج من المفاتيح، وتشترط إثبات هوية المستعملين المحتملين وتتحقق في الوثائق الأصلية التي تُثبت تلك الهوية.

لذا يمكن توسيع نطاق مرافق المفاتيح العمومية المنظّمة في بنية هرمية وذلك بإدماج مجموعات جديدة من هذه المرافق من خلال قيام السلطة الرئيسية بإنشاء علاقة ثقة بالسلطة الرئيسية للمجموعة الجديدة، ويجوز إدماج السلطة الرئيسية للمجموعة الجديدة مباشرة في الكيان الرئيسي لمرفق المفاتيح العمومية المستقبِل لتصبح بالتالي(م.خ.ت.إ) تابعا ضمن ذلك المرفق، كما يمكن للسلطة الرئيسية للمجموعة الجديدة أن تصبح مقدّما لخدمات تصديق تابعا لأحد(م.خ.ت.إ) التابعين ضمن المرفق القائم، ومن بين السمات الإيجابية للمرافق الهرمية للمفاتيح العمومية أنها تسهِّل تطوير مسارات التصديق لأنها تسير في اتجاه واحد فقط، أي من الشهادة الموجودة بحيازة المُستعمِل رجوعا إلى جهة الثقة، كما أنّ لهذه المرافق الهرمية أيضا سلبياتها لاسيما السلبيات المترتبة عن التعويل على جهة ثقة وحيدة، فإذا ضعفت سلطة التصديق الرئيسية ضعف مرفق المفاتيح العمومية بكامله، زيادة على ذلك وجدت بعض البلدان أنّه من الصعب اختيار كيان واحد ليكون سلطة رئيسية، وفرض تلك البنية الهرمية على جميع (م.خ.ت.إ).

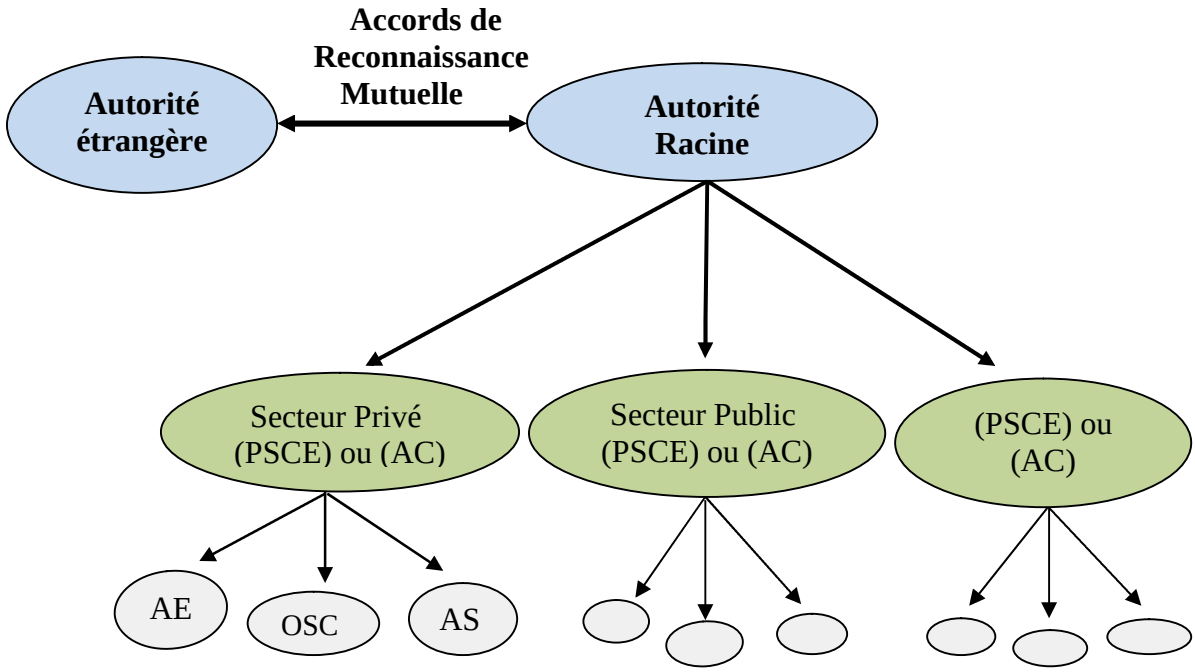
من بين جهات التصديق الإلكتروني التي طبقت هذا النهج، نجد كلٍّ من شركة (CertEurop) و(Chambersign Europe) كسلطات تصديق إلكتروني في أوروبا والشركة الأمريكية العملاقة (Verisign) وفروعها التي سيطرت على خدمات التصديق الإلكتروني في

---

1) - **Paul Axayacatl FRAUSTO BERNAL,** Infrastructure de Confiance sur des Architectures de Réseaux pour les Services de Signature évoluée, Thèse de doctorat, spécialité Informatique et Réseaux**,** École Nationale Supérieure de Télécommunications, Paris, 2004, pp. 16, 17, 61.

العالم، مثل (Thawte) و(GeoTrus)[1] الخ...، كما نجد كذلك سلطة التصديق الإلكتروني (IdenTrust) التي تتصدر مخطط التصديق الإلكتروني في العالم، المُنشئة عام 1999 عن طريق تكتل بنكي(consortium bancaire) التي تقوم بضمان خدمات تبادل البيانات الإلكترونية فيما بين البنوك الأعضاء وفيما بين الشركات في مجال الخدمات المصرفية[2].

**- النموذج الهرمي: (Modèle Hiérarchique) -الشكل رقم 02-**




**المصدر:** من إعداد الطالب اعتمادا على:

- **Manel ABDELKADER,** La Certification Électronique en Tunisie Expérience et Défis, SICE' 2011 ARPT, Alger du 08 et 09 décembre 2009, p.7. http://www.arpt.dz

---

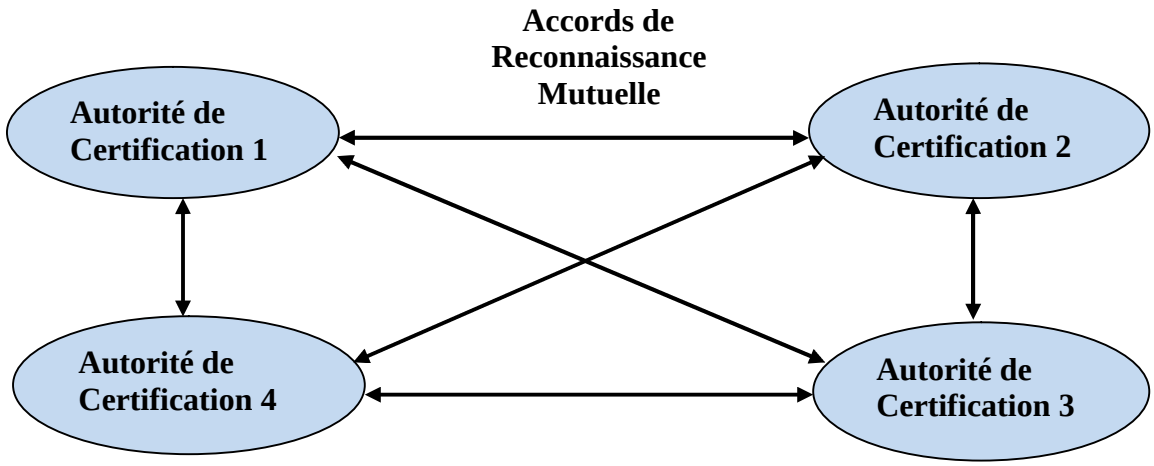
1) - **Verisign** sécurise 3000 entreprises et 450 000 sites Web à l'échelle mondiale et assure une présence marquée sur les cinq continents, en plus, les autorités de certification Thawte (Afrique, Amérique du Nord, Amérique du Sud) Esign Australia (Australie), Soltrus, Wis@Key (Suisse), et GeoTrust, sont des filiales de Verisign, consolidant sa position de leader mondial. Pour avoir plus d'information consulter : http://www.verisign.com/

2) – **IdenTrust** (Connue sous le nom **Identrus**) a été fondé par un consortium de huit banques : ABN AMRO, Bank of America, Bankers Trust, Barclays, Chase Manhatan Bank, CitiGroup, Deutsche Bank, HypoVereinsbank. **Renaud HOFFMAN**, Une architecture de certification à l'échelle mondiale, Disponible sur: http://www.01net.com/article/168355.html.

**ثانيا– مرفق المفاتيح العمومية المتشابك: (Mesh PKI)**

يعتبر هذا المرفق كبِنْيَة بديلة عن المرفق الهرمي ففي إطار هذا النموذج يرتبط مقدّموا خدمات التصديق بعلاقة بين الأقران، إذ يمكن لجميع مقدّمي خدمات التصديق في هذا النموذج أن يكونوا جهات موثوق بها عن طريق إبرامهم لاتفاقات الثقة (Accords de Confiance) بعضهم البعض، حول الاعتراف بشهادات التصديق التي يُصدرها كل(م.خ.ت.إ) إذ يبيّن زوج الشهادات المصدرة علاقة الثقة المتبادلة فيما بينهم، ومن مميزات هذا النموذج نجد أنّه يفتقد إلى الترتيب الهرمي كما أن(م.خ.ت.إ) لا يستطيعون فرض شروط تحكم أنواع الشهادات التي يصدرها مقدّمون آخرون لخدمات التصديق، فإذا رغب (م.خ.ت.إ) تقييد حدود الثقة المتاحة إلى(م.خ.ت.إ) آخرين، وجب عليه تحديد هذه القيود في الشهادات التي يصدرها لأقرانه، غير أن المواءمة بين شروط وقيود الاعتراف المتبادل قد تكون هدفا معقدا للغاية، مما يؤدي إلى فقدان الثقة في الخدمات التي تُقدمها سلطات التصديق الإلكتروني لكونها لا تخضع لمُستويات هرمية في الرقابة، وبالتالي فإنّ هذا النموذج يصلح فقط لدى (م.خ.ت.إ) من نفس المستوى الذين يشتغلون في مجال معين.

**– النموذج المتشابك (Modèle Maillé)**




- Absence de hiérarchisation et de contrôle.
- Reconnaissance mutuelle entre toutes les AC.

**- الشكل رقم (03)– المصدر:** من إعداد الطالب اعتمادا على: **Ahmed BERBAR, -**
Certification Électronique en Algérie Situation et Perspectives, SICE' 2011 ARPT, Alger du 08 et 09 décembre 2009, p. 09. http://www.arpt.dz

**ثالثا– مقدم خدمات التصديق الجسر: (Bridge CA)**

فوفقا لهذه البنية يمكن لمجموعات مرافق المفاتيح العمومية من خلالها أن تثق بشهادات كلّ منها، فعلى خلاف(م.خ.ت.إ) في مرفق المفاتيح العمومية المتشابك فإن مقدّم خدمات التصديق الجسر لا يصدر شهادات التصديق الإلكتروني مباشرة إلى المستعملين، كما أنّه(Bridge CA) لا يعتبر **كجهة ثقة** يعول عليها مستعملي مرفق المفاتيح العمومية مثلما هو الحال فيما يتعلق بمقدّم خدمات التصديق **الرئيسي**[1]، وعوضا عن ذلك يقوم "مقدّم خدمات التصديق الجسر" بإنشاء علاقة ثقة بمختلف مجموعات المستعملين بوصفها أقرانا مع تمكينهم(المستعملين)، من الإبقاء على جهات الثقة الخاصة بهم ضمن كلّ مرفق من مرافق المفاتيح العمومية لديهم، فإذا أرادت مجموعة من المستعملين تكوين مجال ثقة في شكل مرفق مفاتيح عمومية هرمي فإن "مقدّم خدمات التصديق الجسر" سوف يقيم علاقة بالسلطة الرئيسية لذلك المرفق.

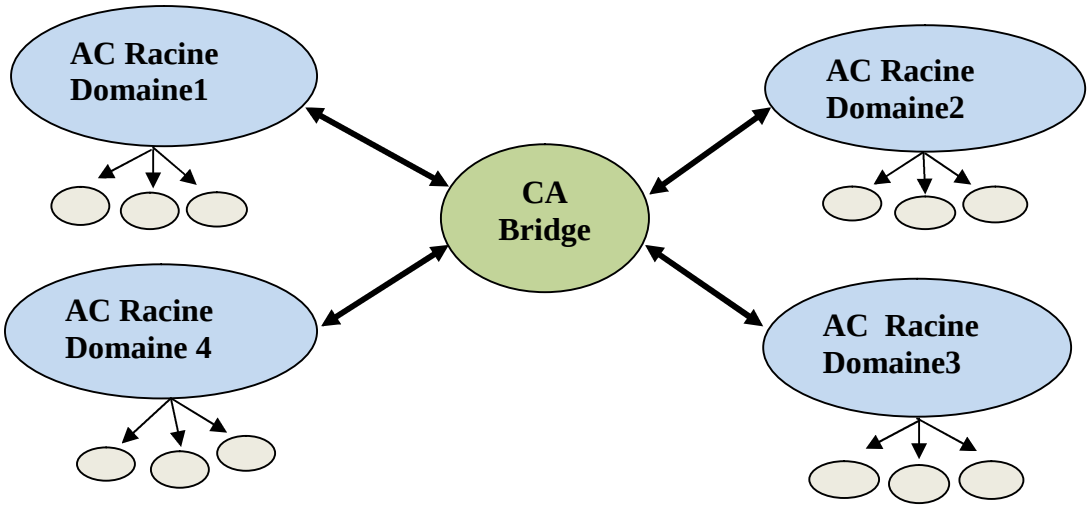
ففي حالة ما إذا أرادت مجموعة من المستعملين تكوين مجال ثقة من خلال إنشاء مرفق مفاتيح عمومية متشابك، فلن يحتاج "مقدّم خدمات التصديق الجسر" إلا إلى إرساء علاقة بأحد مقدّمي خدمات التصديق التابعين لمرفق المفاتيح العمومية، الذي يصبح عندئذ مقدّم خدمات التصديق الرئيسي داخل ذلك المرفق لغرض إرساء جسر الثقة لمرفق المفاتيح العمومية الآخر، فبفضل جسر الثقة الذي يربط مرفقين أو أكثر من مرافق المفاتيح العمومية من خلال علاقتهما المشتركة بمقدّم خدمات التصديق الجسر، يتمكّن المستعملين التابعين لمرافق المفاتيح العمومية المختلفة من التفاعل فيما بينهم من خلال مقدّم خدمات التصديق الجسر بمستوى ثقة محدد.

انطلاقا من ذلك يعتبر "مقدم خدمات التصديق الجسر" كحلقة وصل رئيسية في الهيكل التنظيمي العام لمرافق المفاتيح العمومية، من خلال ضمان عملية تقاطع شهادات التصديق الإلكتروني سواء على المستوى الوطني لكل دولة، وبالخصوص فيما بين القطاع العام والخاص، أو على المستوى الدولي أو الإقليمي وذلك في إطار اتفاقيات الاعتراف المتبادل

1) - **Arnaud-F. FAUSSE**, op.cit., pp. 126, 128.

لشهادات التصديق الإلكتروني الأجنبية، التي تسمح بخلق التوازن والتكافؤ فيما بين سياسات التصديق الإلكتروني، مع توسيع نطاق مرافق المفاتيح العمومية ضمن نطاق أكبر حجم الشيء الذي يسمح للمستعملين بالتفاعل فيما بينهم، بمستوى محدد من الثقة والأمان مع إبقاءهم لجهات الثقة في كلّ مرفق مفاتيح عمومية، لذا تم اعتماد هذا النموذج "مقدم خدمات التصديق الجسر" كبنية لإقامة أو استحداث نظام مرفق المفاتيح العمومية للحكومة الفيدرالية للولايات المتحدة الأمريكية وحكومة اليابان.

- **النموذج الجِسْرْ: (Modèle Bridge)**




- Diminue le nombre de reconnaissances mutuelles (CA Bridge).
- AC Bridge n'est pas émetteur du Certificats mais prestataire de liaison effectuant un pont de certification entre les domaines de certification.
- Dédié généralement à un modèle d'organisation Fédéral.

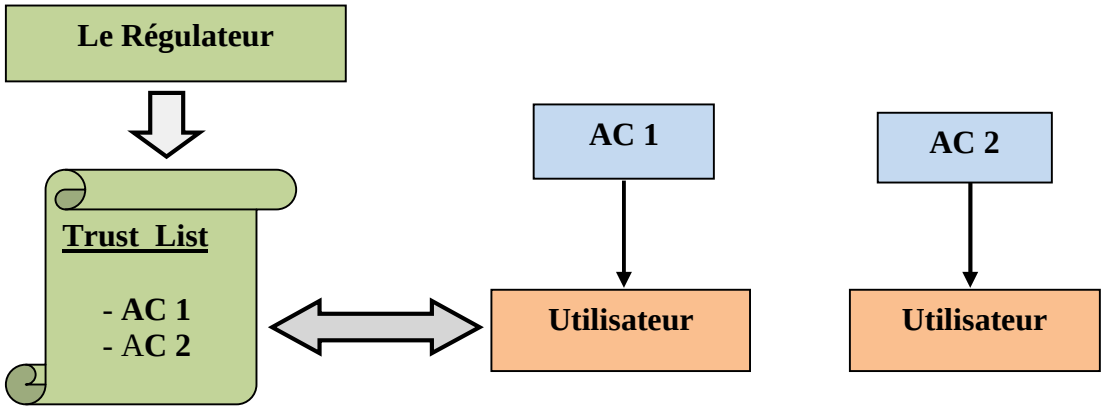
- **الشكل رقم (04)- المصدر:** من إعداد الطالب اعتمادا على **: Ahmed BERBAR, -** op.cit., p. 09 et - **Arnaud-F. FAUSSE,** p. 127.

## 4- نموذج قائمة الثقة: (Trust List)

يقوم هذا النموذج على وجود قائمة ثقة(Trust List) التي هي عبارة عن وثيقة ينشرها كيان مستقل الذي يكون في الغالب كمنظم(Régulateur) لنشاط التصديق، بحيث تتضمن هذه الوثيقة قائمة سلطات التصديق المرخص لها والمعترف بها إضافة لمُعَرِّفْ(L'identifiant) مفاتيحها العمومية، كما يقوم نموذج قائمة الثقة برسم حدود لسلطات

التصديق، وبالتالي فهو لا يوفر عملية مصادقة إلكترونية موحدة ومتقدمة بالقدر الذي يوفره نموذج مرفق المفاتيح العمومية الهرمي، فغياب التوحيد قد يُسبب مشاكل توافقية عِدّة بين (م.خ.ت.إ)، ومن مُميزات هذا النموذج نجد غياب سلطة تصديق تُشرف على رقابة نشاطات (م.خ.ت.إ) المعترف بهم، كما أنّ عملية الاعتراف بشهادات التصديق الأجنبية تستدعي تدخل سلطة وطنية تقوم بمهمة إبرام اتفاقيات الاعتراف المتبادل لشهادات التصديق الإلكتروني، ومن بين الدول التي أخذت بهذا النموذج نجد كلٌّ من إسبانيا وسويسرا.

**- نموذج قائمة الثقة: Modèle Trust List**




- Modèle plus ouvert, plus flexible que le modèle hiérarchique.
- Absence de : Contrôle et un Processus de normalisation et de validation (interopérabilité), et d'une entité nationale qui signe les conventions de reconnaissance mutuelles avec les instances internationales.

**-الشكل رقم (05)- المصدر:** من إعداد الطالب اعتمادا على: **-Ahmed BERBAR,** op.cit., p.08

فمن خلال استعراضنا لمُختلف النماذج المتعلقة بمرافق المفاتيح العمومية يبدو لنا أنّ النموذج الموثوق به من طرف غالبية دول العالم في مجال المعاملات الإلكترونية، هو الذي تتوافر فيه معايير الرقابة التي تتواجد في مرفق المفاتيح العمومية الهرمي (Hierarchy PKI) كنموذج تصديق مُوَحَّدْ بالرغم من بعض السلبيات المتصلة به، وفي كلّ الظروف تتم عملية انتهاج نموذج التصديق الإلكتروني وفقا للسياسة العامة لكلّ دولة، كما أنّ جدارة الثقة في (م.خ.ت.إ) تتوقف على مدى امتثاله لمقتضيات السياسة العامة المتبعة في خدمات التصديق الإلكتروني ومراعاته للتأكيدات المقدمة فيه.

## المبحث الثاني

## إجراءات التوثيق الإلكتروني

إنّ معاملات التجارة الإلكترونية التي تعتمد على الأجهزة التقنية الحديثة أصبحت تتخذ أشكالا وأنماطا متعددة، كعرض البضائع والخدمات وإبرام عقود البيع بالوصف عبر مواقع شبكة الويب العالمية، مع إجراء عمليات الدفع الإلكتروني بالبطاقات المالية أو غيرها من وسائل الدفع الإلكتروني وإنشاء متاجر إفتراضية ومحلات بيع على الإنترنيت، والقيام بأنشطة التزويد والتوزيع وممارسة العمليات المصرفية وخدمات النقل والشحن، التي تتم في بيئة إلكترونية مفتوحة تُعَرِّض أطراف التصرف الإلكتروني إلى مشاكل أمنية وتقنية وقانونية ذات صلة بتحديد إرادة وهوية كل متعامل ومدى نسبتها إليه، وسلامة مضمون التصرف الإلكتروني الخ...، مما تستدعي بهم الحاجة إلى ضرورة الإستعانة بجهة تصديق إلكتروني محايدة، معتمدة أو مرخص لها من طرف الجهات الرسمية لمزاولة نشاطاتها وفقا للقانون المعمول به في كلّ دولة(المطلب الأول)، تُتيحهم في إطار سياسة التصديق الإلكتروني المنتهجة لإجراءات توثيق التوقيعات الإلكترونية وتعزيزها بشهادات تصديق إلكتروني موصوفة وفقا للمواصفات المعترف بها دوليّا(المطلب الثاني).

### المطلب الأول

### الجهة المختصة بتوثيق التصرف الإلكتروني

إنّ إرساء الثقة والأمان في جميع المعاملات الإلكترونية مرتبط بالتنظيم المحكم والدقيق لمرفق المفاتيح العمومية المنتهج حسب السياسة العامة لكلّ دولة، التي ينبغي عليها تحديد شكل المرفق وعدد مستويات سلطات التصديق الإلكتروني، وإمكانية تفويض هيئات عمومية أو خاصة كسلطات تصديق تشرف على إدارة وتنظيم ورقابة نشاطات التصديق الإلكتروني المعتمدة(الفرع الأول)، التي تسمح لـ(م.خ.ت.إ) بمزاولة خدماتهم وفقا لشروط محددة مُسبقا بموجب الأحكام التشريعية والتنظيمية المنظمة لها(الفرع الثاني).

## الفرع الأول

## الهيئة المكلفة بإعتماد أو ترخيص نشاط مُقدمي خدمات التصديق الإلكتروني

لا شك أنّ ممارسة أيّ عمل أو نشاط مهني بشكل غير مُنظم من قِبَلِ السلطات الرسمية في الدولة المعنية يترتب عنه حتما فوضى عارمة، وعدم الإستقرار في المعاملات مِمَّا يُؤدي إلى ضياع حقوق الأطراف المَعْنِيَّةَ بالتصرف، لذا قامت مُختلف التوجيهات والتشريعات الدولية والوطنية بتنظيم نشاطات(م.خ.ت.إ) في إطار مخططات الإعتماد أو التراخيص، تحت إشراف وإدارة ورقابة هيئات عامة أو خاصة مُفوضة من طرف السلطات الرسمية، والتي سنتطرق إليها على النحو التالي:

### أولا: التوجيه الأوروبي رقم 93/99 المتعلق بالتوقيعات الإلكترونية.

ألزمت المادة 1/03 من التوجيه الأوروبي رقم 93/99 المتعلق بالتوقيعات الإلكترونية دول الإتحاد الأوروبي، بعدم إخضاع نشاطات(م.خ.ت.إ) لأيِّ ترخيص مُسبق (Autorisation préalable) وذلك بهدف تشجيع التنافس الحرّ والنزيه بين(م.خ.ت.إ) في الأسواق الأوروبية، على النحو الذي ينعكس إيجابا على مُستوى وجودة الخدمات المُقدمة في المعاملات الإلكترونية، لكن المشرع الفيدرالي الأوروبي سمح لدول الإتحاد بموجب الفقرات الثانية والثالثة من نفس المادة(2/03-3) بتأسيس أنظمة اختيارية لاعتماد(م.خ.ت.إ) (Accréditation volontaire)، من أجل رقابة وتحسين مُستوى خدمات التصديق الإلكتروني المتاحة من طرف(م.خ.ت.إ) المقيمين على أراضيها، فقد عرفت المادة 13/02 من التوجيه الإعتماد الاختياري على أنّه[1]:" **كل ترخيص يُحدّد الحقوق والالتزامات الخاصة بتقديم خدمات التصديق الممنوح بناءا لطلب (م.خ.ت.إ) المعني، من طرف هيئة عامة أو خاصة**

---

1) – **Art 02/13** (Directive européenne n° 99-93 sur les signatures électroniques) : «**accréditation volontaire** : toute **autorisation** indiquant les droits et obligations spécifiques à la fourniture de services de certification, accordée, sur **demande du prestataire de service de certification concerné**, par **l'organisme public ou privé** chargé d'élaborer ces droits et obligations et d'en contrôler le respect, lorsque le prestataire de service de certification n'est pas **habilité** à exercer les droits découlant de **l'autorisation** aussi longtemps qu'il n'a pas obtenu la décision de cet organisme. »

**مكلفة بإعداد هذه الحقوق والالتزامات ورقابة مدى احترامها، ويُعَدْ كل (م.خ.ت.إ) غير مؤهل لمُزاولة نشاطه في حالة عدم إستيفاءه للمتطلبات المحددة في الترخيص."**

لذا ألزم التوجيه الأوروبي المتعلق بالتوقيع الإلكتروني أن تكون الشروط التي تضعها الدول الأعضاء مبنية على الشفافية والموضوعية ومتناسبة وغير تمييزية، وذلك من أجل انتقاء جهات توثيق إلكتروني تتوافر فيها أحسن مُستويات الأمان في خدمات التصديق الإلكتروني، وتُضيف المادة 4/03 على تولي كلّ دولة بتعيين هيئات عامة أو خاصة تُشرف على مدى مُطابقة معدّات إحداث التوقيعات الإلكترونية الموصوفة، للشروط المحددة في الملحق الثالث من التوجيه الأوروبي رقم 93/99 وفقا للمعايير التي تحددها لجنة التوقيعات الإلكترونية(Comité sur les signatures électroniques)[1]، وكنتيجة لذلك تم الإتفاق الأوروبي المتعدد الأطراف في إطار التعاون الأوروبي لمنظمات الإعتماد (European Cooperation for Accreditation)(EA) بهدف الإعتراف بشهادات التصديق الإلكتروني المعتمدة فيما بين دول الإتحاد الأوروبي.

---

1) - **Art 03** (Directive européenne n° 99-93…) : **« 1**-Les États membres ne soumettent la fourniture des services de certification à aucune **autorisation préalable**.
**2**- Sans préjudice des dispositions du paragraphe 1, les États membres peuvent instaurer ou maintenir **des régimes volontaires d'accréditation** visant à améliorer le niveau du service de certification fourni. Tous les critères relatifs à ces régimes doivent être objectifs, transparents, proportionnés et non discriminatoires. Les États membres ne peuvent limiter le nombre de prestataires accrédités de service de certification pour des motifs relevant du champ d'application de la présente directive.
**3**- Chaque État membre veille à instaurer un système adéquat permettant de **contrôler** les prestataires de service de certification établis sur son territoire et délivrant des **certificats qualifiés au public.**
**4**- La conformité des dispositifs sécurisés de création de signature aux conditions posées à l'annexe III est déterminée par les organismes compétents, publics ou privés, désignés par les États membres. La Commission, suivant la procédure visée à l'article 9, énonce les critères auxquels les États membres doivent se référer pour déterminer si un organisme peut être désigné. La conformité aux exigences de l'annexe III qui a été établie par les organismes visés au premier alinéa est reconnue par l'ensemble des États membres. »
- **Art.10** : « Le comité clarifie les exigences visées dans les annexes de la présente directive, les critères visés à l'article 3, paragraphe 4, et les normes généralement reconnues pour les produits de signature électronique établies et publiées en application de l'article 3, paragraphe 5, conformément à la procédure visée à l'article 9, paragraphe 2. »

**ثانيا: في التشريعات الوطنية الأجنبية.**

**1- القانون الفرنسي.**

تطبيقا لأحكام التوجيه الأوروبي وملاحقه، قامت فرنسا بإعداد مخطط إعتماد جهات التوثيق الإلكتروني تحت إشراف جهازين ذي صلاحيات مُختلفة، فالأول نص عليه المرسوم رقم 2002-535 الصادر في 18 أفريل 2002 المتعلق بتصديق وتقييم معدات وأنظمة أمن تكنولوجيا المعلومات، أمّا الجهاز الثاني نص عليه قرار وزير الصناعة المنتدب الصادر في 2004/07/26 المتعلق بالإجراءات الخاصة بالتأهيل الاختياري لـ(م.خ.ت.إ) واعتماد الهيئات التي تشرف على تقييمهم.

**أ- الهيئة المكلفة بإعتماد مراكز تقييم مطابقة معدات وأنظمة تكنولوجيا المعلومات:**

إنّ المرسوم رقم 2002-535 الصادر في 18 أفريل 2002 المتعلق بتصديق وتقييم معدات وأنظمة أمن تكنولوجيا المعلومات، قد أنشأ نظام تصديق وتقييم خاص بمختلف المعدات والتجهيزات المستخدمة في نشاطات التصديق الإلكتروني الذي تتدخل في مراحله هيئات عِدَّة، فحسب المادة 12 منه فإنّ إعتماد مراكز تقييم مطابقة معدات وأنظمة أمن تكنولوجيا المعلومات، يتم بموجب قرار إعتماد مدة صلاحيته عامين(02) قابلة للتجديد صادر من طرف الوزير الأول بعد الأخذ برأي اللجنة المركزية للتصديق على تكنولوجيا أمن المعلومات (le Comité directeur de la certification en sécurité des technologies de l'information) المنشئة لدى الوزير الأول، بموجب المادة الرابعة(04) من المرسوم رقم 2001-272 المتعلق بالتوقيع الإلكتروني كسلطة مراقبة، يترأسها الأمين العام لوزير الدفاع الوطني أو نائبه، بالإضافة إلى ممثلين عن مختلف الوزارات وشخصيات ذي كفاءات معينة يعينها الوزير الأول لمدة 03 سنوات.

لذا يجب على المركز الراغب في ممارسة مهام تقييم المطابقة أن يقوم بإيداع طلب لدى الوكالة الوطنية لأمن أنظمة المعلومات(ANSSI)، كأمانة لدى اللجنة المركزية للتصديق والتقييم مُكلّفة بتنظيم إجراءات إعتماد مراكز تقييم المطابقة(CESTI) وتقدير مهامهم، بحيث

يُثبت فيه مؤهلاته التقنية التي تسمح له بالتقييم وفقا للمادة II-11 من نفس المرسوم[1] فمن خلال هذه المدة يخضع المركز المعتمد، لتدقيقات دورية من طرف وكالة الأمن[2] التي يمكن أن يترتب عنها سحب الإعتماد بنفس إجراءات منحه، وذلك بعد الأخذ بملاحظات ممثل الهيئة أمام اللجنة المركزية للتصديق والتقييم، ونظرا للدور الفعّال للوكالة(A.N.S.S.I) في رقابة مراكز تقييم المطابقة المعتمدة(CESTI) منح لها القانون بموجب المادة 09 من نفس المرسوم صلاحية إبرام إتفاقيات الإعتراف المتبادل لشهادات المطابقة، مع الهيئات الأجنبية المثيلة لها المقيمة خارج الإتحاد الأوروبي بعد الأخذ برأي اللجنة المركزية للتصديق والتقييم[3].

إنطلاقا مما سبق فإنّ اللجنة المركزية للتصديق والتقييم تُشرف بموجب المادة 15 من نفس المرسوم على عدّة مهام رئيسية، كتقديم آراء واقتراحات حول سياسة التصديق والقوانين والمعايير المتعلقة بإجراءات التقييم والتصديق الإلكتروني، كما تُصدر آراء حول قرارات منح وسحب الإعتماد لمراكز تقييم المطابقة، وكذلك حول إتفاقيات الإعتراف المتبادل التي تبرمها وكالة(A.N.S.S.I) مع الأطراف الأجنبية المثيلة لها، وإلى جانب ذلك تقوم اللجنة المركزية (أو تفوض أحد أعضاءها) عن طريق المصالحة، بحلّ النزاعات المطروحة عليها من الأطراف بشأن إجراءات تقييم المطابقة.

---

1) - Décret n° 2002-535 du 18 avril 2002, relatif à l'évaluation et la certification de la sécurité offerte par les produits et systèmes des technologies de l'information. J.O.R.F, n° 92 du 19 avril 2002. http://www.legifrance.gouve.fr/

- **Art. 11/I-II (c)** : « **I-** La demande d'agrément est formulée auprès de la direction centrale de la sécurité des systèmes d'information. Cette demande précise le domaine dans lequel l'organisme demandeur entend exercer son activité. II - l'organisme demandeur doit faire la preuve:[…] de sa compétence technique à conduire une évaluation. »

2) – Le **(SCSSI)** se transforme en **(DCSSI)**, et en **(ANSSI)** au sein du secrétariat général de la défense nationale (service du premier ministre). ⇒ **Décret n° 2001-693 du 31 juillet 2001** créant au secrétariat général de la défense nationale une direction centrale de la sécurité des systèmes d'information. J.O.R.F n° 177 du 02 août 2001.

- **Décret n° 2009-834 du 7 juillet 2009** portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information ». J.O.R.F n°156 du 8 juillet 2009. http://www.legifrancce.org.fr

3) - **Eric A. CAPRIOLI,** signature et confiance dans les communications électroniques en droits français et européen, pp. 14, 15. Article publié sur : http://www.caprioli-avocats.com

**ب- اللجنة الفرنسية للإعتماد (COFRAC).**

قام وزير الصناعة المنتدب(Patrick DEVEDJIAN) بإصدار قرار بتاريخ 26 جويلية 2004، (الملغي لقرار وزير الإقتصاد والمالية(Francis MER) الصادر في 31 ماي 2002) المتعلق بالإعتراف بمؤهلات(م.خ.ت.إ) واعتماد الهيئات التي تقوم بتقييمها[1]، الذي من خلاله يجب على الهيئة الراغبة(Organismes) في الحصول على إعتماد يُمَكِّنُهَا من تدقيق خدمات(م.خ.ت.إ)[2]، أن تُقدّم طلب للمركز الفرنسي للإعتماد(COFRAC)، أو أيّ مركز إعتماد منظم إلى الإتفاق الأوروبي لمنظمات الإعتماد(EA)، يبرهن فيه متطلبات المادة الثانية من القرار المتعلقة بتحديد هوية الهيئة، وتقديمها لوصف حول نشاطها والإمكانيات التقنية والإجراءات والوسائل المسخرة منها للتقييم، مع إعلانها بجميع الروابط المحتملة مع أيّ(م.خ.ت.إ)، فبعد الفحص الإيجابي لمركز الإعتماد(COFRAC) للطلب يُصدر قرار إعتماد مُسبب يُبلغ إلى كلّ من صاحب الطلب ووكالة(A.N.S.S.I)، مدّة صلاحيته لا تتجاوز 05 سنوات، وفي خلال هذه المدّة تخضع هيئة التأهيل المعتمدة لرقابة منتظمة ومُستمرة من قِبَلِ مركز الإعتماد الذي يتمتع بصلاحية إيقاف أو سحب الإعتماد بعد الأخذ بعين الإعتبار بملاحظات ممثل الهيئة المعتمدة مع إعلام وكالة(A.N.S.S.I) بذلك.

تجدر الإشارة أنّ الهيئة التي تشرف على تقييم مقدمي خدمات الثقة(PSCO) الذين يتيحون خدمات التصديق الإلكتروني لحساب السلطات العمومية، المشار إليهم بموجب المادة 09 من الأمر رقم 2005-1516 المؤرخ في 2005/12/08 المتعلق بالمبادلات

---

1) - **Arrêté** de ministre de l'économie et de finance et de l'industrie du 31 mai 2002, relatif à la reconnaissance de qualification des prestataires de services de certification électronique et à l'accréditation des organismes chargés de l'évaluation. J.O.R.F. n° 132 du 08 juin 2002.
- **Arrêté** de ministre délégué à l'industrie, du 26 juillet 2004 relatif à la reconnaissance de qualification des prestataires de services de certification électronique et à l'accréditation des organismes qui procèdent à leur évaluation. J.O.R.F n° 182 du 07 août 2004. http://www.legifrance.org.fr

2) - **Art.1-12** (décret n° 2001-272 sur la signature électronique): « Qualification de Prestataires de Service de Certification Électronique : L'acte par lequel un tiers dit, organisme de qualification, atteste qu'un prestataire de service de certification électronique fournit des prestations conformes à des exigences particulières de qualité. »

الإلكترونية بين المستعملين والسلطات الإدارية أو فيما بين هذه السلطات[1]، يجب أن تتحصل على تأهيل(Habilitation) من طرف الوزير الأول، لمدة ثلاث سنوات قابلة للتجديد وذلك بعد التأكد من حصولها على إعتماد من طرف مركز الإعتماد(COFRAC)، وخضوع الهيئة لتدقيق من طرف وكالة(A.N.S.S.I) حول مدى مطابقة المعدات والوسائل المستعملة للتقييم، للقواعد (تحدد في دفتر الشروط) المحدّدة في المرجع العام للأمان Référentiel Général de Sécurité (RGS) المشار إليه في المادة 09 أعلاه، على أن تتم إجراءات التأهيل وفقا للمواد 10 إلى 14 من المرسوم رقم 2010-112 المؤرخ في 2010/02/02 المتعلق بتطبيق أحكام المواد 09 و10 و12 من الأمر رقم 2005-1516[2].

فعلى(م.خ.ت.إ) الراغب في تأهيل نشاطاته اختيار هيئة معتمدة من أجل القيام على نفقاته بإجراء تأهيل خدماته المقترحة، ومدى مُطابقتها للمواصفات التقنية المحددة بموجب أحكام المادة 06 من المرسوم رقم 2001-272 المتعلق بالتوقيع الإلكتروني، وبعد التقييم تحرّر الهيئة تقرير إمّا بالإعتراف أو الرفض الذي تُبلغه إلى كلّ من صاحب طلب التأهيل ولوكالة الأمن(A.N.S.S.I)، ففي حالة الإعتراف بخدمات التصديق تُصدر الهيئة المُعتمدة لـ(م.خ.ت.إ)، شهادة تأهيل لمدة لا تتعدى ثلاثة(03) سنوات التي ترسل نسخة منها لوكالة

---

1) - Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives. J.O.R.F, n° 286 du 9 décembre 2005.

2) - Décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives. J.O.R.F, n° 0029 du 4 février 2010.http://www.legifrance.gouve.fr

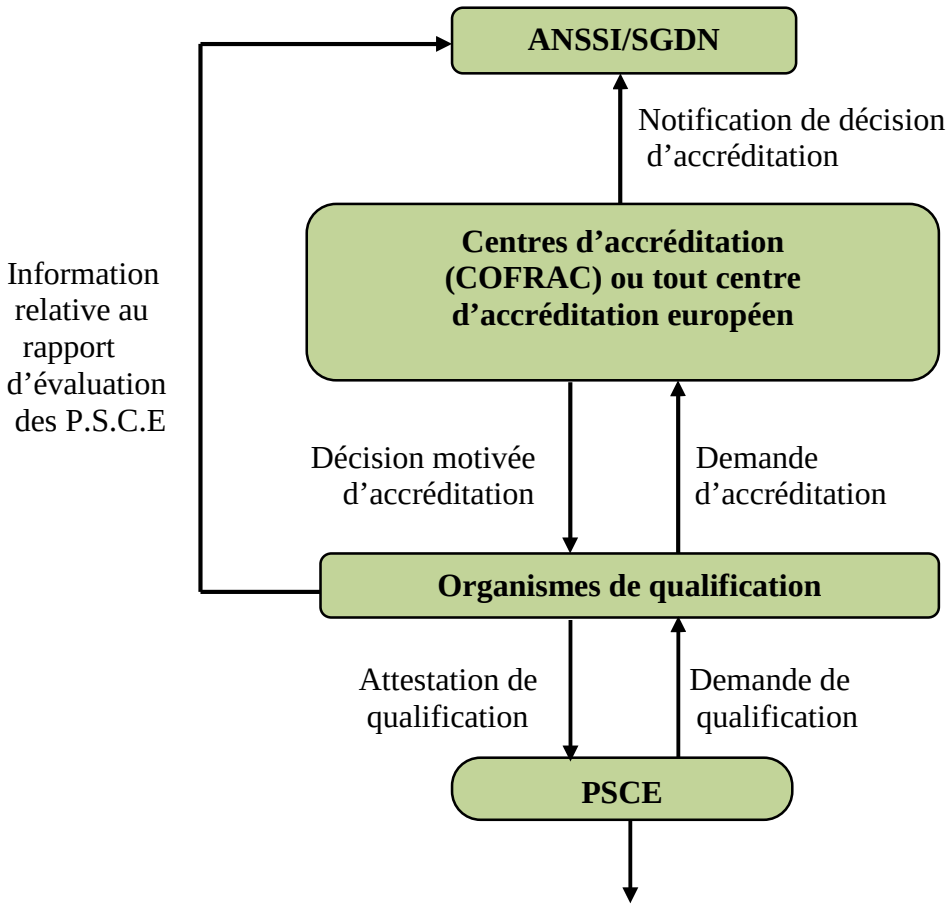
**- Art.10** : « **I.** - L'habilitation des organismes qui procèdent à la qualification des prestataires de services de confiance prévue par l'article 9 de l'ordonnance du 8 décembre 2005 susvisée est délivrée par le Premier ministre, après vérification : **1-** De l'accréditation de l'organisme selon les normes et règles en vigueur, notamment en matière d'impartialité, de responsabilité et de confidentialité. Cette accréditation est délivrée par une instance d'accréditation mentionnée à l'article L. 115-28 du code de la consommation.

**2-** De la compétence technique de l'organisme à conduire l'évaluation de fonctions de sécurité mises en œuvre par un prestataire de services de confiance au regard des règles du référentiel général de sécurité. Cette compétence est appréciée par l'Agence nationale de la sécurité des systèmes d'information à partir d'un audit des moyens, des ressources et de l'expérience de l'organisme.

**II.-** L'habilitation est valable pour une durée maximale de trois ans renouvelable. Elle peut énoncer des obligations particulières auxquelles est soumis l'organisme bénéficiaire.»

(A.N.S.S.I)(أنظر الشكل رقم 06)، فمن خلال هذه المدة يخضع(م.خ.ت.إ) المؤهل لتدقيق(Audit) من طرف الهيئة المعتمدة الذي يمكن أن يترتب عنه إيقاف أو سحب شهادة التأهيل الممنوحة له، وتجدر الإشارة أنّ إجراءات تأهيل مقدمي خدمات الثقة(PSCO) لحساب الهيئات العمومية الفرنسية تتم وفقا للإجراءات المحدّدة بموجب المواد 15 إلى 19 من المرسوم رقم 2010-112 المؤرخ في 2010/02/02 المتعلق بتطبيق أحكام المواد 09 و10 و12 من الأمر رقم 2005-1516، والتي على إثرها يتحصل على شهادة تأهيل لمدة ثلاث سنوات قابلة للتجديد.

**Dispositif mis en place en France en matière de qualification de P.S.C.E.**




Certificat qualifié ou présenté comme tel bénéficiant de la présomption de qualification pour une durée de 3 ans maximum.

**-الشكل رقم (06)- المصدر:** من إعداد الطالب اعتمادا على: **-Eric A. CAPRIOLI,** op.cit., p. 12

**2- القانون البلجيكي:**

مراعاة لأحكام المادة 3-2/03 من التوجيه الأوروبي رقم 93/99 المتعلق بالتوقيع الإلكتروني، كلّف المشرع البلجيكي إدارة وزير الشؤون الإقتصادية (L'Administration du ministre des affaires économiques) بالإشراف على إجراءات منح الإعتماد الاختياري (BE.SIGN) بهدف رقابة(م.خ.ت.إ) المقيمين في بلجيكا، فوفقا للمادة 18 من القانون الملكي الصادر في 09 جويلية2001 المحدد للقواعد المتعلقة بالإطار القانوني بالتوقيع الإلكتروني وبخدمات التصديق، فإنّ الإدارة تتكفل بالمهام المتعلقة بمنح وسحب الإعتمادات وفقا للقانون عن طريق مصالح وأشخاص ذي كفاءات معينة، مع تنسيق التطبيق المتكامل والشفاف لمبادئ وإجراءات الإعتماد وفقا لمُقتضيات هذا القانون، ورقابة نشاطات وإجراءات تقييم الهيئات المحددة بموجب المادة 13/02 من القانون في إطار إجراءات الإعتماد[1]، بالإضافة إلى ذلك تقوم بتبليغ دول الإتحاد واللجنة الأوروبية بكل المعلومات المتعلقة بنظام الإعتماد الاختياري المؤسس بموجب هذا القانون، وبأسماء وعناوين(م.خ.ت.إ) المعتمدين، وبالتالي يحق لكلّ(م.خ.ت.إ) طلب الحصول على الإعتماد الاختياري(BE.SIGN) لدى الإدارة، وفقا للإجراءات التي حددها القرار الملكي المؤرخ في 06 ديسمبر 2002 المنظم لإجراءات رقابة واعتماد(م.خ.ت.إ) الذين يُصدرون شهادات تصديق إلكتروني موصوفة[2].

---

1) - Art. 2-13(Loi du 09 juillet 2001...): « organisme qui démontre sa compétence sur base d'un certificat délivré par le système belge d'accréditation conformément à la loi du 20 juillet 1990 concernant l'accréditation des organismes de certification et de contrôle, ainsi que des laboratoires d'essais, ou par un organisme équivalent établi dans l'Espace économique européen. »

2) - **Arrêté royal** du 6 décembre 2002, organisant le contrôle et l'accréditation des prestataires de service de certification qui délivrent des certificats qualifiés. MB n° 192 du 17.01.2003. http:// www.moniteur.be

**3- القانون السويسري.**

نص المشرع الفيدرالي السويسري في المادة 04 من قانون التوقيع الإلكتروني لعام 2003(SCSE)، على تكليف المجلس الفيدرالي السويسري كسلطة تنفيذية في الكنفيدرالية بمهمة تعيين هيئة إعتماد مراكز الإعتراف بـ(م.خ.ت.إ) في إطار نموذج قائمة الثقة في التصديق(Modèle Trust List)[1]، ففي حالة عدم تواجد أيّ مركز إعتراف معتمد يتولى الديوان الفيدرالي للإتصالات بموجب المادة 2/01 من الأمر الصادر من المجلس الفيدرالي بتاريخ 03 ديسمبر 2004 المتعلق بخدمات التوثيق في مجال التوقيع الإلكتروني، مهمة إعتراف(م.خ.ت.إ) بحيث تقوم هذه المراكز بإعداد وتسليم قائمة ثقة تضم جميع(م.خ.ت.إ) المعترف بهم، إلى هيئة الإعتماد التي تقوم بإعلانها للعموم وفقا لنص المادة 05 من القانون الفيدرالي المتعلق بالتوقيع الإلكتروني[2].

تتمثل هيئة الإعتماد وفقا للمادة 1/01 من الأمر الفيدرالي في مصلحة الإعتماد السويسرية(SAS) Services d'accréditation suisse لدى أمانة الدولة للاقتصاد، المُفَوَضَة بإعتماد المراكز التي تقوم بإعتراف(م.خ.ت.إ) وفقا لأحكام الأمر الفيدرالي المتعلق بالنظام السويسري للإعتماد والتعيين الصادر بتاريخ 17 جوان 1996، كما تتولى هذه المراكز مهمة

---

1) - **Art. 04** du (LFSCSE) : « - Le Conseil fédéral désigne l'organisme d'accréditation des organismes de reconnaissance (**organisme d'accréditation**). Si aucun organisme n'a été accrédité pour effectuer des reconnaissances, le Conseil fédéral désigne l'organisme d'accréditation ou un autre organisme compétent comme organisme de reconnaissance. »
- **Art.05** : « Les organismes de reconnaissance annoncent à l'organisme d'accréditation les fournisseurs qu'ils reconnaissent. L'organisme d'accréditation tient à la disposition du public la liste des fournisseurs reconnus. »

2) - Ordonnance de conseil fédéral suisse sur les services de certification dans le domaine de la signature électronique (Ordonnance sur la signature électronique, OSCSE), du 3 décembre 2004, publiée sur le site : http://admin.chopcfrclassified-compilation20011277index.html
- **Art.1**: «1- Le Service d'accréditation suisse (SAS) du Secrétariat d'État à l'économie accrédite les organismes de reconnaissance des fournisseurs de services de certification selon les dispositions de l'ordonnance du 17 juin 1996 sur l'accréditation et la désignation.
2- S'il n'existe aucun organisme de reconnaissance accrédité, c'est **l'Office fédéral de la communication (office)** qui reconnaît les fournisseurs de services de certification. »
– Ordonnance du 6 octobre 1995 sur les entraves techniques au commerce, LETC (RS 946.51) et les dispositions d'exécution pertinentes. Disponible sur le même site.

رقابة(م.خ.ت.إ) وفقا للإجراءات التي نص عليها القانون الفيدرالي حول العراقيل التقنية للتجارة الصادر في 06 أكتوبر 1995، التي يمكن أن يترتب عنها سحب الإعتراف الممنوح لـ(م.خ.ت.إ) مع تبليغه لهيئة الإعتماد(SAS) التي تُكلف(م.خ.ت.إ) آخر معترف يشرف على مهامه، وذلك وفقا للمادتين 13 و15 من القانون الفيدرالي المتعلق بالتوقيع الإلكتروني.

**ثالثا- التشريعات الوطنية العربية.**

على خلاف تشريعات دول الإتحاد الأوروبي التي أخذت بمخططات الإعتماد الاختياري لمزاولة نشاط خدمات التصديق الإلكتروني، فإنّ التشريعات العربية قد أخذت بنظام الترخيص الإجباري الذي جعلته كشرط جوهري لمزاولة خدمات التصديق الإلكتروني، والتي سنتناول البعض منها على النحو التالي:

**1- القانون التونسي.**

نص القانون التونسي عدد 83-2000 المتعلق بالمبادلات والتجارة الإلكترونية في الفصل الثامن منه، على إنشاء الوكالة الوطنية للمصادقة الإلكترونية(ANCE)[1] كسلطة تصديق رئيسية(مؤسسة عمومية) على مرفق المفاتيح العمومية في تونس، تحت إشراف الوزير المكلّف بالقطاع تتمتع بالشخصية المعنوية وبالاستقلال المالي، إذْ تتولى بكلّ المهام المتعلقة بمنح التراخيص لمزاولة نشاط(م.خ.ت.إ) على كامل التراب التونسي، وممارسة الرقابة حول مدى إحترام(م.خ.ت.إ) للأحكام والنصوص التطبيقية المفروضة عليهم بموجب هذا القانون، مع تحديد مواصفات منظومة إحداث الإمضاء والتدقيق، كما تقوم بإبرام إتفاقيات الإعتراف المتبادل مع الأطراف الأجنبية، وتساهم في أنشطة البحث والتكوين

---

[1] - أنظر الأمر عدد 1044-2008 مؤرخ في 14 أفريل 2008 يتعلق بالمصادقة على النظام الأساسي الخاص بأعوان الوكالة الوطنية للمصادقة الإلكترونية، المنشور في (ر.ر.ج.ت) عدد 32 الصادر في 18 أفريل 2008. http://www.legislation.tn

- **سمير حامد عبد العزيز جمال**، التعاقد عبر تقنيات الإتصال الحديثة، الطبعة الأولى، دار النهضة العربية، القاهرة، 2006، ص 324.

والدراسة ذات العلاقة بالمبادلات والتجارة الإلكترونية، وبصفة عامة تقوم بكلّ نشاط آخر يقع تكليفها به من قِبل "سلطة الإشراف" وله علاقة بميدان تدخلها، وفي الآخير تقوم الوكالة بإصدار وتسليم وحفظ شهادات المصادقة الإلكترونية الخاصة بالأعوان العموميين المؤهلين للقيام بالمبادلات الإلكترونية ويمكن أن يتم ذلك مباشرة أو عبر(م.خ.ت.إ) عموميين.

فوفقا لأحكام الفصلين 21 و22 من الأمر عدد 1667-2001 المتعلق بالمصادقة على كراس الشروط الخاص بممارسة نشاط مزود خدمات المصادقة الإلكترونية[1]، يُمكن لـ (و.و.م.إ) في ظل مهامها الرقابية أن تدخل بصفة دورية إلى أيّ محل لـ(م.خ.ت.إ) قصد مراقبة الموزعات المستعملة منه لتوفير الخدمة، من أجل التدقيق في موثوقية المعدات والقواعد المعتمدة ومدى احترامه لإجراءات السلامة(عمليات قبول الشهادة وأنظمة النفاذ إلى المعلومات السرية)، ومُطابقتها لدفتر الشروط المتعلق بطلب الترخيص كما يُمكن لها طلب الإطلاع من مزود الخدمة على جميع الوثائق والملفات التي تراها ضرورية مع تقديمه لجميع الدفاتر الحسابية والعقود أو أيّة وثيقة تراها ضرورية منه.

**2- القانون المصري.**

قام المشرع المصري بموجب المادة الثانية من قانون رقم 15-2004 المتعلق بتنظيم التوقيع الإلكتروني، بإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات(ITIDA) تحت وصاية الوزير المختص في القطاع تتمتع بالشخصية المعنوية العامة، وذلك بإعتبارها كسلطة تصديق رئيسية تشرف على تنظيم وإدارة مرفق المفاتيح العمومية الهرمي في مصر، وإنطلاقا من ذلك فإنّ الهيئة تباشر المهام المتعلقة بإصدار وتجديد التراخيص اللازمة لمزاولة أنشطة خدمات التوقيع الإلكتروني وفقا لأحكام القوانين واللوائح المنظمة له، وتحديد معايير منظومة التوقيع الإلكتروني مع ضبط مواصفاتها الفنية، كما تقوم بتلقي الشكاوى المتعلقة بأنشطة التوقيع الإلكتروني والمعاملات الإلكترونية وتكنولوجيا المعلومات، مع تقييم الجهات العاملة

---

[1] - الأمر عدد 1667-2001 مؤرخ في 17 جويلية 2001 يتعلق بالمصادقة على كراس الشروط الخاص بممارسة نشاط مزود خدمات التصديق الإلكتروني.http://www.legislation.tn

في مجال أنشطة تكنولوجيا المعلومات وتحديد مستوياتها الفنية بحسب نتائج هذا التقييم، وتنظر في المنازعات التي تنشأ بين الأطراف المعنية بأنشطة التوقيع الإلكتروني مع تقديم المشورة إلى الجهات العاملة في أنشطة تكنولوجيا المعلومات وتدريب العاملين فيها[1].

بالإضافة إلى ذلك تشرف الهيئة على إيداع وقيد وتسجيل النسخ الأصلية لبرامج الحاسب الآلي وقواعد البيانات، التي تتقدم بها الجهات أو الأفراد الناشرون والطابعون والمنتجون لها للمحافظة على حقوق الملكية الفكرية وغيرها من الحقوق، كما تقوم الهيئة بإعتماد الجهات الأجنبية المختصة بإصدار شهادات التصديق الإلكتروني.

**3- قانون الإمارات العربية المتحدة.**

نصت المادة 20 من القانون الإتحادي رقم 01-2006 بشأن المعاملات والتجارة الإلكترونية، على إنشاء جهة مُكلفة بمراقبة خدمات التصديق الإلكتروني والمتمثلة في هيئة تنظيم الإتصالات(TRA) كمراقب لخدمات التصديق الإلكتروني تحت إشراف وزير الإقتصاد الإماراتي، التي تقوم بمهام منح التراخيص والتصديق ومراقبة أنشطة(م.خ.ت.إ) والإشراف عليها، واقتراح اللوائح الخاصة بتنظيم نشاطات التصديق الإلكتروني للوزير الذي يقوم بإصدارها وفقا للمادة 22 من القانون، التي على إثرها تم إصدار لائحة بشأن(م.خ.ت.إ) بموجب القرار الوزاري رقم 2008/01، بحيث تطرق من خلال أحكامها[2] إلى تنظيم خدمات التصديق الإلكتروني المتعلقة بالمستندات والسجلات والتوقيعات الإلكترونية ذات الصلة بالتجارة الإلكترونية، كما منحت للهيئة سلطات واسعة في إطار مهامها التنظيمية والرقابية التي تمارسها على أنشطة(م.خ.ت.إ).

---

[1] – أنظر المادة 04 من قانون رقم 15-2004 المتعلق بالتوقيع الإلكتروني وبإنشاء (هـ.ت.ص.ت.م).

[2] – القرار الوزاري رقم (1) لسنة 2008 بشأن إصدار لائحة مزودي خدمات التصديق الإلكتروني.
http://www.tra.gov.ae/ ou http://www.government.ae
– قامت هيئة تنظيم الإتصالات (TRA) حاليا بمنح التراخيص لـ(م.خ.ت.إ) لكلٍّ من مؤسسة الإمارات للإتصالات، مصرف الهلال، الشركة الدولية لتكنولوجيا المعلومات. http://www.tra.gov.ae/

**4- القانون العمّاني.**

نصت المادة 25 من القانون العمّاني المتعلق بالمعاملات الإلكترونية على السلطة المختصة بمنح التراخيص لمزاولة نشاط خدمات التصديق الإلكتروني، المتمثلة في هيئة تقنية المعلومات(ITA) التي تقوم بالمهام المتعلقة بإصدار التراخيص لممارسة خدمات التصديق، وفقا للأحكام والشروط الواردة في هذا القانون واللوائح والقرارات المنفذة له[1]، مع تحديد رسوم استخراج التراخيص، كما تُشرف على عمليات استيراد أو الترخيص بإستيراد أدوات التشفير اللازمة لأغراض خدمات التصديق أو التي تستخدمها الجهات الحكومية فيما عدا الجهات الأمنية، وزيادة إلى ذلك تُمارس الرقابة والإشراف والتفتيش على أنشطة(م.خ.ت.إ) والتحقق من أنّهم يستخدمون مكونات مادية وبرمجيات وإجراءات آمنة ضد التدخل وسوء الاستعمال، وأنّهم يلتزمون بمستويات الأداء المقررة لضمان سرية وأمن التوقيعات الإلكترونية والشهادات، مع تحديد المستويات والشروط التي يخضع لها (م.خ.ت.إ) والمؤهلات والخبرات التي يتعين أن يحصل عليها موظفوه، كما تقوم الهيئة بتسهيل تأسيس أية أنظمة إلكترونية بواسطة(م.خ.ت.إ) إمّا مُنفردا أو مع(م.خ.ت.إ) آخرون.

**5- القانون الجزائري.**

إنّ حتمية انتقاء نموذج تصديق إلكتروني موثوق به في الجزائر[2]، دفع بـ(س.ض.ب.م) إلى الإعلان عن مناقصة دولية في 6 سبتمبر 2009، لتقديم المساعدة لتنفيذ التصديق الالكتروني في الجزائر، بحيث تمحورت أهم الخدمات المطلوبة في دفاتر الشروط حول اقتراح واحد أو أكثر من نماذج الثقة في التصديق الإلكتروني المناسب للجزائر، ووضع

---

[1] – المرسوم السلطاني رقم 52-2006 الصادر في 31 ماي 2006 بإنشاء هيئة تقنية المعلومات، الجريدة الرسمية لسلطنة عمّان عدد 816. http://www.omanlegal.org/law/search.aspx

[2] – نظمت سلطة ضبط البريد والمواصلات السلكية واللاسلكية مؤتمرين دوليين حول التصديق الإلكتروني بالجزائر بالشراكة مع الإتحاد الدولي للإتصالات السلكية واللاسلكية، فالأول تم تنظيمه يومي الثامن والتاسع ديسمبر 2009 بفندق الهيلتون، أما الثاني يُعد كتكملةً للمؤتمر الأول والذي تم تنظيمه في النادي الوطني للجيش أيام 28، 29، 30، جوان 2011. http://www.arpt.dz/

مخطط خدمات التصديق الإلكتروني يُحدد الإجراءات التي يجب تطبيقها والمعدات أو الوسائل، والموارد البشرية الضرورية، مع تحديد حقوق والتزامات(م.خ.ت.إ) والمُستخدم مع اقتراح الوسائل التقنية والتنظيمية المطبقة على التشفير والإحاطة بإجراءات منح الترخيص لمزاولة نشاط(م.خ.ت.إ)، فحسب(س.ض.ب.م) حوالي ثمانية(م.خ.ت.إ) قدموا عروضهم من أصل 21 الذين سحبوا دفاتر الشروط.

في الأخير تم اختيار مرفق المفاتيح العمومية الهرمي(Hierarchy PKI) كنموذج ثقة للتصديق الإلكتروني في الجزائر[1]، بعد الأخذ بعين الاعتبار تجارب مختلف تشريعات الدول الأجنبية والعربية التي أخذت بنموذج التصديق الهرمي الموحد، بحيث قام المشرع الجزائري بموجب المادة 16 من قانون رقم 15-04 المتضمن القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، بإنشاء "سلطة وطنية للتصديق الإلكتروني" لدى الوزير الأول كسلطة رئيسية إدارية مستقلة تتمتع بالشخصية المعنوية وذمة مالية مستقلة، على مستوى أعلى في هرم مرفق المفاتيح العمومية بالجزائر(يحدد مقرها عن طريق التنظيم) مُكلّفة بترقية استعمال التوقيع والتصديق الإلكترونيين، وتطويرهما وضمان موثوقية استعمالهما وبإعداد سياستها المتعلقة بالتصديق الإلكتروني والسهر على تطبيقها، بعد الحصول على الرأي الإيجابي "للهيئة المكلفة بالموافقة"، كما تقوم السلطة بالموافقة على سياسات التصديق الإلكتروني الصادرة عن "السلطتين الفرعيتين الحكومية والاقتصادية للتصديق الإلكتروني"، وإبرام اتفاقيات الاعتراف المتبادل على المستوى الدولي، والمساهمة في اقتراح مشاريع النصوص التشريعية أو التنظيمية ذات صلة بالتوقيع الإلكتروني أو التصديق الإلكتروني على الوزير الأول، كما تقوم بعمليات التدقيق على مستوى السلطتين "الحكومية والاقتصادية" عن طريق "الهيئة الحكومية المكلفة بالتدقيق" التي لم تنشأ بعد.

إنّ السلطة الحكومية المنشأة لدى وزير البريد وتكنولوجيا الإعلام والاتصال بموجب المادة 26 من نفس القانون، كسلطة تصديق إلكتروني تتمتع بالاستقلال المالي والشخصية المعنوية مكلّفة بالمهام المتعلقة بمتابعة ومراقبة نشاط التصديق الإلكتروني للأطراف الثالثة

---

1) - **Ahmed BERBAR**, op.cit., pp. 26 -29.

الموثوقة مع توفير خدمات التصديق الإلكتروني لفائدة المتدخلين في الفرع الحكومي، أمّا سلطة ضبط البريد والمواصلات السلكية واللاسلكية عُيّنت بموجب المادة 29 من نفس القانون، كسلطة اقتصادية للتصديق الإلكتروني مكلفة بمتابعة ورقابة(م.خ.ت.إ)، وبإعداد سياسة التصديق الخاصة بها وعرضها للموافقة على "السلطة" والسهر على تطبيقها، ومنح التراخيص لـ(م.خ.ت.إ) بعد موافقة "السلطة الوطنية للتصديق الإلكتروني"، والموافقة (س.ض.ب.م) على سياسات التصديق الصادرة عن(م.خ.ت.إ) والسهر على تطبيقها.

إلى جانب ذلك تقوم(س.ض.ب.م) بكلّ المهام المتعلقة بنشر شهادة التصديق الإلكتروني للمفتاح العمومي للسلطة، مع حفظ شهادات التصديق الإلكتروني المنتهية صلاحيتها والبيانات المتصلة بها لغرض تسليمها إلى السلطات القضائية المختصة عند الاقتضاء طبقا للأحكام التشريعية والتنظيمية المعمول بها، واتخاذ التدابير اللازمة لضمان استمرارية الخدمات في حالة عجز(م.خ.ت.إ) عن تقديمها، مع إرسال كلّ المعلومات المتعلقة بنشاط التصديق الإلكتروني إلى السلطة دوريا أو بناء على طلب منها، كما تشرف كذلك(س.ض.ب.م) على التحقق من مطابقة طالبي التراخيص مع سياسة التصديق الإلكتروني بنفسها أو عن طريق مكاتب تدقيق معتمدة، والتأكد من مدى مراعاة(م.خ.ت.إ) المرخص لهم للتأكيدات المقدمة في دفتر الشروط الخاص بمزاولة خدماتهم مع مطالبتهم بأية وثيقة أو معلومة تساعدها أثناء تأدية مهامها الرقابية.

بالإضافة إلى ذلك تشرف(س.ض.ب.م) على عملية إعداد دفتر الشروط الذي يحدد شروط وكيفيات تأدية خدمات التصديق الإلكتروني وعرضه على السلطة الوطنية للتصديق الإلكتروني للموافقة عليه، والسهر على وجود منافسة فعلية ونزيهة باتخاذ كل التدابير اللازمة لترقية أو استعادة المنافسة فيما بين(م.خ.ت.إ)، والتحكيم في النزاعات القائمة بينهم أو مع المستعملين طبقا للتشريع المعمول به، وفي كلّ الظروف تقوم سلطة الضبط بإصدار التقارير والإحصائيات العمومية والتقرير السنوي المتعلق بوصف نشاطاتها، مع احترام مبدأ السرية كما تُبلّغ النيابة العامة بكلّ فعل ذي طابع جزائي يُكتشف بمناسبة تأدية مهامها.

بصدور المرسوم التنفيذي رقم 09-410 المؤرخ في 10 ديسمبر 2009 المحدد لقواعد الأمن المطبقة على النشاطات المنصبة على التجهيزات الحسّاسة، وضع المشرع الجزائري نظام قانوني مُوَحَّدْ لتقييم جميع التجهيزات الحسّاسة بما فيها، معدات وأنظمة أمن تكنولوجيا المعلومات(البرامج ووسائل التشفير) المستخدمة في نشاطات التصديق الإلكتروني وفقا للمعايير والتنظيمات التقنية المعمول بها، والتي أخضعها بموجب المواد 06 و07 و08 من المرسوم[1] لنظام الإعتماد المُسبق على نوعين، يُصدرهما وزير الداخلية والجماعات المحلية بعد أخذ رأي السلطة المؤهلة المُكلفة بالمُصادقة على تجهيزات وبرامج التشفير المصنفة في القسم الفرعي الثالث من القسم(أ)، وبالتالي فإنّ تسليم الإعتماد من النوع الأول يُغطي نشاطات الاتجار، التجهيزات الحسّاسة واستيرادها وتصديرها وصنعها وبيعها، أمّا الإعتماد من النوع الثاني يُغطي نشاط تقديم الخدمات، تركيب التجهيزات الحسّاسة وصيانتها وتصليحها، وذلك بعد تقييم من طرف السلطة المعنية بالمسائل المتعلقة بمؤهلات المتعامل وقدراته المهنية وكذا الشروط الأمنية للمحلات والتجهيزات.

فعلى كلّ راغب في الحصول على إعتماد التجهيزات والبرامج المعلوماتية للتشفير أن يقوم بإيداع طلب في ثلاث نسخ لدى مصالح وزارة الداخلية(مقابل وصل) وفقا للنموذج المعتمد في الملحق الثاني من المرسوم، يكون مُرفقا بتعهد كتابي وفقا للنموذج المعتمد في الملحق الثالث من نفس المرسوم، مع ملف يتضمن جميع الوثائق التي حددتها المادة 09 من المرسوم سواءا كان صاحب الطلب شخص طبيعي أم معنوي، وبعدها تقوم مصالح الوزارة بدراسته في أجل لا يتعدى 65 يوم، التي من خلالها يتم في الحالة الإيجابية منح الإعتماد لمدة 05 سنوات قابلة للتجديد على أن يودع طلب التجديد قبل 06 أشهر من إنقضاء صلاحية الإعتماد الساري، أما في الحالة السلبية يجب تعليل رفض الطلب مع تبليغه للمعني وفقا للمادة 10 من نفس المرسوم.

---

[1] – مرسوم تنفيذي رقم 09-410 المؤرخ في 10 ديسمبر 2009 المحدد لقواعد الأمن المطبقة على النشاطات المنصبة على التجهيزات الحساسة، ج ر عدد 73 الصادر في 13 ديسمبر 2009.

– المادة 02: "يعني بالتجهيزات الحساسة المحددة في الملحق الأول من المرسوم كل عتاد يمكن أن يمس استعماله الغير المشروع بالأمن الوطني وبالنظام العام."

تجدر الإشارة إلى أنّ إقتناء معدات وبرامج التشفير على المستوى الوطني من طرف المتعاملين المعتمدين قانونا يخضع لترخيص من طرف الوالي لمكان ممارسة النشاط (الشخص الطبيعي)، ومقر الشركة في حالة الشخص المعنوي(المادة 13 من المرسوم) أمّا إذا تم اقتناءها على المستوى الوطني من طرف الشخص الطبيعي أو المعنوي لأغراض الحيازة والاستعمال، فتخضع لترخيص(Autorisation) من طرف(س.ض.ب.م) استنادا لترخيص الإستغلال المذكور في المادة 20 من المرسوم،(أي بعد موافقة السلطة المكلفة بالمصادقة على تجهيزات وبرامج التشفير المصنفة في القسم الفرعي 03 من القسم(أ) من الملحق الأول) وذلك لمدة ثلاثة(03) سنوات قابلة للتجديد لمدة (02)عامين[1].

زيادة على ذلك يخضع إقتناء المعدات وبرامج التشفير من السوق الأجنبية وفقا للمادة 14 من المرسوم لتأشيرة(Visa)، تمنح من طرف الوزير المُكلّف بتكنولوجيا الإعلام والاتصال بعد الموافقة المُسبقة لمصالح الوزارتين المكلفتين بالدفاع الوطني والداخلية، على أن تكون المعدات وبرامج التشفير المقتناة مُرَكَّبَة وفي شكل قِطَعٍ أو مُدمجة ضمن نظام، مُطابقة للمعايير والتنظيمات التقنية المعمول بها( تُحدد بموجب التنظيم)[2]، كما يجب أن تتم عملية بيع معدات وبرامج التشفير من متعامل لمتعامل إلاّ لفائدة متعاملين حائزين على إعتماد من النوع الأول وبناءا على ترخيص الإقتناء المذكور في المادة 13 من المرسوم.

---

1) – **Décision n° 16/SP/PC/ARPT** du 11/06/2012 portant sur la durée de validité de l'autorisation d'exploitation des équipements et des logiciels d'encryption. http://www.arpt.dz

-**Art.01** : « La présente décision a pour objet de définir la durée de validité de l'autorisation portant sur l'exploitation des équipements et des logiciels d'encryptions, classés dans la sous-section 3 de la section A du décret exécutif n°09-410 fixant les règles de sécurité applicables aux activités portant sur les équipements sensibles. »

-**Art.02** : « L'autorisation d'exploitation des logiciels d'encryptions visée à l'article 1er ci-dessus est délivrée pour une durée maximale de **trois (03) ans. »**

-**Art.05** : « L'autorisation d'exploitation des logiciels d'encryptions visée à l'article 1er ci-dessus est renouvelable pour une durée maximale de **deux (02) ans. »**

-**Art.06** : « La présente décision est applicable à compter de la date de sa publication sur le site web de l'ARPT. »

2) - **Hadjira BOUDER**, le cadre juridique de la signature et de la certification électronique en Algérie: que reste-t-il à faire?, Intervention présentée au (SICE' 2011) ARPT, Alger du 28 Au 30 Juin 2011, pp. 20-24. http://www.arpt.dz/

بالإضافة إلى ما سبق يخضع إستغلال معدات وبرامج التشفير بموجب المادة 20 من المرسوم لترخيص مُسبق(autorisation préalable) من طرف وزارة تكنولوجيا المعلومات والاتصال أو(س.ض.ب.م) حسب الحالة، بعد موافقة مصالح وزارتي الدفاع الوطني والداخلية والسلطة المكلفة بالمصادقة على تجهيزات وبرامج التشفير(التي لم تُؤسس بعد) على أن تُحدد شروط وكيفيات إقتناء وحيازة واستغلال واستعمال والتنازل، عن معدات وأنظمة أمن تكنولوجيا المعلومات من قبل الأشخاص الطبيعية والمعنوية بقرار مُشترك بين الوزراء المكلفين بالداخلية، والدفاع الوطني وتكنولوجيا الإعلام والاتصال والنقل وفقا للمادة 21 من المرسوم التنفيذي رقم 09-410.

من خلال كل ما سبق نصل إلى أنّ أغلبية التشريعات الوطنية انتهجت نماذج الثقة في إطار مرافق المفاتيح العمومية تشرف عليها جهات رسمية تقوم بإدارة وتنظيم نشاطات التصديق الإلكتروني التي تخضع بدورها لمجموعة من الشروط وفقا للمعايير المعمول بها.

## الفرع الثاني:

## شروط ممارسة نشاط مزود خدمات التصديق الإلكتروني.

نصت مُختلف التشريعات المنظمة للمعاملات الإلكترونية على مجموعة من الشروط المتعلقة بمُزاولة خدمات التصديق الإلكتروني التي تجعل من(م.خ.ت.إ) جدير بالثقة، التي سنتطرق إليها من خلال التشريعات الدولية وبالخصوص قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية لعام2001، والتوجيه الأوروبي رقم 93/99 المتعلق بالتوقيعات الإلكترونية(أولا)، ثم للتشريعات الوطنية الأجنبية(ثانيا)، والتشريعات الوطنية العربية(ثالثا).

### أولاً- التشريعات الدولية:

### 1- قانون الأونسيترال الدولي النموذجي بشأن التوقيعات الإلكترونية لعام 2001.

نصت المادتين09 و10 من القانون النموذجي بشأن التوقيعات الإلكترونية على مجموعة من الشروط الفنية والتقنية لمزاولة خدمات التصديق الإلكتروني، والمتمثلة في:

أ)- يجب أن تتوافر لدى(م.خ.ت.إ) الموارد المالية التي من شأنها أن تُساهم في تغطية مُختلف الأضرار، أو تُمكنه من تطوير نفسه(شخص طبيعي) أو شركته بالتقنيات التكنولوجية الحديثة، كما يتعين أن تكون لديه(م.خ.ت.إ) موارد بشرية جديرة بالثقة حاصلين على كفاءات عالية من المهارات والمؤهلات الفنية والخبرة، مع القدرة على استيعاب فنون التكنولوجيا الحديثة والتنفيذ الفعّال لمسؤولياتهم وواجباتهم المهنية وفقا للتشريعات والتنظيمات المتعلقة بخدمات التصديق الإلكتروني؛

**ب)**- أن يستخدم في أداء خدماته لمعدات وبرامج معلوماتية حديثة مُرتبطة ببعضها البعض بنظام شبكي مُؤمن بنظم أمن معلومات، مُطابقة للمواصفات والمعايير الدولية المعترف بها التي تمنع كافة أشكال التهديد والاختراق في المعلومات أو سرقة البيانات المخزنة أو التلاعب فيها من طرف الغير؛

**ج)**- أن يُوفر إجراءات معالجة طلبات إصدار شهادات التصديق والحصول عليها وفقا للبيانات الحقيقية التي يقدمها صاحب الشهادة، مع مراعاة المتطلبات التقنية للشهادات المحددة بموجب المعايير الدولية المعترف بها؛

**د)**- أن يكون لديه نظام مؤمن خاص بحفظ المعلومات الخاصة بأصحاب الشهادات وبالخصوص البيانات الإلكترونية المتعلقة بإحداث التوقيعات الإلكترونية، والبيانات الدقيقة والحسّاسة ذات صلة بالمعطيات الشخصية لأصحاب شهادات التصديق الإلكتروني، وأن يعمل على إتاحة المعلومات الخاصة بالموقعين كلما طلبوا ذلك وفقا لشروط معينة؛

**هـ)**- إستيفاءه(م.خ.ت.إ) لمعايير التفتيش والتدقيق التي تُشرف عليها هيئة مُستقلة قبل مباشرته لمهامه، لتقييم مدى كفاءته وقدرته على القيام بخدمات التصديق الإلكتروني وفقا للمعايير المعمول بها وفقا لتشريع كلّ دولة، إذ يمكن لهذه الهيئات أن تقوم بعمليات تدقيق وتفتيش دورية حتى أثناء مباشرته لنشاطات التصديق الإلكتروني؛

**و)**- التأكيد في بيان سياسة التصديق الإلكتروني عن تواجد خدمات تصديق إلكتروني موثوق بها، التي ينبغي عليه(م.خ.ت.إ) أن يُنشرها على مُستوى موقعه الإلكتروني عبر شبكة الإنترنيت، بمعرفة الهيئة المانحة للإعتماد أو الترخيص، لذا يجب على المزود أن يوضح بدقة في الإعلان لجميع أسعار الخدمات التي يُوفرها بدون غموض، وأن يُبين ما إذا كانت خاضعة لرسوم أو ضرائب، مع تقديمه لضمانات الإمتثال لما قدمه في بيان ممارسة

خدمات التصديق الإلكتروني المُعلن، مع تحديد الإلتزامات والمسؤولية المترتبة عند الإخلال بها من جانب كلّ طرف في عملية التصديق الإلكتروني وطرق حلّ النزاعات؛

ز)- حيازة أنظمة خاصة بإيقاف وإلغاء شهادات التصديق الإلكتروني(LCR) على مستوى الموقع الإلكتروني لـ(م.خ.ت.إ)، تضمن عملية الإدراج الفوري والإتاحة اللحظية لقوائم شهادات التصديق الإلكتروني الموقوفة أو المُلغاة، فور التحقق من توافر الأسباب التي تستدعي ذلك قصد السماح للعموم بالإطلاع بصفة مُستمرة على المعلومات المُدونة فيها وفقا لشروط معينة[1].

## 2- التوجيه الأوروبي رقم 93/99 المتعلق بالتوقيعات الإلكترونية.

نص المشرع الفيدرالي للإتحاد الأوروبي في الملحق الثاني من التوجيه الأوروبي رقم 93/99 المتعلق بالتوقيعات الإلكترونية، على مجموعة من الشروط الفنية والتقنية الواجب توافرها لدى(م.خ.ت.إ) الراغب في الحصول على تأهيل لخدماته والمتمثلة في:

1- يجب أن يُثبت جدارته في تقديم خدمات تصديق إلكتروني موثوق بها، مع ضمان خدمة دليل إرشادي سريع ومؤمن لإصدار وإلغاء شهادات التصديق الإلكتروني مع التحديد الدقيق لتاريخ ووقت إصدارها أو إلغاءها(الفقرات a-b-c)؛

2- امتلاك معدات ووسائل موثوق بها تمكن من فحص هوية والصفات الخصوصية للأشخاص التي تطلب إصدار شهادات التصديق الإلكتروني الموصوفة، كما يجب أن تتوافر لديه(م.خ.ت.إ) موارد بشرية ذات معارف وكفاءات عالية في مجال تقديم خدمات التصديق الإلكتروني وفقا للمعايير المعمول بها، بالإضافة إلى ذلك يجب أن تتوافر لديه موارد مالية كافية لتغطية المسؤولية المترتبة عن الأضرار في إطار عقود التأمين(d-e-h)؛

3- إستعمال أنظمة ومُعدات موثوق بها تضمن سرية إحداث بيانات التوقيعات الإلكترونية الموصوفة، مع اتخاذ الإجراءات اللازمة لحماية شهادات التصديق من التزوير(f-g-j)؛

---

[1] - **عبد الفتاح بيومي حجازي**، مرجع سابق، ص 120.

4- إعلان بيان السياسة العامة المتبعة في تقديم خدمات التصديق الإلكتروني(DPC) يُوضح فيه جميع الإلتزامات الملقاة على أطراف التصديق الإلكتروني، (قبل إبرامه لأيّة علاقة عقدية مع المشتركين)، وطرق إستعمال الشهادات وبتواجد نظام الإعتماد الاختياري وبكل طرق إيداع الشكاوى وحلّ النزاعات في حالة نشوبها، الخ...(k)،

5- إستعمال أنظمة موثوقا بها في حفظ شهادات التصديق الإلكتروني في شكلها الإلكتروني، تضمن الإتاحة اللحظية لها عند الحاجة(i-l)، بالإضافة إلى هذه الشروط يجب على (م.خ.ت.إ) التقيد بالمواصفات المحددة في الملحق الأول المتعلقة بشهادات التصديق الإلكتروني الموصوفة.

**ثانيا- في التشريعات الوطنية الأجنبية.**

قامت الدول التي أخذت بمخططات أنظمة الإعتماد الإختياري بوضع مجموعة من الشروط التقنية والفنية على كلّ(م.خ.ت.إ)، يرغب في طلب تأهيل إختياري لخدماته والتي سنتطرق إليها على النحو التالي:

**1- المشرع الفرنسي.**

منح المشرع الفرنسي بموجب المادة 07 من المرسوم رقم 2001-272 المتعلق بالتوقيع الإلكتروني، لكلّ(م.خ.ت.إ) تتوافر فيه المواصفات التقنية والفنية التي حددتها المادة 06 من نفس المرسوم، إمكانية طلب الحصول على تأهيل اختياري لخدماته من أيّة هيئة معتمدة(Organismes de qualification) من طرف اللجنة الفرنسية للإعتماد (COFRAC)، وفقا لإجراءات الفصل الثاني المحددة بموجب قرار وزير الصناعة المنتدب المؤرخ في 26 جويلية 2004 المتعلق بالإعتراف بمؤهلات(م.خ.ت.إ) واعتماد الهيئات التي تقوم بتقييمها[1]، وبالتالي فعلى أيّ راغب في الحصول على تأهيل اختياري لخدمات تصديق

---

1) - **Art. 07 :** (Décret n° 2001-272 du 30 mars 2001 relatif à la signature électronique.)

« Les prestataires de services de certification électronique qui satisfont aux exigences fixées à l'article 06 peuvent demander à être reconnus comme qualifiés. Cette qualification qui vaut présomption de conformité aux dites exigences, est délivrée par les organismes ayant reçu à cet effet une accréditation délivrée par une instance désignée par arrêté du ministre chargé de

إلكتروني مؤهلة، أن يقوم باختيار هيئة معتمدة وعلى نفقاته(PSCE)، لتقييم خدماته في مجال التصديق الإلكتروني عن طريق التحقق من مدى مطابقتها للمواصفات الفنية والتقنية التي حددتها المادة 2/06 من المرسوم رقم 2001-272 المتعلق بالتوقيع الإلكتروني والمتمثلة في:

1- إثبات وثاقة خدمات التوثيق الإلكتروني المُتَاحَة مع ضمان تقديم خدمة فعالة لإصدار شهادات التصديق إلكتروني تسمح لصاحبها من طلب إلغاءها عند الضرورة، مع التحديد الدقيق لتاريخ ووقت إصدار أو إلغاء الشهادة الإلكترونية (الفقرات a-b-c-d)؛

2- الإعتماد على موارد بشرية ذي خبرات ومعارف وكفاءات مهنية كافية لتوفير خدمات التصديق الإلكتروني، مع إستخدام معدات وأنظمة أمن تكنولوجيا معلومات معتمدة من طرف الجهات الرسمية(e-f-g)؛

3- اتخاذ التدابير اللاّزمة ضدّ أيّ إستعمال تعسفي يستهدف الشهادة الإلكترونية، مع ضمان سلامة وسرية بيانات إحداث التوقيع الإلكتروني الأحادية الاتجاه، ومُطابقتها مع بيانات فحصه (التوقيع) (h-I-j)؛

4- إستخدام أنظمة مؤمنة لحفظ الشهادات الإلكترونية تضمن عدم النفاذ إلى بياناتها الإلكترونية من دون الحصول على ترخيص من طرف(م.خ.ت.إ)، وأيّ إستعمال للشهادة يجب أن لا يتم إلاّ بعد موافقة صاحبها، ويجب على الأنظمة أن تضمن كشف أيّ تعديل أو تغيير يَمُسّ بسلامتها(k-l)؛

5- القيام بكلّ الإجراءات المتعلقة بفحص هوية صاحب طلب إصدار الشهادة الإلكترونية والتحقق أثناء إصدارها من دقة المعلومات، التي تحتويها ومُطابقة بيانات إحداث التوقيع الإلكتروني مع بيانات فحصه(m-n)،

---

l'industrie. Elle est précédée d'une évaluation réalisée par ces mêmes organismes selon des règles définies par arrêté du premier ministre. L'arrêté du ministre chargé de l'industrie prévu à l'alinéa précédent détermine la procédure d'accréditation des organismes et la procédure d'évaluation et de qualification des prestataires de services de qualification électronique. » http:// www.legifrance.gouve.fr/

6- نشر بيان ممارسة خدمات التصديق الإلكتروني عبر الإنترنيت يبين فيه طرق وشروط إستعمال شهادات التصديق الإلكتروني، ومدى حصوله أم لا على تأهيل اختياري وفقا للمادة 07 من نفس المرسوم، مع تحديد طرق إبداء الشكاوى وحلّ النزاعات(o-p).

بالإضافة إلى الشروط السابقة يجب على كلّ راغب في تأهيل خدماته المتعلقة بالتصديق الإلكتروني أن يتقيد بالمواصفات التقنية المعمول بها وفقا للفقرة الأولى من المادة السادسة(1/06) من نفس المرسوم المتعلقة ببيانات الشهادة الإلكترونية الموصوفة.

بعد الانتهاء من التقييم تقوم الهيئة المعتمدة بإصدار تقرير تُبدي من خلاله بإعتراف أو من عدمه بمؤهلات(م.خ.ت.إ)، بالإضافة إلى الملاحظات المحتملة من طرفه والذي تُبلغه لوكالة(ANSSI)، ففي حالة اعترافها بخدمات(م.خ.ت.إ) تُصدر شهادة تأهيل مدة صلاحيتها لا تتعدى ثلاثة(03) سنوات، (بعدما أن كانت **سنة واحدة** في ظل القرار المُلْغَى لوزير الإقتصاد والمالية الفرنسي بتاريخ 31 ماي 2002)، التي تُبَلَّغْ نسخة منها إلى وكالة (ANSSI)[1] ، ففي خلال هذه المدة يخضع(م.خ.ت.إ) المؤهل لتدقيق سنوي على الأقل من طرف الهيئة المعتمدة(Organisme accrédité)، الذي يمكن أن يترتب عنه(التدقيق) إيقاف أو سحب الشهادة الممنوحة له (الشكل رقم 05).

## 2- المشرع البلجيكي.

قام المشرع البلجيكي بتأسيس نظام إعتماد اختياري (BE.SIGN) من أجل رفع مستوى الثقة والأمان في خدمات التصديق الإلكتروني التي يُتيحها المزودين، وإخضاع أنشطتهم لرقابة الدولة من خلال إنشاء إدارة تحت سلطة وزير الشؤون الإقتصادية، تُشرف على إجراءات منح وسحب الإعتماد، فعلى كلّ(م.خ.ت.إ) الراغب في الحصول على الإعتماد

---

1) – **Arts. 6, 7, 8, 9, 10**, de l'Arrêté de ministre délégué à l'industrie, du 26 juillet 2004 relatif à la reconnaissance de qualification des prestataires de services de certification électronique et à l'accréditation des organismes qui procèdent à leur évaluation.
- **Lionel BOUCHURBERG**, Internet et commerce électronique (Site web- Contrats- Responsabilité- Contentieux), 2e édition, DELMACE, France, 2001, p. 147.

وفقا للمادة 1/17-2 من القانون الملكي البلجيكي[1]، أن يستجيب للمواصفات التقنية والفنية المحددة في **الملحق الثاني** منه(المتعلق بـ(م.خ.ت.إ) المعتمدين)، **والملحق الأول** منه (الخاص بإصدار شهادات التصديق الموصوفة)، **والملحق الثالث** منه(المتعلق بمنظومة أمن إحداث التوقيعات الإلكترونية)، والتي نقلها المشرع البلجيكي حرفيا من التوجيه الأوروبي رقم 93/99 المتعلق بالتوقيعات الإلكترونية.

فبعد إستيفاء(م.خ.ت.إ) للشروط والمواصفات التقنية والفنية المحددة في الملاحق السابقة، ما عليه إلاّ مُراعاة إجراءات الحصول أو تجديد الإعتماد(BE.SIGN) المحددة بموجب المادتين الثالثة والرابعة من القرار الملكي، التي تبدأ بإيداع أو إرسال طلب موقع ومؤرخ من طرفه كتابيا أو إلكترونيا وفقا للنموذج المحدد من طرف إدارة النوعية والأمن فرع الإعتماد(مصلحة التوقيعات الإلكترونية)، التابعة لوزير الشؤون الإقتصادية عن طريق البريد العادي أو الإلكتروني عبر الموقع الإلكتروني للوزارة، وبمُجرد إستلام الإدارة للطلب بمقابل إيصال يُثبت استلامه، تقوم في خلال العشرة أيام(10) الموالية للاستلام، بإعلام(م.خ.ت.إ) بالإجراءات الواجبة الإتباع وبالهيئات والمراكز المُعتمدة، التي تقوم على نفقاته بتدقيق تقييمي (Un audit d'évaluation)، لمؤهلات خدماته في مجال التصديق الإلكتروني، ومدى مُطابقتها للمواصفات التقنية المحددة في الملحق الثالث من القانون الملكي السالف الذكر[2].

---

1) – **Art. 17** : « 1- Un prestataire de service de certification qui répond aux exigences de l'annexe II, délivrant des certificats qualifiés qui répondent aux exigences de l'annexe I et qui utilise des dispositifs de création répondant aux exigences de l'annexe III, peut demander une accréditation à l'Administration. L'accréditation prévue par la présente loi se base sur le résultat d'une évaluation, par une entité visée à l'article 2, 13°, de la conformité aux exigences des annexes I, II et III, et le cas échéant, à celles liées à d'autres services et produits délivrés par les prestataires de service de certification.
2- Le Roi précise les conditions visées au § 1er et fixe : 1- la procédure de délivrance, de suspension et de retrait de l'accréditation;
2- les redevances dues au « Fonds pour l'accréditation » pour la délivrance, la gestion et la surveillance de l'accréditation;
3- les délais d'examen de la demande;
4- les modalités du contrôle des prestataires de service de certification accrédités. »

2) – **Art. 3**(Arrêté royal du 6 décembre 2002) : « **§1-** La demande visant à l'obtention ou au renouvellement d'une accréditation ″BE.SIGN″ doit parvenir à l'Administration de la Qualité et de la Sécurité, Division Accréditation, Service de la Signature électronique du Ministère

بعدها يقوم(م.خ.ت.إ) بموجب المادة 1/04 من القرار الملكي باختيار أحد الهيئات المعتمدة، التي تقوم بتقييم خدماته في ظرف ستة أشهر(06) الموالية لتعيينها، التي تقوم من خلال هذه الفترة بتسليم تقرير التدقيق للإدارة، فإذا كان التقرير إيجابي تمنح الإدارة قرار الإعتماد(BE.SIGN) لمدة ثلاثة(03) سنوات قابلة للتجديد، وفقا لتقرير تدقيق إيجابي الذي يتم في ظرف ثلاثة(03) أشهر السابقة لتاريخ انتهاء الإعتماد الأول، أو تقوم الإدارة لسبب شرعي بتمديد مُؤقت لصلاحية الإعتماد لمُدة أقصاها ستة أشهر(06)، التي تنتهي بمُباشرة الإجراءات العادية بالتجديد، كما يُمكن للإدارة في حالة تشكيكها في التقرير أن تَطلبَ تدقيق تقييمي إضافي على نفقة(م.خ.ت.إ) وفقا للمادة 4/04 من القرار الملكي، وفي كلّ الظروف يخضع(م.خ.ت.إ) أثناء مدة الإعتماد لرقابة من طرف الهيئات المُعتمدة التي تقوم بتدقيقات دورية(Audits périodiques) منتظمة، تُبلّغ على إثرها النتائج المتحصل عليها للإدارة وفقا للمادة 6/04 من القرار الملكي، كما يُمكن للإدارة وعلى نفقاتها أن تقوم في أيّة لحظة برقابة فجائية لدى(م.خ.ت.إ)، مع استعانتها بخبراء مُختصين مُستقلين ماليا وإداريا عن(م.خ.ت.إ) المؤهل أثناء أدائها بمهامها التي يترتب عنها وقف أو سحب الإعتماد(BE.SIGN) [1].

---

des Affaires économiques par courrier ordinaire, via le site internet http://mineco.fgov.be, ou par courrier électronique à BE.SIGN@mineco.fgov.be.

**§ 2-** Les demandes visées aux §§ 1er et2 se font sur un formulaire établi par l'Administration, disponible également sous forme électronique. La demande doit être datée et signée, qu'elle soit sous forme manuscrite ou électronique. La signature, quand elle se présente sous forme électronique, doit répondre aux exigences de l'article 4. § 4 de la loi. En annexe à sa demande d'accréditation, le prestataire de service de certification communique sa déclaration de pratique de certification.

**§ 3-** Dans les dix jours après réception de la demande, l'Administration fait un accusé de réception et informe le prestataire de service de certification des procédures à suivre…

En particulier, l'Administration communique les dernières mises à jour des listes suivantes, en fonction des besoins:**1-** les entités définies à l'article 2, 13° de la loi; **2-** les organismes compétents pour l'évaluation des dispositifs sécurisés de création de signature électronique par rapport aux exigences de l'annexe III de la loi, comme précisé à l'article 7, § 2 de la loi. »

1) –**Art. 4§4** (Arrêté royal du 6 décembre 2002) : « Si tous les éléments du rapport d'audit initial sont positifs, l'Administration octroie une accréditation ″BE.SIGN″ pour une durée de 3 ans. En cas de doute, l'Administration peut demander un audit complémentaire. Ces frais d'audits sont à charge des prestataires de service de certification. L'accréditation est renouvelable, sur base de rapports d'audits positifs. Ces derniers, appelés audits de renouvellement, sont aussi complets que les audits initiaux et sont effectués dans les trois mois qui précèdent la date d'expiration de l'accréditation. »

**ثالثا- التشريعات الوطنية العربية:**

على خلاف تشريعات دول الإتحاد الأوروبي التي انتهجت مخططات الإعتماد الاختياري لمزاولة نشاطات التصديق الإلكتروني، فإنّ التشريعات العربية المنظمة للمعاملات الإلكترونية، أخذت بنظام الترخيص الإجباري الذي جعلته كشرط جوهري لمزاولة نشاطات التصديق الإلكتروني، والتي سنتطرق إليها على النحو التالي:

**1- القانون التونسي.**

فرض المشرع التونسي مجموعة من الشروط الفنية والتقنية لمزاولة نشاط(م.خ.ت.إ) التي حددها بموجب القانون عدد 83-2000 المؤرخ في 09 أوت 2000 المتعلق بالمبادلات والتجارة الإلكترونية، والأمر عدد 1667-2001 مؤرخ في 17 جويلية2001 المتعلق بالمصادقة على كرّاس الشروط الخاص بممارسة نشاط(م.خ.ت.إ)، فوفقا للفصل 11 من القانون المتعلق بالمبادلات والتجارة الإلكترونية يجب على(م.خ.ت.إ) سواءا أكان شخصا طبيعيا أم معنويا أم ممثلا قانونيا للشخص المعنوي، الراغب في الحصول على ترخيص لمزاولة نشاط خدمات التصديق الإلكتروني، أن يكون ذوي الجنسية التونسية منذ خمسة أعوام على الأقل، متحصلا على الأقل على شهادة الأستاذية أو ما يُعادلها، وأن يكون مقيما بالبلاد التونسية متمتعا بحقوقه المدنية والسياسية ونقي السوابق العدلية[1]، كما يجب كذلك أن لا يتعاط نشاطا مهنيا آخر.

كما يتعين على أي راغب في الحصول على ترخيص لمزاولة نشاط خدمات التصديق الإلكتروني وفقا للفصل الثاني من الباب الأول، والفصل الثالث من الباب الثاني من الأمر عدد 1667-2001 المتعلق بالمصادقة على كرّاس الشروط الخاص بممارسة نشاط

---

- Voir aussi l'article 07 de l'arrêté royal du 6 décembre 2002.
- **Didier GOBERT, «** Cadre juridique pour les signatures électroniques et les services de certification: analyse de la loi du 9 juillet 2001», Publié in La preuve, formation permanente CUP, volume 54, mars 2002, pp. 84, 85. http://www.consultandtraining.com

[1] - أنظر الفصل الخامس، من الأمر التونسي عدد 1667-2001 مؤرخ في 17 جويلية 2001 المتعلق بالمصادقة على كرّاس الشروط الخاص بممارسة نشاط مُزود خدمات التصديق الإلكتروني.

(م.خ.ت.إ)، أن يُؤَمِّنَ مسؤوليته المدنية والمهنية لتغطية الأضرار التي يُمكن أن تُلحق بالغير من جرّاء الخدمات التي يُوفرها، فعلى الشخص المعنوي أن يُوَفِّرَ رأسُ مال لا يقل عن مائة ألف دينار تونسي يُسدد بالكامل عند إنشاء المؤسسة، أمّا إذا كان الشخص طبيعي فعليه تقديم شهادة بنكية تُثبت توفر رصيد لا يقل عن مائة ألف دينار تونسي مُخصص لإنجاز المشروع، ومهما كان الشخص(طبيعي أم معنوي) يجب أن لا يكون في حالة تعارض مع شروط ممارسة مهنة تجارية طبقا للتشريع الجاري المعمول به[1].

بالإضافة إلى ما سبق قسم المشرع التونسي الوظائف التقنية لـ(م.خ.ت.إ) من خلال الفصل الثالث من الباب الثاني، إلى ثلاثة أصناف بِحَسَبِ المسئولين الأَوَّلِينَ لكلٍّ منظومة فالمسئول الأول على المنظومة الآلية والموزعات الخاصة بمنظومة المصادقة، يسهر على حسن إستغلال المنظومة وصيانة المعدات والمنظومات الإعلامية وتشغيل هذه الأخيرة وإيقافها وتأمين عملية الخزن الإلكتروني للمعلومات، أمّا المسؤول الأول على أنظمة السلامة يتولى تسيير الأعوان المكلفين بإجراء عمليات المصادقة، وتصور إنجاز قواعد السلامة والتثبت في سجلات المصادقة والتثبت من مطابقة القواعد المستعملة مع القواعد المعتمدة من قِبل(و.و.م.إ)، ويتولى المسؤول الأول على تعديل منظومة المصادقة بتسيير طرق قبول الحرفاء وإحداث وتجديد الشهادات.

لذا يُشترط في المسئولين على الوظائف الثلاثة[2] أن يكونوا متحصلين على الأقل على شهادة الأستاذية أو ما يُعادلها، وتكوين خاص في سلامة منظومة الإتصال وشبكة الإتصالات والمبادلات والتجارة الإلكترونية، مع عدم إمكانية أيّ عون أو مسئول من ممارسة أكثر من وظيفة واحدة من هذه الوظائف، فبإستثناء الأعمال العلمية والأدبية والفنية، لا يحق

---

[1] – **عيسى غسان ربضي**، القواعد الخاصة بالتوقيع الإلكتروني، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2009، ص 124.

[2] – أنظر الفصلين 04 و06 (الباب الثاني) من الأمر عدد 1667-2001 المتعلق بالمصادقة على كرّاس الشروط الخاص بممارسة نشاط مُزود خدمات التصديق الإلكتروني (تونس).

لأيٍّ منهم أن يقوم بعمل مأجور عليه أو كموظفين بصفتهم أعضاء مجلس أو وكلاء، مدراء في مؤسسة تجارية دون الحصول على ترخيص كتابي أو إلكتروني من (و.و.م.إ).

كما يجب على كلّ راغب في مزاولة نشاط (م.خ.ت.إ) أن يراعي الإجراءات المتعلقة بالحصول على الترخيص، التي حددها الأمر عدد 1668-2001 المؤرخ في 17 جويلية 2001، المتعلق بضبط إجراءات الحصول على ترخيص لممارسة نشاط (م.خ.م.إ)، فوفقا لأحكامه[1] توجه طلبات الحصول على الترخيص إلى(و.و.م.إ) بواسطة رسالة موصى عليها أو بوثيقة إلكترونية موثوق بها بمقابل وصل إيداع يبين الإعلام بالوصول أو بالإيداع لدى الوكالة، متضمنة الوثائق التي حددها الفصل الثاني من الأمر، مع الدفع المسبق لرسم إيداع المقدر حسب الفصل الرابع منه بـ200 دينار تونسي غير قابل للرد في حالة رفض الترخيص(الفصل 09 منه)، وبعدها تقوم الوكالة(ANCE) بالرد لصاحب الطلب في خلال ثلاثة أشهر(03) من تاريخ إيداع الطلب مع الوثائق المطلوبة في الفصل الثاني، أو من تاريخ استكمال المعلومات المطلوبة وفقا للفصل السابع من الأمر إمّا بمنح الترخيص أو بالرفض مع التعليل بذلك.

فمن خلال هذه المدة تقوم مصالح الوكالة بإعداد تقرير معاينة(بعد إعلام صاحب الطلب بموعد إجراء المعاينة قبل عشرة(10) أيام من تاريخها بواسطة رسالة موصى عليها) يتضمن(التقرير) تقييم لجميع الوسائل التقنية، والمالية والبشرية وتهيئة المحل ومدى مطابقتها لدفتر الشروط الخاص بمزاولة نشاط خدمات المصادقة الإلكترونية(الفصل 05 منه)، فإذا كان التقرير إيجابي تُصدر الوكالة قرار الترخيص لمدة ثلاثة(03) سنوات قابل للتجديد(الفصل 06 منه)، كما يمكن للوكالة رفض طلب الترخيص لصاحبه إذا لم تتحصل على المعلومات الضرورية التي طلبتها منه لإستكمال الملف في أجل شهر من تاريخ إعلامه برسالة موصى عليها أو بوثيقة إلكترونية موثوق بها، أو في حالة عدم توفر الشروط

---

[1] – الأمر عدد 1668-2001 المؤرخ في 17 جويلية 2001، يتعلق بضبط إجراءات الحصول على ترخيص لممارسة نشاط مزود خدمات المصادقة الإلكترونية، المنشور في ر.ر.ج.ت عدد 60 الصادر في 17 جويلية 2001.

المنصوص عليها في دفتر الشروط الخاص بممارسة نشاط(م.خ.ت.إ) المشار إليها في الفصل الثاني من نفس الأمر.

في حين يُمكن للوكالة أن تسحب الترخيص الذي منحته للمزود بعد سماعه إذا تحصل على الترخيص، بناءا على تصاريح خاطئة أو أيّة وسيلة آخرى غير شرعية أو عدم مراعاته للإلتزامات المفروضة عليه، بموجب القانون المتعلق بالمبادلات والتجارة الإلكترونية أو إخلاله بالشروط المنصوص عليها في دفتر الشروط الخاص بمزاولة نشاط(م.خ.م.إ)، أو في حالة ما إذا أخل المزود بالشروط التي مُنح على أساسها الترخيص(الفصل10 منه).

تجدر الإشارة أن المشرع التونسي ترك مسألة إعتماد(م.خ.ت.إ) الأجانب لـ (و.و.م.إ) بإعتبارها كسلطة تصديق رئيسية على مستوى مرفق المفاتيح العمومية في تونس، التي تقوم بموجب الفصل 4/09 من قانون عدد 83-2000 المتعلق بالمبادلات والتجارة الإلكترونية بإبرام إتفاقيات الإعتراف المتبادل مع الجهات الأجنبية المماثلة لها، بهدف الإعتراف بشهادات التصديق الإلكتروني الأجنبية.

**2- القانون المصري.**

حدّد المشرع المصري بموجب المادة 12 من اللائحة التنفيذية لقانون التوقيع الإلكتروني وبإنشاء(هـ.ت.ص.ت.م)، مجموعة من الشروط الواجب توافرها لدى جهة التصديق الإلكتروني الراغبة في الحصول على ترخيص مُسبق، لمزاولة نشاطاتها المتعلقة بإصدار شهادات التصديق الإلكتروني، والمتمثلة في:

أ)- أن يتوافر لديها نظام تأمين المعلومات وحماية البيانات وخصوصيتها بمستوى لا يقل عن المستوى المذكور في المعايير والقواعد المشار إليها في الفقرة(د) من الملحق الفني والتقني للائحة، مع دليل إرشادي يتضمن كلّ من إصدار شهادات التصديق الإلكتروني- إدارة المفاتيح الشفرية- إدارة الأعمال الداخلية- إدارة التأمين والكوارث، وذلك وفقا للمعايير الفنية والتقنية المذكورة في الفقرة (هـ) من الملحق الفني والتقني للائحة؛

**ب)**- منظومة تكوين بيانات إنشاء التوقيع الإلكتروني مؤمنة وفقا للضوابط الفنية والتقنية المنصوص عليها في المواد(2-3-4) من اللائحة، ونظام لتحديد تاريخ ووقت إصدار الشهادات، وإيقافها، تعليقها، وإعادة تشغيلها وإلغاءها، ونظام آخر للتحقق من الأشخاص المُصدر لهم شهادات التصديق الإلكتروني والتحقق من صفاتهم المميزة، مع الإستعانة بالمتخصصين من ذوي الخبرة الحاصلين على المؤهلات الضرورية لأداء الخدمات المرخص بها؛

**ج)**- أن يكون لديها نظام حفظ بيانات إنشاء التوقيع الإلكتروني وشهادات التصديق الإلكتروني طوال المدة التي تُحددها الهيئة في الترخيص وفقا لنوع الشهادة المُصدرة، وذلك فيما عدا مفاتيح الشفرة الخاصة التي تُصدرها للموقع، فلا يتم حفظها إلاّ بناء على طلب من المُوقِّع وبموجب عقد مُستقل يتم إبرامه بين المرخص له والمُوقِّع، وفقا للضوابط الفنية والتقنية لحفظ هذه المفاتيح التي يضعها مجلس إدارة الهيئة، ونظام آخر للحفاظ على السرية الكاملة للأعمال المتعلقة بالخدمات التي يرخص بها وبالبيانات الخاصة بالعملاء؛

**د)**- أن تتمتع بنظام خاص لإيقاف الشهادة في حالة توافر أحد الحالات التي تُثبت تواجد عبث ببيانات الشهادة أو انتهاء مدة صلاحيتها، أو تلك المتعلقة بسرقة أو فقدان المفتاح الشفري الخاص أو البطاقة الذكية أو عند الشك في حدوث ذلك، أو في حالة عدم إلتزام الشخص المُصدر له شهادة التصديق الإلكتروني ببنود العقد المبرم مع المرخص له، ويكون نظام إيقاف الشهادات وفقا للقواعد والضوابط التي يضعها مجلس إدارة الهيئة، كما يجب على الهيئة أن يكون لديها نظام يتيح لها عملية التحقق من صحة بيانات إنشاء التوقيع الإلكتروني في إطار أعمال الفحص والتحقق.

زيادة إلى الشروط السابقة ألزم المشرع المصري طالب الترخيص أن يُقدم الضمانات والتأمينات، التي يُحددها مجلس إدارة(هـ.ت.ص.ت.م) قصد تغطية الأضرار والأخطار المتعلقة بذوي الشأن في حالة إنهاء الترخيص لأيِّ سبب أو في حالة إخلاله بالإلتزامات الواردة في الترخيص، كما يجب على الراغب في الحصول على الترخيص بمزاولة نشاطات التصديق الإلكتروني أن يقوم بتحرير طلب وفقا للنموذج الذي أعدته الهيئة، مرفقا بالبيانات والمستندات المنصوص عليها في المواد(3-4-12-14) من اللائحة التنفيذية ومن ثمّة تقوم الهيئة بعد فحصها والتأكد من سلامة جميع الوثائق المقدمة لها، بالبت في طلب الترخيص

خلال مدة لا تتجاوز شهر من تاريخ استفاء صاحب الطلب لكل ما طُلب منه وبعدها تُصدر الهيئة في الحالة الإيجابية، لقرار الترخيص مدة صلاحيته خمسة(05) سنوات مع إلتزام صاحب الترخيص بدفع المقابل الذي حدّده مجلس إدارة الهيئة.

تجدر الإشارة أنّ الهيئة تمنح من تلقاء نفسها الإعتماد مباشرة لجهة التصديق الإلكتروني الأجنبية وفقا للحالات المشار إليها في المادة 1/21-3-4، وخارج هذه الحالات يجب على الجهة الأجنبية أن تلتزم بالإجراءات المتعلقة بمنح الإعتماد، التي تمكنها من طلب إعتماد أنواع أو فئات شهادات التصديق الإلكتروني التي تُصدرها، وفي كلّ الظروف يمكن للهيئة أن تصدر قرار مسبب بإيقاف أو إلغاء الإعتماد عند الضرورة.

**3- قانون الإمارات العربية المتحدة.**

قام وزير الإقتصاد لدولة الإمارات العربية المتحدة بناءا على إقتراح من هيئة تنظيم الإتصالات(TRA) كمُراقب على خدمات التصديق الإلكتروني، بإصدار لائحة(م.خ.ت.إ) بموجب القرار الوزاري المشترك رقم 01- 2008 بشأن (م.خ.ت.إ)، التي من خلالها ألزم كلّ مزود يرغب في الحصول على ترخيص يمكنه من مزاولة نشاطاته مراعاة الإجراءات والمعايير الفنية والتقنية، المحددة بموجب أحكام اللائحة والقرارات التنظيمية لـ(هـ.ت.إ) وإنطلاقا من ذلك يجب على المزود أن يقدم طلب منح الترخيص وفقا للنموذج المُحدد من طرف(هـ.ت.إ) مرفوقا بالوثائق التالية:

1- بيان مُمارسة التصديق الإلكتروني المنصوص عليه في المادة الثامنة عشرة (18) من اللائحة، مع عقد التأسيس والنظام الأساسي وفقا للقوانين المعمول بها في الدولة الإماراتية والهيكل التنظيمي للشركة مع سند الملكية؛
2- الرخصة الصادرة من السلطات المحلية المُختصة لمُزاولة النشاط التجاري حسب نوع الشركة في الدولة، مع بيان الأنشطة التجارية الغير المتعلقة بخدمات التصديق الإلكتروني؛
3- بيان بالموارد المالية وتقرير مُدقق الحسابات عن السنتين الماليتين الأخيرتين للشركة إن كانت قائمة، أو من تاريخ تأسيسها وحتى تاريخ تقديم الطلب (أيِّ المُدَتَيْنِ أَقْصَرْ) مع إثبات وجود تأمين كافٍ يُغطي عمليات ونشاطات (م.خ.ت.إ)؛

4- الإقرار بمُطابقة كلٍّ من المعايير التقنية لمقدم الطلب طبقا لما هو مُقرر بالقانون وهذه اللائحة، وبكفاءة الموظفين المؤتمنين وفقا لما هو مُقرر وفقا بأحكام هذا القانون واللائحة؛
5- تقرير المدقق(Auditeur) وفقا لأحكام هذه اللائحة مع رسم طلب الرخصة كما هو مُوضح في جدول الرسوم الصادر بقرار مجلس الوزراء[1]، وتُدفع جميع الرسوم بالطريقة التي تُقررها هيئة تنظيم الإتصالات، كما يجوز للهيئة أن تطلب من مقدم طلب الترخيص توفير معلومات إضافية أو مُستندات وفق ما تراه ضروريا لمنح الرخصة؛

انطلاقا من ذلك يجب على طالب منح الترخيص أن يَسْتَوْفِيَ المعايير الشخصية والفنية المتعلقة بتوظيف الأشخاص المؤتمنين، وذلك بإتخاذ التدابير اللازمة لكل شخص مؤتمن وأن يحرص على أنّه جدير بالثقة مؤهل وكُفء للقيام بمسؤولياته وواجباته، وليست لديه أيّة مصالح أو خدمات أو عمليات قد تتعارض أو تؤثر سلبا مع أمن (م.خ.ت.إ)، ولم يسبق أن حُكم عليه في جناية أو جنحة مُخلة بالشرف أو بالأمانة، أو أُصدر في حقه قرار مُخالفة أحكام هذا القانون واللائحة، التي ينبغي أن تكون لديه معرفة تامة لها(الأحكام)، وببيان ممارسة التصديق الإلكتروني المتعلق خاصة بالواجبات والمسؤوليات المسندة إليه، ويجب على الشخص المعني بالتوظيف أن يكون حاصلا على المؤهلات الفنية والخبرة والتدريب وأن يكون مُلتزما بأيّة معايير، أو متطلبات تراها(هـ.ت.إ) ضرورية بموجب أحكام القانون الإتحادي المتعلق بالمعاملات الإلكترونية أو بلائحة(م.خ.ت.إ)، (المادتين 13 و14 من اللائحة).

زيادة على ذلك يقع على طالب منح الترخيص لدى الهيئة أن يستخدم في جميع أنشطته وعملياته لأنظمة وإجراءات مُعتمدة جديرة بالثقة، وأن يضمن إستيفاء ومطابقة جميع الأنظمة والإجراءات والعمليات، والموظفين والمعدات والمنتجات، والخدمات مع معايير حماية المعلومات المحددة وفقا لمجموعة معايير الأيسو(27000)، أو المعايير التي تقوم الهيئة بتحديدها(المادة 24 من اللائحة).

---

[1] – قرار مجلس الوزراء رقم 8-2009 بشأن الرسوم المستحقة على معاملات مزودي خدمات التصديق الإلكتروني، الصادر في 01 فيفري 2009. http://www.tra.gov.ae/

فبعد إستيفاء طالب الترخيص لكل الشروط السابقة، تُصدر(هـ.ت.إ) لقرار منح الترخيص وفقا للبيانات التي حددتها المادة 4/07 من اللائحة، مدة صلاحيته خمسة سنوات(05) قابلة للتجديد يكون مصحوبا بإشعار خطي، في حين يجب تقديم طلب تجديد الترخيص قبل انتهاء تاريخ الترخيص الساري المفعول به بثلاثة أشهر وذلك وفقا للمواد 04 و05 و06 من اللائحة، أمّا في حالة رفض الترخيص يجب على الهيئة أن تُزود صاحب الطلب بخطاب خطي تبين فيه أسباب رفض منح الترخيص أو تجديده، ويبقى(م.خ.ت.إ) أثناء فترة الترخيص خاضع لرقابة من طرف(هـ.ت.إ)، التي لها صلاحية إلغاء الترخيص بمجرد معاينة إحدى الحالات المبينة في المادة 32 من اللائحة أو تعليق العمل بالترخيص وفقا للحالات المحددة في المادة 31 من نفس اللائحة.

**4- القانون الجزائري.**

قام المشرع الجزائري بموجب المادة 33 من القانون رقم 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، بإدراج نشاط التصديق الالكتروني في المجال الاقتصادي ضمن نظام الترخيص الذي نصت عليه المادة 39 من القانون رقم 2000-03 المؤرخ في 05 أوت 2000 المتعلق بتحديد القواعد العامة المرتبطة بالبريد والمواصلات السلكية واللاسلكية، الذي تُصدره سلطة ضبط البريد والمواصلات السلكية واللاسلكية التي تم إنشاءها بموجب المادة 10 منه[1]، وذلك بإعتبارها كسلطة تصديق فرعية في المجال الإقتصادي تابعة للسلطة الرئيسية على مُستوى مرفق المفاتيح العمومية الهرمي(PKI) في

---

[1] – قانون رقم 2000-03 المُحَدِّدْ للقواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية، ج ر عدد 48 الصادر في 06 أوت 2000.

– المادة 10:" تنشأ سلطة ضبط مُستقلة تتمتع بالشخصية المعنوية و الإستقلال المالي، يكون مقرها بالجزائر العاصمة."

– **زعاتري كريمة**، المركز القانوني لسلطة ضبط البريد و المواصلات السلكية و اللاسلكية، مذكرة شهادة الماجستير، تخصص إدارة ومالية، كلية الحقوق والعلوم السياسية، جامعة أمحمد بوقرة بومرداس، 2001، ص ص 85-88.

الجزائر، مكلفة بمتابعة ورقابة نشاطات(م.خ.ت.إ) المتعلقة بالتوقيع والتصديق الإلكترونيين وبالتالي تمنح(س.ض.ب.م) الترخيص، بعد موافقة السلطة الوطنية للتصديق الإلكتروني لأي شخص طبيعي أو معنوي يلتزم باحترام الشروط التي تحددها في مجال إنشاء واستغلال خدمات التصديق الالكتروني، لذا عرفت المادة 10/02 من القانون رقم 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين الترخيص على أنّه:" **نظام استغلال خدمات التصديق الإلكتروني والذي يتجسد في وثيقة رسمية ممنوحة لمؤدي الخدمات بطريقة شخصية، تسمح له بالبدء الفعلي في توفير خدماته.**"

انطلاقا من ذلك ألزم المشرع الجزائري طالب الترخيص بموجب المادة 34 من نفس القانون بمجموعة من الشروط الفنية والتقنية، كأن يكون خاضع للقانون الجزائري في حالة ما إذا كان شخص معنوي أو يتمتع بالجنسية الجزائرية إذا كان شخص طبيعي، والتمتع بقدرة مالية كافية وبمؤهلات وخبرة ثابتة في ميدان تكنولوجيات الإعلام والاتصال للشخص الطبيعي أو المُسيِّر للشخص المعنوي، وأن لا يكون قد سبق الحكم عليه في جناية أو جنحة تتنافى مع نشاطه، بالإضافة إلى ذلك يجب على الراغب في الحصول على ترخيص لمزاولة نشاط خدمات التصديق الإلكتروني في الجزائر، أن يتحصل على شهادة تأهيل (Attestation d'éligibilité) لتهيئة الوسائل اللازمة لخدمات التصديق الإلكتروني، مدة صلاحيتها سنة(01) قابلة للتجديد مرة واحدة فقط، التي(الشهادة) تسمح له وفقا للمادة 51 من نفس القانون بأن يطلب لدى السلطة الاقتصادية للتصديق الإلكتروني(ARPT) أو لدى مكاتب التدقيق المعتمدة(Cabinet d'audit accrédité)، بإجراء تدقيق تقييمي(Audit d'évaluation) لمعدات وأنظمة أمن تكنولوجيا المعلومات المستعملة في نشاطاته[1].

تلتزم سلطة الضبط بإجراء منح الترخيص في إطار احترام مبادئ الموضوعية والشفافية وعدم التمييز، فبعدما أن تتأكد من توافر ومطابقة الشروط المحددة لدى طالب الترخيص ومن حصوله على شهادة تأهيل، تُصدر سلطة الضبط وفقا للمادة 40 من قانون التوقيع

[1] – قانون رقم 15-04 مؤرخ في 01 فيفري 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين(الجزائر).

والتصديق الإلكترونيين، قرار مسبب بمنح الترخيص مدة صلاحيته خمسة(05) سنوات قابلة للتجديد عند انتهاء المدة، وفقا للشروط المحددة في دفتر الأعباء الخاص بشروط وكيفيات تقديم خدمات التصديق الإلكتروني، الذي يُبلّغ(القرار) لصاحب شهادة التأهيل بصفة شخصية، وغير قابل للتنازل عنه في أجل شهرين من تاريخ استلام الطلب المثبت بوصل إشعار بالاستلام، وذلك بمقابل إتاوة يدفعها(م.خ.ت.إ) تحدد عن طريق التنظيم، وفي أثناء مدة الترخيص يخضع(م.خ.ت.إ) وفقا للمادة 52 من نفس القانون لمراقبات فجائية وعمليات تدقيق دورية، من قِبل السلطة الاقتصادية(س.ض.ب.م) من أجل التحقق من مدى مراعاته لدفتر الأعباء المُحدّد لشروط وكيفيات تقديم خدمات التصديق الإلكتروني.

## المطلب الثاني

## طرق التوثيق الإلكتروني

تسعى جهات التوثيق الإلكتروني على كسب ثقة أطراف التعامل الإلكتروني وفقا للتأكيدات والممارسات المتبعة في إطار سياسة التصديق الإلكتروني المعتمدة، لذا سنتطرق أولا إلى مهام(م.خ.ت.إ) في(الفرع الأول)، ثم إلى مراحل إصدار شهادات التصديق الإلكتروني في (الفرع الثاني)، ومختلف التقنيات المستخدمة في التوثيق أو التصديق الإلكتروني(الفرع الثالث).

### الفرع الأول

### مهام جهات التصديق الإلكتروني

إنّ جهات التوثيق الإلكتروني تقوم بمهام عديدة في إطار السياسة العامة المنتهجة في التصديق الإلكتروني (Politique de certification)، والمتمثلة في:

**أولا: التحقق من هوية الشخص الموقع.**

بعدما أن تتحقق جهة التصديق الإلكتروني في كلّ ما يتعلق بالوثائق المثبتة لهوية وأهلية والصفات المميّزة للطرف الراغب في إحداث توقيع إلكتروني موصوف، تقوم الجهة

بإتاحته لأدوات مؤمنة لإنشاء التوقيع الإلكتروني وفحصه مع وضعها تحت سيطرته في إطار عقد تقديم خدمة التوقيع الإلكتروني، التي تضمن بواسطة شهادة التصديق الإلكتروني الموصوفة أنّ الموقع المعينة هويته فيها كان يتحكم في بيانات إحداث توقيعه الإلكتروني في وقت أو قبل إصدار الشهادة، مع تحديد الطريقة المستخدمة في تعيين هويته، وتوضيح القيود المفروضة على قيمة المعاملة الإلكترونية أو على المسؤولية التي تُستعمل من أجلها الشهادة[1]، حتى يتسنى للطرف المعول عليها من التعرف على هوية الموقّع، والتأكد من صحة توقيعه الإلكتروني ومدى سلامة ونسبة الرسالة الإلكترونية المتصلة به لصاحبها، مما تستبعد احتمالات وقوع أطراف العقد الإلكتروني في طرق الغش والاحتيال أو التدليس التي تحول دون استكمال مراحل إبرام العقد، ولضمان المعلومات الواردة في شهادة التصديق الإلكتروني الموصوفة، يقوم (م.خ.ت.إ) بالتوقيع عليها بالمفتاح الجذري الخاص به.

**ثانيًا: إثبات مضمون التبادل الإلكتروني.**

إنّ دور جهات التصديق الإلكتروني لا يتوقف عند تحديد هوية أطراف العقد الإلكتروني، بل يرقى إلى إثبات مضمون التبادل الإلكتروني بالتيقن على سلامته من أيِّ تعديل أو تغيير أو تبديل في البيانات الإلكترونية، ومن أجل ضمان ثقة ومصداقية مبادلات التجارة الإلكترونية تقوم جهات التوثيق الإلكتروني المعتمدة، بضمان سلامة المواقع التجارية وتأمين البيانات الإلكترونية المتداولة فيها عبر مسالك مؤمنة في شبكة الإنترنيت، بواسطة شهادة التصديق الإلكتروني التي تربط هوية الموزع أو المعلومات بمفتاح عمومي، مع تعقب المواقع التجارية عبر شبكة الإنترنيت[2] عن طريق التحقق والتحري من مِصداقيتها وجِدِّيتها

---

[1] – **وسيم شفيق الحجار**، الإثبات الإلكتروني، المنشورات الحقوقية، بيروت 2002، ص 211.

– **رضا متولي وهدان**، النظام القانوني للعقد الإلكتروني والمسئولية عن الاعتداءات الإلكترونية (دراسة مقارنة في القوانين الوطنية وقانون الأونسيترال النموذجي والفقه الإسلامي)، الطبعة الأولى، دار الفكر والقانون للنشر والتوزيع، المنصورة، 2008، ص ص 14-17.

[2] – **إيمان مأمون أحمد سليمان**، الجوانب القانونية لعقد التجارة الإلكترونية، رسالة دكتوراه في القانون، جامعة المنصورة، مصر، 2006، ص ص 313، 314.

**- Lionel BOUCHURBERG,** op.cit., pp. 29-41.

فإذا شككت من صحتها وسلامتها، تقوم بتوجيه رسائل تحذيرية إلى أطراف التعامل الإلكتروني تُنبههم من عدم مِصداقية وجدية هذه المواقع.

لتأكيد سلامة البيانات الإلكترونية المتداولة يجب أن تضمن منظومة أمن إحداث التوقيعات الإلكترونية لجميع أطراف التعامل الإلكتروني، إتاحة البيانات الخاصة بالتحقق من التوقيعات الإلكترونية[1]، مع وجوب الإستعانة بأنظمة مؤمنة لحفظ شهادات التصديق الإلكتروني على أيّ حامل إلكتروني تتيح إمكانية الإطلاع عليها عند الحاجة، بالشكل الذي أُنشئت أو أُرسلت أو أُستلمت به، لذا أعلنت مؤسسة(AFNOR) عن مجموعة من التوصيات المتعلقة بتصميم واستغلال النظم المعلوماتية لغرض حفظ، وتأمين سلامة البيانات المُخزنة في هذه النظم، ومن بين هذه التوصيات تلك المتعلقة بالطريقة الفنية للحفظ[2]، وبالتعليمات الخاصة باستغلال الأنظمة المعلوماتية المتعلقة بحفظ وأمن أشكال الدعامات الإلكترونية، إذ دعت جميعها على أنّ وسائل الحفظ الفنية للبيانات الإلكترونية تُوفر الأمان والسلامة.

**ثالثا: تحديد لحظة إبرام العقد الإلكتروني.**

إنّ تحديد زمان ومكان إبرام العقد الإلكتروني يُعَدُّ بمثابة بداية سريان الآثار المترتبة عنه بالنسبة لأطرافه، ومن ثمّة فلا يُعتبر كشرط أساسي لصحته كما لا يُقدم الضمانات الكافية لتنفيذ الإلتزامات المترتبة عنه[3]، إذ يمكن لأيّ طرف في العلاقة العقدية أن يُغير زمان إبرام العقد المدون في حاسوبه، أو قيامه بتغيير أو تحديد لأكثر من مكان واحد دون علم الطرف الآخر، وهذا ما يُخلط الحسابات ويخلق عراقيل تحول دون إتمام أو تنفيذ الإلتزامات المترتبة عن العقد، ولتفادي كلّ ذلك تقوم جهات التصديق الإلكتروني بتحديد

---

1) - **Eric A. CAPRIOLI**, L'archivage des documents électroniques, pp. 5,6. Article disponible sur : http://www.caprioli-avocat.com

2) - **Sedallian (V),** preuve et signature électronique, p. 08. http://www.internet-juridique.net

3) – **محمد فواز المطالقة**، الوجيز في عقود التجارة الإلكترونية (أركانها– إثباتها– حمايتها(التشفير)– التوقيع الإلكتروني– القانون الواجب التطبيق)، دار الثقافة للنشر والتوزيع، عمان، 2008، ص ص 70–75.

تاريخ وساعة إبرام العقد الإلكتروني عن طريق خدمة ختم الوقت والتاريخ (Service d'horodatage) بطريقة آلية في منظومة أمن إحداث التوقيعات الإلكترونية، على النحو الذي يسمح بالتحديد الدقيق لزمن ومكان إبرام العقد، في حين يجب أن يرتبط تاريخ وساعة إحداث التوقيع الإلكتروني بمدة صلاحية شهادة التصديق الإلكتروني، فإذا تم بعد إصدارها فيُثير الشكوك أو الشبهة في صحة بيانات إحداثه ومدى نسبتها للموقع.

نظرا للدور الفعال لهذه الخدمة قام المشرع الفرنسي بتنظيمها في إطار قانوني خاص بها، من خلال قيام الوزير الأول(FRANÇOIS Fillon) بإصدار المرسوم رقم 2011-434 المؤرخ في 20 أفريل2011، يتضمن تحديد تاريخ ووقت البريد المُرسل أو المُستلم بالطريقة الإلكترونية لغرض إبرام أو تنفيذ العقد[1]، الذي حدد بموجب المادة ثلاثة(03) من الفصل الثاني منه، المواصفات التقنية التي يجب أن يأخذها بعين الاعتبار كلّ مقدم لخدمات ختم الوقت والتاريخ الإلكترونيين (Le prestataire de services d'horodatage électronique)، الراغب في طلب تأهيل خدماته وفقا للمادة ستة(06) من المرسوم.

انطلاقا من ذلك يجب أن تستجيب وحدة ختم الوقت والتاريخ(Module d'horodatage) للمواصفات المحددة في المادة 04 من نفس المرسوم، وأن يضمن المزود تزامن الساعة الداخلية للوحدة(Horloge de confiance) مع مصادر الوقت الأخرى الموثوق بها، مع استخدام معدات وأنظمة أمن معلومات ضدّ أيّ تزوير قد يمس من سلامة البيانات الإلكترونية المتعلقة بالعلامة الزمنية (CT)[2] التي تُثبت توقيت البيانات الإلكترونية بدقة.

---

1) - Décret n° 2011-434 du 20 avril 2011 relatif à l'horodatage des courriers expédiés ou reçus par voie électronique pour la conclusion ou l'exécution d'un contrat. J.O.R.F, n° 0094 du 21 avril 2011.

2) - **La Contremarque de temps** : « **donnée** sous forme électronique liant une représentation d'une donnée à un temps particulier et attestant de l'existence de la représentation de cette **donnée à cet instant**, la contremarque de temps comporte un **cachet** du prestataire de services d'horodatage électronique établi à l'aide des données de signature de la contremarque de temps. »

كما يجب على مقدم الخدمة أن يتقيد بالشروط المتعلقة بالختم المُرْفَقِ بالعلامة الزمنية المحددة في المادة الأولى فقرة خمسة(5/01) من المرسوم، الذي عن طريقه[1] يتم إثبات الارتباط الموجود بين الختم وعلامة التوقيت والتاريخ، وبالتالي يجب أن يكون الختم الإلكتروني خاص بمقدم الخدمة ويُحدث بوسائل موضوعة تحت سيطرته وأن يضمن الختم المُرْفَقْ بالعلامة الزمنية (CT) كشف أيّ تعديل أو تغيير في منظومتها.

**رابعا: إصدار المفاتيح الإلكترونية.**

إنّ الهدف الرئيسي لجهات التوثيق الإلكتروني يكمن بالدرجة الأولى في خلق مناخ ثقة مؤمن لمبادلات التجارة الإلكترونية عبر الإنترنيت، بحيث تُتيح في إطاره لمجموعة من الأساليب وتقنيات التشفير اللاتماثلي(Cryptologie Asymétrique)، التي تعتمد بدورها على معادلات خوارزمية[2] تُحوِّل النص المرفق بالرسالة الإلكترونية المُراد إرسالها إلى رموز وإشارات وأرقام غير معروفة، أو مُبعثرة في بعض الأحيان تؤدي إلى صعوبة واستحالة

---

1) - **Cachet d'une contremarque de temps** : « donnée sous forme électronique permettant d'identifier le prestataire de services d'horodatage électronique qui la délivre et d'assurer un lien avec la contremarque de temps à laquelle il s'attache. Le cachet d'une contremarque de temps satisfait aux obligations suivantes:
**a)** Être propre au prestataire de services d'horodatage électronique;
**b)** Être créé par des moyens que le prestataire de services d'horodatage électronique peut garder sous son contrôle exclusif;
**c)** Garantir avec la contremarque de temps à laquelle il s'attache un lien tel que toute modification ultérieure de la contremarque de temps est détectable. »
– **ناصر خليل**، التجارة والتسويق الإلكتروني، الطبعة الأولى، دار أسامة للنشر والتوزيع، الأردن، 2009، ص 210.

2) – Le mot **algorithme** n'est pas dérivé d'un mot **latin** ou **grec**, mais d'une contraction et d'une dérivation du nom du mathématicien **arabe (الخَوَارِزْمِي)** qui publia deux livres importants : l'un sur «**l'arithmétique**» et l'autre sur « **l'action de faire passer et d'agencer les parties d'un tout** » (titre original :**كِتابْ الجَبْرِ والمُقَابَلَة**), trois siècles plus tard, le livre, traduit en latin, porta le nom **Algorismus**. La première définition du mot algorithme, dans son **sens actuel**, a été donnée par le **mathématicien russe Markov** : «Tout ensemble de règles précises qui définit un procédé de calcul destiné à obtenir un résultat déterminé à partir de certaines données initiales.» Les algorithmes sont constitués par un ensemble de règles précises et compréhensibles par tous, ils s'appliquent à des données qui peuvent changer et élaborent les résultats en fonction des données initiales. http://www.wikipédia.fr

قراءتها وفهمها من دون إعادتها(الرسالة الإلكترونية) إلى هيئتها الأصلية، التي لا تتم إلاّ بعد القيام بفك الشفرة وتحويل الرموز والإشارات والأرقام إلى نص مقروء، من خلال استخدام مفاتيح التشفير العام والخاص الفريدة بالموقّع، وبالتالي فإنّ عملية التشفير تعتمد على عاملين أساسيين تجعلها قوية وفعالة: **المعادلة الرياضية، وطول مفتاح التشفير المُقدر بالبت (bit)**[1].

انطلاقا من ذلك فإنّ مفاتيح التشفير الخاصة أو العامة التي يُعول عليها في إحداث التوقيعات الإلكترونية الموصوفة، تعتمد على معايير تشفير البيانات الإلكترونية الأحادية الاتجاه(RSA, les courbes elliptiques, DSA) التي تضمن سريتها وعدم كشفها عن طريق الاستنباط أو الاستنتاج[2]، فكلما كان مفتاح التشفير أطول من حيث الوحدات(bits) صَعُبَتْ معها مُهِمَة الكشف عن مضمون البيانات المُشفرة، فالمفتاح الخاص يُستحدث عن طريق عملية حسابية خاصة به لإحداث التوقيع الإلكتروني، أما المفتاح العام الذي تربطه عملية حسابية معقدة بالمفتاح الخاص، يكون متاح للجمهور ويُستخدم لغرض التحقق من التوقيع الإلكتروني، في حين يعتمد عليهما برنامج الحاسوب عن طريق شهادة التصديق الإلكتروني[3]، عند مباشرته لإجراءات فحص مدى صحة ونسبة التوقيع الإلكتروني لصاحبه

---

1) - Informatique, (mot anglais) abréviation de (**binary digit**), 0 ou 1 dans le système de numération binaire. En traitement ou en stockage de l'information, le bit est la plus petite unité d'information manipulable par un ordinateur, et peut être physiquement représenté par une impulsion unique sur un circuit, ou par une petite zone d'une surface de disque, capable de stocker un 0 ou un 1. Considéré isolément, un bit a peu de signification ; groupés par huit, les bits forment des octets qui peuvent représenter différentes informations, en particulier les lettres de l'alphabet et les chiffres 0 à 9. Un **Octet** en informatique⇒ unité d'information composée de **8 bits**. En termes de traitement et de stockage, un **octet** correspond à un seul caractère, tel qu'une lettre, un chiffre ou un signe de ponctuation. Un octet ne représentant qu'une petite quantité d'informations, la quantité de mémoire et la capacité de stockage sont généralement indiquées en **kilo-octets** (**1 Ko = $2^{10}$ octets = 1 024 octets**) ou en **mégaoctets** (**1 Mo = $2^{20}$ octets = 1 048 576 octets**). **En informatique,** le symbole du préfixe **kilo**- s'écrit avec une majuscule **(K)** et correspond à la valeur 1 024, alors que le **k minuscule** désigne la valeur 1 000 dans le système métrique. http://www.wikipédia.fr

2) - **Arnaud-F. FAUSSE**, op.cit., pp. 312, 313.

3) - **Carole AUBERT**, La nouvelle loi sur la signature électronique et le droit du bail, pp.13, 14.Article disponible sur : http://www.unine.chfilescontentsitesbailfilessharedocumentsSeminaires_2006Aubert

وسلامة الرسالة الإلكترونية المرفقة به، كما تُشرف جهة التصديق الإلكتروني بإصدار مفتاح تشفير جِذري خاص بالشهادة الإلكترونية يُمثل توقيعها الإلكتروني عليها.

**خامسا: تزويد المتعاقدين بشهادات تصديق إلكتروني موصوفة(Qualifiés).**

تُعتبر مهمة إصدار شهادات التصديق الإلكتروني الموثوق بها، من بين أهم الخدمات التي تقوم بها جهات التصديق الإلكتروني المعتمدة، إذْ تقوم بتزويد أطراف العقد الإلكتروني بشهادات إلكترونية معتمدة لهدف التعويل عليها سواءا، من طرف الموقع لتعزيز مصداقية نسبة توقيعه الإلكتروني وتأكيد مضمون رسالة العقد الإلكتروني من جهة، ومن جهة آخرى يعول عليها الطرف المستقبل للرسالة الإلكترونية من أجل التعرف على هوية مُرسل الرسالة ومدى نسبة التوقيع الإلكتروني إلى صاحبه وكلّ ما يتعلق بالمعاملة التجارية، فعن طريق الشهادة تقوم البرامج الآلية المُستقبلة للرسالة الإلكترونية، بإعادة نفس العملية الحسابية لوظيفة الهاش الأصلية قصد التوصل إلى قيمة جديدة مُطابقة لقيمة الهاش الأصلية، فإذا تحقق ذلك تعتبر الرسالة الإلكترونية صحيحة ولم تتعرض للتغيير أو التحريف أو التعديل أو ما يُثير الشبهة فيها، وبالتالي فإنّ الدور الرئيسي لشهادات التصديق الإلكتروني يكمن في ربط المفتاح الخاص بصاحب التوقيع الإلكتروني بعملية حسابية مُعقدة بالمفتاح العام، الذي يُتاح للعموم قصد التعرف على هوية صاحب الرسالة الإلكترونية الموقعة، بينما يبقى المفتاح الخاص تحت سيطرة الموقع الذي يقوم بالحفاظ عليه على أيّ حامل إلكتروني مؤمن.

## الفرع الثاني

## مراحل إصدار شهادات التصديق الإلكتروني

إنّ عملية إصدار شهادة التصديق الإلكتروني تمر بعدة إجراءات، والتي يمكن تصنيفها وفقا للواقع العملي لجهات التوثيق إلى ثلاثة مراحل، فالمرحلة الأولى تتمثل في إيداع طلب الحصول على الشهادة أين يتعين على كلّ من يرغب في الحصول على شهادة تصديق إلكتروني موصوفة، في إطار عقد تقديم خدمات التصديق الإلكتروني أن يقوم بتوجيه طلب بالطريقة الكتابية أو الإلكترونية لسلطة التسجيل(AE) التابعة لسلطة التصديق، أو لأحد

وكلاءها المفوضين لهم وفقا للنموذج المُعد مُسبقا من طرفها المتواجد مجانا على مستوى موقعها الإلكتروني، مع إرفاقه بالوثائق(نسخ) التي تُثبت صحة المعطيات المقدمة في النموذج، كبطاقة التعريف الوطنية أو جواز، سفر السجل التجاري[1] الخ...

بعدها تقوم سلطة التسجيل(AE) بمباشرة إجراءات المرحلة الثانية المتعلقة بالتحقق من البيانات المتعلقة بإصدار الشهادة، التي تستلزم عادة الحضور الشخصي لصاحب طلب إصدار شهادة التصديق الإلكتروني الموصوفة، من أجل مُباشرة إجراءات التحقيق في هويته وأهليته في إبرام التصرف الإلكتروني بناءا على الوثائق الأصلية التي يقدمها(صاحب الطلب) لسلطة التسجيل، وفي حالة ما إذا كان هذا الأخير شخص معنوي يتم التحقق في هوية الشخص الطبيعي المُمثل له قانونيًّا ومدى تمتعه بأهلية تسمح له بإبرام التصرف القانوني إلكترونيّا.

في المرحلة الأخيرة تقوم سلطة التسجيل(AE) بإرسال طلب إصدار الشهادة الإلكترونية إلى سُلطة التصديق الإلكتروني(AC) التي تباشر عملية إصدار زوج مفاتيح التشفير(العام والخاص) المتعلقان بالشهادة وفقا للمواصفات التقنية المعمول بها، التي يتعين عليها أن تولي العناية اللازمة لضمان دقة واكتمال كلّ ما تُقدمه من تأكيدات جوهرية ذات صلة بالشهادة في وقت أو قبل إصدارها، مع حفظها في نظام مؤمن خاص يسمح بالرجوع إليها عند الحاجة، كما يتعين على صاحب الشهادة أن يقوم بحفظها وتثبيتها في شكلها الإلكتروني الأصلي على أيّ حامل إلكتروني مؤمن، سواءا في مُذكرة حاسوبه(RAM)[2] أو على أسطوانة مُمَغنطة أو في المفتاح المحمول(Clé USB)، أو في بطاقة الإئتمان الذكية (Carte à puce)، وبالمقابل يقوم الطرف المعول على الشهادة(المرسل إليه) بحفظها بنفس الكيفية

---

1) - **Arnaud- F.FAUSSE**, op.cit., pp 164, 165.

-**Hassan BEZZAZI**, Sécuriser les échanges numérique, pp. 33,34. Article publié sur: http://www.cours.unjf.frfile/

2) – Informatique : Mémoire vive (Acronyme de l'anglais **R**andom **A**ccess **M**emory), composée essentiellement de trois zone : La mémoire conventionnelle, La mémoire supérieure, La mémoire étendue. **Djamel BENABDESSELAM**, op.cit., p 181.

على أيّ حامل إلكتروني مؤمن، أو يتم الإستعانة بخدمات سلطة خاصة بالحفظ (Autorité de Stockage) قصد السماح بالرجوع إليها عند الحاجة[1].

## الفرع الثالث

## تقنيات التصديق الإلكتروني

### أولا: التوقيع بواسطة الرقم السري المُقترن ببطاقة الائتمان. (La Carte à puce)

يعتبر التوقيع باستخدام الرقم السري المُقترن بالبطاقة الممغنطة من بين التقنيات التكنولوجية المُبتكرة، من أجل الإسراع في المعاملات المصرفية وتسهيل إجراءات الحصول على الأموال، لذا قامت مُختلف البنوك منذ المهلة الأولى بإصدار بطاقات إلكترونية ممغنطة لعملائها مرفقة برقم سري (Numéro d'Identification Personnel (NIP))، للاعتماد عليها أثناء مباشرة العمليات المصرفية كسحب أو إيداع النقود أو لسداد ثمن السلع والخدمات على مستوى مختلف الأجهزة الآلية المتاحة لهم، كجهاز الصراف الآلي (Automatic Teller Machine(A.T.M)) أو الموزع الآلي للأوراق النقدية (Distributeur Automatique de Billets (D.A.B)) أو، الشباك الآلي للبنك (Guichet Automatique de Banque (G.A.B)) أو الأجهزة المتواجدة في المحلات التجارية الخ...، وبالتالي تعتبر بطاقة الائتمان الذكية (Carte à puce) من بين وسائل الدفع الإلكتروني الحديثة، الأكثر استعمالا عبر الإنترنيت نظرا لاستجابتها للمعايير والمواصفات التقنية والمادية والشكلية والفنية المُعترف بها دوليا[2].

---

1) - **Maxime WACK et AL**, «certification et archivage légal de dossiers numériques», Revue Document numérique, vol 6, n°1/2002, pp. 152, 153. Article disponible sur : http://www.cairn.info/revue-document-numerique-2002-1-page-145.htm

2) - La Norme ISO 7816-8 décrit les fonctions de sécurité utilisées dans les cartes à puce de signature digitale. La suite des normes ISO 7816 définit les différents éléments d'une carte : physique, système de fichier et de communication, signaux électroniques et protocoles de transmission, etc. - **Arnaud-F. FAUSSE**, op.cit., pp. 203- 206.

- La Norme **EMV** acronyme de (**E**uropay, **M**aster Card et **V**isa), a pour but de permettre et d'assurer l'interbancarité et l'interopérabilité mondiale des cartes à puce et terminaux de lecture dans une opération de paiement. - **Étienne WÉRY**, op.cit., pp. 61- 64.

لضمان الثقة والأمان في إجراءات إبرام الصفقات التجارية والحصول على الأموال عبر الإنترنيت، استدعت الحاجة إلى البحث على أنظمة أمن حماية البيانات الإلكترونية المتداولة يُشرف عليها وسيط مؤتمن محايد في خدمات التصديق الإلكتروني، وبالتالي فقد تُسند عملية التصديق للبنوك التي تحصلت على اعتماد أو ترخيص من قبل الجهات الرسمية لمزاولة نشاطات التصديق الإلكتروني، على سبيل المثال مصرف الهلال في الإمارات العربية المتحدة، وفي فرنسا نجد كلّ من (BNP Paribas, Crédit Agricole, NATIXIS, HSBC France, etc.) التي تستعين بخدمات المتعامل التقني لتأمين طرق الدفع الإلكتروني عبر الإنترنيت (Atos (SIPS), CertEurope, etc.)، وفي كلّ الظروف تتوسط العمليات المصرفية سلطة تصديق رئيسية أعلى على مستوى هرم مرفق المفاتيح العمومية كما هو الحال في تونس من خلال قيام(و.و.م.إ) كسلطة تصديق جذرية، بتأمين وضمان تقنيات الدفع الإلكتروني والصفقات التجارية التي يبرمها أطراف التصرف الإلكتروني عبر الإنترنيت، عن طريق تأمينها لمواقع الويب بإصدارها لشهادة تصديق إلكتروني(شهادة موزع الويب)، التي يتم تثبيتها على مستوى المواقع التجارية من أجل إثبات هويتها وضمان سلامتها[1] على النحو الذي يسمح للمشتري بإقامة علاقة الثقة بالمحترف أو البائع، فعن طريق الشهادة يتم ربط هوية موزع الويب(Serveur) بمفتاح عمومي يُمَكِّنْ من تأمين المبادلات بين الموزع والمحترف أو البائع في إطار مناخ آمن للشراء أو الدفع إلكترونيا (https).

لتأمين عمليات إبرام الصفقات التجارية وضمان تقنيات الدفع الإلكتروني عبر شبكة الإنترنيت، قامت الشركة المصرفية لتونس((Société Monétique de Tunisie (SMT) في شكل تكتل بنكي يضم جميع البنوك التونسية(consortium)، بإحداث مُشَغِّلْ دفع إلكتروني آمن(SPS)[2] يعتمد على بطاقات الائتمان الذكية المحلية والأجنبية أثناء عمليات الدفع

---

– **واقد يوسف**، النظام القانوني للدفع الإلكتروني، مذكرة ماجستير في القانون العام، تخصص قانون التعاون الدولي، كلية الحقوق و العلوم السياسية، جامعة مولود معمري تيزي وزو، 2011، ص 73.

[1] - **Louise MARTEL et René ST-GERMAIN**, op.cit., pp. 93-95.

[2] – أنظر الموقع التالي : www.clictopay.com.tn

الإلكتروني عبر الإنترنيت (carte CIB, Master Card, VISA, American Express, Diner Club International)، من خلال إتاحته لتراخيص يستعملها أطراف التعامل الإلكتروني في وسط أمن وسليم، مع تمكين المواقع التجارية الإلكترونية للتجار من قبول عملية الدفع الفوري وتوفير أقصى مُستوى الأمان لدى الأطراف.

تجدر الإشارة إلى أنّ المشغل يقبل التشغيل بنظام ((Secure Stockt Layer (SSL) على أي برنامج مهما كان الجهاز المستعمل، يسمح له بالدخول مباشرةً لخدمة الدفع الآمن ويتولى تشفير الصفقات التي أبرمت على موقع التاجر، مع مُعالجة البيانات المصرفية المتبادلة بصفة آمنة[1]، بحيث يتلقى مشغل الدفع الإلكتروني لدى التاجر تأكيد بالدفع مع تسليمه للسلعة(Acquittement)، ويتلقى المستهلك بدوره وصل(Reçu) بدفعها(السلعة) مما يُزيدهما ثِقَةً على إتمام المراحل النهائية للعملية، ولكي تتم عملية الدفع الإلكتروني باستعمال بطاقة الائتمان الذكية(Carte à puce)، يجب أن تربط البنك وصاحب البطاقة علاقة عقدية وأن يُبرم البنك مع صاحب المَوْقِعْ التجاري(التاجر)، عقد حول قبول بطاقة الدفع الإلكتروني المؤمن عن بُعد، كضمان لعملية الدفع من قبل صاحب البطاقة بمجرد حصوله على ترخيص من قِبل بنكه، كما يتعين أن يكون لدى المشتري أو المستهلك متصفح ويب مثل (Internet Explorer ou Netscape) يقبل التشغيل بنظام(3-D Secure ou SSL).

من مميزات مُشغل الدفع الإلكتروني الآمن (SPS) نجد أنّه يُقلص من تعرض البنوك لمختلف المخاطر، وبالخصوص تلك الناجمة عن النزاعات، ويُساهم على تحديد هوية أطراف التصرف التجاري مع ضمان تقنية الدفع الإلكتروني عبر الإنترنيت في إطار مناخ آمن وسليم، بحيث يُشجع ثقة التاجر تجاه المشترى الذي يستخدم بطاقته البنكية لدفع مُستحقاته، كما أنّ تحديد هوية التاجر يزيد أكثر من ثقة المشتري.

---

- **David BOUNIE**, « quelques incidences bancaires et monétaires des systèmes de paiement électronique », Revue économique/ Presses de Sciences Po, 2001/7 Vol, 52, pp. 315- 317. Article disponible sur : http://www.cairn.info/revue-economique-2001-7-page-313.htm

1) - **Carole AUBERT**, op.cit., pp. 55, 56.

يُعتبر نظام((Secure Electronique Transaction (SET) من أهم بروتوكولات أمن الصفقات التجارية على الإنترنيت، تم تطويره من طرف مجموعة من الشركات الأمريكية (Visa, MasterCard, Netscape, Microsoft, IBM, HP et Oracle, etc.)، من أجل ضمان إجراءات الدفع الإلكتروني ببطاقات الائتمان الذكية بوساطة(م.خ.ت.إ) مؤتمن به من طرف أطراف التعامل الإلكتروني، إذ يقوم بتأمين المواقع التجارية(https) بشهادة تصديق إلكتروني تضمن من خلالها إجراءات إبرام العقد الإلكتروني وتسهل عملية الدفع الإلكتروني عبر الإنترنيت، وبالتالي يجب أن تربط صاحب البطاقة علاقة عقدية مع البنك المصدر للبطاقة وأن يكون بين صاحب المَوْقِعْ التجاري والبنك، عقد خاص بقبول الدفع الإلكتروني بالبطاقة الإلكترونية حتى يتسنى لجهة التوثيق الإلكتروني، بتسجيل كل البيانات المتعلقة بالبطاقة الذكية لصاحبها والتحقق من بيانات هوية التاجر أو البائع عن طريق إرسالها للمصرف الذي بدوره يتحقق من صلاحيتها وصحة المعلومات، المتعلقة بصاحب البطاقة الذكية ومن قبول البنك بالدفع الإلكتروني باستعمال البطاقة الذكية.

لذا يحتاج المستهلك إلى متصفح ويب يقبل التشغيل بنظام (SET) أمّا بالنسبة للبائع أو المحترف فيكفي أن تكون لديه شهادة موزع الويب تُمكنه من إثبات هوية موقعه التجاري (https) وضمان سلامة التبادلات الإلكترونية، والتي تتواجد على مستوى مقفل (cadenas) صفحة الإبحار للموقع التجاري، فإذا أراد المشتري أن يتأكد من مدى حماية الموقع التجاري ما عليه إلاّ الضغط، على المقفل المتواجد على صفحة الإبحار(Page de navigation) من أجل التأكد من تواجد شهادة التصديق الجذرية، وبعدها يقوم المشتري بإرسال رسالته الإلكترونية الموقعة مُرفقة بجميع البيانات المصرفية المشفرة بمفتاحه الخاص والمفتاح العام إلى البائع الذي لا يملك إمكانية فك تشفيرها، مما يقوم مباشرة بإرسالها إلى البنك (الذي يربطه عقد بقبول الدفع الإلكتروني بالبطاقة الذكية)، للتحقق من صحة بيانات شهادة التصديق للمشتري والبيانات المصرفية له فإذا كان الأمر بذلك يُوافق البنك على عملية الدفع، فغالبا ما تُسْنِدُ الشركات المصرفية الضخمة مسؤولية منح الشهادات، لجهات توثيق

فرعية تابعة لجهات توثيق رئيسية(Root CA) على أعلى هرم مرفق المفاتيح العمومية الموثوق به، بإعتبارها المسؤول الأخير عن إثبات وثاقة شهادات التصديق الإلكتروني[1].

من أجل عصرنة النظام المصرفي بالجزائر وتشجيع إستعمال طرق الدفع الإلكتروني الآمن في التجارة الإلكترونية، قامت البنوك العمومية في عام 1995 بإنشاء شركة تالية العمليات المصرفية فيما بين البنوك(SATIM) (Société d'Automatisation des Transactions Interbancaires et de Monétique) كشركة مساهمة تضم 08 بنوك (BADR, BDL, BEA, BNA, CPA, CNEP, CNMA, ALBARAKA)، (تضم الشركة حاليا حوالي 18 بنك + بريد الجزائر)[2] من أجل تأمين جميع المعاملات المصرفية التي تعتمد على طرق الدفع الإلكتروني بواسطة بطاقات الإئتمان،((Carte Interbancaire (CIB) عبر الشبكة المصرفية المُشتركة فيما بين البنوك (Réseau Monétique Interbancaire (RMI))، وذلك بإعتبارها كطرف ثالث موثوق به في المعاملات المصرفية.

لذا تقوم الشركة بإصدار شهادة تصديق إلكتروني تربط من خلالها الشبكة النقدية بمفتاح عمومي يضمن قبول جميع البطاقات البنكية المشتركة على مستوى جميع الموزعات الآلية للنقود(D.A.B)، ونهائيات الدفع الإلكتروني للتجار المنخرطين في الشبكة (Terminal de Paiement Électronique (TPE)) مع تأمين عمليات المقاصة فيما بين المصارف، وهكذا ينحصر إستخدام البطاقات البنكية على المستوى المحلي في إنتظار تعميمها على المستوى الدولي.

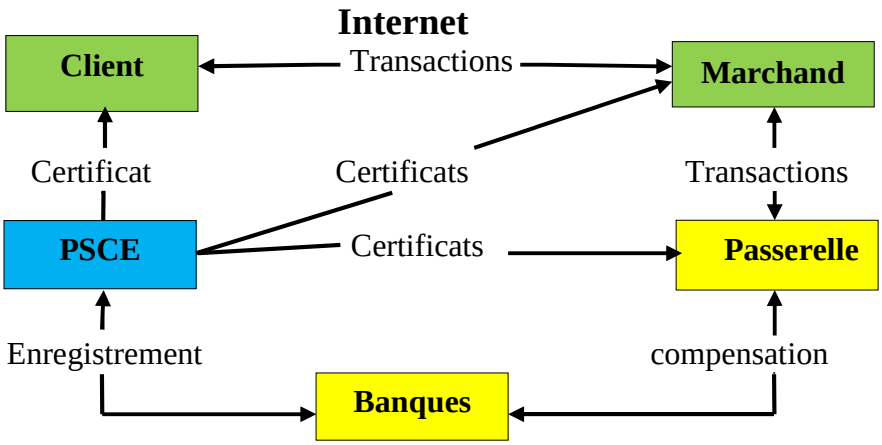
---

1) - **Garance MATHIAS et Jean-Michel SAHUT**, Le Paiement : Enjeu Du E- Commerce, p. 232. Disponible sur : http://www.iae.univ-arochelle.fr/

- **David BOUNIE et Marc BOURREAU**, « Sécurité des Paiements et Développement du Commerce Électronique », Revue économique/ Presses de Sciences Po, vol, 55, n° 04/ 2004, pp. 693- 695. Publié sur : http://www.cairn.info/revue-economique-2004-4-page-689.htm

2) – أنظر الموقع التالي: http://www.satim.dz.com

**- نموذج يبيّن أطراف المبادلة التجارية عبر الإنترنيت. -الشكل رقم 07-**




**المصدر:** من إعداد الطالب اعتمادا على: - **Arnaud-F. FAUSSE**, op.cit., pp. 259, 260.

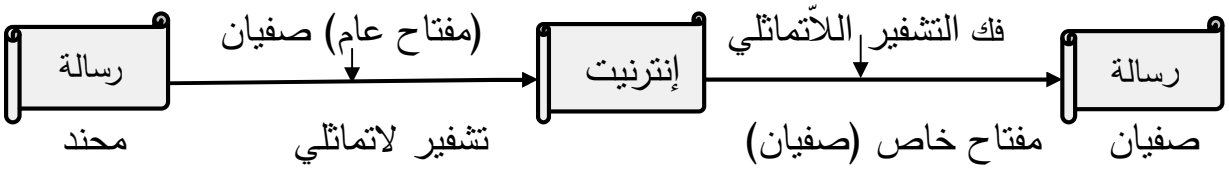
**ثانيا: التوقيع الرقمي. (Signature Numérique)**

تُستخدم تقنية التشفير اللاتماثلي(Cryptologie Asymétrique) كوسيلة لحماية المعاملات الإلكترونية، والمحافظة على سرية المعلومات أو البيانات الإلكترونية المتداولة فيها والتحقق من مصدرها، بحيث نالت التقنية على اعتراف وثقة العديد من دول العالم التي نظمتها في تنظيمات قانونية خاصة بها، نظرا لطابع الأمان والثقة التي تُوفرهما في مبادلات التجارة الإلكترونية عبر الإنترنيت بما فيها طرق الدفع الإلكتروني، في حين يرتكز نظام التشفير اللاتماثلي على زوج مفاتيح التشفير الخاص(Clé Privée) والعام(Clé Publique) المستحدثان في نفس الوقت، بعملية حسابية معقدة ودقيقة عن طريق آلية إنشاء البيانات التي تقوم بتوزيع دور وعلاقة كلّ مفتاح بصاحب التصرف الإلكتروني[1]، فإذا أراد مُحَنْذْ وفقا لآلية التشفير اللاتماثلي في إرسال رسالة إلكترونية مُشفرة لي صُفْيَان، فإنّ حاسوبه يبحث في الدليل الإلكتروني(Annuaire électronique) من أجل إيجاد المفتاح العام لصفيان الذي

1) - **Jean-Luc ARCHIMBAUD**, « les principes techniques des certificats électroniques », Les Cahiers du numérique, vol. 4, n° 3-4/2003, pp. 103,104. Disponible sur : http://www.cairn.info/revue-les-cahiers-du-numerique-2003-3-page-101.htm
- **Béatrice FRAENKEL et David PONTILLE**, « La Signature au temps de l'électronique », Revue Langage et société, vol.02 n°74, 2006, pp. 107- 111. Disponible sur : http://www.cairn.info/revue-politix-2006-2-page-103.htm

يقوم عن طريقه بتشفير الرسالة الإلكترونية الموجهة له، والتي لا يتم فك تشفيرها إلاّ باستعمال المفتاح الخاص لصفيان.

**- نموذج لآلية التشفير اللاتماثلي دون التوقيع الإلكتروني: -الشكل رقم (08)-**




**– المصدر:** من إعداد الطالب اعتمادا على: **Jean-Luc ARCHIMBAUD**, « les principes techniques des certificats électroniques », P. 104. http://www.cairn.info/ -

لذا تعتبر آلية التوقيع الإلكتروني المعزز بشهادة التصديق الإلكتروني الأكثر استخداما من طرف جهات التوثيق الإلكتروني الموثوق بها، نظرا لمستويات الأمان والثقة التي تُتيحها لأطراف التعامل الإلكتروني، بحيث تضمن سلطة التصديق الإلكتروني المعتمدة إتاحة آلية أمن إحداث التوقيعات الإلكترونية التي تضعها تحت سيطرة الموقع لوحده، التي على إثرها يقوم برنامج حاسوب مرسل الرسالة الإلكترونية قبل توقيعها، إستخدام وظيفة الهاش الأحادية الاتجاه(hachage à sens unique) لغرض استخلاص قيمة هاش أصلية للرسالة في صورة رقمية معينة(bits) أو بصمة بطول مقياسي يكون عادة، أصغر من الرسالة ومحصورا بها[1] على النحو الذي يضمن سرية وكشف أيّ تغيير في البيانات الإلكترونية عند استخدام وظيفة الهاش نفسها، وبعدها يقوم البرنامج بتشفير قيمة الهاش عن طريق خوارزميات المفتاح

---

1) - **Duc-PHONG LÊ**, Protocoles Cryptographique (Multi signature et Horodatage), Thèse de doctorat en Informatique, Spécialité Informatique, Université de Pau et des Pays de l'Adour, France, 2009, pp. 14,15.

- **Étienne WÉRY,** Facture, Monnaie et paiement électroniques, édition du Juris-Classeur, Litec, France, 2003, pp. 50, 51**.**

- Parmi **les algorithmes** les plus utilisés par la **fonction de hachage** sont : MD5, SHA-1, RIP-MD-160 et le MAC DES. - **Arnaud-F. FAUSSE**, op.cit., pp. 316, 321.

– **محمد خالد جمال رستم**، التنظيم القانوني للتجارة والإثبات الإلكتروني في العالم، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2006، ص ص 44-48.

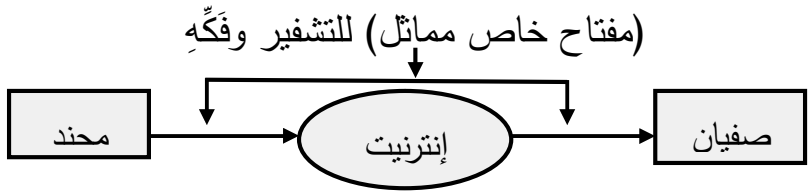
العام(DSA, ECC,RSA...) باستعمال المفتاح الخاص للمرسل، الذي يُستخدم لإحداث التوقيع الإلكتروني الموصوف.

بعد ذلك يقوم المرسل بإرسال الرسالة الإلكترونية الموقعة بوساطة جهة التصديق الإلكتروني إلى المرسل إليه، الذي يتعين عليه التأكد من مصداقية جميع المعلومات الواردة في شهادة التصديق الإلكتروني، التي عن طريقها يقوم برنامج حاسوبه بإعادة احتساب نتيجة هاش جديدة للرسالة الأصلية(le premier calcul du condensat) ويُقارنها مع قيمة الهاش المحصلة، فإذا كانت هذه الأخيرة مُطابقة لنتيجة الهاش الأصلية، فيعني سلامة بيانات إحداث التوقيع الإلكتروني ولم تتعرض البيانات الإلكترونية المرفقة به لما يثير الشبهة في مصداقيتها، أمّا إذا تحصل البرنامج على قيمة هاش غير مُطابقة لقيمة الهاش الأصلية تُثَارْ الشبهة من تعرض بيانات الرسالة الإلكترونية للتغيير أو التزوير(الشكل رقم10)، فعندما يتأكد المُستقبِل من صحة الرسالة الإلكترونية يقوم عن طريق المفتاح الخاص له(المستقبل) بتشفير الهاش والتوقيع الإلكتروني المتعلقان بالرسالة(Le Cryptogramme)، الذي يقوم بإرساله للمرسل(Émetteur) الذي يتحقق بدوره من مصداقية وصل الاستلام عن طريق المفتاح العام للمُستقبل(Destinataire)[1].

إنطلاقا من ذلك أصبح نظام التشفير المتماثل (Cryptologie Symétrique) الذي يعتمد على مفتاح واحد في آلية تشفير التوقيع الإلكتروني وفكّه، لا يستجيب لمستويات الأمان والثقة التي تتطلبها معاملات التجارة الإلكترونية، بالرغم من اعتماده على خوارزميات التشفير، فإذا أراد محند إرسال رسالة إلكترونية لصفيان، فيجب أن يمتلك كلٌّ واحدٍ منهم خوارزمية ومفتاح خاص مماثلين يُستعمله المرسل في تشفير توقيعه الإلكتروني، ثم يبعثه عبر الإنترنيت لصفيان الذي يقوم بفك شفرته بعد إتفاق الطرفين منذ البداية على كلمة المرور المُستخدمة في التشفير، في حين تشكل عملية تبادل المفتاح الخاص بينهما إحدى عيوب هذا النظام الذي يصلح فقط في الشبكات المغلقة (أنظر الشكل رقم 09).

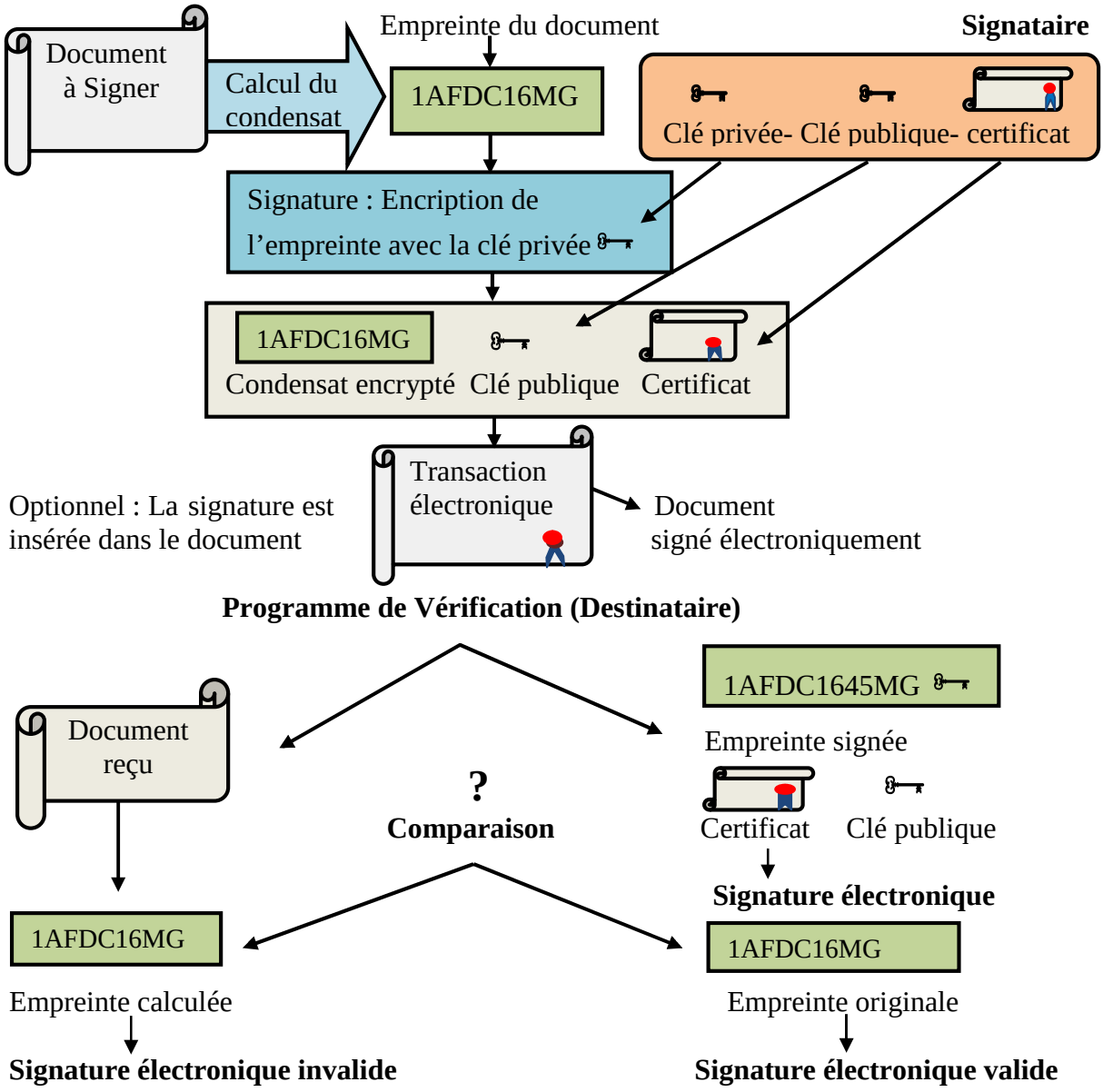
1) - **Arnaud-F. FAUSSE**, op.cit., pp. 322.

- نموذج لآلية التشفير المماثل. - الشكل رقم (09)-




- المصدر: من إعداد الطالب اعتمادا على : **Jean-Luc ARCHIMBAUD,** op.cit., p. 103 -

- نموذج لآليتي أمن إحداث التوقيع الإلكتروني وفحصه - الشكل رقم (10)-




المصدر: من إعداد الطالب اعتمادا على: **Romain KOLB,** Signature électronique, p. 08.

http://www.calis.fr/

**ثالثا: التوقيع البيومتري.(La Signature Biométrique)**

يُستعمل التوقيع البيومتري كإجراء للتوثيق لغرض التحقق من شخصية أطراف التصرف الإلكتروني بالإعتماد على الخواص الفيزيائية والطبيعية والسلوكية لكل طرف، إذ تدخل هذه الطريقة ضمن تكنولوجيا البصمات والخواص الحيوية الطبيعية التي تشمل على[1] البصمة الشخصية (Empreinte génétique)، خواص اليد البشرية (La Géométrie de la main)، مسح العين البشرية أي (بصمة القزحية) ((Image rétinienne (Vascularisation)، التحقق من نبرة الصوت (Empreinte vocale)، التعرف على الوجه البشري (La reconnaissance de la face)، التوقيع الشخصي (Écriture de la signature manuscrite).

لذا فإنّ إقبال أطراف التعاقد الإلكتروني إلى التوقيع البيومتري كإجراء أساسي لتوثيق معاملاتهم الإلكترونية، يستدعي تواجد(م.خ.ت.إ) محايد مُعتمد أو مُرخص به من طرف الجهات الرسمية، الذي يقوم في إطار مرفق المفاتيح العمومية بإستخدام الوسائل والأجهزة التقنية الخاصة بالتقاط واستقبال مُختلف الأشكال، والصفات الذاتية والحيوية للإنسان كبصمة الأصبع ومسح شبكية العين ونبرة الصوت والمخطط الحراري للوجه، نمط الأوعية الدموية، خط الكتابة باليد، رائحة الجسم الخ...، لغرض الحصول على عيّنة بيومترية بالشكل الرقمي، بحيث يقوم برنامج الكمبيوتر بتشفيرها بالإستناد على منظومة أمن إحداث البيانات وفحصها، التي تضمن عن طريق شهادة التصديق الإلكتروني هوية المُوَقِّع وسلامة مُحتوى المحرر الإلكتروني المتصل به، كما أنّ تخزين البيانات البيومترية على بطاقة ذكية مؤمنة أو جهاز حاسوب يمنع الوصول إليها(البيانات) من دون الحصول على إذن[2].

---

1) - **Arnaud-F. FAUSSE**, op.cit., pp. 325-327.

2) - **Le Duc BAO**, Authentification des empreintes digitales dans un système BioPKI, L'institut de la Francophonie pour l'Informatique (Hanoi), 2007, pp. 10-12. http://www.ifi.vnu.edu/

- **Matthieu WIROTIUS**, Authentification par Signature Manuscrite sur Support Nomade, Thèse de doctorat, Discipline: Informatique, École Doctorale: Santé, Sciences et Technologies, Université François Rabelais, Tours, 2005, pp. 18, 19, 24-27, 123-126.

من بين التقنيات البيومترية الأكثر استخداما في المعاملات الإلكترونية بوساطة (م.خ.ت.إ)، نجد التوقيع بالقلم الإلكتروني(Pen-op) على شاشة الحاسوب، بحيث يقوم برنامج هذا الأخير بالتقاط أشكال التوقيع بواسطة القلم الإلكتروني المكتوبة على لوحة البيانات، من أجل الحصول على عينة بيومترية في شكل رقمي[1]، ومن ثمة تشفيرها وتدعيمها بشهادة تصديق إلكتروني موصوفة في إطار منظومة أمن إحداث التوقيعات الإلكترونية وفحصها، في حين يُنظر إلى التقنيات البيومترية على أنّها وسيلة توفر مستوى عالٍ من الأمان والثقة في معاملات التجارة الإلكترونية، إلاّ أنّ نطاقها الرئيسي الحالي ينحصر بالتطبيقات الحكومية ذات صلة بتنفيذ القانون، كتلك التطبيقات الخاصة المتعلقة بإجراءات الموافقة في دائرة الهجرة وتدابير مراقبة الدخول الخ...

**رابعا: التوقيع بواسطة الماسح الضوئي. (Le scanner)**

إنّ دور الماسح الضوئي يكمن بالدرجة الأولى في قراءة وتحويل المُستندات الورقية الموقعة إلى مُستندات إلكترونية مُتوافقة مع شبكة الإنترنيت، وإدخال الصور العادية والفوتوغرافية في هيئتها الأصلية إلى مواقع الويب المؤمنة، بحيث يُعول عليه كثيرا في عمليات المقاصة الإلكترونية فيما بين البنوك التي تعتمد على منظومة التعويض مع ضمان التبادل الإلكتروني للقيمة المُراد تعويضها، عن طريق تصوير الصكوك والسفتجات التي تُرسل فيما بعد في مسالك مؤمنة عبر شبكة الإنترنيت بوساطة سلطة التصديق الإلكتروني.

تلعب شهادة التصديق الإلكتروني دور مُهم في ضمان سلامة البيانات والمُعطيات الخاصة بالقيم المُراد تعويضها، التي تمر عبر شبكة الإتصالات العالمية مثل(SWIFT) كما أنّ صور الصكوك والقيم المُراد تعويضها، يتم توقيعها إلكترونيا من قِبل مُختلف البنوك من أجل تسهيل عملية التعرف على هوية كلّ بنك، مع ضمان سلامة الوثائق المُصورة بالماسح

---

[1] – **نضال سليم برهم**، أحكام عقود التجارة الإلكترونية، دار الثقافة للنشر والتوزيع، عمان، 2009، ص ص 240، 241.

– **عايض راشد المري**، مدى حجية الوسائل التكنولوجية الحديثة في إثبات العقود التجارية، رسالة دكتوراه، جامعة القاهرة، 1998، ص 114.

الضوئي في حين يُعتبر التوقيع الإلكتروني للبنك كدليل على صحة المعاملة الإلكترونية المُرتبط بها، وإنطلاقا من ذلك قام البنك المركزي التونسي بإحداث المنظومة التونسية الإلكترونية تُشرف عليها شركة المصرفية المُشتركة للمقاصة الإلكترونية، (Société interbancaire de télé compensation (SIBTEL)) التي تم تأسيسها عام 1999 من طرف البنوك والمؤسسات المالية التونسية بصفتها كمكتب خدمات شبكة الهيئة العالمية للإتصالات المصرفية والمالية(SWIFT) تقوم بضمان تبادل البيانات المعلوماتية المتعلقة بالأوراق المالية، مع تسوية عمليات مقاصتها في ظرف 24 ساعة وكذلك الصور الضوئية للصكوك والسفتجات عبر شبكة تراسل البيانات ونقلها(SWIFT)[1]، كما تُشرف على إجراءات التوثيق والأرشيف الإلكتروني قصد الإطلاع عليها عبر شبكة الإنترنيت، وبالتالي القضاء نهائيا على عملية التبادل اليدوي للأوراق المالية.

من خلال ما سبق ذكره نصل إلى أنّ كلّ تقنية من تقنيات التوقيع الإلكتروني تهدف إلى تلبية احتياجات ومُقتضيات تقنية مختلفة وفقا لمُستويات معينة من الأمان، فمهما كانت التقنية المستعملة في توثيق التصرفات الإلكترونية فلا بد من مراعاتها، لمتطلبات منظومة أمن إحداث التوقيعات الإلكترونية ومنظومة فحصها الموثوق بها وفقا للمعايير الدولية المعترف بها، في حين كرّس قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية لعام 2001 بموجب المادة 03 منه، مبدأ عدم تفضيل طريقة على غيرها للتوقيع الإلكتروني بهدف السماح بإستعمال التكنولوجيات الآخرى التي من شأنها أن تنال الفرصة في إستخدامها وفقا للشروط التي يستوجبها قانون كلّ دولة، إلاّ أنّ ذلك لا يمنع من حرية الأطراف الراغبة في إبرام العقد الإلكتروني في الإتفاق حول إستبعاد طرق معينة في توثيق تصرفهم الإلكتروني وفقا لأحكام المادة 05 من نفس القانون.

---

[1] – كلمة مختصرة لـ: (**S**ociety for **W**orld wide **I**nterbank **F**inancial **T**elecommunication)

– لمزيد من المعلومات أنظر الموقع التالي : http://www.sibtel.com.tn

من خلال إستعراضنا للإطار القانوني للتوثيق أو التصديق الإلكتروني تبين لنا أنّ عملية التصديق الإلكتروني أملتها ظروف حتمية متصلة بالإقتصاد الرقمي، أين عرفت فيه المعاملات الإلكترونية تطورات عميقة وسريعة من حيث طرق أو تقنيات إبرام مختلف التصرفات الإلكترونية عبر شبكة الإنترنيت، الشيء الذي دفع بالتشريعات الدولية والجهوية والوطنية إلى تنظيم مسألة التصديق الإلكتروني، من أجل بعث الثقة والأمان في المعاملات الإلكترونية التي تتم في بيئة إلكترونية إفتراضية، وبالتالي تُعتبر القوانين النموذجية الدولية المتعلقة بالتجارة الإلكترونية لعام 1996 والتوقيعات الإلكترونية لعام 2001، التي أصدرتها لجنة الأمم المتحدة للقانون التجاري الدولي(الأونسيترال)، الإطار القانوني الدولي النموذجي المُعول عليه من طرف غالبية دول العالم أثناء تحديثها لتشريعاتها الداخلية المتعلقة بالمعاملات والتجارة الإلكترونية، التي على إثرها توصلنا إلى أنّ التصديق الإلكتروني، عبارة عن وسيلة فنيّة آمنة للتحقق من صحة التوقيع أو المحرر الإلكتروني، بحيث يتم نسبته إلى شخص أو كيان مُعيّن بوساطة جهة محايدة موثوق بها، يُطلق عليها إسم مُقدم خدمات التصديق الإلكتروني أو الطرف الثالث الموثوق به.

لذا اعترفت غالبية التشريعات بضرورة تنظيم النشاطات المتعلقة بتقديم خدمات التصديق الإلكتروني، في إطار مخططات الثقة المتبعة في التصديق الإلكتروني (بنية مرافق المفاتيح العمومية)، وذلك نظرا للثقة والأمان التي تُتيحهما تقنيات التصديق الإلكتروني المعتمدة لأطراف التعامل الإلكتروني، كتحديد هويتهم في شهادة التصديق الإلكتروني الموصوفة، وضمان سلامة وسرية محتوى البيانات المتداولة فيما بينهم في سرية تامة مع عدم إنكارها في وقت أو قبل إصدار الشهادة، في حين يجب أن تتم إجراءات التوثيق الإلكتروني المعتمدة تحت إشراف(م.خ.ت.إ) معتمد أو مرخص له من طرف الجهات الرسمية بإصدار شهادات التصديق الإلكتروني الموصوفة التي تُثبت ارتباط بيانات إحداث التوقيع الإلكتروني الموصوف لصاحبه، التي تسمح(الشهادة) للموقّع بالتعويل عليها من أجل تأكيد هويته وصحة توقيعه الإلكتروني المرتبط بالرسالة الإلكترونية، كما تسهل لمستقبل الرسالة الإلكترونية إجراءات التأكد من مصداقية البيانات الواردة في الشهادة، مما يُزيده ثقة وأمانا في ذمته المالية ومدى قُدرته على الوفاء بمُستحقاته المترتبة عن الصفقة الإلكترونية.

نظرا لفقدان تنسيق على الصعيد الدولي لمرفق المفاتيح العمومية مُنظم لخدمات جهات التصديق الإلكتروني، قامت مختلف التشريعات الوطنية بتنظيم المسائل التقنية المتعلقة بإنشاء مرافق المفاتيح العمومية حسب السياسة العامة لكل دولة، كتحديد شكل مرفق المفاتيح العمومية وعدد مُستويات السلطة التي يشملها، وما إذا كان لا يُسمح إلاّ لسلطات تصديق معينة تنتمي لمرفق المفاتيح العمومية بإصدار أزواج مفاتيح التشفير، أو من الممكن أن يُصدر أطراف التعامل الإلكتروني بأنفسهم تلك الأزواج من المفاتيح، وتحديد ما إذا كانت سلطات التصديق الإلكتروني التي تشهد بصحة أزواج مفاتيح التشفير ينبغي أن تكون عمومية أو خاصة، ومدى خضوعها للترخيص أو الإعتماد من طرف الدولة.

بالإضافة إلى ذلك يجب على الدول أن تنظر في إمكانية الإعتماد على طرق آخرى لرقابة نشاطات جهات التصديق الإلكتروني، الغير الحاصلة على ترخيص أو إذن معين لمزاولة خدماتها، ومدى إمكانية إعطاء الصلاحيات القانونية للسلطات الحكومية بالإطلاع على المعلومات السريّة المشفرة، عبر آلية استيداع المفاتيح (Key escrow) لدى طرف ثالث إيداعا مشروطا أو بأية وسيلة آخرى، كما أنّ العلاقات المنشئة فيما بين سلطات التصديق الإلكتروني المنتمية لأكثر من مرفق مفاتيح عمومية تشكل مصدر قلق مُهدّد للمعاملات الإلكترونية، الشيء الذي يستدعي النظر في مدى إمكانية إبرام إتفاقيات التصديق المتبادل للاعتراف بالمفعول القانوني بالتوقيعات الإلكترونية، وشهادات التصديق الإلكتروني المعتمدة التي يُصدرها(م.خ.ت.إ) التابع لكلّ مرفق مفاتيح عمومية.

إنّ الدور الفعّال الذي تلعبه جهة التصديق الإلكتروني كطرف ثالث مستقل موثوق به في معاملات التجارة الإلكترونية، دفع بمشرعي مُختلف الدول إلى وضع أُطُرٍ قانونية نظموا من خلالها كلّ ما يتعلق بنشاطات التصديق الإلكتروني، وبالخصوص الإلتزامات المفروضة على كلٍّ من(م.خ.ت.إ) المعتمدين أو المرخص لهم، والأطراف المعولة على شهادات التصديق الإلكتروني الموصوفة، مع تحديد المسؤوليات والجزاءات المتعلقة بالتصديق الإلكتروني والتي سنتناولها بالتفصيل في الفصل الثاني.

# الآثار القانونية
# المترتبة عن عملية
# التوثيق الإلكتروني

# الفصل الثاني

## الآثار القانونية المترتبة عن عملية التصديق الإلكتروني

لتحقيق التوازن في معادلة الإقتصاد الرقمي في مجال التجارة الإلكترونية التي تربط بين(م.خ.ت.إ) المعتمد كوسيط مُحايد في مركز أسمى، وبين أطراف التصديق الإلكتروني لضمان المبادلات الإلكترونية التي تتم فيما بين المحترفين(B2B) business-to-business أو بين هؤلاء وشخص المستهلك كطرف ضعيف(B2C) business-to-consumer، قامت مُعظم التشريعات الدولية والوطنية المنظمة لمعاملات التجارة الإلكترونية بالتنسيق فيما بين تشريعاتها الداخلية، لغرض تحديثها وتطبيعها مع المُستجدات والتطورات التي عرفتها التجارة الدولية، القائمة على إحترام قواعد التنافس الحرّ النزيه والشفاف والمشروع التي أصبحت تتم عبر شبكة الإنترنيت.

لذا فلا بدّ من وضع حدود للشروط التعسفية من خلال تنظيم العلاقة العقدية التي تجمع بين جهة التوثيق كطرف أقوى مُستقل يضمن الثقة والأمان في الصفقات الإلكترونية المبرمة فيما بين المحترف والمستهلك، عن طريق تحديد الإلتزامات المُلقاة على أطراف عملية التصديق الإلكتروني، وبالخصوص مُقدمي خدمة التصديق والأطراف المُعولة على التوقيعات وشهادات التصديق الإلكتروني، مما يفسح المجال للتكييف القانوني لمسؤولية كلّ طرف مُخِلٌّ بالتزاماته المفروضة عليه، بغض النظر ما إذا كانت تجمعهم علاقة عقدية أم لا تربطهم في إطار خدمة التصديق الإلكتروني(يعني الغَيْرْ(Tiers) المُتَضَرِّرْ من جرّاء تعويله على شهادة التصديق الإلكتروني)، لذا تقوم جهات التصديق الإلكتروني بإعداد نماذج محددة مُسبقا لمُختلف عقود تقديم خدمات التصديق الإلكتروني، وبالخصوص عقود تقديم خدمات إحداث التوقيعات الإلكترونية الموصوفة، التي تسمح لأطراف التعامل الإلكتروني بالتعويل على شهادات التصديق الإلكتروني.

لبيان أهمية كلّ هذه المحاور سنتطرق إلى الإلتزامات المترتبة عن عملية التصديق الإلكتروني في المبحث الأول، والمسؤولية المترتبة على عملية التصديق الإلكتروني في المبحث الثاني.

## المبحث الأول

## الإلتزامات المترتبة عن عملية التصديق الإلكتروني

فرضت مُعظم التشريعات الدولية والوطنية المنظمة للمعاملات الإلكترونية مجموعة من الإلتزامات المتعلقة بنشاطات التصديق الإلكتروني، على عاتق(م.خ.ت.إ) المرخص لهم أو المعتمدين من طرف الجهات الرسمية، أثناء قيامهم بإبرام عقود تقديم خدمات التصديق الإلكتروني مع الأطراف المعنية بتوثيق تصرفاتهم الإلكترونية(المطلب الأول)، والذين بدورهم يخضعون لمجموعة من الإلتزامات الناشئة عن تعويلهم على شهادات التصديق الإلكتروني الموصوفة (المطلب الثاني).

### المطلب الأول

### إلتزامات مُقدمي خدمات التصديق الإلكتروني

بإطلاعنا على نصوص مُختلف القوانين المنظمة للمعاملات الإلكترونية ونماذج عقود خدمات التصديق الإلكتروني، لبعض جهات التوثيق الإلكتروني المرخص لها أو المعتمدة يمكن تقسيم واجبات(م.خ.ت.إ) إلى طائفتين، فالأولى تتمثل في الإلتزامات المتعلقة بحماية المعلومات وتأمين صحتها التي تقع على عاتق(م.خ.ت.إ)(الفرع الأول)، والطائفة الثانية تتعلق بنشاط(م.خ.ت.إ)(الفرع الثاني).

#### الفرع الأول:

#### الإلتزامات المتعلقة بحماية المعلومات وتأمين صحتها

فرضت مختلف التشريعات المنظمة لمبادلات التجارة الإلكترونية على عاتق (م.خ.ت.إ)، مجموعة من الإلتزامات المتعلقة بحماية المعلومات وتأمين صحتها والمتمثلة في:

**أولا- ضمان صحة المعلومات الشخصية بالمُشتركين:**

يجب على(م.خ.ت.إ) أثناء تلقيه لطلبات إصدار شهادات تصديق التوقيعات الإلكترونية الموصوفة، أن يتحقق من أهلية صاحب الطلب في إبرام التصرف القانوني ومن صحة البيانات الشخصية المتصلة بهويته، وذلك بمُطالبته بالإدلاء أو الكشف عن الوثائق الرسمية في إثبات الهوية الشخصية، كبطاقة التعريف الوطنية أو جواز السفر أو أيّة أوراق ثبوتية آخرى مُعترف بها تحتوي على البيانات الشخصية لصاحبها، التي يمكن الحصول عليها عبر الإتصال المباشر به(صاحب الطلب)، أو عن طريق إرسال نسخ الوثائق الخاصة به عبر شبكة الإنترنيت أو البريد العادي برسالة موصى عليها[1].

نظرا لأهمية البيانات الشخصية لكلّ فرد وما تكتسيه من حماية قانونية من طرف التشريعات الدولية والوطنية، ألزمت هذه الأخيرة جهة التصديق الإلكتروني ببذل العناية اللازمة والمعقولة أثناء قيامها باستقبال البيانات الشخصية لصاحب طلب إصدار شهادة التصديق الإلكتروني[2]، وعدم الحصول عليها(البيانات) إلاّ بعد الموافقة الصريحة له كتابيا أم إلكترونيا وأن يتعلق مجال استعمالها، بإصدار شهادة التصديق الإلكتروني أو حفظها فقط مع الإلتزام بعدم الإضافة أو الحذف أو التعديل في مضمونها (البيانات الشخصية).

إنطلاقا من ذلك ألزم المشرع الفيدرالي الأوروبي بموجب أحكام المادة 1/08 من التوجيه الأوروبي رقم 99-93 المؤرخ في 13 ديسمبر 1999 المتعلق بالتوقيع الإلكتروني[3]، الدول

---

1) - Voir l'article **06- II (m)** du décret n° 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique.

2) – المادة 21/(أ)-(ب) (القانون الاتحادي للإمارات العربية المتحدة رقم 01-2006 بشأن المعاملات والتجارة الإلكترونية):" يلتزم مزود خدمات التصديق الإلكتروني أن يتصرف وفقا للبيانات التي يُقدمها بشأن ممارسته لنشاطه، وأن يُمارس عناية معقولة لضمان دقة واكتمال كلّ ما يُقدمه من بيانات جوهرية ذات صلة بشهادة التصديق الإلكتروني أو مُدرجة فيها طيلة مُدة سريانها."

3) - **Art.08/1-2-3** (Directive européenne n° 99-93 sur les signatures électroniques) :

« **1**- Les États membres veillent à ce que les prestataires de service de certification et les organismes nationaux responsables de l'accréditation ou du contrôle satisfassent aux exigences prévues par la directive 95/46/CE du Parlement européen et du Conseil du 24

الأعضاء في الإتحاد الأوروبي بالسهر على إلتزام كلّ من(م.خ.ت.إ) والهيئات الوطنية المسئولة على منح الإعتمادات والرقابة على خدمات التصديق الإلكتروني، إحترام أحكام التوجيه الأوروبي رقم 95-46 المؤرخ في 24 أكتوبر1995 المتعلق بحماية الأشخاص الطبيعية لدى معالجة معطياتهم الشخصية مع حرية تنقلها، وتُضيف الفقرة الثانية من نفس المادة(2/08) على إلتزام(م.خ.ت.إ) في حالة تلقيه لطلبات إصدار شهادات التصديق الإلكتروني من ذوي الشأن، بعدم استقبال معطياتهم الشخصية إلاّ بالحضور الشخصي للمعني(مباشرة منه) أو بناءا على الموافقة الصريحة له، وذلك في حالة وحيدة تتعلق بإصدار أو حفظ الشهادة فقط، وبالتالي فإنّ المعطيات الشخصية لا يُمكن استقبالها أو مُعالجتها لأغراض آخرى خارج الحالة المذكورة دون الحصول على الموافقة الصريحة للمعني بالأمر، بالإضافة إلى ذلك ألزمت الفقرة الثالثة من نفس المادة(3/08) الدول الأعضاء بعدم منع(م.خ.ت.إ) من وضع الاسم المُستعار(Pseudonyme) في شهادة التصديق بدلاً من الاسم الحقيقي لِلْمُوَقِّعِ[1].

فالمعطيات الشخصية وفقا لأحكام المادة 02(a) من التوجيه الأوروبي رقم 95-46 المؤرخ في 24 أكتوبر 1995 المتعلق بحماية الأشخاص الطبيعية لدى معالجة معطياتهم

---

octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

**2-** Les États membres veillent à ce qu'un prestataire de service de certification qui délivre des certificats à l'intention du public ne puisse recueillir des données personnelles que directement auprès de la personne concernée ou avec le consentement explicite de celle-ci et uniquement dans la mesure où cela est nécessaire à la délivrance et à la conservation du certificat.

Les données ne peuvent être recueillies ni traitées à d'autres fins sans le consentement explicite de la personne intéressée.

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

[1] - **Art.05/1** (loi du 9 Juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification, (Belgique)) :

« **1-** Sans préjudice de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, un prestataire de service de certification qui délivre des certificats à l'intention du public ne peut recueillir des données personnelles que directement auprès de la personne concernée ou avec le consentement explicite de celle-ci et uniquement dans la mesure où cela est nécessaire à la délivrance et à la conservation du certificat. Les données ne peuvent être recueillies ni traitées à d'autres fins sans le consentement explicite de la personne intéressée. »

الشخصية مع حرية تنقلها، تتمثل في كلّ معلومة تتصل بشخص مُحدد الهوية أو قابلة للتحديد وأنّ المعلومات التي تُميزه عن غيره، يُمكن أن تتصل بالعناصر الطبيعية الخاصة به أو تكون ذات طابع نفسي أو ثقافي أو اجتماعي ما دامت تُحدد بطريق مُباشر أو غير مباشر شخصيته، في حين يُقصد بآلية معالجة المعطيات الشخصية وفقا للفقرة(b) من نفس المادة(02)، كلّ عملية أو مجموعة من العمليات المنجزة أم لا عن طريق آلية معالجة المعطيات الشخصية، التي تهدف خاصة إلى جمع مُعطيات شخصية، أو تسجيلها أو حفظها أو تنظيمها أو تغييرها، أو استغلالها أو استعمالها أو إرسالها أو توزيعها أو نشرها، أو أية عملية آخرى تهدف إلى تقريب أو تبادل أو تشفير أو محو أو إتلافها، كما أنّ الموافقة الصريحة للشخص المعني وفقا للفقرة(h) من نفس المادة(02)، يُقصد بها موافقة الشخص بعد إعلامه وقبوله وفقا لإرادته الحرة على معالجة معطياته الشخصية[1].

لذا ألزمت المادة 07 من التوجيه رقم 46/95 المسؤول القائم بمعالجة المعطيات الشخصية، بالحصول على الموافقة الصريحة للمعني بالأمر مع مراعاة حالات الضرورة التي تقتضي تنفيذ عقد يكون فيه الشخص المعني بمعالجة معطياته الشخصية طرفا فيه، أو عندما تستدعي إجراءات ما قبل إبرام العقد تنفيذ ذلك، أو في حالة قيام المسؤول بالمعالجة بمهمته مراعاةً لإلتزام قانوني أو لحماية المصلحة الحيوية للشخص المعني بمعالجة معطياته

---

1) - Directive 95/46/CE du Parlement Européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. J.O.C.E, n° L 281/31 du 23/11/1995. Disponible sur : http://www.eur-lesc.europa.eu

- **Art.02** : **a)** « données à caractère personnel: toute information concernant une personne physique identifiée ou identifiable (personne concernée); est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale;

**b)** - traitement de données à caractère personnel : toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction;

**h)** - consentement de la personne concernée: toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement. »

الشخصية، أو في حالة تنفيذ مهمة قانونية ذات مصلحة عامة من طرف السلطة العمومية أو الغير أو المسؤول بمعالجة المعطيات الشخصية، بشرط عدم المساس بالحقوق والمصالح والحريات الأساسية للشخص المعني[1].

كما ألزم المشرع الفيدرالي السويسري بموجب المادة 08/1-3-4 من القانون الفيدرالي المتعلق بالتوقيع الإلكتروني لعام 2003(SCSE) (م.خ.ت.إ) المُعترف بهم، أن يشترطوا على الأشخاص التي تطلب إصدار شهادات تصديق إلكتروني موصوفة بالحضور شخصيا مُرفقين بمُستندات إثبات الهوية، سواءا أمام سلطة التصديق أو على مُستوى مكاتب التسجيل التابعة لها لغرض استقبال بياناتهم الشخصية والتحقق من هويتهم، والصفات الخصوصية لهم في حالة تمثيل شخص معنوي معين وفقا للمادة 2/07(a) من نفس القانون، وتُضيف الفقرة الثانية من نفس المادة(2/08) على تولي المجلس الفيدرالي مهمة تحديد الوثائق التي تُثبت هوية أو الصفات الخصوصية، لأصحاب طلبات إصدار الشهادات الموصوفة ومدى إلزامية حضورهم شخصيا أو إعفائهم من ذلك[2].

---

1) – Voir **l'Art. 07** du Directive n° 95/46 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

2) - **Art.08** (LFSCSE) : « **1**- Les fournisseurs reconnus doivent exiger des personnes qui demandent un certificat qualifié qu'elles se présentent en personne et qu'elles apportent la preuve de leur identité, s'agissant de l'art. 7, al. 2, let. A → (les qualités spécifiques du titulaire de la clé de signature, telle que la qualité de représenter une personne morale déterminée), les pouvoirs du représentant doivent faire l'objet d'une vérification; les renseignements professionnels ou autres relatifs à cette personne doivent être confirmés par l'organisme compétent.

**2**- Le Conseil fédéral détermine les documents de nature à prouver l'identité et, le cas échéant, les qualités des personnes qui demandent un certificat. Il peut, à certaines conditions, prévoir l'exemption de l'obligation de se présenter en personne.

**3**- Les fournisseurs reconnus doivent en outre s'assurer que les personnes qui demandent un certificat qualifié possèdent la clé de signature qui s'y rapporte.

**4**- Ils peuvent déléguer leur tâche d'identification à des tiers (bureaux d'enregistrement). Ils répondent de l'exécution correcte de cette tâche par le bureau d'enregistrement. »

- **Art. 14/1-2** (LFSCSE): « **1**- Les fournisseurs reconnus et les bureaux d'enregistrement qu'ils ont mandatés ne peuvent traiter que les données personnelles nécessaires à l'accomplissement de leurs tâches. Tout commerce de ces données est interdit.

**2**- Au surplus, la législation sur la protection des données est applicable. »

زيادة إلى ذلك نصت المادة 1/14-2 من نفس القانون على إلتزام المزود المعترف به أو مكاتب التسجيل المفوضة، بعدم معالجة المعطيات الشخصية للمعنيين خارج المهام المتعلقة بالتصديق الإلكتروني، مع الأخذ بعين الإعتبار أثناء معالجتها لأحكام القانون الفيدرالي المتعلق بحماية المعطيات(LPD) المؤرخ في 19 جوان 1992[1].

أمّا المشرع الفرنسي فألزم هو الآخر بموجب المادة 07 من القانون رقم 2004-801 المؤرخ في 06 أوت 2004 المتعلق بحماية الأشخاص الطبيعية لدى معالجة المعطيات ذات الطابع الشخصي، المعدل للقانون رقم 78-17 المؤرخ في 06 جانفي 1978 المتعلق بالإعلام الآلي والحريات[2]، المسؤول على آلية معالجة المعطيات الشخصية بوجوب الحصول على الموافقة الصريحة للشخص المعني قبل الحصول على معطياته الشخصية، التي تعني(المعطيات) وفقا للمادة الثانية(02) من نفس القانون[3]، كلّ معلومة تتعلق

---

1) - Loi Fédérale sur la protection des données (LPD) du 19 juin 1992. http://www.admin.chopcfrclassified-compilation20011277index.html

2) - Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. J.O.R.F, n° 182 du 07 août 2004. http://www.legifrance.gouve.fr

- **Art. 07** : « Un traitement de données à caractère personnel doit avoir reçu le consentement de la personne concernée ou satisfaire à l'une des conditions suivantes :
1- Le respect d'une obligation légale incombant au responsable du traitement ;
2- La sauvegarde de la vie de la personne concernée ;
3- L'exécution d'une mission de service public dont est investi le responsable ou le destinataire du traitement ;
4- L'exécution, soit d'un contrat auquel la personne concernée est partie, soit de mesures précontractuelles prises à la demande de celle-ci ;
5- La réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée. »

3) - **Art. 02** : (Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.)
- « Constitue une **donnée à caractère personnel** toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne. »
- « Constitue **un traitement de données à caractère personnel** toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et

بالشخص الطبيعي المعرف بهويته، أو من المحتمل أن تحدد هويته بالطريقة المباشرة أو الغير المباشرة بالرجوع إلى رقم تعريف هويته، ولتحديد ما إذا كان الشخص مُعرَّف الهوية ينبغي على المسؤول بمعالجة المعطيات الشخصية أو أيّ شخص آخر الإستعانة بالوسائل اللازمة التي تسهل العملية.

بالإضافة إلى ما سبق ألزم المشرع التونسي(م.خ.ت.إ) بموجب الفصل 16 من القانون عدد 83-2000 المتعلق بالمبادلات والتجارة الإلكترونية، عند طلب إصدار شهادة التصديق منه بضرورة الحصول على المعطيات الشخصية مباشرة من الشخص المعني بالطلب أو بواسطة الغير، بشرط الحصول على موافقة صاحب الطلب بالطريقة الكتابية أو الإلكترونية وأن يستخدمها(البيانات) في إطار أنشطة التصديق الإلكتروني فقط، إذْ يمكن للمزود أن يتحصل على الموافقة الصريحة إلكترونيا في حالة ما إذا ضمن(المزود) لصاحب الشهادة الإعلام بحقه في سحب الموافقة في أيّ وقت، وإمكانية تحديد هوية الأطراف المُسْتَعْمِلَة للمعطيات الشخصية له مع الإحتفاظ بحجية الموافقة التي لا يُمكن تغييرها[1].

فإذا اعترض صاحب الشهادة على إستخدام معطياته الشخصية لأغرض لا علاقة لها بإصدار شهادة التصديق الإلكتروني، يجب عليه إعلام(و.و.م.إ) بالاعتراض في رسالة موصى عليها بالوصول مع إعلام بالإستلام، ويُعتبر هذا الاعتراض كقرينة قاطعة بالنسبة لكل المزودين والغير، كما يُمنع على مُستعملي المُعطيات الشخصية التي تم جَمْعِهَا طبقا للفصل39 من نفس القانون، من إرسال الوثائق الإلكترونية إلى صاحب الشهادة الذي يرفض صراحة قبولها(الفصل 40 من نفس القانون).

---

notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction. »

[1] – الفصول 38 و39 و41 من القانون عدد 83-2000 المتعلق بالمبادلات والتجارة الإلكترونية.

– أنظر كذلك الفصلين 08 و09 من الأمر عدد1667-2001 المؤرخ في 17 جويلية 2001 المتعلق بالمصادقة على كراس الشروط الخاص بمُمارسة نشاط مُزودي خدمات المصادقة الإلكترونية.

تجدر الإشارة أنّ المعطيات الشخصية للشخص الطبيعي مَحْمِيَّة بموجب أحكام القانون الأساسي عدد 63-2004 المؤرخ في 27 جويلية 2004 المتعلق بحماية المعطيات الشخصية، التي إعتبرها بموجب الفصل الأول منه ضمن الحقوق الأساسية المتعلقة بالحياة الخاصة للأشخاص والمضمونة بموجب الدستور، إذْ لا يمكن معالجتها إلاّ في إطار الشفافية والأمانة وإحترام كرامتهم وفقا لمُقتضيات هذا القانون، وإنطلاقا من ذلك نص الفصل 27 من نفس القانون على عدم إمكانية معالجة المعطيات الشخصية إلاّ بعد الحصول على الموافقة الصريحة والكتابية للمعني بالأمر، وأن تتم عملية جمع المعطيات بهدف تحقيق الغرض الذي جُمعت من أجله، بإستثناء الحالات المذكورة في المادة 12 من نفس القانون والمتمثلة في مُوافقة المعني بالأمر، وما إذا كان في ذلك تحقيق مصلحة حيوية له (المعني بالأمر) أو إذا كانت لتحقيق أغراض عِلمية ثابتة[1].

**ثانيّا- الإلتزام بالإعلام:**

يُعتبر الإلتزام بالإعلام من أهم الحقوق المستحدثة في عقود التجارة الإلكترونية والمضمون(الإعلام) لصاحب طلب إصدار شهادة التصديق الإلكتروني الموصوفة، لذا يجب على(م.خ.ت.إ) أن يلتزم بإعلام صاحب الطلب بالطرق الكتابية أو الإلكترونية قبل مُباشرة إجراءات إبرام العقد المتعلق بتقديم خدمات التصديق الإلكتروني، بكلّ الشروط المتعلقة بإستخدام شهادات التصديق الإلكتروني وحالات إلغاءها وإيقافها وبطرق تقديم الشكاوى وحلّ مُختلف الخلافات والنزاعات المترتبة عن عملية التصديق الإلكتروني، وما إذا كان(م.خ.ت.إ) خاضع لنظام الترخيص الخ...، التي ينبغي عليه أن يُوضحها في بيان

---

[1] - المادتين 10 و11 من القانون الأساسي عدد 63-2004 المؤرخ في 27 جويلية 2004 المتعلق بحماية المعطيات الشخصية، المنشور في ر.ر.ج.ت عدد 61 الصادر في 30 جويلية 2004. http://www.legislation.tn

- المادة 43 من قانون رقم 15-04 مؤرخ 2015/02/01 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين(الجزائر).

- **عبد الفتاح بيومي حجازي**، التجارة الإلكترونية في القانون العربي النموذجي، الطبعة الأولى، الكتاب الثاني، دار الفكر الجامعي، الإسكندرية، مصر، 2006، ص 230.

السياسة العامة(DPC) المُتبعة في التصديق الإلكتروني المُتاح عبر شبكة الإنترنيت على مستوى موقعه الإلكتروني.

إنطلاقا من ذلك ألزم التوجيه الأوروبي رقم 93/99 المتعلق بالتوقيعات الإلكترونية في الملحق الثاني فقرة(k) منه، (م.خ.ت.إ) قبل إبرامه لعقد تقديم خدمات التصديق الإلكتروني بوجوب إعلام كتابة الشخص الراغب في إصدار شهادة تصديق إلكتروني موصوفة، بجميع الطرق والشروط المتعلقة بإستعمال الشهادة مع القيود المفروضة عليها، وبتواجد نظام الإعتماد الاختياري، مع إعلامه بجميع إجراءات إيداع الشكاوى وطرق حلّ النزاعات[1].

بالإضافة إلى ذلك فرضت المادة التاسعة(09) من القانون الفيدرالي السويسري المتعلق بالتوقيع الإلكتروني لعام 2003(SCSE) على عاتق(م.خ.ت.إ) المُعترف به، الإلتزام بإعلام العموم بجميع المعلومات المتعلقة بشروط إبرام عقود تقديم خدمات التصديق الإلكتروني والآثار المترتبة عن الاستعمال التعسفي، للمفاتيح الخاصة بتوقيعاتهم الإلكترونية في حالة

---

1) - **ANNEX II (k) :** (Directive européenne n° 99-93 sur les signatures électroniques.)
« Avant d'établir une relation contractuelle avec une personne demandant un certificat à l'appui de sa signature électronique, informer cette personne par un moyen de communication durable des modalités et conditions précises d'utilisation des certificats, y compris des limites imposées à leur utilisation, de l'existence d'un régime volontaire d'accréditation et des procédures de réclamation et de règlement des litiges. Cette information, qui peut être transmise par voie électronique, doit être faite par écrit et dans une langue aisément compréhensible. Des éléments pertinents de cette information doivent également être mis à la disposition, sur demande, de tiers qui se prévalent du certificat. »

– بإطلاعنا على نموذج عقد الاشتراك في خدمات التوثيق (contrat d'abonnement au service de Certification) المتاح على الموقع الإلكتروني لسلطة التصديق الإلكتروني المعتمدة CertEurope، نص في البند 15 منه على طرق حلّ النزاعات التي يمكن حلّها بالاعتماد على الطرق البديلة في حل النزاعات وبالخصوص التحكيم Arbitrage، فإذا اتفق الأطراف على تطبيق إجراءاته فيتم اللجوء إلى مركز ATA للمصالحة والتحكيم في التقنيات المتطورة، (Centre de conciliation et d'arbitrage des techniques avancées) الذي يوجد مقره في باريس (http://www.legalis.net/ata) فإذا لم يتفق الأطراف، على إجراء التحكيم فيتم اللجوء إلى إجراءات التقاضي على مستوى محكمة الاستئناف بباريس أين يتواجد مقر سلطة التصديق الإلكتروني. http://www.certeurope.fr

إصدارها للشهادات والتدابير التي يجب إتخاذها وفقا للظروف لضمان سريتها والتي يوضحها في سياسة التصديق الإلكتروني (PC)[1].

كما أقرّ المشرع التونسي كذلك أهمية الإلتزام بالإعلام في الفصلين 19 و20 من الأمر عدد1667-2001 المتعلق بالمصادقة على كرّاس الشروط الخاص بمُمارسة نشاط (م.خ.م.إ)، أين ألزم هذا الأخير بأن يضع على ذمة العموم لبنك من المعلومات مفتوح 24/24 ساعة على كامل أيام الأسبوع، يتضمن المعلومات المتعلقة بشهادات التصديق الإلكتروني السارية المفعول أو المُلغاة أو الموقفة، مع تحديده(المزود) للشروط العامة والإجراءات المُعتمدة من قِبَلِهِ في خدمات التصديق الإلكتروني والتعريفات المُطبقة عليها(الخدمات)، وبحقوق وواجبات حُرفائه ومُستعملي الشهادات عند إستعمال الشهادة، كما يلتزم المزود بنشر كلّ الإجراءات والشروط المتعلقة بالتصديق الإلكتروني الموقعة إلكترونيا من طرف ممثله القانوني ضمن موزع الويب الذي يملكه[2]، ولضمان الثقة في المعلومات المتاحة من طرف المزود يجب أن تُصادق عليها (و.و.م.إ).

بالإضافة إلى ذلك نص قرار وزير الإقتصاد الإماراتي رقم01-2008 بشأن إصدار لائحة مُزودي خدمات التصديق الإلكتروني في المادة 18 منه، على إلتزام(م.خ.ت.إ) وفقا للإرشادات التي تُحددها الهيئة العامة لتنظيم قطاع الإتصالات بصفتها كمُراقب، بإعداد وتوفير ونشر أحدث بيان ممارسة التصديق الإلكتروني في موقعه الإلكتروني، يُحدد فيه جميع الممارسات والإجراءات التي يُوظفها في إصدار شهادات التصديق الإلكتروني والخدمات الآخرى المُرخص بها، مع تقديم نسخة من ذلك البيان للمراقب عند تقديمه لطلب

---

[1] - **Art.09** du (LFSCSE 2003) : « **1-** Les fournisseurs reconnus doivent tenir à la disposition du public leurs conditions contractuelles générales et des informations sur leur politique de certification.
**2-** Ils doivent informer leurs clients des conséquences de l'utilisation abusive de leur clé de signature, au plus tard lors de la délivrance des certificats qualifiés, ainsi que des dispositions à prendre, selon les circonstances, pour assurer la confidentialité de leur clé de signature.
**3-** Ils tiennent un journal de leurs activités. Le Conseil fédéral règle la durée pendant laquelle le journal et les documents qui s'y rapportent doivent être conservés. »

[2] – أنظر الفصل 20 من الأمر عدد1667-2001، المتعلق بالمصادقة على كراس الشروط الخاص بمُمارسة نشاط مُزودي خدمات المصادقة الإلكترونية. http://wwwlegislation.tn

الموافقة على منح أو تجديد الترخيص، وإعلامه(المراقب) خطيًّا بأيّةِ تَغْيِيرات على البَيَان(DPC) خلال 30 يوم من تاريخ تنفيذ تلك التغييرات التي ينبغي عليه تسجيلها فيه(البيان).

**ثالثا– الإلتزام بالمحافظة على معدّات وأنظمة أمن المعلومات:**

يجب على(م.خ.ت.إ) الإلتزام بإعداد خُطّة أمنية لإدارة الكوارث التي تسمح بمُواجهة مُختلف الأمور المتعلقة بأيّ تهديد يمس في الإجراءات الأمنية أو تجهيزات التصديق الإلكتروني الخاصة بالمزود، بما في ذلك أمن المعلومات المتعلقة بشهادات التصديق الإلكتروني وأجهزة إصدار التوقيعات الإلكترونية الموصوفة، وضمان عدم تعرض أنظمة الأمن أو الشبكة لأيّ خلل من شأنه أن يفسح المجال بحدوث إنزلاقات واختراقات أمنية، بما فيها المساس بأنظمة أمن حفظ السجلات المتعلقة خاصةً بإصدار وتجديد وتعليق وسحب وإلغاء شهادات التصديق الإلكتروني، وبإجراءات التصرف في التجهيزات وبرمجيات المعلومات المتعلقة بمنظومات أمن إحداث التوقيعات الإلكترونية وفحصها، كما يتعين على(م.خ.ت.إ) وضع موزعاته والأجهزة الطرفية التي تُمكن من النفاذ إلى هذه الموزعات بمواقع إلكترونية مُؤمنة[1] لا يدخلها إلاّ الأعوان المُرخص لهم، مع إلتزامه بمسك سجل خاص مؤمن على مُستوى كلّ مُوزع تُدون فيه جميع عمليات النفاذ إليه (الموزع).

---

[1] – أنظر المادة 21 من قرار وزير الاقتصاد الإماراتي رقم رقم01–2008 بشأن إصدار لائحة مُزودي خدمات التصديق الإلكتروني. http://www.government.ae

– تُعتبر مقاهي الإنترنيت (Cyber Café) المكان اللائق لأصحاب الاختصاص بارتكاب مُختلف الجرائم المعلوماتية دون إمكانية تحديدهم، لكون أنّ مُسيّري المقاهي لا يتطلبون من عملائهم بضرورة إثبات وتحديد شخصياتهم، وهذا ما أكدته المباحث الفيدرالية بالولايات المتحدة الأمريكية بعد تتبعها لأحد القراصنة التي لم تتمكن من تحديد شخصيته والتعرف عليها، بحيث استطاع من اختراق شبكة معلومات أحد المصارف، لكون المجرم اعتمد على عِدّة مقاهي إنترنيت لتنفيذ عمليته. لمزيد من التفاصيل أنظر:

– **طارق إبراهيم الدسوقي عطية**، الأمن المعلوماتي (النظام القانوني للحماية المعلوماتية)، دار الجامعة الجديدة للنشر، الإسكندرية، 2009، ص 596.

– من بين أهم وسائل اختراق نظم أمن المعلوماتية نجد:

– **مُصدّع كلمات العبور (Passwords Cracker):** يعتمد على أيّ برنامج تطبيقي يمتلك القدرة على تجاوز عقبة التشفير المستخدم في نظم الأمن أو إحباط آليات الحماية المُصاحبة بها، والجدير بالذكر أنّ المُصدع لا يُلغي الشفرة المُستخدمة أو يعمل على إظهارها في شكل مقروء، بل يُتيح إمكانية تجاوز الجدار الأمني الذي توفره (الشفرة) لصاحبها في درء أيّ نشاط يسعى إلى اختراق الحدود الأمنية الخاصة بالمعطيات الشخصية لصاحبها، وبالتالي يعتمد مُصدع كلمات العبور مُسبقا على خوارزميات مُعدة مُسبقا ومماثلة للخوارزميات الأصلية المُستعملة في التشفير بحيث تعمل على توليد شفرات حديثة تُناظر الشفرات المُعتمدة في صياغة كلمة العبور الأصلية، لذا تقوم البرامج باستغلال الفجوات التي تنشأ أثناء استعمال الأفراد والجهات لكلمات العبور بصفة مُتكررة.

– **الفيروسات البرمجية (Program Viruses):** يمكن تعريف الفيروس الإلكتروني على أنّه برنامج مُهدّد لجهاز الحاسوب لتحقيق غرض معين يهدف إلى تغيير البيانات الإلكترونية أو إتلافها، و الذي يُشبه الفيروس البيولوجي من حيث الأداء بحيث يعمل على نقل الأضرار إلى أجهزة الحاسوب الأخرى، ومن بين السمات التي تتميز بها الفيروسات الإلكترونية نجد القدرة على الاختفاء والانتشار، والاختراق والتدمير أو التخريب، وتعود جذور ظهور تقنية الفيروسات لسنوات الستينات (1960) أين قام مهندسان أمريكيان بالتلاعب فيما بينهم ببرامج الإعلام الآلي صغيرة الحجم من دون وصول أيّ منهما لإلحاق أضرار بالطرف الآخر، لذا قام الطالب الأمريكي في الإعلام الآلي Frederik COHEN بتطوير التقنية إلى أن توصل عام 1983 بخلق أول برنامج فيروسي يمكن أن يُلحق الأضرار بأجهزة الحاسوب الأخرى بمُجرد نقله على حامل إلكتروني، وهكذا تم التعويل على تقنيات إحداث برامج خاصة بالفيروسات عبر شبكة الإنترنيت بغرض الإضرار بأنظمة أمن المعلومات تصل إلى حدّ التخريب في بعض الأحيان ويُعد الفيروس الذي أعدّته جماعة تخريبية غير معروفة في زمن الحرب الباردة، الأكثر إضرارا إلى حدّ الساعة والذي مَسَّ بالنظام الأمني للمُفاعل النووي(Réacteur Nucléaire) الذي إنفجر في 26 أفريل 1986 الذي يبعد عن مدينة **تَشِرْنُوبِيلْ(Tchernobyl)** الأوكرانية، بحوالي 20 كلم و130 كلم شمالا عن عاصمتها **Kiev**. لمزيد من التفاصيل حول الحادثة أنظر الموقع التالي:
http://www.atlas-historique.net/1949-1989/carte/FranceTchernobyl.html

من بين الفيروسات التي تمس أنظمة أمن المعلوماتية نجد فيروسات قاطع التحميل (Boot Sector Virus DSV) التي تمتلك القدرة على إصابة قاطع التحميل في المُخَزِّنْ الإلكتروني Boot Sector حيث تستبدل القطاع الرئيسي بقطاع آخر من صنع الفيروس مع إمكانية تكوين نُسخة إضافية منه، مع إيهام المُستخدم بعدم وجود فيروس في حاسوبه الشخصي، مما يستدعي الحاجة إلى البحث عن برامج أمنية مُضادة

لضمان حسن سير الخُطَّة الأمنية المُنتهجة في خدمات التصديق الإلكتروني ألزمت بعض التشريعات(م.خ.ت.إ)، بوجوب تجهيز مَقَرَّاتِهِ بشبكة كهربائية وأنظمة تكييف تُؤمِّن استمرارية العمل واستغلال التجهيزات والمنظومات التي يُعول عليها في تقديم خدمات التصديق الإلكتروني، مع تأمين جميع الحاويات المُعدّة للتخزين ضد الحرارة والرطوبة والتأثيرات المغناطيسية وكلّ شكل من أشكال التشويش، والاستعانة بخدمات البرامج المعلوماتية الحديثة المُعدة خصيصا بإتلاف المعلومات المُضمنة بالحاويات قبل إتلافها أو استغلالها لأغراضٍ آخرى[1]، لذا نص المشرع العمّاني بموجب المادة 19 من القانون المتعلق بالمعاملات الإلكترونية لعام 2008، على طرق حماية أنظمة المعلومات المتمثلة في كلٍّ من التشفير بطريق المفتاح العام، والجدران النارية، مُرشحات المعلومات، ومجموعة الوسائل المتعلقة بمنع الإنكار، تقنيات تشفير المُعطيات والملفات، إجراءات حماية نسخ الحفظ الاحتياطية، البرامج المُضادة للديدان والفيروسات، وأيّة طريقة آخرى تُجيزها هيئة تقنية المعلومات.

---

للفيروسات والبرامج الخبيثة التي يُمكن من خلالها كشف وتحديد مصدر الفيروسات وردعها بكامل الأشكال. لمزيد من المعلومات أنظر الموقع التالي: http://www.users.pandora.be/martin.melchior/

– **محمد عبد الرحيم**، جرائم الإنترنيت والاحتساب عليها، ص ص 880، 882. – **إسماعيل عبد النبي شاهين**، أمن المعلومات في الإنترنيت بين الشريعة والقانون، ص ص 973، 978، 988، 989. (الجزء الثالث) بحوث مقدمة في مؤتمر القانون والكمبيوتر والإنترنيت، المنعقد في 1–3 ماي 2000 بجامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، بالتعاون مع مركز الإمارات للدراسات والبحوث الإستراتيجية ومركز تقنية المعلومات بالجامعة. منشور على الموقع التالي: –http://www.slconf.uaeu.ac.aearabic_prev_conf2000.asp

**العاني إيمان**، البنوك التجارية وتحديات التجارة الإلكترونية، مذكرة شهادة الماجستير في العلوم الإقتصادية، تخصص بنوك وتأمينات، كلية العلوم الإقتصادية وعلوم التسيير، جامعة منتوري قسنطينة، 2007، ص ص 83–103.

[1] – راجع الفصلين 17 و18 من الأمر عدد1667–2001، المتعلق بالمصادقة على كراس الشروط الخاص بمُمارسة نشاط مُزودي خدمات المصادقة الإلكترونية. http://wwwlegislation.tn

لذا أصبحت معدّات وأنظمة أمن تكنولوجيا المعلومات في الوقت الحديث تُشكل الشغل الشاغل لكلّ دولة أو أي مسئول عن كيان أو منشأة ما، التي تُعتبر عصب الحياة بالنسبة لها وتقدير مدى إستمرارها أو بقاءها، وبالتالي ينبغي على(م.خ.ت.إ) الإعتماد على معدات وأنظمة أمن تكنولوجيا معلومات موثوق بها من طرف الجهات الرسمية في كلّ دولة وفقا للمعايير المعترف بها دوليا، وهذا ما قام به المشرع التونسي الذي كلّف المجلس الوطني لاعتماد مراكز تقييم المطابقة، بمهمة تنظيم ومراقبة عمليات التدقيق ومتابعتها وتكوين المدققين ورسكلتهم دوريا، وفقا للمواصفات الوطنية والدولية المعمول بها في مجال الاعتماد والمطابقة وفي كلّ الظروف يشرف هذا المجلس على تنفيذ سياسة الدولة في مجال الاعتماد وتقييم المطابقة[1].

بالإضافة إلى ذلك كلّف المشرع الجزائري بموجب المادة 14 من القانون رقم 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، "الهيئة الوطنية المكلفة بالاعتماد" بمهمة التأكد من مطابقة آليات إنشاء التوقيع الإلكتروني الموصوف وفحصه والقيام وفقا للمعايير المعمول بها في الجزائر، بتدقيق السلطة الوطنية للتصديق الإلكتروني والسلطتين الاقتصادية والحكومية والطرف الثالث الموثوق و(م.خ.ت.إ)، لذا قام المشرع الجزائري بموجب المادتين 78 و79 من نفس القانون بتوكيل هذه المهام للمصالح المختصة في هذا المجال لفترة انتقالية إلى حين إنشاء "الهيئة المكلفة بالإعتماد" في خلال مدة لا تتجاوز خمسة (05) سنوات إبتداءا من تاريخ صدور هذا القانون في الجريدة الرسمية.

تجدر الإشارة أنّ دور وكالة الأمن القومي للولايات المتحدة الأمريكية(NSA)[2] لا يتعلق فقط بخدمة الأغراض التي تمس بالأمن الداخلي للدولة الفيدرالية، بل يتعدى ذلك لأغراض

---

[1] – الفصل 08 من القانون عدد 92-2005 المؤرخ في 03 أكوبر 2005، المتعلق بتنقيح وإتمام القانون عدد 70-1994 المؤرخ في 20 جوان 1994 المتعلق بإحداث نظام وطني لاعتماد هيئات تقييم المطابقة، المنشور في (ر.ر.ج.ت) عدد 79 الصادر في 04 أكتوبر 2005.
http://www.legislation.tn

[2] – تعتبر وكالة (**NSA**) المُنشئة في عام 1952 كأكبر وكالة استعلامات أمريكية، مكلفة برقابة الاتصالات الإلكترونية والتنبؤ من التهديدات الخارجية ضد الولايات المتحدة الأمريكية، تمارس مهامها

(بالتعاون مع شقيقتها الوكالة الحكومية البريطانية للاستعلامات (GCHQ) التي تعتبر الحليف الأقرب لها) في إطار رقابة قانونية من طرف جهاز Foreign Intelligence Surveillance Court (FISC) الذي نص على تأسيسه قانون 1978 Le Foreign Intelligence Surveillance Act (FISA) الذي لم يستطيع من مراقبتها لغياب الوسائل اللازمة بذلك على حدّ تعبير مديرها الفني لـ Washington Post، فحسب الوثائق التي نشرها Edward Snowdon فإنّ الوكالة اعتمدت على مجموعة من برامج التجسس والقرصنة عالية المستوى منها:

1- **برنامج (XKeyScore)**: قادر على فحص جميع التصرفات التي يقوم بها أيّ شخص من العالم عبر شبكة الإنترنيت، بحيث يتظاهر في هيئة مُحرك بحث (Google) بهدف القرصنة، والمُزَوَّد ببيانات مُختلف برامج الرقابة ذات صلة بالوكالة، قادرة على الاحتفاظ بالمعلومات المُقرصنة لعدة سنوات، إنّ قوة هذا النظام تكمن في قدرته على البحث عن أيّة معلومات متعلقة بشخص معين، وإن كان غير مُشتبه فيه بالإضافة إلى إمكانيته على الإطلاع بأكبر قدر معين من مواقع الإنترنيت المتصلة به (حوالي أكثر من 150 موقع ذات صلة به)، وقدرته من التنصت على مُختلف وسائل الاتصالات التابعة لمُختلف المراكز الدبلوماسية والقنصلية التابعة لمُختلف دول العالم وحتى حكوماتها، لأهداف وكالة الاستخبارات الأمريكية الخارجية (CIA) والأمن الداخلي (FBI)، كما أنّه قادر على كشف مُحتوى البريد الإلكتروني الخاص بزبائن الشبكات الاجتماعية على سبيل المثال (Facebook, twiter,etc)، وهكذا قام الأعوان التابعين لوكالة الإستخبارات الحكومية البريطانية (GCHQ) بتزويد وكالة الإستعلامات الخارجية الألمانية (BND) Le Bundes nachricht endienst بهذا البرنامج، لإستخدامه لأغراض تتعلق بمُكافحة الإرهاب بالتعاون مع فرع الوكالة الأمريكية(NSA) المقيم على الأراضي الألمانية، والذي اعتمدت عليه كثيرا وكالة الاستعلامات الداخلية الألمانية(BFV) دون وكالة الاستعلامات الخارجية(BND)، الشيء الذي سمح للبرنامج بفحص جميع التصرفات الإلكترونية للمواطنين الألمان عبر شبكة الإنترنيت، وحتى على رئيسة الوزراء للحكومة الألمانية (Angela MERCKEL) بالتنصت على هاتفها الشخصي، كما تعرض رؤساء الجمهورية الفرنسية الخامسة في عهد كلّ من جاك شيراك(Jacques CHIRAC) ونيكولا ساركوزي (Nicolas SARKOZY) وفرانسوا هولاند(François HOLLANDE) إلى عمليات التنصت على هواتفهم الشخصية، من طرف وكالة(NSA)، التي باشرت مهام التجسس حسب بعض الخبراء منذ عهد الجنرال شارل ديغول(Charles DE GAULLE) مؤسس الجمهورية الفرنسية الخامسة(1958-1969) وذلك من دون علم الفرنسيين بذلك.

2- **برنامج المضلة (Fairview)**: مُبرمج لرقابة الإنترنيت حسب المسؤول الأعلى السابق لدى الوكالة

تخدم معاملات التجارة الإلكترونية، كالتكفل بمهام اعتماد مراكز تقييم مطابقة معدات وأنظمة أمن تكنولوجيا المعلومات للمعايير أو المواصفات الأمنية والتقنية المعمول بها، في إطار مُخطط التقييم والتوثيق الذي تقوم بإعداده، وتراقب مهام هذه المراكز وتشرف على عمليات إصدار شهادات المطابقة، كما يتم استشاراتها في عملية إعداد القوانين المتعلقة بسلامة وأمن المعدات والتجهيزات، وتضمن العلاقات التقنية مع الأطراف الأجنبية المثيلة لها[1].

---

(Thomas Drake) وهو الآخر يجمع العديد من برامج الرقابة التابعة للوكالة من أجل هدف مشترك لذا قامت الوكالة بإبرام علاقات الشراكة مع العديد من وكالات الاتصالات التابعة لمختلف دول العالم مثل ألمانيا والمكسيك والبرازيل الخ ... قصد التنصت على الاتصالات ويُعتبر برنامج (**Silverzephyr**) من بين برامج التنصت في البرازيل.

**3- برنامج (Prism):** لقد أبرمت الوكالة سلسلة من عقود الشراكة مع العديد من عمالقة شبكة الإنترنيت (Microsoft, Yahoo, Google, Facebook, PalTalk, Youtube, Skype, AOL et Apple.) فعن طريق هذا البرنامج تستطيع الوكالة الأمريكية ووكالة (GCHQ) في التصرف في جميع البيانات الإلكترونية التي تحتويها هذه الشبكات، من رسائل وصور وبريد الخ...، إذ أقدمت ميكروسوفت على إتاحة مفتاح التشفير المتعلق بالبريد الإلكتروني المباشر لـ Outlook للوكالة قصد تمكينها من تحويل أنظمة حماية البيانات للمستخدمين كما سمحت لها بالإطلاع على البيانات المخزنة المتعلقة بملفات SkyDrive الخ...

**4- برنامج** (**Tempora**): موجود منذ 2011 تحت إدارة الوكالة البريطانية(GCHQ)، التي ألزمت شركات الإتصالات الدولية بالتعاون (British Telecom, Vodafone Cable, Verizon Business, Global Crossing, Level 3,Viatel et Interoute) ، من أجل التنصت على الإتصالات الدولية.

**5- برنامج (Boundless Informant):** يهدف إلى التحليل المباشر لجميع المعلومات المحصلة في كل بلد من العالم وهو قادر على الكشف عن مصدر مجيء أيّة معلومة عبر العالم ومن بين الدول المستهدفة كثيرا (فرنسا، إيران، باكستان، مصر، الأردن، الخ...) فحسب جريدة The Guardian استطاع البرنامج من تحصيل حوالي 97 مليار من البيانات الإلكترونية في شهر واحد فقط.

**6- برنامج (EvilOlive)** شُغِلَ في 2012 لرقابة كبار المُتعاملين في مجالات الإتصالات المقيمين داخل الأراضي الأمريكية. لمزيد من التفاصيل راجع: - **Maxime VAUDANO**, article de journal le monde, publié sur : http://www.lemonde.fr

[1] - **Arnaud-F.FAUSSE** , op.cit., pp. 64, 65.

## الفرع الثاني

## الإلتزامات المتعلقة بنشاط مُقدمي خدمات التصديق الإلكتروني

ألزمت مُختلف التشريعات(م.خ.ت.إ) المعتمد أو المرخص له بمزاولة خدمات التصديق الإلكتروني بمراعاة النصوص التشريعية والتنظيمية المتعلقة بها، التي فرضت عليهم مجموعة من الإلتزامات الخاصة بنشاطاتهم والمتمثلة في:

**أولا- الإلتزام بأحكام الترخيص أو الإعتماد:**

يمكن تصنيف عقود تقديم خدمات التصديق الإلكتروني التي تُبرم بين المزود كمُقدم لخدمات التصديق الإلكتروني(شخص طبيعي أو شخص معنوي عام أو خاص)، مع الأشخاص الراغبة في التعويل على شهادات التصديق الإلكتروني الموصوفة كمُستخدمين للخدمة، ضمن عقود الإيجار(Contrats de Louage) التي بمُقتضاها يقوم المؤجر(م.خ.ت.إ) بتمكين المستأجر(مُستخدم الخدمة) من الانتفاع بمعدات وأنظمة أمن تكنولوجيا المعلومات الممنوحة له لمدة محددة مُقابل بدل الإيجار، كما يمكن تصنيفها كذلك ضمن عقود بيع خدمات التصديق الإلكتروني الموثوق بها، بحيث يلتزم بموجبه(م.خ.ت.إ) المرخص أو المعتمد به بنقل ملكية خدمة التصديق الإلكتروني للمشتري بمقابل ثمن نقدي متفق عليه مُسبقا، ففي إطار عقد الاشتراك يتعين على(م.خ.ت.إ) إتاحة المشتركين لمعدات وأنظمة أمن تكنولوجيا معلومات، التي يضعها تحت سيطرتهم لغرض إحداث توقيعات إلكترونية موصوفة، والخدمات الآخرى المتصلة بها[1].

---

[1] – **Art. 1708** (Code Civil Français) : « Il y a deux sortes de contrats de louage : Celui des choses, et celui d'ouvrage. »

- **Art.1709** : « Le louage des choses est un contrat par lequel l'une des parties s'oblige à faire jouir l'autre d'une chose pendant un certain temps, et moyennant un certain prix que celle-ci s'oblige de lui payer. » http://www.legifrance.gouve.fr

- **Art. 1710** : « Le louage d'ouvrage est un contrat par lequel l'une des parties s'engage à faire quelque chose pour l'autre, moyennant un prix convenu entre elles. »

فمهما كان تصنيف عقود تقديم خدمات التصديق الإلكتروني فهي تتميز بمجموعة من الخصوصيات القانونية والتقنية، المتعلقة بنمط ومستوى الخدمة المتاحة التي تُضفيها طابع الإذعان لأحد أطراف العقد، في حين تُصنف عقود تقديم خدمات التصديق الإلكتروني ضمن العقود النموذجية أو ما تُعرف بعقود الإذعان(Contrats d'adhésion)[1]، التي لا تُعطي لأحد طرفيها الضعيف حرية الاختيار والتفاوض لأنّ عقد الإذعان معناه عقد نموذجي لا يقبل المساومة ولا التفاوض حول بنود العقد، فليس للشخص الواثق في بيان ممارسة خدمات التصديق الإلكتروني سوى قبول التعاقد أو رفضه عند عدم الوثوق به، دون أيّة مُناقشة أو تفاوض حول شروطه، فما يقع على الطرف المذعن(المُحترف أو المستهلك) كمُستخدمين لخدمة التصديق الإلكتروني سوى الرضوخ والموافقة، على الشروط المحررة مُسبقا من طرف(م.خ.ت.إ) في العقد النموذجي المتعلق بتقديم خدمات التصديق الإلكتروني.

لتفادي وقوع الأطراف المعولة على خدمات التصديق الإلكتروني في الشروط التعسفية (Les Clauses abusives)[2] التي يتضمنها العقد النموذجي الخاص بالخدمة، ألزمت

---

– المادة 467 (أمر رقم 58/75 مؤرخ في 26 سبتمبر 1975 يتضمن القانون المدني، معدل ومتمم): "الإيجار عقد يمكن المؤجر بمقتضاه المستأجر من الانتفاع بشيء لمدة محددة مقابل بدل إيجار معلوم. يجوز أن يحدد بدل الإيجار نقدا أو بتقديم أيّ عمل آخر."

– المادة 351 (نفس الأمر): "البيع عقد يلتزم بمقتضاه البائع أن ينقل للمشتري ملكية شيء أو حقا ماليا آخر في مقابل ثمن نقدي."

[1] – **بركات كريمة**، "الحماية القانونية للمستهلك في عقود الإذعان"، المجلة النقدية للقانون والعلوم السياسية، عدد 2011/02، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، ص ص 278-282.

– المادة 70 (نفس الأمر): "يحصل القبول في عقد الإذعان بمجرد التسليم لشروط مقررة يضعها الموجب ولا يقبل المناقشة فيها."

[2] - Directive 93/13/CEE du Conseil, du 5 avril 1993, concernant les clauses abusives dans les contrats conclus avec les consommateurs, Journal officiel n° L 095 du 21/04/1993.

- **Art. 03** : « 1- Une clause d'un contrat n'ayant pas fait l'objet d'une négociation individuelle est considérée comme abusive lorsque, en dépit de l'exigence de bonne foi, elle crée au détriment du consommateur un déséquilibre significatif entre les droits et obligations des parties découlant du contrat…

مُختلف التشريعات والتنظيمات المنظمة للمعاملات الإلكترونية(م.خ.ت.إ) المُعتمد أو المرخص له، بضرورة التقيد بما وُرد في الترخيص أو الإعتماد الذي يُمارس في إطاره نشاطاته المتعلقة بتقديم خدمات التصديق الإلكتروني، وهذا ما نصت عليه المادة 13 من اللائحة التنفيذية لقانون التوقيع الإلكتروني وبإنشاء(هـ.ت.ص.ت.م)، التي فرضت على(م.خ.ت.إ) المُرخص لهم الإلتزام بعدم إبرام أيِّ عقد مع العملاء إلاّ بعد إعتماد نموذج هذا العقد من طرف هيئة تنمية صناعة تكنولوجيا المعلومات(ITIDA)، طبقا للقواعد والضوابط التي يضعها مجلس إدارتها في هذا الشأن لضمان حقوق المعنيين، كما ألزم مشرع الإمارات العربية المتحدة بموجب المادة 25 من قرار وزير الاقتصاد الإماراتي رقم 01-2008 بشأن إصدار لائحة مزود خدمات التصديق الإلكتروني[1]، أن يكون العقد المبرم بين(م.خ.ت.إ) والمُوقِّع كتابيًّا بطريقة نزيهة وواضحة وقابلة للإدراك، مع التقيد بالإرشادات المُصدرة من قِبل هيئة تنمية قطاع الإتصالات(TRA) التي تُنشر على موقعه الإلكتروني.

**ثانيّا- إستخدام مُعدات وأنظمة أمن تكنولوجيا معلومات موثوق بها:**

لضمان مستويات عالية من الثقة والأمان في خدمات التصديق الإلكتروني فرضت غالبية التشريعات الدولية والوطنية، على(م.خ.ت.إ) أثناء مباشرتهم لخدمات التصديق الإلكتروني، ضرورة إستعمال معدات وأنظمة أمن تكنولوجيا معلومات موثوق بها من طرف الجهات الرسمية وفقا للمعايير والمواصفات المعترف بها دوليًّا، بحيث إعتبرت هذا الإلتزام ضمن الشروط التي يتعين تواجدها في طلبات منح أو تجديد التراخيص في مجال خدمات

---

2- Une clause est toujours considérée comme n'ayant pas fait l'objet d'une négociation individuelle lorsqu'elle a été rédigée préalablement et que le consommateur n'a, de ce fait, pas pu avoir d'influence sur son contenu, notamment dans le cadre d'un **contrat d'adhésion**.
Le fait que certains éléments d'une clause ou qu'une clause isolée aient fait l'objet d'une négociation individuelle n'exclut pas l'application du présent article au reste d'un contrat si l'appréciation globale permet de conclure qu'il s'agit malgré tout d'un **contrat d'adhésion**.
Si le professionnel prétend qu'une clause standardisée a fait l'objet d'une négociation individuelle, la charge de la preuve lui incombe.
3- L'annexe contient une liste indicative et non exhaustive de clauses qui peuvent être déclarées abusives. »

[1] - قرار وزير الاقتصاد الإماراتي رقم 01-2008 بشأن إصدار لائحة مُزودي خدمات التصديق الإلكتروني. http://www.government.ae/

التصديق الإلكتروني، وبالتالي يجب على كلّ(م.خ.ت.إ) مرخص له أن يعتمد على آليات أمن إحداث توقيعات إلكترونية وفحصها موثوق بها تشتمل على مجموعة فريدة من عناصر التشفير، فآلية أمن إحداث التوقيعات الإلكترونية تحتوي لوحدها على مجموعة من عناصر التشفير الشخصية أو مُعِدَّاتٍ مهيأة خصيصا بإنشاء التوقيعات الإلكترونية الموثقة، وبالمقابل تحتوي آلية فحص التوقيع الإلكتروني على مجموعة من عناصر التشفير العمومية أو المعدات التي تُمكن من فحص التوقيع الإلكتروني الموصوف[1].

في كلّ الظروف يجب أن تُحدث أزواج المفاتيح بواسطة منظومات وإجراءات موثوق بها وفقا للمعايير الدولية المعمول بها، مع استجابتها(أزواج المفاتيح) لشروط خوارزميات الإحداث والفحص في التوقيع الإلكتروني وضمان أحادية كلّ زوج مفاتيح وفقا للوظيفة المُخصصة لها، وإنطلاقا من ذلك ألزمت(س.ض.ب.م) كسلطة إقتصادية للتصديق الإلكتروني في الجزائر، بموجب المادتين الأولى والثانية من القرار رقم 17/س خ/ر م/س.ض.ب.م المؤرخ في 11 جوان 2012 المتضمن إلزام حراسة(الإيداع القانوني) المفاتيح لأصحاب رخص إستغلال تجهيزات وبرمجيات التشفير،(م.خ.ت.إ) المرخص لهم بضرورة الإيداع القانوني لمفاتيح وبرمجيات التشفير لدى السلطة الإقتصادية قبل مباشرتهم لخدمات التصديق الإلكتروني[2].

---

1) - **HILLARIUS Kludze et W. Glenn Rowe**, « le rôle de la confiance dans le commerce électronique : une analyse stratégique », HEC Montréal / Gestion, 2002/5 vol, 27, pp. 83-85. Article disponible sur : http://www.cairn.info/revue-gestion-2002-5-page-80.htm

2) - Décision n° 17/ SP/PC/ARPT du 11/06/2012. http://www.arpt.dz

**Art.1** : « La présente décision a pour objet l'obligation pour le titulaire d'**autorisation d'exploitation des équipements et des logiciels d'encryptions** de déposer auprès de l'autorité de régulation de la poste et des télécommunications les clés et les procédés de chiffrement avant leur utilisation effective. »

**Art.2** : « L'autorité de régulation a la charge de conserver de manière sécurisée les clés secrètes mises en œuvre à des fins de confidentialité et ce, afin de les remettre aux propriétaires s'ils les demandent et aux autorités judiciaires ou de sécurité conformément aux dispositions législatives et règlementaires en vigueur. A cet effet, l'autorité de régulation veille à protéger la confidentialité des clés de chiffrement qu'elle gère, au recouvrement des clés qu'elle séquestre et à la vérification de la légitimité des demandes de recouvrement qu'elle traite. »

**ثالثا- الإلتزام بالتأمين:**

اشترطت التشريعات المنظمة لخدمات التصديق الإلكتروني على(م.خ.ت.إ) سواءا كان شخص طبيعي أو معنوي، بضرورة إبرام عقود تأمين من المخاطر التي من شأنها أن تُلحق أضرارًا بأصحاب التوقيعات الإلكترونية الموثقة أو بالأطراف المعولة على شهادات التصديق الإلكتروني الموصوفة، بغض النظر عن ما إذا كانت تربطهم علاقة عقدية أم لا تربطهم مع (م.خ.ت.إ)، ولمواجهة المخاطر المعلوماتية تقوم جهات التوثيق الإلكتروني بإبرام عقود تأمين معلوماتي مع شركات تأمين لتغطية الأضرار المُلحقة بالمعلومات، التي(الشركات) تأخذ بعين الإعتبار قبل إبرام عقد التأمين نوعية الأخطار المعلوماتية وتحليلها وفقا لمعايير غالبا ما تكون هيكلية[1].

فالتأمين عن الأضرار ينقسم إلى تأمين على الأشياء والتأمين من المسؤولية فبعدما أن كان الأول(التأمين على الأشياء)، ينصب على تعويض المؤمن له عن الأضرار التي تمس الأشياء المادية المحسوسة،(أجهزة الحاسوب، أعطال الماكينات، السرقة والحرائق الخ...) أصبح بتطور الفكر البشري وظهور تقنيات حديثة في تكنولوجيا المعلومات، يُغطي الأشياء الغير المادية ذات الطابع الغير المحسوس(البرامج المعلوماتية وأخطاء البرمجة، البيانات الإلكترونية والأرقام والمعلومات الخ..)، أمّا التأمين من المسؤولية يعني قيام(م.خ.ت.إ) الموثوق به، بتأمين مسؤوليته المدنية من أجل تغطية الأضرار التي يُمكن أن تُلحق بالطرف المعول على خدمات التصديق المتاحة له.

---

- **Art.3** : « La présente décision est applicable à compter de la date de sa publication sur le site web de l'ARPT. »

[1] – التأمين المعلوماتي ليس إلاّ تأمينا مثل غيره من أنواع التأمينات الأخرى، بحيث ينصب محل عقد التأمين على المخاطر المعلوماتية المُحتملة الحدوث في المستقبل. أنظر: **نبيلة إسماعيل رسلان**، التأمين في مجال المعلوماتية والشبكات، بحث مُقدم في مؤتمر القانون والكمبيوتر والإنترنيت، مرجع سابق، ص ص 847، 848، 854- 856.

- الفصل 02 من الأمر عدد1667-2001 المتعلق بالمصادقة على كراس الشروط الخاص بمُمارسة نشاط مُزودي خدمات المصادقة الإلكترونية. http://wwwlegislation.tn

إنطلاقا من ذلك ألزم المشرع السويسري بموجب المادة الثانية(02) من الأمر الفيدرالي المتعلق بخدمات التصديق في مجال التوقيع الإلكتروني، (م.خ.ت.إ) الراغب في الحصول على إعتراف به من طرف هيئة الإعتراف المعتمدة، بتأمين مسؤوليته المدنية بمبلغ تأمين على الأقل مليونين(02) فرنك سويسري عن كل حالة تأمين وثمانية(08) ملايين فرنك سويسري، لكل سنة تأمين وعند الإقتضاء يُمكن له أن يُوفر ضمان مُعادل للتأمين[1]، كما ألزم المشرع الإتحادي للإمارات العربية المتحدة(م.خ.ت.إ) بموجب المادة 1/08(د) من قرار وزير الإقتصاد الإماراتي رقم 01-2008 بشأن إصدار لائحة مُزودي خدمات التصديق الإلكتروني، بضرورة إبرام عقد تأمين خاص بتغطية أيّة خسائر مالية مُحتملة الوقوع، حسبما يراه المراقب(TRA) مُلائما لالتزاماته بموجب القانون وهذه اللائحة، زيادة إلى ذلك نص المشرع الجزائري بدوره في المادة 60 من القانون رقم 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، على إلتزام(م.خ.ت.إ) باكتتاب عقود تأمين المنصوص عليها في سياسة التصديق الإلكتروني للسلطة الإقتصادية(ARPT).

**رابعا- الإلتزام بالمحافظة على السرّ المهني:**

لضمان الثقة والأمان في المعاملات الإلكترونية التي تتم عبر شبكة الإنترنيت بوساطة (م.خ.ت.إ) موثوق به، يتعين على هذا الأخير وأعوانه الإلتزام بالمحافظة على سرية المعلومات التي عُهِدَتْ إليهم، من طرف صاحب طلب إصدار شهادة التصديق الإلكتروني أثناء مُباشرتهم لخدمات التصديق الإلكتروني، وذلك بإستثناء المعلومات التي رخص بها المعني بالأمر كتابيا أو إلكترونيا في نشرها أو إعلامها عمدا منه، فوفقا لأحكام المادة 21 من القانون المصري رقم 15-2004 المتعلق بالتوقيع الإلكتروني وبإنشاء(هـ.ت.ص.ت.م) فإنّ البيانات المتعلقة بالتوقيع الإلكتروني، والوسائط الإلكترونية والمعلومات التي يُقدمها ذوي

---

1) - Ordonnance sur les services de certification dans le domaine de la signature électronique (Ordonnance sur la signature électronique, OSCSE), du 3 décembre 2004.
- Art.02 : « 1- Le fournisseur de services de certification qui entend se faire reconnaître doit conclure une assurance responsabilité civile pour un montant d'au moins 2 millions de francs par cas d'assurance et 8 millions de francs par année d'assurance .
2- En lieu et place d'une assurance, il peut produire une garantie équivalente. »

الشأن لـ(م.خ.ت.إ) المُرخص بهم أو المعتمدين بإصدار شهادات التصديق الإلكتروني تبقى سرّية، ولا يجوز لمن قُدّمت إليه من أعوانه بحكم عملهم أن يقوموا بإفشائها للغير أو إستخدامها خارج الأغراض التي قُدمت من أجلها، وبالتالي يجب على(م.خ.ت.إ) أن يلتزم بمعايير توظيف الأشخاص المؤتمنين عن طريق حسن اختيارهم لأشخاص مؤهلة جديرة بالثقة للقيام بمسؤولياتهم وواجباتهم، وأن يكونوا على دِراية ومعرفة تامّة بأحكام القوانين والتنظيمات الخاصة بالمعاملات الإلكترونية وبسياسة التصديق الإلكتروني المتبعة.

**خامسا- الإلتزام بإيقاف العمل بالشهادة أو إلغاءها:**

يجب على كلّ (م.خ.ت.إ) أن يكون لديه سجل إلكتروني خاص بشهادات التصديق الإلكتروني مُتاح على موقعه الإلكتروني عبر شبكة الإنترنيت(LCR)، من أجل الإطلاع عليه من طرف العموم بصفة دورية ومُستمرة على المعلومات المُدوّنة فيه، بحيث يُبيّن فيه جميع شهادات التصديق الإلكتروني المنتهية صلاحيتها، أو التي تم إخضاعها لإجراءات الإيقاف أو الإلغاء، مع توضيح وقت وتاريخ تعليقها أو إلغاءها عند الإقتضاء[1]، لذا سنتطرق إلى إبراز أهم حالات إيقاف وإلغاء العمل بشهادات التصديق الإلكتروني التي حددتها معظم التشريعات الدولية والوطنية[2]:

**1- حالات وقف العمل بشهادة التصديق الإلكتروني:**

من بين حالات وقف العمل بشهادات التصديق الإلكتروني التي نصت عليها غالبية التشريعات الدولية والوطنية نجد:

---

[1] - الفصلين 19 و20 من القانون التونسي عدد 83-2000 المتعلق بالمبادلات والتجارة الإلكترونية، مرجع سابق. المادتين 36 و37 من قانون المعاملات الإلكترونية لسلطنة عمّان، مرجع سابق.

[2] - يعتبر المشرع التونسي الأكثر تنظيما وتفصيلا عند تطرقه لنظام العمل بشهادات التصديق الإلكتروني الذي ميّز بين نظامين، فالأول يتعلق بحالات تعليق العمل بشهادة التصديق الإلكتروني التي حددها في الفصل 19 من القانون عدد 83-2000 المتعلق بالمبادلات والتجارة الإلكترونية، أما النظام الثاني يتعلق بحالات إلغاء شهادة التصديق الإلكتروني المحددة في الفصل 20 من نفس القانون.

**أ)- وقف العمل بالشهادة بناءا على طلب صاحبها:** يُمكن أن يَطْلُبَ من سلطة التصديق الإلكتروني أو أحد وكلائها بإيقاف العمل بشهادة التصديق الإلكتروني، كلّ شخص طبيعي مُرخص له باستخدامها(الشهادة) سواءا كان ذلك بصفة أصلية أم باعتباره ممثلا شرعيا لأحد الأشخاص المعنوية، وذلك متى توفر ما يُبرر طلبه من سند واقعي مُقنِع لـ(م.خ.ت.إ) لغرض تعديل أو تغيير البيانات المتعلقة بالشهادة التي ترتبط بها حقوق الغير(Tiers).

**ب)- تغيير البيانات الواردة في الشهادة أو العبث فيها:** يتحقق ذلك في حالة تعرض البيانات الصحيحة التي تضمنتها شهادة التصديق الإلكتروني، إلى تغيير أو تزوير أو حذف سواءا من طرف صاحب الشهادة(المُوقع) أو من الغير(Tiers) دون علمٍ لجهة التصديق الإلكتروني، وذلك بهدف الإيقاع بالطرف الثاني المُستقبل للرسالة الإلكترونية في التدليس أو الغلط أو الإكراه، كأن تُستعمل الشهادة من طرف المرسل بغرض إقناع أيّ شخص راغب في التعاقد بملاءته المالية التي تدفعه للتعاقد معه بالرغم من عدم صحة وضعيته المالية.

**ج)- سرقة البطاقة الذكية لصاحبها أو فقدان المُوَقِّعْ لمفتاحه الخاص:** ألزمت غالبية التشريعات المنظمة للمعاملات الإلكترونية(م.خ.ت.إ)، بإيقاف العمل بشهادة التصديق الإلكتروني متى ثَبُتَ فقدان مفتاح التشفير الخاص بالمُوَقِّعِ، أو سرقة البطاقة الذكية لصاحبها التي تحتوي على عناصر وبيانات إنشاء التوقيع الإلكتروني وشهادة التصديق الإلكتروني الموصوفة وحتى عند الشّك في حدوث ذلك.

**د)- عدم مراعاة صاحب الشهادة لبنود عقد تقديم خدمات التوقيع الإلكتروني:** إنّ صاحب شهادة التصديق الإلكتروني تربطه علاقة عقدية مع سلطة التصديق الإلكتروني حول إحداث التوقيع الإلكتروني الموصوف، لذا يمكن لمُقدم الخدمة إيقاف العمل بشهادة التصديق الإلكتروني في حالة إخلال صاحبها بالإلتزامات المفروضة عليه بموجب العقد.

**هـ)- تعليق الشهادة المُسلمة بناءا على معلومات خاطئة:** تتحقق هذه الحالة إذا قدّم صاحب طلب الحصول على شهادة التصديق لمُستندات تُثبت قُدرته على إبرام التصرفات القانونية، ويَتَبَيَّنْ فيما بعد لـ(م.خ.ت.إ) أنّ شهادة التصديق الإلكتروني تم إصدارها وفقا لمعلومات غير صحيحة الشيء الذي يدفعها إلى إيقاف العمل بها فورًا [1].

---

[1] - **إبراهيم خالد ممدوح**، مرجع سابق، ص 229.

**و)- إنتهاك منظومة أمن إحداث التوقيع الإلكتروني:** إنّ التلاعب بمنظومة إنشاء التوقيع الإلكتروني الموصوف يدفع بـ(م.خ.ت.إ) إلى تعليق العمل بشهادة التصديق فورا، لذا يجب على المُوقِّع عند استخدامه لأداة إحداث توقيع إلكتروني مأذون بها من طرف(م.خ.ت.إ) موثوق به، أن يُمارس العناية اللازمة لتفادي إستخدامها خارج النطاق المرخص به وأن يُخطر(م.خ.ت.إ) أو الطرف المعول على الشهادة عند تعرض بيانات إنشاء التوقيع الإلكتروني لما يثير الشبهة فيها أو عند الشك في حدوث ذلك[1].

## 2- حالات إلغاء شهادة التصديق الإلكتروني:

بالإضافة إلى حالات وقف شهادة التصديق الإلكتروني توجد حالات آخرى تسمح لمقدم خدمة التصديق الإلكتروني، بإلغاء شهادة التصديق الإلكتروني حالا بمجرد معاينة أحد الحالات التالية:

**أ)- بناءا على طلب صاحب شهادة التصديق:** تُلغى شهادة التصديق الإلكتروني متى طلب صاحبها لذلك، غير أنّه لا يحق لغيره طلب إلغاء الشهادة حتى وإن كان طرفا مُعول على شهادة التصديق في إبرام صفقة تجارية، وبالتالي يجب على صاحب طلب إلغاء الشهادة أن يُخبر سلطة التصديق عن مبرر الإلغاء، التي تتمتع بالسلطة التقديرية في إلغاء الشهادة أو من عدمه[2].

**ب)- وفاة الشخص الطبيعي أو إنقضاء الشخص المعنوي:** تقوم سلطة التصديق الإلكتروني بإلغاء شهادة التصديق الإلكتروني في حالة وفاة الشخص الطبيعي، أو في حالة

---

[1] - **عبد الفتاح بيومي حجازي**، مرجع سابق، ص 177.

- أنظر الفصل 06 من قانون عدد 83- 2004 المتعلق بالمبادلات والتجارة الإلكترونية(تونس)، والمادة 45 من القانون رقم 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين (الجزائر).

[2] - **Art. 10 du (LFSCSE/2003)** : « **1**- Les fournisseurs reconnus annulent immédiatement les certificats qualifiés :- si le titulaire ou son représentant le demande ; ou s'il s'avère qu'ils ont été obtenus de manière frauduleuse ; ou s'ils ne permettent plus de garantir le lien entre une clé de vérification de signature et une personne.

**2**- En cas d'annulation sur demande selon l'al. 1, let. a, les fournisseurs s'assurent que le requérant a qualité pour demander l'annulation.

**3**- Les fournisseurs informent immédiatement les titulaires de certificats qualifiés de l'annulation de ces derniers. »

حلّ الشخص المعنوي أو انقضائه كحلّ الشركة أو تصفيتها أو إفلاسها، كما تُلغِي شهادة التصديق الإلكتروني المُصدرة باسم الممثل القانوني للشركة[1].

**ج)- نهاية مدة صلاحية الشهادة:** تعتبر من بين البيانات الإلزامية التي فرضتها المعايير أو المواصفات الدولية المتعلقة بشهادات التصديق الإلكتروني، والتي يجب على (م.خ.ت.إ) ذكرها والتأكد منها عند مباشرته لإجراءات إصدار الشهادات، فمن الطبيعي أن تُصدر جهة التوثيق الإلكتروني لقرار إلغاء العمل بالشهادة الإلكترونية عند انتهاء مُدة صلاحيتها.

**د)- إلغاء الشهادة التي سبق تعليقها بصفة مؤقتة:** يُمكن لجهة التوثيق الإلكتروني أن تُلغيَ شهادة التصديق التي تم إيقاف العمل بها بناءا على أحد الأسباب المبررة لذلك، فإذا تبين لها إثر التحريات التي تقوم بها من صحة تلك الأسباب كأن تُثبت أنّ المعلومات الواردة في الشهادة مُزيفة أو في حالة استعمالها لغرض التدليس، فإنّها تقوم بالإلغاء النهائي لشهادة التصديق الإلكتروني[2].

**هـ)- توقف مُقدم خدمات التصديق عن تقديم الخدمات المُرخص بها:** إذا توقف (م.خ.ت.إ) المُرخص له من طرف الهيئة المُكلفة بمنح التراخيص عن تقديمه لخدمات التصديق بمحض إرادته، فإنّه يلتزم بعد مُوافقة الهيئة بإلغاء جميع شهادات التصديق الإلكتروني المُصدرة منه للمتعاملين معه، إبتداءا من تاريخ التوقف عن الخدمة[3] مع إخطاره مُسبقا للأطراف المعولة على شهادات التصديق عن طريق رسالة إلكترونية قبل إجراءهم لأيّة معاملة إلكترونية تعتمد على التوقيع الإلكتروني إبتداءا من هذا التاريخ، وتُلغى بنفس الطريقة

---

[1] – راجع الفصل 20 من القانون التونسي عدد 83-2004 المتعلق بالمبادلات والتجارة الإلكترونية.
http://www.legislation.tn

[2] – عبد الفتاح بيومي حجازي، مرجع سابق، ص 185.

[3] – **Art.12§2 /3-4** (Loi Belge du 9 Juillet 2001 …) :
«Le prestataire de service de certification révoque également un certificat lorsque:
**3-** le prestataire de service de certification arrête ses activités sans qu'il n'y ait reprise de celles-ci par un autre prestataire de service de certification garantissant un niveau de qualité et de sécurité équivalent;
**4-** le prestataire de service de certification est informé du décès de la personne physique ou de la dissolution de la personne morale qui en est le titulaire. Le prestataire de service de certification informe le titulaire de certificat, sauf en cas de décès, de la révocation et motive sa décision. Un mois avant l'expiration d'un certificat, le prestataire de service de certification informe son titulaire de celle-ci. »

الشهادات في حالة سحب الترخيص من طرف الهيئة المُكلفة بمنح وسحب التراخيص لمُزاولة النشاطات المتعلقة بإصدار شهادات التصديق الإلكتروني، ففي كلّ الأحوال يلتزم صاحب الشهادة التي تم توقيفها أو إلغاءها بعدم إستعمال عناصر التشفير الشخصية للمصادقة عليها من جديد لدى(م.خ.ت.إ) آخر.

**سادسا- إبلاغ السلطة المكلفة بمنح وسحب التراخيص في حالة إيقاف النشاط:**

وفقا للفصل 24 من القانون التونسي رقم 83-2000 المتعلق بالمبادلات والتجارة الإلكترونية، يلتزم(م.خ.ت.إ) الراغب في إيقاف نشاطه المتعلق بخدمات التصديق الإلكتروني بإعلام (و.و.م.إ) قبل تاريخ الإيقاف بثلاثة(03) أشهر على الأقل، كما يجوز له تحويل جزء أو كلّ نشاطه لمزود آخر بشرط إعلام أصحاب الشهادات الجاري العمل بها برغبته في تحويل نشاطاته، قبل شهر من التحويل المنتظر على الأقل مع تحديده (المزود الراغب في إيقاف نشاطه) لهويته، وهوية(م.خ.ت.إ) الجديد الذي ستُحول إليه الشهادات الإلكترونية مع إعلام أصحاب الشهادات بإمكانية رفض التحويل المُنتظر وكذلك بآجال وطرق الطعن، وفي حالة رفضهم كتابيا أو إلكترونيا في هذا الآجل للتحويل تُلغى هذه الشهادات، وفي كلّ حالات إيقاف خدمات التصديق الإلكتروني يجب أن تتم عملية إتلاف كلّ البيانات الإلكترونية المتعلقة بالمعطيات الشخصية، التي بقيت تحت تصرف المزود الذي تخلى عن نشاطه وذلك بحضور مُمثل عن(و.و.م.إ).

بالإضافة إلى ذلك نص المشرع الفيدرالي السويسري في المادة 3-2-1/13 من القانون الفيدرالي المتعلق بالتوقيع الإلكتروني لعام 2003، والمادة 1/10 من الأمر الفيدرالي المتعلق بخدمات التصديق في مجال التوقيع الإلكتروني، على وجوب قيام المزود المُعترف به الراغب في إيقاف نشاطات التصديق الإلكتروني بإعلام هيئة الإعتماد(SAS) مسبقا في حدود 30 يوم، من أجل السماح لها بتكليف(م.خ.ت.إ) آخر معترف به يشرف على جميع القوائم التي تحتوي على شهادات التصديق الموصوفة السارية المفعول، أو التي تم إيقافها أو إلغاءها وأن يحتفظ بخدمات المزود المُوقِف لنشاطاته مع جميع وثائق الإثبات، وفي حالة ما إذا لم يتواجد(م.خ.ت.إ) مُعترف به للإشراف على هذه النشاطات، يتولى الديوان الفيدرالي

للإتصالات(Office) بمهمة الإشراف عليها(الخدمات) وفقا للفقرتين الثانية والثالثة من المادة 10 من الأمر الفيدرالي[1].

كما ألزم المشرع الجزائري بموجب المادتين 58 و59 من القانون رقم 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، (م.خ.ت.إ) بضرورة إعلام السلطة الإقتصادية للتصديق الإلكتروني(ARPT) وفقا للآجال المحددة في سياستها المتعلقة بالتصديق، برغبته في وقف نشاطاته أو بأيّ فعلٍ قد يؤدي إلى ذلك، مع الإلتزام بأحكام سياسة التصديق المتعلقة باستمرارية الخدمة، مع اتخاذ التدابير اللازمة بحفظ المعلومات المرتبطة بشهادات التصديق الإلكتروني الموصوفة الممنوحة له.

**سابعا- الإلتزام بإصدار شهادات تصديق إلكتروني موصوفة:**

لشهادة التصديق الإلكتروني الموصوفة أهميّة بالغة بالنسبة للأطراف المعولة عليها لتأكيد المسائل المتعلقة بصحة التوقيع الإلكتروني ونسبته لصاحب الشهادة، وضمان الإرتباط الوثيق للمحرر الإلكتروني بالتوقيع الإلكتروني المُثبَّت فيه، لذا فرضت التشريعات المنظمة للمعاملات الإلكترونية على(م.خ.ت.إ) المعتمدين أو المرخص لهم، واجب إصدار

---

1) - **Art.13 (LFSCSE 2003)** : **« 1-** Les fournisseurs reconnus annoncent en temps utile à l'organisme d'accréditation la cessation de leur activité. Ils lui annoncent immédiatement toute commination de faillite qui leur a été notifiée.
**2-** L'organisme d'accréditation charge un autre fournisseur reconnu de tenir la liste des certificats qualifiés valables, échus ou annulés et de conserver le journal de ses activités ainsi que les pièces justificatives correspondantes. Le Conseil fédéral désigne l'organisme compétent pour reprendre ces tâches lorsqu'il n'y a pas de fournisseur reconnu. Le fournisseur reconnu qui cesse son activité supporte les frais qui en résultent.
**3-** L'al. 2 est également applicable en cas de **faillite** d'un fournisseur **reconnu**. »
- **Art.10 (OSCSE 2004)** : « **1-** Les fournisseurs de services de certification reconnus annoncent immédiatement, mais au moins 30 jours à l'avance, au SAS et à l'organisme de reconnaissance qu'ils vont cesser leur activité.
**2-** Lorsqu'il n'existe aucun autre fournisseur de services de certification reconnu auquel le SAS pourrait transférer les tâches conformément à l'art. 13, al. 2, SCSE, l'office se charge des tâches suivantes: **a)** il continue de traiter les demandes d'annulation des certificats qualifiés;
**b)** il garantit aux tiers l'accès en ligne aux informations relatives à l'annulation des certificats qualifiés jusqu'à l'échéance de ces derniers;
**c)** il tient à jour et conserve le journal des activités et les pièces justificatives correspondantes.
**3-** Il peut annuler de lui-même les certificats encore valables. »

شهادات التصديق الإلكتروني وفقا لإجراءات توثيق مُعتمدة في حالة طلبها من طرف العموم حسب الغرض الذي تُستعمل من أجله الشهادة، وأن يُولِي قَدْرًا معقولا من العناية اللازمة لضمان دقة واكتمال كلّ ما يُقدمه من تأكيدات جوهرية ذات صلة بالشهادات طيلة مدة صلاحيتها[1]، مع توفيره للأطراف المعولة عليها(الشهادات) الوسائل الضرورية التي تُمَكِّنُهُمْ من التأكد من هوية(م.خ.ت.إ) المُصدر لها، وأنّ المُوقِّع المعينة هويته في الشهادة كان يتحكم في بيانات إحداث توقيعه الإلكتروني، مع ضمان صحتها في وقت أو قبل إصدار الشهادة من كلّ ما يُثير الشبهة فيها، كما يجب توضيح الطريقة المُستعملة في تعيين هويته(المُوقِع) والقيود المفروضة على الغرض، أو القيمة أو نطاق المسؤولية التي يجوز أن تُستخدم من أجلها شهادة التصديق الإلكتروني.

إنطلاقا من ذلك ألزم المشرع الجزائري بموجب المادة 44 من القانون رقم 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، (م.خ.ت.إ) بعدم منح شهادة التصديق للشخص الطبيعي إلاّ بعد التحقق من هويته ومن صفاته الخاصة، وإذا كان الشخص معنوي يتم التحقق في هوية وَصِفَة ممثله القانوني المُستعمِل للتوقيع المتعلق بالشهادة الإلكترونية الموصوفة، فعادة ما تُستعمل الشهادات لأداء العمليات المتعلقة بالتجارة الإلكترونية والخدمات المصرفية والتعريف بهوية صاحبها، أو الإستعانة بها قصد الإشهاد أو الإثبات بحصول مبادلة تجارية مع تحديد تاريخ وتوقيت حصولها[2].

---

[1]- نصت المادة 1/09 (أ)-(ب) من قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية لعام 2001 على:" حيثما يُوَفِّرُ مقدم خدمات التصديق خدمات لتأييد توقيع إلكتروني يجوز استخدامه لإعطاء مفعول قانوني بصفته توقيعا، يتعين على مقدم خدمات التصديق الإلكتروني المشار إليه :

(أ)- أن يتصرف وفقا للتأكيدات التي يقدمها بخصوص سياساته وممارساته.

(ب)- أن يولي قدرا معقولا من العناية لضمان دقة واكتمال كل ما يقدمه من تأكيدات جوهرية ذات صلة بالشهادة طيلة دورة سريانها، أو مُدرجة في الشهادة."

[2] - الفصل 04 من قرار وزير تكنولوجيا الاتصالات التونسي المؤرخ في 19 جويلية2001، يتعلق بضبط المعطيات التقنية المتعلقة بشهادات المصادقة الإلكترونية والوثوق بها.

لذا يجب على المزود الموثوق به في إطار مرفق المفاتيح العمومية مراعاة المعايير والمواصفات الدولية المعترف بها عند مباشرة عمليات التصديق الإلكتروني المتعلقة بإصدار الشهادات، فعادة ما يتم إعتماد المواصفة الدولية(X509) الصادرة عن الإتحاد الدولي للإتصالات(ITU) التي تُعتبر الركيزة الأساسية لأنظمة التعريف بالهوية عن طريق الشهادات، كما يجب على المزود التقيّد ببيان الممارسات المتبعة في شهادات التصديق الإلكتروني(DPC) المصادق عليه من طرف سلطة التصديق الرئيسية، بحيث يُوضح فيه جميع الممارسات المتبعة في إصدار أو إيقاف أو إلغاء شهادات التصديق الإلكتروني[1].

بالإضافة إلى ما سبق يجب على(م.خ.ت.إ) الإلتزام بتحديث الشهادة لأصحابها بصفة دورية ومُستمرة كلما طلبوا ذلك، وفقا لأسس تقنية وقانونية تمكنه من تحديد هوية المتعاملين في مجال التوقيع الإلكتروني، من خلال المتابعة المُستمرة لهم والتحديث المُستمر لكافة التعاملات(Transactions) ومفاتيح التشفير المتعلقة ببيانات ومعلومات المحرر الإلكتروني وضمان سلامة مُحتواه من الإتلاف، والسهر على تعقب جميع محاولات الغش والتلاعب في المعاملات الإلكترونية مع ضمان فعالية منظومة أمن إنشاء بيانات التوقيع الإلكتروني من عدم قابليتها للإستنتاج، والتأكد من الطابع الأحادي لزوج مفاتيح التشفير الشخصية أو العمومية وعدم إمكانية إستخدامها إلاّ من طرف حاسب واحد لكلّ مفتاح سرّي[2].

**ثامنا- الإلتزام بحفظ شهادات التصديق الإلكتروني:**

اشترطت التشريعات المنظمة للمعاملات الإلكترونية عند قيام(م.خ.ت.إ) بإصدار شهادات تصديق إلكتروني موثوق بها، أن يلتزم بحفظها في شكلها الأصلي الذي أنشئت أو أرسلت أو أُستلمت فيه على حوامل إلكترونية مؤمنة لمدة معينة تُيسّر الإطلاع على معلوماتها على نحو يُتيح الرجوع إليها لاحقا، لذا نص المشرع التونسي في الفصلين 15 و16 من الأمر عدد 1667-2001 المتعلق بالمصادقة على كراس الشروط الخاص

---

1) - **A. Arsenault** et **S. Turner**, X.509 Internet Public Key Infrastructure PKIX Feuille de route, article disponible sur : http://www.ietf.org/internet-drafts/draft-ietf-pkix-roadmap-04.txt

2) – **أسامة بن غانم العبيدي**، مرجع سابق، ص ص 195، 196.

بممارسة نشاط مزود خدمات المصادقة الإلكترونية، على إلتزام(م.خ.ت.إ) بحفظ السجلات المتعلقة بإصدار وتجديد وتعليق وسحب وإلغاء شهادات التصديق لمدة لا تقل عن 20 سنة على حامل إلكتروني مؤمن، كما أوجب حفظ الحوامل الإلكترونية في حاويات خزن إلكترونية مُؤمنة ضد الحرارة والرطوبة والتأثيرات المغناطيسية وكلّ شكل من أشكال التشويش.

لضمان خدمة حفظ مؤمنة لشهادات التصديق الإلكتروني يجب على(م.خ.ت.إ) أن يلتزم بحفظ مفاتيح التشفير الجذرية، المستعملة في التوقيع على شهادات التصديق الإلكتروني التي أصدرتها(المفاتيح) لهم سلطة التصديق الرئيسية على مستوى مرفق المفاتيح العمومية، قصد منع الغير من استعمالها في تزوير الشهادات عن طريق إحداث أنواع مشابهة للشهادات الأصلية، أو العمل على تغيير البيانات التي تحتويها الشهادات الأصلية لغرض استعمالها في أغراض غير مشروعة، ومن بين الوسائل المُستخدمة في حفظ واسترجاع المحررات الإلكترونية نجد، الشريط المغناطيسي الذي يحتوي على بلاستيك مطلي بمادة معدنية، قابلة للمغنطة وقد يكون ملفوفا على بكرة كالتي تُستخدم في أجهزة التسجيل الصوتي والمرئي، تحتوي على رأس للقراءة والكتابة يُسجل على شكل نقطة مغناطيسية بشفرة خاصة تدل على البيانات المتوافرة في الحاسب، كما أنّ الرأس ذات حساسية عالية تُمكنه من التحسس بوجود معلومات وقراءتها ليتم إرسال النبضات الكهربائية المقابلة لشفرة البيانات المخزنة بالحاسب وتحويلها إلى نص مقروء، كما يحتوي الشريط على أكثر من مسار أو قناة تُمكن من الكتابة عليها مع تخزين كمية هائلة من البيانات واسترجاعها عند الحاجة.

كما نجد الأقراص المرنة التي تكون في شكل دائرة تُصنع من مادة رقيقة من البلاستيك مَطْلِيَّة بمادة حسَّاسَة ومُمَغْنَطَة من أُكْسِيدْ الحديد، فمنها ما يقبل التسجيل على وجه واحد للسطح ومنها ما يكون مُزدوج السطح للتسجيل، ومنها ما يحتوي على مصغر للقرص الصلب يتم توصيله بجهاز الحاسوب ويكون ذات سعة عالية بالنسبة لمثيلاته من وسائل الحفظ، لذا يُعول على وحدة الأقراص من خلال مُلامسة الرأس لسطح القرص المغناطيسي التي ينتج عنها عملية الكتابة أو القراءة سواءا من حيث الإسترجاع أم الإدخال، أمّا أقراص (CD-DVD) الدائرية تحتوي هي الآخرى في داخلها على شريط مغناطيسي يتم تسجيل البيانات واسترجاعها عليه، وفي حالة تمرير القرص على العدسة يتم قراءة ما يحتويه القرص

من معلومات وتحويلها إلى الشكل الذي يظهر على شاشة الحاسب، وما يميز هذه الأقراص هو تمتعها بسعة عالية تفوق القرص العادي كما لا يُمكن الكتابة عليها بل للقراءة فقط.

ظهرت في الآونة الآخيرة وسائل جديدة في حفظ المعلومات واسترجاعها مثل (Flash Disk) الذي يحتوي على سعات عالية من التخزين، إذ يكفي توصيله بجهاز حاسوب من خلال وصل خاص به مُتوافر على الجهاز أو منفصل عنه(USB)[1] ليتم قراءة البيانات المدونة عليه، بنفس طريقة عمل القرص الصلب (Hard Disk) الذي يتواجد كذلك في جهاز الحاسوب في شكل قرص معدني رقيق، مطلي بمادة مغناطيسية يتم صنعه في الغالب من سبائك الألمنيوم، ومن مميزات القرص الصلب قدرته العالية في التخزين التي تفوق كثيرا الأنواع الآخرى، والسرعة العالية في تسجيل واسترجاع البيانات[2] لكونه من بين الأجهزة المادية المكونة للحاسوب مما يجعله أسرع من الأقراص المرنة، وتجدر الإشارة أن التكنولوجيات الحديثة سمحت بخلق أقراص صلبة محمولة تحتوي على سعات عالية من التخزين، قابلة للتشغيل على الحاسوب عن طريق الوصل الخاص(USB) بالقرص الصلب.

**تاسعا- الإلتزام بفسخ عقد تقديم خدمة التصديق الإلكتروني:**

إذا كانت حرية التعاقد ومبدأ سلطان الإرادة يظهران بشكل كبير في الصورة العادية للتعاقد اللذان يوفران قدرا كبيرا من الحرية لأيّ متعاقد في التفاوض بشأن العقد المزمع إبرامه، فإنّ هذه الحريّة تنقص بشكل كبير ويضيق مبدأ سلطان الإرادة بصورة واضحة في

---

[1] – كلمة مُختصرة لـ: Universial Serail Bus

[2] – إنّ تقنية التشفير لا تقتصر فقط على البيانات الإلكترونية المتداولة عبر شبكة الإنترنيت بل وصل الحدّ إلى إمكانية تشفير القرص الصلب المُتواجد في داخل الحاسب الآلي، عن طريق إحداث قُرص افتراضي مُنفصل عن القرص الرئيسي (مثلا يسمى C) الذي عادة ما يُثَبَّتْ فيه برنامج تشغيل الحاسوب، لذا يقوم المستخدم بتحديد مُسبقا مساحة القرص الافتراضي مع تسميته بأحد الحروف الهجائية مثلا(: F) وذلك حسب احتياجات الشخص، وبعدها يقوم بتشفير القرص الافتراضي بمفتاح خاص به واستعماله (القرص) في عملية تحميل البيانات أو البرامج أو نقل الملفات ومُعالجتها أو في حفظ واسترجاع البيانات والمعطيات المتصلة بالمحررات أو الوثائق الإلكترونية الخ... http://www.scramdisk.clara.net

حالات خاصة بعقود الإذعان التي يتم إعداد أحكامها مسبقا في نماذج خاصة بها، ولتفادي عدم التوازن في العلاقة العقدية التي تجمع بين(م.خ.ت.إ) كطرف قوي ومستخدم خدمة التصديق الإلكتروني كطرف ضعيف، حدّدت التشريعات والتنظيمات المنظمة لمجال الاستهلاك في أحكامها، البنود التعسفية التي يحظر على المحترف إدراجها في العقود المبرمة مع المستهلك، كالاحتفاظ بصفة منفردة بحق تعديل العقد أو فسخه من دون تعويض الطرف المذعن، أو عدم السماح لهذا الأخير بفسخ العقد وفقا للظروف التي تستدعي إلى ذلك مع إجباره بالتعويض الخ[1]...

لذا يحق لـ(م.خ.ت.إ) القيام بإلغاء الخدمات محلّ التعاقد عند قيام مستخدم الخدمة بالإخلال بأيّ من الشروط الواجبة التي تَضَمَّنَهَا العقد، وبالخصوص في الحالات التي تتعلق عادة بقيام مستخدم الخدمة بتجاوز حدود استخدام الخدمات مَحَلّْ التعاقد، أو انتهاك عناصر الأمان من قبل مستخدم الخدمة بسبب الإهمال أو التعمد، وتراكم المطالبات المالية على مستخدم الخدمة مقابل الخدمات محل التعاقد، أو سوء استخدام الخدمات مَحَلّْ التعاقد على نحو يخالف القانون والنظام والآداب العامة أو دواعي الأمن القومي، كما يحق للطرف المذعن(مستخدم خدمة التصديق) أن يقوم وفقا لقواعد حماية المستهلك بفسخ العقد، في حالة ما إذا لم يحترم(م.خ.ت.إ) الالتزامات المفروضة عليه بموجب العقد أو في حالة تواجد شروط تعسفية بعد إبرام العقد.

---

[1] – Directive 93/13/CEE du Conseil, du 5 avril 1993, concernant les clauses abusives dans les contrats conclus avec les consommateurs. J.O.C.E, n° L 095 du 21/04/1993.

- **Art.03** : « 1- Une clause d'un contrat n'ayant pas fait l'objet d'une négociation individuelle est considérée comme **abusive** lorsque, en dépit de l'exigence de bonne foi, elle crée au détriment du consommateur un déséquilibre significatif entre les droits et obligations des parties découlant du contrat. »

-Voir aussi l'ANNEX (clauses visées à l'article 3/1).

– راجع كذلك المادة 05 من المرسوم تنفيذي رقم 06–306 مؤرخ في 10 سبتمبر 2006، يحدد العناصر الأساسية للعقود المبرمة بين الأعوان الاقتصاديين والمستهلكين والبنود التي تعتبر تعسفية، ج ر عدد 56 الصادر في 2006/09/11، معدل ومتمم بموجب مرسوم تنفيذي رقم 08–44 مؤرخ في 2008/02/03، ج ر عدد 07 الصادر في 2008/02/10.

## المطلب الثاني

## إلتزامات الطرف المُعَوِّلْ على خدمات التصديق الإلكتروني

من بين الخدمات الجوهرية التي تُتيحها جهات التوثيق الإلكتروني لأطراف عقود التجارة الإلكترونية، نجد خدمة التوقيع الإلكتروني الموصوف وتلك المتعلقة بإصدار أو إيقاف أو إلغاء شهادات التصديق الإلكتروني، التي على إثرها يتحمل الأطراف المعولة على التوقيعات الإلكترونية أو على شهادات التصديق الإلكتروني، مجموعة من الإلتزامات المفروضة عليهم بموجب الأحكام التشريعية والتنظيمية المتعلقة بالتصديق الإلكتروني.

إنطلاقا من ذلك يُقصد بالطرف المُعَوِّلْ حسب المادة الثانية فقرة(و) من قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية لعام 2001، أيّ شخص يُعَوِّلُ على توقيع إلكتروني أو على شهادة تصديق إلكتروني له علاقة تعاقدية بالمُوَّقِعِ، أو بمقدم خدمات التصديق الإلكتروني المعتمد أو المرخص له، أو ليست له(الشخص المعول) علاقة تعاقدية بهما، وبالتالي يمكن التصور أن يصبح(م.خ.ت.إ) أو المُوقِّع نفسه طرفًا معولاً وحتى الغير(Tiers) كطرف ثالث، إذْ يُمكن لهذا الأخير الذي لا تربطه علاقة تعاقدية لا بالمُوقِّع أو بمقدم خدمة التصديق، بالتعويل على شهادات التصديق الإلكتروني لغرض إبرام مختلف صفقات التجارة الإلكترونية عبر شبكة الإنترنيت[1].

لتوضيح هذه الإلتزامات التي ما هي في الحقيقة إلاّ حقوق منحتها القوانين والتنظيمات المتعلقة بالمعاملات الإلكترونية للأطراف المعنية، إرتأينا التطرق إلى إلتزامات المُوَقِّع باعتباره كمُستخدم لخدمة التوقيع الإلكتروني(الفرع الأول)، ولالتزاماته كصاحب شهادة التصديق الإلكتروني الموصوفة(الفرع الثاني)، ولالتزامات الغَيْرْ كطرف ثالث مُعوّل على شهادة التصديق الإلكتروني(الفرع الثالث).

---

[1] – لمزيد من التفاصيل راجع دليل التشريع الخاص بقانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية لعام 2001، مرجع سابق، ص ص 81-83.

## الفرع الأول

## إلتزامات مُستخدم خدمة التوقيع الإلكتروني

فرضت التشريعات الدولية والوطنية مجموعة من الإلتزامات التي يجب احترامها من الطرف الراغب في إحداث توقيع إلكتروني موصوف بوساطة(م.خ.ت.إ) معتمد أو مرخص له، الذي(الطرف) ينبغي عليه أن يُحيط نفسه عِلْمًا قبل إبرام عقد تقديم خدمة التوقيع الإلكتروني مع مقدم الخدمة، ببيان الممارسة العامة لخدمات التصديق الإلكتروني وبالخصوص خدمات تصديق التوقيعات الإلكترونية الموصوفة والممارسات المتبعة في إصدار وإيقاف وإلغاء شهادات التصديق الإلكتروني[1]، فبمجرد إبرام العقد مع(م.خ.ت.إ) تترتب عنه على عاتق مُستخدم الخدمة(المُوقِّع) مجموعة من الإلتزامات والمتمثلة:

**أولا- إستخدام أدوات إحداث توقيعات إلكترونية مُرخص بها:**

يجب على الشخص الراغب في إحداث توقيع إلكتروني مصدق التقيد بمنظومة أمن إنشاء التوقيعات الإلكترونية المأذون بها من طرف جهة التصديق الإلكتروني أثناء جميع مراحل إحداث توقيعه الإلكتروني، كما ينبغي عليه (مُستخدم الخدمة) أن يحرص على عدم خروج أداة إنشاء التوقيع الإلكتروني من سيطرته الكاملة عليها عن طريق اتخاذ الإحتياطات اللازمة والمناسبة لمنع فقدانها أو العبث فيها، وأن يمارس العناية الكافية من عدم إستخدام

---

[1] – بإطلاعنا على مختلف نماذج عقود تقديم خدمات التصديق أو التوثيق الإلكتروني لمعظم جهات التوثيق الإلكتروني المعتمدة أو المرخص بها من طرف الجهات الرسمية المنشورة على مستوى مواقعها الإلكترونية عبر الإنترنيت، وجدنا أنّها تشترط من مستخدم خدمة التصديق الإلكتروني (الموقع) الإقرار بأنّه قد اطلع على بيان الممارسة CPS أو DPC واستخدام خدمات التوقيع الإلكتروني محل التعاقد، الذي ينظم علاقة تقديم تلك الخدمات من طرف مقدم خدمة التصديق الإلكتروني، كما تُلزم كذلك مستخدم الخدمة بالإقرار على أنّه قد اطلع إطلاعا تاما على أحكام عقد تقديم خدمة التصديق الإلكتروني مما يدل على قبوله للخدمة وعدم جهله للبنود المذكورة في العقد، وأنّه قد استوعب كافة التبعات القائمة عن عدم التزامه ببنوده (العقد). لمزيد من المعلومات أنظر المواقع الإلكترونية التالية: http://www.universign.eu et http://acedicom.edicomgroup.com/

الأداة لأغراض غير مشروعة لا تتعلق بإحداث التوقيع الإلكتروني، كما لا يحق له التدخل في الأمور الفنيّة لتطبيقات خدمات التوقيع الإلكتروني بالتعديل أو الإضافة أو التغيير، إلاّ بعد الحصول على موافقة مكتوبة من طرف جهة التوثيق الإلكتروني المُعتمدة أو المرخص لها من طرف الجهات الرسمية.

لضمان الثقة والأمان في خدمة إحداث التوقيعات الإلكترونية الموصوفة يجب أن تكون بيانات إحداثها سريّة، لا يُمكن إنشاءها لأكثر من مرّة واحدة وغير قابلة للكشف عن طريق الإستنباط أو الإستنتاج، وأن تُتيح منظومة أمن إحداث التوقيع الإلكتروني الحماية اللازمة للتوقيع الإلكتروني من التزوير أو التقليد أو التحريف أو تُسهل من إحداثه بالوسائل المتاحة أو غير ذلك من صور التلاعب، وأن لا تُساهم في إحداث تغييرات في مُحتوى المحرر الإلكتروني الذي يجب توقيعه أو تمنع المُوَقِّعْ من معرفته الدقيقة لمضمون المحرّر قبل توقيعه، ولضمان الاستخدام الأمثل والفعال لأدوات إنشاء التوقيعات الإلكترونية الموصوفة تشترط بعض جهات التوثيق الإلكتروني المعتمدة، على الراغب في إحداث توقيع إلكتروني موصوف بضرورة حصوله على تدريب مناسب للتعامل مع خدمات مَحَلّْ التعاقد وذلك قبل البدء في الخدمة.

لتسهيل إمكانية كشف أيّ تعديل أو تبديل في بيانات المحرّر أو التوقيع الإلكتروني ألزمت مُختلف التشريعات، أن تستجيب منظومات أمن إحداث التوقيعات الإلكترونية للمواصفات التقنية المعترف بها على دوليا، وبالخصوص تقنيات التشفير اللاتماثلي المُرتكز على المفتاح الخاص والعام الذي تُصدرهما جهات التصديق الإلكتروني[1]، بحيث يُستخدم المفتاح الخاص لغرض إحداث التوقيع الإلكتروني والمفتاح العام يُستعمل لغرض فحص بيانات إحداث التوقيع الإلكتروني المرتبطة بالمحرر الإلكتروني، إذ تربط فيما بين زوج المفاتيح(الخاص والعام) معادلة حسابية معقدة وفقا لتقنيات رياضية آمنة مُبرمجة ضمن نظم التشفير الغير المتناظرة، فبالرغم من إتاحة المفتاح العام للعموم(الجمهور) إلاّ أنّه يستحيل

[1] – **عمر خالد زريقات**، عقود التجارة الإلكترونية: عقد البيع عبر الإنترنيت (دراسة تحليلية)، الطبعة الأولى، دار الحامد للنشر والتوزيع، الأردن، 2007، ص ص 273–278.

عليهم كشف المفتاح الخاص بالمُوقِّع وإستخدامه لغرض تحريف أو تزوير أو تغيير بيانات المحرر الإلكتروني المرتبط بالتوقيع الإلكتروني الموصوف.

**ثانيّا- الإلتزام بإخطار جهة التوثيق الإلكتروني عن كل ما يثير الشبهة:**

لضمان السير الفعّال لمنظومة أمن إحداث التوقيعات الإلكترونية يقع على عاتق مُستخدمها، أن يُخطر في الوقت اللائق بدون تأخير جهة التوثيق الإلكتروني الموثوق بها عند تعرض أداة إحداث التوقيع الإلكتروني لما يُثير الشبهة، أو عندما تؤدي الظروف بالمُوقِّعِ إلى إعتقاده أو شكوكه من تعرض الأداة لما يُثير الشبهة في درجة أمانتها كتعرضها لاختراق في النظام الأمني[1]، من طرف أحد فيروسات عدوى النظام (System infector) أو فيروسات الماكرو(Macro viruses) أو أحد البرامج الخبيثة التي يعول عليها في قرصنة

---

[1] – من بين أخطر أشكال التهديد الحديثة في نظم المعلومات عبر شبكة الإنترنيت نجد:

– **التهديد بالتغيير:** يُعد من أخطر الأعمال الغير المشروعة ضد مُستخدمي شبكة الإنترنيت إذْ يُمكن للقائم بالعمل الغير المشروع (مهاجم النظام) من تعديل برنامج تصفح الانترنيت (Web Browser) أو أيّ برنامج آخر يتم تشغيله عن التحكم في أيّ حاسب آلي للغير، الشيء الذي يسمح للمجرم بقراءة وتعديل ومسح أيّ ملف أو سرقته عن طريق إرساله بالبريد الإلكتروني إلى المكان الذي يريده، كما يُمكن لمهاجم النظام باستخدام أو تغيير الخادم (Serveur) وتعديل الذاكرة وما بالك بالبيانات الإلكترونية.

– **التهديد بكشف سرية المعلومات:** يتمثل في إفشاء سرية المعلومات الخاصة بأجهزة الكمبيوتر الداخلة في تكوين نظام المعلومات، مثل البيانات التي تصف إمكانات ونوعية الكمبيوتر والأماكن التي يتصل به مع عناوينها.

– **استخدام العناوين بطرق غير شرعية:** يتم ذلك عن طريق قيام المجرم بإعداد عناوين مُماثلة لبروتوكولات الإنترنيت المملوكة لبعض جهات التوثيق الإلكتروني أو الأفراد، فعندما يريد شخص الاتصال بالجهة أو الفرد الأصلي مالك العنوان، فإنّه يتصل بجهة الفرد المجرم بدلا من الجهة الأصلية.

– **منع تقديم الخدمة أو إبطائها:** يُعد من بين أخطر الأفعال الغير المشروعة ضد نظم المعلومات الذي تُستخدم فيه أساليب عديدة لمنع تقديم الخدمة أو إبطائها، مثل الدخول على موقع أي جهة على الإنترنيت وطلب كم هائل من الخدمات في وقت واحد من خلال خادم خاص بها، مما يُؤدي به إلى عجزه عن توفير الخدمة أو إبطائها بما لا يُرضي المُشتركين في الخدمة عن مدى كفاءته بتقديم المعلومات لهم. لمزيد من التفاصيل أنظر: **طارق إبراهيم الدسوقي عطية**، مرجع سابق، ص ص 538-540.

المعلومات التي تظهر في هيئة برامج عادية تُوفر خدمات معينة لكن باطنها بُرْمِجَ لأداء أنشطة غير متوقعة ولا تُلفت إنتباه مُستخدمه، مثل سرقة كلمة العبور أو استنتاج أو استنباط تقنية إحداث التوقيعات الإلكترونية والملفات، أو إلغاءها من دون عِلْمِ المُوَقِّعْ، على النحو الذي لا يمكن كشف أو تحديد الخدمات الباطنية إلاّ عن طريق المصادفة من خلال ظهور عطب أو خلل معين في أداء النظام[1].

لذا يبقى برنامج(Sniffer) من بين أهم وسائل اختراق نظم أمن المعلوماتية الذي يرتكز على بروتوكولات تشغيل شبكة الإنترنيت السائدة في أجهزة الحاسوب مثل (TCP/IP, Ethernet, IPX, etc.) وبطاقة الشبكة(Carte réseau) المتواجدة في جهاز الحاسوب بوصفها أداة ربط الحاسوب بالشبكات، والتي تُعتبر(البطاقة) المفتاح الأساسي الذي يعتمد عليه البرنامج في أداء مهامه، إذْ يعمل البرنامج(Sniffer) على تَحَسُّسِ جميع أنواع المرور المعلوماتي على شبكة الإنترنيت قصد سرقة المعلومات السرية، التي تسمح له باقتناص كلمات العبور بجميع أشكالها أو أنماطها، والحصول على المعلومات الخاصة التي تمتاز بدرجة عالية من السريّة، مع إمكانية إستخدامها في خرق النظم الأمنية للشبكات الحاسوبية بشتى مُستوياتها[2]، ومن هنا تكمن الأهمية البالغة لشهادة التصديق الإلكتروني وبالخصوص شهادة الشبكات الإفتراضية(Certificats VPN) في تحديد هوية الشبكات الخاصة الإفتراضية، عن طريق ربط جميع المعلومات المتعلقة ببعض المواقع على الشبكة، (محولات Routeurs، جدران نارية Firewalls، مركزات Concentrateurs الخ...) بالمفتاح العمومي

---

[1]- Les attaques par **chevaux de Troie** sont parfois dévastatrices dans le domaine du commerce électronique : - Il espionne les entrées clavier pour capturer le **passphrase** qui autorise l'usage et le déchiffrement de clef privée, alors le **cheval de Troie** peut faire signer le message que son propriétaire n'a jamais écrit ;
- Lorsque l'opérateur qui remplit un formulaire HTLM demande à sa machine la signature, le cheval de Troie l'intercepte et change des valeurs à l'insu de l'opérateur, le document est signé et envoyé par un POST HTTP sans aucune nouvelle vérification de l'opérateur, par exemple le cheval de Troie a modifié le numéro du compte bancaire cible d'un virement signé sans que l'auteur ne s'en aperçoive. **Arnaud-F. FAUSSE**, op.cit., p. 196.

[2] – لمزيد من المعلومات حول برنامج **Sniffer** يمكن الإطلاع على الموقع الإلكتروني التالي :
http://www.hacked-inhabitants.com/warez/sunsniff.c.

لسلطة التصديق الإلكتروني من أجل ضمان سلامة المبادلات في مسارات أو مسالك مؤمنة عبر شبكة الإتصالات الإفتراضية.

إنطلاقا من ذلك اشترطت المادة 08 من قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية لعام 2001، على الطرف الراغب في إحداث توقيع إلكتروني موصوف أن يستخدم أدوات مؤمنة في إحداث التوقيع الإلكتروني المتاحة له من طرف(م.خ.ت.إ) المعتمد أو المرخص له، وأن يولي العناية اللازمة لضمان التأكيدات المقدمة في شهادة التصديق الإلكتروني، مع إخطار مُقدم الخدمة أو أي شخص يتوقع منه أن يعول على الشهادة من تعرض بيانات إحداث توقيعه الإلكتروني لما يثير الشبهة فيها.

**ثالثا- الإلتزام بحفظ المفتاح الخاص بالتوقيع الإلكتروني:**

ألزمت القوانين المنظمة للمعاملات الإلكترونية المُوقِّع بضرورة توفير شروط السلامة والحماية للمفتاح الخاص بتوقيعه الإلكتروني الموصوف من أجل تجنب مخاطر استعماله من طرف الغير، وذلك بالعمل على تشفيره(المفتاح الخاص) بكلمة سريّة ووضعها في حاوية إلكترونية مؤمنة من الحرارة والرطوبة والتأثيرات المغناطيسية، وكلّ أشكال التشويش أو الإختراقات التي من شأنها أن تؤدي إلى كشف أو تحديد المفتاح الخاص، وبالتالي يتعين على صاحب المفتاح الخاص أن يتأكد من عدم تواجد معلومات(فيروسات) في الحاوية الإلكترونية، والعمل على إتلافها إن تواجدت في داخلها[1]، وأن يحرص على حمايتها (الحاوية) بأنظمة حماية المعلومات وبالخصوص البرامج المُضادة لمُختلف الفيروسات والبرامج الخبيثة(Anti-malware)، ولضمان سرية بيانات إحداث التوقيع الإلكتروني المتصلة بالمحرر الإلكتروني يجب أن تكون أزواج مفاتيح التشفير(العام والخاص) وحيدة وشخصية على النحو الذي لا يُمكن من تفويتها أو إحالتها للغير، كما اشترطت القوانين في منظومة أمن إحداث التوقيعات الإلكترونية أن تؤمن عملية إنشاء مفاتيح التشفير العام والخاص

[1] – الفصل 18 من الأمر التونسي عدد 1667-2001 المتعلق بكراس الشروط الخاص بممارسة نشاط مزود خدمات المصادقة الإلكترونية. http://wwwlegislation.tn

الأحادية الاتجاه وفقا للمعايير والمواصفات الدولية المُعترف بها، وأن تستجيب لشروط خوارزميات الإحداث والفحص المعمول بها مع الحفاظ عليها، لذا يتعين على صاحب المفتاح الخاص والمزود أن يستعملا منظومة إحداث توقيع إلكتروني مؤمنة تُمكن من حفظ واستعمال المفتاح الخاص بواسطة كلمة سرّ، مع إخفاءه بعد كلّ إستعمال[1].

**رابعا- تعزيز التوقيع الإلكتروني المؤمن بشهادة تصديق إلكتروني موصوفة:**

تُعتبر شهادة التصديق الإلكتروني الموصوفة من بين الوسائل التقنية الحديثة التي يُعول عليها المُوقِّع في مجال حماية المعلومات وفي إثبات تصرفاته الإلكترونية، وبالتالي ألزمت التشريعات الدولية والوطنية المُوَقّع بضرورة تعزيز توقيعه الإلكتروني بشهادة تصديق إلكتروني موصوفة، وأن يمارس العناية المعقولة لضمان دقة واكتمال كلّ التأكيدات الجوهرية التي يُقدمها في نموذج طلب خدمة التوقيع الإلكتروني المُتاح من طرف(م.خ.ت.إ)، لذا نصت الفقرة(ج) من المادة الثامنة(08/ج) من قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية لعام 2001، على ضرورة أن يولي المُوقِّع في حالة استخدامه لشهادة تصديق إلكتروني لغرض تعزيز توقيعه الإلكتروني، قدرا معقولا من العناية الكافية في تأكيد دقة واكتمال المعلومات التي قَدَّمَهَا لجهة التوثيق الإلكتروني المعتمدة أو المرخص بها طيلة مدة صلاحية الشهادة[2].

**خامسا- الإلتزام بإحترام حقوق الملكية الفكرية:**

يجب على مُستخدم خدمة التوقيع الإلكتروني مراعاة جميع حقوق الملكية الفكرية المرتبطة بالبرامج أو الأفكار أو المفاهيم والأساليب أو الاختراعات أو العمليات المنهجية أو المؤلفات المحتواة، أو التي يتم ممارستها فيما يتصل بالمعدات أو الخدمات التي يتيحها مقدم

---

[1] – أنظر الفصول 03-04-05-06-10 من قرار وزير تكنولوجيا الإتصال التونسي المؤرخ في 19 جويلية 2001، الخاص بضبط المواصفات التقنية لمنظومة إحداث الإمضاء الإلكتروني.

[2] – قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية مع دليله التشريعي 2001. http://www.uncitral.org

خدمات التصديق الإلكتروني بموجب عقد تقديم خدمات التصديق الإلكتروني، والمملوكة لسلطة التصديق الرئيسية على مستوى هرم مرفق المفاتيح العمومية و(م.خ.ت.إ) المرخص له وذلك وفقا لأحكام قوانين حماية حقوق الملكية الفكرية، ويشمل ذلك على سبيل المثال لا الحصر أدوات إحداث التوقيعات الالكترونية الموصوفة، المتاحة من طرف مقدم الخدمة والمَوْقِعْ الإلكتروني المرخص له على شبكة الإنترنت والمخصص لمستخدم الخدمة.

لذا لا يحق لمستخدم خدمة التصديق الإلكتروني أن يقوم بإزالة أو طمس أو تقليد أيّة علامة تجارية، أو إشعارات حقوق النشر الموجودة علي أيّ من مواد أو مستندات مقدم الخدمة، كما لا يحق لأي طرف من الطرفين اكتساب أيّة حقوق من أي نوع تجاه العلامات التجارية أو علامات الخدمة أو الأسماء التجارية أو أسماء المنتجات الخاصة بالطرف الآخر، ولضمان حماية حقوق الملكية الفكرية في مجال التصديق الإلكتروني تقوم جهات التوثيق الإلكتروني بإصدار شهادة إمضاء الرمز (Certificat de signature de code)، التي تسمح بالإمضاء على أي برنامج أو نص أو برمجية لضمان تعريفه بتوقيع صاحبه، وحمايته ضد مخاطر القرصنة.

## الفرع الثاني

## إلتزامات صاحب شهادة التصديق الإلكتروني الموصوفة

فرضت القوانين الدولية والوطنية المنظمة للمعاملات الإلكترونية على صاحب شهادة التصديق الإلكتروني، مجموعة من الإلتزامات التي يجب احترامها في إطار عقد تقديم خدمة التصديق الإلكتروني والمتمثلة في:

### أولا- الإلتزام بتقديم جميع المعلومات الصحيحة المتعلقة بالشهادة:

يجب على صاحب طلب إصدار شهادة التصديق الإلكتروني أن يتقيد بنموذج بطاقة الإرشادات الفردية الموضوعة تحت تصرفه من طرف(م.خ.ت.إ) على مستوى موقعه الإلكتروني، وأن(صاحب الطلب) يمارس العناية اللازمة لضمان دقة واكتمال كلّ ما يقدمه من المعلومات الضرورية المتعلقة بمعطياته الشخصية، وبالخصوص تحديد هويته من اسم

ولقب وعنوانه الشخصي، أو المقر الاجتماعي في حالة الشخص المعنوي أو عنوان البريد الإلكتروني، ورقم السجل التجاري والتعريف الجبائي وكلّ ما يتعلق بإثبات صفته وأهليته في القيام بالتصرف القانوني الخ...، كما يجب على صاحب الطلب تقديم كلّ المعلومات المتصلة بالغرض والمجال الذي تُسْتَخدم من أجله الشهادة مع القيود الواردة على نطاق إستخدامها أو على قيمة الصفقة التي ستستعمل من أجلها الشهادة عند الإقتضاء، بالإضافة إلى اسم المجال وهوية المتصرف بالنسبة لموزعات الويب واسم المجال مع هوية المتصرف بالنسبة للشبكات، كما يجب على صاحب الطلب الإقرار بشهادة صحة كلّ المعلومات التي حددها في النموذج وأنّه مُحاط عِلمًا بجميع الإلتزامات المترتبة بموجب الشهادة.

لذا يجب على صاحب طلب إصدار الشهادة أن يقوم بإرفاق المعلومات التي قدمها في النموذج بجميع الوثائق المثبتة لها، كالنُسَخْ من بطاقة التعريف الوطنية أو جواز السفر بالنسبة للأجانب الغير المقيمين أو بطاقة الإقامة للمقيمين، السجل التجاري وبطاقة التعريف الجبائية الخ...، من أجل السماح لسلطة التسجيل(AE) بالتحقق من مدى مطابقتها للوثائق الأصلية عند إيداع الطلب.

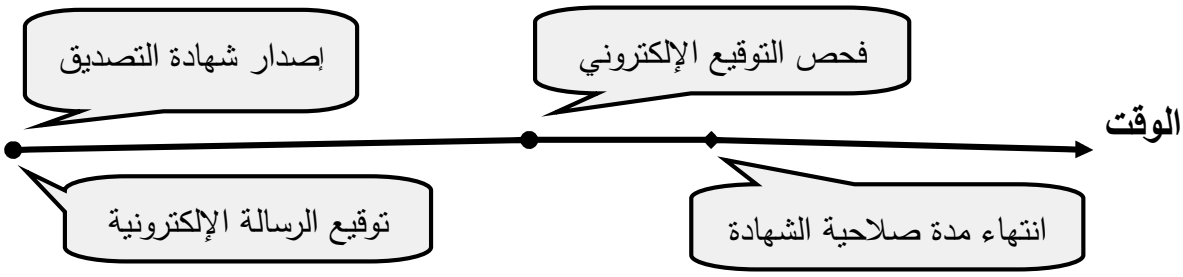
**ثانيّا– الإلتزام بمدّة صلاحية شهادة التصديق الإلكتروني:**

يجب على صاحب شهادة التصديق الإلكتروني الأخذ بعين الإعتبار سريان مدة صلاحية الشهادة المُقيَّدة بمدة صلاحية زوج مفاتيح التشفير(العام والخاص) مع التأكد من عدم خضوعها للإيقاف أو الإلغاء، والعمل عند الإقتضاء على طلب تحديثها من جهة التصديق الإلكتروني كلما قَرُبَتْ مُدَّة انتهاء سريانها، قصد الحفاظ على المفعول القانوني للتوقيع الإلكتروني، ومن هنا تبرز أهمية مدة صلاحية شهادة التصديق في تقرير مصير التصرف الإلكتروني المتصل بالتوقيع وذلك على حالتين[1]:

فالحالة الأولى تتمحور حول ما إذا قام مُستقبل الرسالة الإلكترونية بفحص التوقيع الإلكتروني خلال مدة صلاحية الشهادة، فإنّ صحة التوقيع الإلكتروني مُقترن بالضرورة بمدة

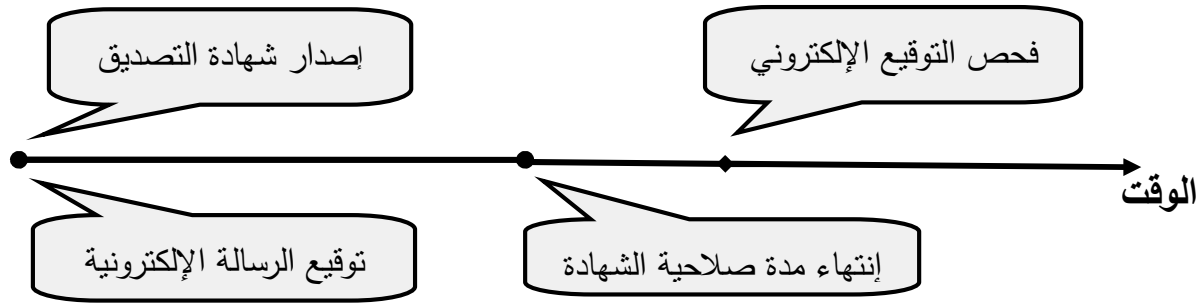
1) – **Arnaud-F. FAUSSE**, op.cit., pp. 106-108.

صلاحيتها، وبالتالي تُثار الشبهة من صحة كلّ توقيع إلكتروني تم استقباله بعد مدة انتهاء صلاحية الشهادة.




**الشكل رقم (11) المصدر**: من إعداد الطالب اعتمادا على: **Arnaud-F.FAUSSE**, op.cit., p. 108.

أمّا الحالة الثانية تتعلق حول ما إذا قام مستقبل الرسالة الإلكترونية بفحص التوقيع الإلكتروني بعد انتهاء مدة صلاحية شهادة التصديق الإلكتروني، ففي هذه الحالة يجب على المتلقي أن يتحقق عن طريق الوسائل التكنولوجية الحديثة المتاحة له، من أنّ المُوقِّع المُعَيَّنَة هويته في الشهادة كان يتحكم في بيانات إحداث توقيعه الإلكتروني في وقت أو قبل إصدار شهادة التصديق الإلكتروني، ومن عدم تعرضها لما يثير الشبهة فيها.




**الشكل رقم (12) المصدر**: من إعداد الطالب اعتمادا على المرجع ذاته.

**ثالثا- الإلتزام بمجالات إستعمال شهادة التصديق الإلكتروني:**

إنّ مجالات إستعمال الشهادات يمكن أن تتعلق بإثبات هوية صاحب التوقيع الإلكتروني أو للقيام بإحدى عمليات التجارة الإلكترونية أو للإشهاد بحصول مبادلة تجارية مع تحديد تاريخ وتوقيت حصولها، لذا يتعين لدى تقرير قابلية التعويل على الشهادة المعززة للتوقيع

الإلكتروني الموثق مراعاة الظروف التجارية الخاصة بأطراف التعامل الإلكتروني وبالخصوص طبيعة وحجم المعاملة التجارية التي تُستخدم فيها الشهادة، كأن تكون المعاملة ذات قيمة مالية كبيرة أو بضائع ذات خصوصية معينة ودرجة دراية كلّ طرف من أطرف التصرف الإلكتروني بالمعاملة التي يتم توثيقها، والخبرة الفنيّة التي يتمتع بها كلّ واحد منهم مع الأخذ بعين الإعتبار قيمة وأهمية المعاملة التجارية مع الإجراءات المُعتادة فيها.

**رابعا- الإلتزام بإبلاغ جهة التوثيق الإلكتروني بالمعلومات المُغَيّرَة:**

ألزمت مختلف التشريعات[1] صاحب شهادة التصديق الإلكتروني بصفته المسؤول الوحيد عن سرية وسلامة المعلومات الواردة فيها، بضرورة إعلام جهة التوثيق(المُصدِرة لها) بجميع التغييرات التي تمس بالمعلومات الواردة في الشهادة، سواءا كان التغيير من طرفه أو بسبب ظروف خارجة عن إرادته، حتى يتسنى للجهة المُصدرة للشهادة إتباع الإجراءات اللازمة في إخطار الأطراف الآخرى المعولة عليها، كما يجب على صاحب الشهادة أن يُخطر كذلك على وجه معقول كلّ شخص يتوقع منه أن يعول على شهادته.

**خامسا- الإلتزام بطلب إيقاف أو إلغاء العمل بالشهادة:**

منحت مختلف القوانين المنظمة للمعاملات الإلكترونية لصاحب شهادة التصديق الإلكتروني الحق في طلب إيقاف أو إلغاء شهادته، في حالة فقدانه لمفتاحه الخاص بالتوقيع الإلكتروني أو الشك في عدم مُطابقة المعلومات التي تحتويها الشهادة مع الواقع، لذا يتعين

---

[1] – المادة 1/08(ب) من قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية لعام 2001:" [...] يتعين على كل موقِّع:- أن يبادر دون تأخر لا مسوّغ له، إلى استخدام الوسائل التي يوفّرها (م.خ.ت.إ) بمقتضى المادة 09 من هذا القانون، أو خلافا لذلك، إلى بذل جهود معقولة لإشعار أي شخص يجوز للموقّع أن يتوقّع منه على وجه معقول أن يعوّل على التوقيع الالكتروني أو أن يقدّم خدمات تأييدا للتوقيع الالكتروني، وذلك في حالة: 1- معرفة الموقِّع بأن بيانات إنشاء التوقيع تعرّضت لما يثير الشبهة؛ 2- كون الظروف المعروفة لدى الموقِّع تؤدي إلى نشوء احتمال قوي بتعرض بيانات إنشاء التوقيع لما يثير الشبهة."

على صاحب الحق عندما يتعرض مفتاحه الخاص بتوقيعه الإلكتروني للسرقة أو الفقدان، أن يُبلغ فورًا الجهة المُصدِرة للشهادة قصد اتخاذ إجراءات الإيقاف أو الإلغاء اللازمة حسب ما يُبرره السند الواقعي المُقدَّم من طرف المعني بالأمر[1]، وبالخصوص عندما يتعلق الأمر بسرقة أو ضياعه للحامل الإلكتروني الذي تتواجد فيه الشهادة الإلكترونية، أو البطاقة الذكية التي يتواجد بداخلها البيانات الفريدة بإحداث التوقيع الإلكتروني الموصوف.

**سادسا– التقيد بشروط إستعمال الشهادة:**

لا يجوز لصاحب شهادة التصديق الإلكتروني التي ألغيت أو انتهت صلاحيتها أن يستعملها لتحقيق الأغراض التي أُصدِرت من أجلها، وبالتالي يتعين عليه التقيد بمدة سريان صلاحية الشهادة المبينة فيها والعمل على تحديثها كلما اقتضت الضرورة بذلك، مع التزامه بعدم إستعمال عناصر التشفير الشخصية له من جديد المبينة في شهادة التصديق الإلكتروني الموقفة أو الملغاة لدى(م.خ.ت.إ) آخر، ويظل صاحب الشهادة مسؤولا عن سلامة منظومة أمن إحداث توقيعه الإلكتروني طيلة مدة صلاحيتها، لذا ألزمت مختلف القوانين(م.خ.ت.إ) بضرورة توضيح السياسة المتبعة في إصدار وإيقاف وإلغاء شهادات التصديق الإلكتروني في بيان ممارسة خدمات التصديق الإلكتروني، حتى يتسنى للأطراف المعولة على الشهادات بمعرفتها والسماح لهم بإتخاذ جميع الإحتياطات اللاّزمة في تقدير قابلية التعويل عليها قبل اتخاذ أيّ قرار بشأن ذلك، مع ضمان خدمة الإدراج الفوري والإتاحة اللحظية لقوائم الشهادات الموقوفة أو الملغاة.

---

[1] – **Art 58** : (loi du Québec concernant le cadre juridique des technologies de l'information)
« Le titulaire qui a des motifs raisonnables de croire que le dispositif a été volé ou perdu ou que sa confidentialité est compromise doit aviser, dans les meilleurs délais : - la personne qu'il a autorisée à utiliser le dispositif ; ou - le tiers dont il peut raisonnablement croire qu'il agit en se fondant sur le fait que le dispositif a été utilisé par la personne qui en a le droit ; ou - le prestataire de services de certification pour que celui-ci puisse suspendre ou annuler le certificat lié au dispositif. Il en est de même pour la personne autorisée qui doit aviser le titulaire et les personnes visées aux paragraphes 2 et 3. Il est interdit d'utiliser un dispositif, tangible ou logique, pour signer un document sachant que le certificat auquel le dispositif est lié est suspendu ou annulé. »

**سابعا- الإلتزام بدفع مستحقات تقديم خدمة التصديق الإلكتروني:**

يلتزم صاحب شهادة التصديق الإلكتروني بدفع جميع التكاليف المالية المستحقة لمقدم خدمة التصديق الإلكتروني، المحددة بموجب عقد تقديم خدمة التصديق الإلكتروني التي تتوافق مع نوع وفئة الخدمة المطلوبة من طرف مستخدمها، لذا تسعى سلطات التصديق الإلكتروني بالتحديد المسبق لجميع المستحقات المالية، التي يجب تسديدها من طرف صاحب شهادة التصديق الإلكتروني بصفته كمستخدم للخدمة بما فيها الرسوم المتعلقة بحفظ بيانات إحداث التوقيع الإلكتروني، وبشهادات التصديق الإلكتروني حسب المُدَّة المقررة في ذلك، وفي جميع الأحوال يقع على عاتق أطراف عقد تقديم خدمة التصديق الإلكتروني الإلتزام بدفع جميع الرسوم والضرائب المستحقة بموجب القوانين المعمول بها.

## الفرع الثالث

## إلتزامات الغير(Tiers) كطرف مُعَوّل على شهادة التصديق الإلكتروني

أجازت المادة الثانية فقرة(و) من قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية لعام 2001 لأيّ شخص من الغَيْرِ(Tiers)، أن يتصرف استنادا إلى شهادة تصديق إلكتروني أو إلى توقيع إلكتروني للقيام بمعاملاته الإلكترونية، سواءا تربطه علاقة عقدية مع المُوقِّع أو بـ(م.خ.ت.إ) أو ليست له علاقة تعاقدية معهما، لذا فرضت المادة 11 من نفس القانون على الطرف المعول على التوقيع الإلكتروني أو شهادة التصديق الإلكتروني، أن يتبع الخطوات اللاّزمة لإقرار قابلية التعويل على التوقيع الإلكتروني، واتخاذ الخطوات المعقولة حول ما إذا كان(التوقيع) مؤيّدا بشهادة تصديق إلكتروني من أجل التحقق من صلاحيتها أو وقفها أو إلغاءها، مع مراعاة أيّة قيود بخصوص الشهادة[1].

إنطلاقا من ذلك ألزمت مختلف التشريعات الطرف المُعوّل(Tiers)على التوقيع الإلكتروني أن يولي الأهمية لطبيعة وحجم المعاملة التجارية المعنية، مع الأخذ بعين

---

[1] – قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية لعام 2001.http://www.uncitral.org

الإعتبار لقيمتها متى كان ذلك معروفا أو أي إتفاق مع المُوقِّع أو بين هذا الأخير و(م.خ.ت.إ) أو أي عامل أو عرف تجاري سائد ذات صلة بالمعاملة، كما يجب على الطرف المعول أن يتخذ الخطوات المناسبة للتحقق من أنّ التوقيع الإلكتروني معزز بشهادة تصديق إلكتروني أو كان من المُتوقَّع أن يكون ذلك، لذا ينبغي عليه التحقق من مدى تعزيز التوقيع الإلكتروني بشهادة تصديق إلكتروني موصوفة التي تسمح لبرنامج حاسوبه بمباشرة منظومة فحص التوقيع الإلكتروني، بعد التأكد من مصداقية البيانات الواردة فيها وعدم خُضوعها لإجراءات الإيقاف أو الإلغاء مع مراعاة القيود الواردة فيها بشأن قيمة الصفقة التجارية أو على مسؤولية جهة التوثيق الإلكتروني[1].

## الفرع الرابع

## القيمة القانونية لشهادة التصديق الإلكتروني في الإثبات

نالت التوقيعات الإلكترونية الموصوفة في شتى التشريعات حجية قانونية في الإثبات مماثلة لتلك المقررة للتوقيعات التقليدية في قوانين الإثبات، والتي سنتطرق إليها على النحو التالي:

### أولا- التشريعات الأجنبية.

### 1- التوجيه الأوروبي رقم 99-93 المتعلق بالتوقيعات الإلكترونية.

حثّ المشرع الفيدرالي للإتحاد الأوروبي بموجب المادة 1/05 من التوجيه الأوروبي رقم 93/99 المتعلق بالتوقيعات الإلكترونية الدول الأعضاء، على أن تضمن التوقيعات الإلكترونية الموصوفة التي تم إحداثها بموجب منظومة أمن إحداث التوقيعات الإلكترونية والمُعززة بشهادات تصديق إلكتروني موصوفة، المُتطلبات القانونية التي يُحققها التوقيع التقليدي (اليدوي) وأن تكون مقبولة كدليل في الإثبات أمام العدالة، مع الأخذ بعين الإعتبار عدم إنكار المفعول القانوني للتوقيعات الإلكترونية البسيطة(المادة 2/05) في حالة اعتمادها

---

1) – **Étienne WÉRY**, Facture, Monnaie et paiement électroniques, op.cit., pp. 53, 54.

كوسيلة للإثبات أمام العدالة، وذلك بغض النظر عن ما إذا كان التوقيع قد تم إحداثه في شكل إلكتروني أو لم يُعزز بشهادة تصديق إلكترونية موصوفة تم إصدارها من طرف (م.خ.ت.إ) مُعتمد، أو أنّ التوقيع الإلكتروني لم يتم إحداثه عن طريق منظومة أمن إنشاء التوقيعات الإلكترونية الموثوق بها من طرف الجهات الرسمية[1].

**2- القانون الفرنسي.**

بالرغم من إعتراف المشرع الفرنسي بالدليل الإلكتروني ومُساواته مع الدليل الكتابي من حيث القيمة القانونية في الإثبات بموجب المواد 1316، 1316-1، 1316-3، إلاّ أنّه ميّز فيما بين الأدلة الإلكترونية من حيث الإثبات أمام القضاء بحسب مُستويات الأمان والثقة المتطلبة في التوقيعات الإلكترونية، لذا نصت المادة 1316-4/2 من التقنين المدني الفرنسي على أنّه في حالة، إحداث توقيع إلكتروني يجب أن يضمن التعرف على هوية المُوقِّع ويؤكد سلامة المحرر الإلكتروني المرتبط به، وفقا للشروط التي يحددها مرسوم بمجلس الدولة الفرنسي، فوفقا لنص المادة 02 من المرسوم التطبيقي رقم 2001-272 المتعلق بالتوقيع الإلكتروني، فإنّ التوقيع الإلكتروني الموصوف الذي تم إحداثه بموجب منظومة أمن إحداث التوقيعات الإلكترونية، المعزز بشهادة تصديق إلكتروني موصوفة صادرة من طرف(م.خ.ت.إ) مُؤهل وفقا للمادة 12/01 من نفس المرسوم، يتمتع بالحجية القانونية في الإثبات إلى غاية إثبات عكس ذلك.

---

[1] – **Art. 05** : (Directive 1999/93 du 13 décembre 1999 sur les signatures électroniques)
« 1- Les États membres veillent à ce que les signatures électroniques avancées basées sur un certificat qualifié et créées par un dispositif sécurisé de création de signature:
a) répondent aux exigences légales d'une signature à l'égard de données électroniques de la même manière qu'une signature manuscrite répond à ces exigences à l'égard de données manuscrites ou imprimées sur papier et
b) soient recevables comme preuves en justice.
2- Les États membres veillent à ce que l'efficacité juridique et la recevabilité comme preuve en justice ne soient pas refusées à une signature électronique au seul motif que: - la signature se présente sous forme électronique ; ou - qu'elle ne repose pas sur un certificat qualifié ; ou
- qu'elle ne repose pas sur un certificat qualifié délivré par un prestataire accrédité de service de certification ; ou - qu'elle n'est pas créée par un dispositif sécurisé de création de signature. »

إنّ المشرع الفرنسي ميّز فيما بين التوقيع الإلكتروني المؤمن المعزز بشهادة التصديق الإلكتروني الموصوفة، والتوقيع الإلكتروني البسيط المُعزز بشهادة التصديق الإلكتروني البسيطة من حيث القيمة القانونية في الإثبات، ففي حالة التعويل على شهادة تصديق إلكتروني موصوفة صادرة من طرف(م.خ.ت.إ) مُعتمد، في إثبات صحة التوقيع الإلكتروني الموصوف الذي تم إحداثه بموجب منظومة أمن إحداث التوقيعات الإلكترونية بوساطة(م.خ.ت.إ) معتمد، فإنّ عبء الإثبات يقع على من أنكر وثاقة منظومة أمن إنشاء التوقيع الإلكتروني الموثق وعليه أن يُثبت عدم صحتها، وما يقع على القاضي سوى التحقق وفقا لأحكام المادتين 1324 و287 و288-1 من قانون الإجراءات المدنية الفرنسي، من إستيفاء التوقيع الإلكتروني الموصوف للشروط التي نصت عليها أحكام المادتين 1316-1 و1316-4 من القانون المدني الفرنسي، أمّا إذا تم التعويل على شهادة تصديق إلكتروني صادرة من طرف(م.خ.ت.إ) غير مُعتمد، فإنّ عبء الإثبات في هذه الحالة يتم وفقا لأحكام المادة 1315 من القانون المدني الفرنسي، التي تُلزم صاحب التوقيع الإلكتروني البسيط بإثبات وثاقة منظومة إحداث توقيعه الإلكتروني والظروف التي تم وفقها حفظ الشهادة الإلكترونية[1].

---

1) - **Maximilien AMEGEE**, La signature électronique fragilise-t-elle le contrat, pp. 09-11. http://www.lafrique.free.fra/

- **Art. 1315** (Code Civil Français) : « Celui qui réclame l'exécution d'une obligation doit la prouver. Réciproquement, celui qui se prétend libéré doit justifier le paiement ou le fait qui a produit l'extinction de son obligation. »

- **1316-1**(Code Civil Français) : « L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité. » http://www.legifrance.gouve.fr

- **Art. 1324** du Code de procédure civile français : « Dans le cas où la partie désavoue son écriture ou sa signature, et dans le cas où ses héritiers ou ayants cause déclarent ne les point connaître, la vérification en est ordonnée en justice. »

- **Art. 287** du Code de procédure civile français : « […] Si la dénégation ou le refus de reconnaissance porte sur un écrit ou une signature électroniques, le juge vérifie si les conditions, mises par les articles **1316-1 et 1316-4** du Code civil à la validité de l'écrit ou de la signature électroniques, sont satisfaites. »

- **Art. 288-1**(Code de procédure civile français) : « Lorsque la signature électronique bénéficie d'une présomption de fiabilité, il appartient au juge de dire si les éléments dont il dispose justifient le renversement de cette présomption. » http://www.legifrance.gouve.fr

ففي كلّ الظروف منح المشرع الفرنسي السلطة التقديرية لقاضي الموضوع للفصل في النزاع وفقا لأحكام المادتين 1324 و287 و288-1 من قانون الإجراءات المدنية الفرنسي مع الأخذ بعين الإعتبار الإتفاقات المبرمة بين الأطراف حول الإثبات، ما طالما أنّ المواد 1316-2 و1134 و1322 من القانون المدني الفرنسي تسمح لهم بذلك[1] والمعترف بها(الإتفاقات) فقهاً وقضاءاً، فعلى سبيل المثال ذلك الإتفاق المبرم بين البنك وزبونه حول عدم إنكار الطرفين لأيّة معاملة إلكترونية تتم بإستعمال الرقم السرّي من طرف صاحب بطاقة الإئتمان البنكية(الزبون)، أو يتفق أطراف العقد الإلكتروني على عدم إنكار البيانات الإلكترونية المتداولة بمجرد إثبات منظومة فحص التوقيع الإلكتروني لصحته، الخ...

إنّ المشرع الفرنسي لم يحسم إشكالية إستخدام المحررات الرسمية في التصرفات الإلكترونية(العقود)، التي تُعد الرسمية فيها رُكنا من أركان التصرف القانوني إلاّ بعد صدور القانون رقم 2004-575 المؤرخ في 21 جوان 2004، المُتعلق بالثقة في الإقتصاد الرقمي[2] الذي حَسَمَ المسألة بتعديل المادة 1108 من التقنين المدني الفرنسي التي استحدثها بموجب المادة 1108-1 التي تنص:" **عندما تُشترط الكتابة في صحة تصرف**

---

1) - **Yousef SHANDI**, la formation du contrat a distance par voie électronique, thèse de doctorat, mention Droit privé, université Robert SCHUMAN Strasbourg III, Faculté de droit, de sciences politiques et de gestion, 2005, pp. 299, 300, 319.
- **Art. 1316-2** du code civil Français stipule : « Lorsque la loi n'a pas fixé d'autres principes, et à défaut de convention valable entre les parties, le juge règle les conflits de preuve littérale en déterminant par tous moyens le titre le plus vraisemblable, quel qu'en soit le support. »
- **Art. 1322** : « L'acte sous seing privé, reconnu par celui auquel on l'oppose, ou légalement tenu pour reconnu, a, entre ceux qui l'ont souscrit et entre leurs héritiers et ayants cause, la même foi que l'acte authentique. » http://www.legifrance.gouve.fr
- **Art. 1134** : « Les conventions légalement formées tiennent lieu de loi à ceux qui les ont faites. Elles ne peuvent être révoquées que de leur consentement mutuel, ou pour les causes que la loi autorise. Elles doivent être exécutées de bonne foi. »

2) – Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, J.O.R.F, n° 143 du 22 juin 2004. http:// www.legifrance.gouve.org
**Art.1108-1** : « Lorsqu'un écrit est exigé pour la validité d'un acte juridique, il peut être établi et conservé sous forme électronique dans les conditions prévues aux articles 1316-1 et 1316-4 et, lorsqu'un acte authentique est requis, au second alinéa de l'article 1317. Lorsqu'est exigée une mention écrite de la main même de celui qui s'oblige, ce dernier peut l'apposer sous forme électronique si les conditions de cette apposition sont de nature à garantir qu'elle ne peut être effectuée que par lui-même. »

**قانوني، يُمكن تحريرها وحفظها في شكل إلكتروني وفقا للشروط المحددة في المواد 1316-1 و1316-4، وذلك عندما يتعلق الأمر بتحرير المحرر الرسمي وفقا للفقرة الثانية من المادة 1317. وعندما يُشترط بيان يدوي بالكتابة حتى من طرف المُلتزم، يُمكن لهذا الأخير وضع البيان في شكل إلكتروني إذا كانت الظروف لا تسمح بوضعه إلاّ من طرفه."**

إنطلاقا من ذلك قام الوزير الأول(Dominique DE VILLEPIN) بإصدار مرسوم رقم 2005-973 المؤرخ في 10 أوت 2005 المنظم لأعمال الموثقين، الذي سمح بموجب المادتين 16 و17 منه للموثق العادي بتحرير العقود الرسمية في شكل إلكتروني، وفقا لنظام معالجة وإرسال المعلومات مُوافق عليه من طرف المجلس الأعلى للموثقين، كما يجب على الموثق عند توقيعه على المحررات أن يستعين بمنظومة أمن إحداث التوقيعات الإلكترونية المحددة بموجب المرسوم رقم 2001-272 المتعلق بالتوقيع الإلكتروني[1]، وبالتالي فإنّ المشرع الفرنسي اشترط في نظام تداول الوثائق والعقود الإلكترونية، أن يضمن سلامة وسريّة مُحتويات العقود والمحرّرات الإلكترونية، بشكل مُتوافق ومُرتبط مع نُظُم نقل المعلومات

---

1) - Décret n° 2005-973 du 10 août 2005 modifiant le décret n° 71-941 du 26 novembre 1971 relatif aux actes établis par les notaires. J.O.R.F, n° 186 du 11 août 2005.

**Art. 16** : « Le notaire qui établit un acte sur support électronique utilise un système de traitement et de transmission de l'information agréé par le Conseil supérieur du notariat et garantissant l'intégrité et la confidentialité du contenu de l'acte.

Les systèmes de communication d'informations mis en œuvre par les notaires doivent être interopérables avec ceux des autres notaires et des organismes auxquels ils doivent transmettre des données. »

**Art. 17** : « L'acte doit être signé par le notaire au moyen d'un procédé de signature électronique sécurisée conforme aux exigences du **décret n° 2001-272 du 30 mars 2001** pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique.

- Cette signature est **apposée** par le notaire dès l'acte établi, si besoin après réunion des annexes à l'acte. - Pour leur signature, les parties et les témoins doivent utiliser un procédé permettant l'apposition sur l'acte notarié, visible à l'écran, de l'image de leur signature manuscrite. - Lorsque l'acte doit contenir une mention manuscrite émanant d'une personne qui y concourt, le notaire énonce que la mention a été apposée dans le respect des conditions prévues au second alinéa de l'article 1108-1 du code civil. » http:// www.legifrance.gouve.org

- **Samarcq (N)**, Les actes authentique électronique, une réalité au 1er février, article publié sur : http://www.droit-ntic.com

- **GRANIER Laurent**, op.cit., pp. 93-98.

الآخرى التي أنشئت من قِبَلْ موثقين آخرين، وأن يتم الإقرار والمُوافقة عليه(النظام) من طرف المجلس الأعلى للمُوثقين.

تجدر الإشارة أنّ المشرع الفرنسي قد أبقى على الشروط التقليدية المتعلقة بالمحررات الرسمية الكتابية، التي نص عليها بموجب المادة 1317 من القانون المدني الفرنسي والمتمثلة في أن يُصدر المحرر الإلكتروني بشهادة موظف عام أو شخص مكلف بخدمة عامة مُعين من طرف الدولة للقيام بعمل من أعمالها، كما يجب أن يُصدر المحرر الرسمي في حدود سلطة الضابط العمومي واختصاصه النوعي والمكاني، مع مراعاة الأشكال القانونية في إنشاء المحررات الإلكترونية، وهذا ما أدّى إلى استبعاد(م.خ.ت.إ) المعتمد من فئتهم كضابط عمومي، كما أنّه لا يوجد نص قانوني(سواءا في التشريعات العربية أم الأجنبية) يقرر صراحة شروط منح الرسمية للمحررات الإلكترونية التي تتم بشهادة الموثق الإلكتروني(م.خ.ت.إ) المعتمد من طرف الجهات الرسمية.

بالإضافة إلى ذلك نجد أنّ المحرر الإلكتروني الرسمي الذي تم بشهادة الضابط العمومي لا يمكن دحضه أو إنكاره إلاّ عن طريق دعوى التزوير أمام الجهة القضائية المختصة، أمّا المحررات الإلكترونية التي تم توقيعها عن طريق التوقيع الإلكتروني الموصوف بوساطة(م.خ.ت.إ) المعتمد، فلا يُشترط الطعن عليها بالتزوير من أجل إنكارها فيكفي اللجوء إلى القواعد العامة في الإثبات لدحضها، ما دامت موثوقية التوقيع الإلكتروني الموصوف مفترضة إلى غاية إثبات عكس ذلك بجميع طرق الإثبات[1].

---

[1] – هناك من يعتبر (م.خ.ت.إ) بمثابة كاتب عدل (ضابط عمومي) يُسند إليهم مُهمة توثيق المعلومات والاحتفاظ بأصولها مع تسليم الشهادات، وأمّا البعض الآخر يرى أنّه يوجد اختلاف بين (م.خ.ت.إ) وكاتب عدل، بحجة أنّه يتطلب تدخلهم كلما رغب المُشرع في حماية المتعاملين ومُراقبة أعمالهم، كما أنّ عمل كاتب عدل يتعدى مُجرد التعريف بالأشخاص ومراقبة هويتهم. لمزيد من التفاصيل أنظر: **طارق كميل**، حجية شهادات المصادقة الإلكترونية الأجنبية (دراسة مقارنة)، ما كُتِبَ على الهامش ص 577، بحث مقدم في مؤتمر المعاملات الإلكترونية(التجارة الإلكترونية–الحكومة الإلكترونية) الذي نظمه مركز الإمارات للدراسات والبحوث الإستراتيجية المنعقد في دبي من 19 إلى 20 ماي 2009، المجلد الثاني.

لكي تسمح الظروف بالتعويل على شهادة التصديق الإلكتروني الموصوفة في الإثبات أمام القضاء، يجب أن يتم حفظها في شكلها الإلكتروني الذي أنشئت أو أُرسلت أو تُسَلَّمَتْ به في الأصل، على أيّ نظام معلوماتي مؤمن أو حامل إلكتروني مؤمن على النحو الذي يسمح بإثبات ارتباطها الدقيق بالرسالة الإلكترونية في شكلها الإلكتروني، الذي أنشئت أو أرسلت أو أستلمت به في الأصل من أجل الرجوع إليها عند الحاجة، لذا نصت المادة 1316-1 من القانون المدني الفرنسي على أن تُقبل الكتابة بالشكل الإلكتروني في الإثبات شأنها شأن الكتابة على دعامة ورقية، بشرط أن يكون بالإمكان تحديد هوية الشخص الذي صدرت عنه وأن تُحَرَّرْ وتحفظ في ظروف من طبيعتها أن تضمن سلامتها، فعادة ما تقوم بمهمة حفظ وتخزين المستندات أو السجلات الإلكترونية سلطة أرشيف (Autorité d'archivage) مُستقلة، أو عن طريق المخزن الإلكتروني المؤمن لـ(م.خ.ت.إ)[1].

---

http://slconf.uaeu.ac.aeslconf17arabic_prev_conf2009.asp

- **Art 1317** du code Civile Français : «- L'acte authentique est celui qui a été reçu par officiers publics ayant le droit d'instrumenter dans le lieu où l'acte a été rédigé, et avec les solennités requises.

Il peut être dressé sur support électronique s'il est établi et conservé dans des conditions fixées par décret en conseil d'état. »

- **Laurent GRANIER**, L'authenticité notariale électronique, Mémoire du diplôme supérieure du notariat, Université de Montpelier 1, Faculté de Droit, 2003, PP. 88, 89.

http://www.droit-tic.com/

1) - **Thierry PIETTE-COUDOL**, « Conservation et archivage de l'écrit sous forme électronique », pp. 01,02. Article disponible sur : http://www.pin.association-aristote.frlibexefetch.phppublicdocuments20030115_resume_tpc.pdf

- نص المادة 1/10-2-3 من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية لعام 1996.

1- عندما يقتضي القانون بالاحتفاظ بمستندات أو سجلات أو معلومات بعينها، يتحقق الوفاء بهذا المقتضى إذا تم الاحتفاظ برسائل البيانات، شريطة مراعاة الشروط التالية: (أ) أن تُيسر الإطلاع على المعلومات الواردة فيها على نحو يتيح استخدامها في الرجوع إليها لاحق؛ (ب) الاحتفاظ برسالة البيانات بالشكل الذي أُنشئت أو أُرسلت أو أُستلمت به أو بشكل يمكن إثبات أنّه يمثل بدقة المعلومات التي أُنشئت أو أُرسلت أو أُستلمت به؛ (ج) الاحتفاظ بالمعلومات إن وُجدت التي تمكن من استبانة منشأ رسالة البيانات و جهة وصولها و تاريخ و وقت إرسالها و استلامها.

2- لا ينسحب الالتزام بالاحتفاظ بالمستندات أو السجلات أو المعلومات وفقا للفقرة (1) على أيّة معلومات يكون الغرض الوحيد منها هو التمكين من إرسال الرسالة أو استلامها.

**3- القانون البلجيكي.**

طبق المشرع البلجيكي نص المادة 1/05-2 من التوجيه الأوروبي رقم 99-93 المتعلق بالتوقيع الإلكتروني، في المادة 4/04 من القانون الملكي المتعلق بالإطار القانوني للتوقيعات الإلكترونية وبخدمات التصديق، من خلالها ساوى بين التوقيع الإلكتروني الموصوف الذي تم إنشاءه وفقا لمنظومة أمن إحداث التوقيعات الإلكترونية، مع التوقيع اليدوي من حيث القيمة القانونية في الإثبات، وذلك من دون إنكار المفعول القانوني للتوقيعات الإلكترونية البسيطة أمام العدالة[1].

**4- القانون السويسري:**

أقرّ المشرع الفيدرالي السويسري بموجب المادة 2/14 مكرر من قانون الإلتزامات (CO) المؤرخ في 30 مارس1911، المعدل والمتمم بموجب قانون التوقيع الإلكتروني لعام 2003(SCSE)[2] بمُساواة التوقيع الإلكتروني الموصوف الذي تم إحداثه بموجب منظومة أمن إنشاء التوقيعات الإلكترونية، بوساطة(م.خ.ت.إ) مُعترف به وفقا لأحكام القانون

---

3- يجوز للشخص أن يستوفي المقتضى المُشار إليه في الفقرة (1) بالاستعانة بخدمات أيّ شخص آخر شريطة مُراعاة الشروط المنصوص عليها في الفقرات الفرعية (أ) و (ب) و (ج) و الفقرة (1).

1) - **Art.4/4-5** (Loi Belge du 9 Juillet 2001…): « - Sans préjudice des articles 1323 et suivants du Code civil, une signature électronique avancée réalisée sur la base d'un certificat qualifié et conçue au moyen d'un dispositif sécurisé de création de signature électronique, est assimilée à une signature manuscrite, qu'elle soit réalisée par une personne physique ou morale.
- Une signature électronique ne peut être privée de son efficacité juridique et ne peut être refusée comme preuve en justice au seul motif: - que la signature se présente sous forme électronique, ou - qu'elle ne repose pas sur un certificat qualifié, ou- qu'elle ne repose pas sur un certificat qualifié délivré par un prestataire accrédité de service de certification, ou
- qu'elle n'est pas créée par un dispositif sécurisé de création de signature.»

2) - Loi fédérale complétant le Code civil suisse (Livre cinquième: Code des obligations) du 30 mars 1911 (état le 1er janvier 2014). http://www.admin.chopcfrclassified-compilation/
-**Art.14$^{2bis}$** : « La signature électronique qualifiée, basée sur un certificat qualifié émanant d'un fournisseur de services de certification reconnu au sens de la loi du 19 décembre 2003 sur la signature électronique est assimilée à la signature manuscrite. Les dispositions légales ou conventionnelles contraires sont réservées.»

الفيدرالي المتعلق بالتوقيع الإلكتروني لعام 2003(SCSE)، مع التوقيع اليدوي من حيث القيمة القانونية في الإثبات.

**ثالثا- التشريعات العربية.**

**1- القانون الأردني:**

إنّ المشرع الأردني اعترف بدوره بمساواة التوقيع الإلكتروني الموثق المعزز بشهادة تصديق إلكتروني موصوفة مع التوقيعات اليدوية من حيث القيمة القانونية في الإثبات، الذي أكدّ من خلال نص المادة 33 من القانون رقم 85-2001 المتعلق بالمعاملات الإلكترونية على أنّه في حالة ما إذا تضمن السجل الإلكتروني، أو أيّ جزء منه توقيعا إلكترونيا موثقا تم إحداثه خلال مُدّة سريان شهادة توثيق مُعتمدة ومُطابقته مع رمز التعريف المُبيّن فيها، يُعتبر ذلك السجل موثقا بكامله أو فيما يتعلق بذلك الجزء حسب واقع الحال، في حين اشترط المشرع الأردني بموجب المادة 34 من نفس القانون للاعتراف بحجية شهادة التصديق الإلكتروني في الإثبات أمام القضاء، أن تكون صادرة من جهة توثيق إلكتروني مرخصة أو مُعتمدة من سلطة مُختصة في إقليم الأردن أو في دولة آخرى مُعترف بها في الأردن وافق أطراف المعاملة الإلكترونية على اعتمادها.

**2- القانون المصري:**

اعترف المشرع المصري بموجب المادة 14 من القانون رقم 15-2004 المتعلق بالتوقيع الإلكتروني، بحجية التوقيعات الإلكترونية التي تم إحداثها وفقا للضوابط الفنية والتقنية المحددة في اللائحة التنفيذية لقانون التوقيع الإلكتروني، مع التوقيعات التقليدية التي نصت عليها أحكام قانون الإثبات في المواد المدنية والتجارية، كما ألزم المشرع بضرورة حفظ شهادة التصديق الإلكتروني الموصوفة في الشكل الذي تم إرسالها به من طرف المرسل أو الذي تم وفقه استلامها من طرف المستقبل في شكلها الأصلي، في نظام حفظ إلكتروني مؤمن مُستقل وغير تابع للموقع أو منشئ المحرر الإلكتروني أو أيّ شخص آخر له مصلحة

تتعلق بالوثيقة الإلكترونية[1]، مما يحقق ثقة وقناعة القاضي في الطريقة المستعملة في إنشاء وحفظ الدليل الإلكتروني على نحو يسمح بالرجوع إليها عند الحاجة.

لضمان المفعول القانوني لشهادات التصديق الإلكتروني المعتمدة في الإثبات، يجب أن تُحفظ بطريقة مؤمنة على أيّ حامل إلكتروني أو نظام معلوماتي من أجل السماح للأطراف المعنية بالرجوع إليها عند الحاجة، وإجراء مُضاهاة بين ما هو محفوظ أو مُخزن لدى جهة التوثيق الإلكتروني أو أية جهة حفظ آخرى موثوق بها وما هو مُتنازع فيه قصد كشف أيّ تعديل أو تبديل في البيانات الإلكترونية.

### 3- القانون الجزائري:

اعترف المشرع الجزائري بدوره في المادتين 323 مكرر و323 مكرر1 من القانون المدني بمساواة المحررات الكتابية مع المحررات الإلكترونية، من حيث القيمة القانونية في الإثبات بغض النظر عن الوسيلة التي تتضمنها وطرق إرسالها، بشرط أن تضمن إمكانية التأكد من هوية الشخص الذي أصدرها وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها[2]، وبالتالي فإنّ موقف المشرع من التوقيع الإلكتروني لم يتضح إلاّ بعد صدور القانون رقم 15-04 المؤرخ في 2015/02/01 المتضمن القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، الذي نص بموجب المادتين 08 و09 منه على اعتبار التوقيع الإلكتروني الموصوف مماثلا لوحده للتوقيع المكتوب سواء كان لشخص طبيعي أو معنوي مع عدم إنكار التوقيع الإلكتروني البسيط، من فعاليته القانونية أو رفضه كدليل أمام القضاء

---

[1] – محمد محمد سادات، مرجع سابق، ص ص 191، 236-239.

– راجع نص المادة 08/(أ) من اللائحة التنفيذية لقانون التوقيع الإلكتروني وبإنشاء (هـ.ت.ص.ت.م).

[2] – أمر رقم 75-58 مؤرخ في 26 سبتمبر 1975 يتضمن القانون المدني، معدل ومتمم.

– المادة 323 مكرر:" ينتج الإثبات بالكتابة من تسلسل حروف أو أوصاف أو أيّة علامات أو رموز ذات معنى مفهوم، مهما كانت الوسيلة التي تتضمنها، وكذا طرق إرسالها."

– المادة 323 مكرر1:"يعتبر الإثبات بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة على الورق، بشرط إمكانية التأكد من هوية الشخص الذي أصدرها وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها."

بسبب شكله الإلكتروني، أو أنّه غير معزز بشهادة تصديق إلكتروني موصوفة أو لم يتم إحداثه بموجب منظومة أمن إحداث التوقيعات الإلكترونية.

فما يقع على قضاة الموضوع في حالة ما إذا طُرح عليهم نزاع يتعلق بإثبات صحة التوقيع الإلكتروني الموصوف لصاحبه، سوى التحقق من أنّ التوقيع قد تم إحداثه بموجب منظومة أمن إحداث التوقيعات الإلكترونية وفحصها، بوساطة(م.خ.ت.إ) مرخص له بمزاولة نشاطاته مع مراعاة الشروط المحددة في المادة 323 مكرر1 من القانون المدني، أمّا إذا تعلق الأمر بالتوقيع الإلكتروني البسيط فعلى صاحبه إثبات عدم تعرضه لما يثير الشبهة في بيانات إحداثه، وفقا لنص المادة 323 من القانون المدني: "**على الدائن إثبات الالتزام وعلى المدين إثبات التخلص منه.**"

إنطلاقا من كلّ ما سبق نصل إلى أنّ شهادات التصديق الإلكتروني الموصوفة دور أساسي في ضمان وإثبات مبادلات التجارة الإلكترونية عبر الإنترنيت، التي تستوجب على الأطراف المعولة عليها إحترام الإلتزامات المفروضة عليهم بموجب التشريعات المنظمة للمعاملات الإلكترونية مع تحمل المسؤولية المترتبة عند الإخلال بها.

## المبحث الثاني

## المسؤولية المترتبة على عملية التصديق الإلكتروني

يلعب(م.خ.ت.إ) المعتمد دور الوسيط المؤتمن فيما بين أطراف التعامل الإلكتروني، إذ يعمل على تعزيز الثقة فيما بينهم والحفاظ على حقوقهم مع ضمان مصداقية تصرفاتهم الإلكترونية، عن طريق إصدار شهادات تصديق إلكتروني موصوفة تضمن صحة توقيعاتهم الإلكترونية وسلامة البيانات الإلكترونية المرفقة بها، وفقا لمواصفات تقنية محددة تسمح بإقرار قابلية التعويل عليها(الشهادة) في بيئة إلكترونية مفتوحة مملوءة بالمخاطر، فقد يُعوِّل شخص ما على شهادة توثيق مُعتقدا أنّها تتضمن معلومات صحيحة ويتعامل على هذا الأساس، ثم يكتشف لاحقا عدم صحة البيانات الإلكترونية من جرّاء تعرضه لخسائر وأضرار غالبا ما تكون جسيمة بالنظر إلى قيمة الصفقة التجارية المبرمة إلكترونيا، لذا تُثار مسؤولية

أطراف التصديق الإلكتروني من جرّاء إخلالهم بالإلتزامات المفروضة عليهم(المطلب الأول) التي يمكن أن تُعرضهم لمختلف الجزاءات المتعلقة بالتصديق الإلكتروني(المطلب الثاني).

## المطلب الأول

## التكييف القانوني لمسؤولية أطراف التصديق الإلكتروني

تُعتبر المسؤولية الإلكترونية المترتبة عن عملية التصديق الإلكتروني من بين المسائل الحديثة التي تُثيرها المعاملات الإلكترونية في مجالات التجارة الإلكترونية والمعاملات المصرفية، نظرا لحداثتها وعدم تنظيمها تنظيما كافيا من قِبلِ التشريعات الدولية والوطنية المنظمة لها، لذا تُركت لقضاة الموضوع مسألة تقدير وتحديد الأساس القانوني لمسؤولية (م.خ.ت.إ) وفقا للقواعد المدنية أو الجزائية(الفرع الأول)، مع الأخذ بعين الإعتبار العلاقة التي تربطه مع الأطراف المعولة على شهادات التصديق الإلكتروني الموصوفة(الفرع الثاني) وذلك في إطار القواعد الخاصة المنظمة للمعاملات ومبادلات التجارة الإلكترونية.

### الفرع الأول

### مسؤولية مقدم خدمة التصديق الإلكتروني

إنّ التكييف القانوني للمسؤولية المترتبة عن عملية التصديق الإلكتروني يكون عادة على الأسس المبنية في القواعد المدنية والجزائية(أولا)، كما أنّ القوانين الخاصة بتنظيم المعاملات ومبادلات التجارة الإلكترونية قد وضعت أحكام خاصة بالمسؤولية للإستعانة بها وفقا لقاعدة الخاص يقيّد العام (ثانيا).

#### أولا- مسؤولية مقدم خدمة التصديق الإلكتروني وفقا للقواعد المدنية والجزائية.

يمكن أن تُثار مسؤولية(م.خ.ت.إ) في إطار العلاقة التعاقدية التي تربطه بالمُوقِّع، أو خارج إطار هذه العلاقة من جرّاء التعويل المعقول على بيانات شهادة التصديق الإلكتروني الموصوفة.

**1- المسؤولية العقدية لمقدم خدمة التصديق الإلكتروني.**

إنّ طبيعة ونطاق المسؤولية العقدية تُحدد بالعلاقات الناشئة عن عقد صحيح بين المسؤول والمضرور، فلقيام المسؤولية يجب أن يتوافر ركنان، فالأول يتمثل في وجود عقد صحيح (Existence d'un contrat valable) بين الطرف المسؤول والطرف المضرور الذي تترتب عنه مجموعة من الإلتزامات المُلقاة على الأطراف المعنية، فبِغَيْرِ هذا العقد لا يمكن تصور قيام مسؤولية عقدية وبإنتفاءه تختفي معه المسؤولية العقدية، أمّا الركن الثاني يتمثل في تحقق ضرر ناتج عن الإخلال بالإلتزامات المفروضة بموجب العقد (Violation d'une obligation contractuelle)، وبالتالي يجب أن يكون الضرر نتيجة عدم تنفيذ إلتزام تعاقدي سواءا كان إلتزاما رئيسيا أو ثانويا أو فرضته نصوص قانونية أو أوجدته بنود العقد، غير أنّه يقع على القاضي الفاصل في موضوع النزاع واجب القيام بتفسير الإرادة المُشتركة لأطراف العقد حتى يُحيط نفسه عِلماً بمضمونه، من أجل تحديد الإلتزامات الناشئة عنه بحيث تُثار المسؤولية العقدية في حالة الإخلال بها[1].

إنطلاقا من ذلك يُعتبر العقد المبرم بين(م.خ.ت.إ) والمُوقِّع كمُستخدم للخدمة، صحيحا بتوافر الأركان الثلاثة(الرضا والمحل والسبب)، فالتراضي يستوجب أن تتوافق إرادة الطرفين حول إحداث أثر قانوني بمجرد تطابق إيجاب جهة التوثيق الإلكتروني مع قبول مستخدم خدمة التصديق الإلكتروني، الذي غالبا ما تستوجب الإقرار بأنّه قد إطلع على بيان ممارسة خدمات التصديق الإلكتروني، وأن يقرّ بأنّه إطلع إطلاعا تاماً بأحكام عقد تقديم خدمة التوقيع الإلكتروني الموصوف، ولكي يكون التراضي صحيحا يجب أن يكون صادرا من ذي أهلية قانونية خالية من عيوب الإرادة كالغلط والتدليس والإكراه، أمّا مَحَلُّ العقد يتعلق بإحدى خدمات التصديق الإلكتروني كإحداث التوقيع الإلكتروني الموصوف، أو تحديث مدة صلاحية شهادة التصديق، الخ...، ولكي تتم مراحل إبرام العقد يجب أن يكون سبب إبرامه مشروعا بالنسبة لطرفي العقد، والمتمثل في تقديم خدمات التصديق الإلكتروني بطريقة قانونية للعملاء مقابل أجر يدفعه هذا الأخير لمقدم الخدمة، لذا إتفقت التشريعات المنظمة

---

1) - **Patrice JOURDAIN**, La Distinction des Responsabilités Délictuelle et Contractuelle : État du Droit Français, pp. 05-10. Article disponible sur : http://www.grerca.univ-rennes1.fr/

للقواعد العامة للمسؤولية المدنية بضرورة توافر الشروط الثلاثة لقيام المسؤولية العقدية[1] والمتمثلة في:

**أ- الخطأ العقدي: (Faute contractuelle)**

يتحقق الخطأ العقدي لجهة التوثيق الإلكتروني بمجرد الإخلال بأحد الإلتزامات المفروضة عليها بموجب عقد تقديم خدمة التصديق الإلكتروني، وبالتالي فإذا كان الإلتزام المُلقى على عاتق جهة التوثيق الإلكتروني يتعلق ببذل عناية معقولة كالتحقق من صحة المعلومات التي يُقدمها صاحب طلب إصدار شهادة التصديق الإلكتروني، أو التزامها بواجب الإعلام قبل إبرام عقد تقديم خدمة التصديق الإلكتروني، فيتحقق بالتالي الخطأ العقدي بمجرد إثبات صاحب الشهادة عدم بذل العناية الكافية في تحقيق الإلتزام المفروض عليها بموجب العقد، أمّا إذا كان الإلتزام يتعلق بتحقيق النتيجة أو الغاية (Obligation de résultat) المطلوبة كالإلتزام بالسرية وعدم إفشاء البيانات الإلكترونية، أو بتعليق وإلغاء الشهادات بعد طلب ذلك من طرف صاحب الشهادة، أو إلتزام جهة التوثيق بإصدار شهادات توثيق موصوفة وفقا للمتطلبات المعمول بها، أو العمل على إصدارها وفقا لبيانات مزورة الخ...، فيتحقق الخطأ العقدي بمجرد إثبات صاحب الشهادة عدم تحقيق النتيجة المطلوبة.

إنّ الخطأ في الميدان العقدي لا يُنشئ إلتزاما جديدا وإنّما هو أثر لإلتزام قائم، والمسؤولية العقدية الناتجة عن الخطأ لا تعدو أن تكون إلاّ تنفيذا بمقابل للالتزام الثابت في العقد، ومن هنا فإنّ الخطأ العقدي مرهون بعدم تحقق النتيجة أو الغاية المرجوة من الإلتزام[2]، إلاّ إذا أثبتت جهة التوثيق الإلكتروني أنّ عدم تنفيذ الإلتزام راجع إلى فعل المتضرر (صاحب شهادة التصديق الإلكتروني) أو إلى سبب أجنبي لا يد له فيها.

---

[1] – Ibid.

[2] – **محمود محمد أبو فروة**، الخدمات البنكية الإلكترونية عبر الإنترنيت، الطبعة الأولى، دار الثقافة للنشر و التوزيع، الأردن، 2009، ص ص 181، 182.

**ب- الضرر: (Le Dommage)**

يعتبر الضرر الركن الثاني الذي يجب توافره لتحقق المسؤولية العقدية الذي يستوجب أن يكون العقد قائما وقت حدوثه، وتُستبعد من المسؤولية العقدية الأخطاء التي تقع قبل إبرام العقد أو بعد انحلاله[1]، وبالتالي يجب أن يكون الضرر ناتج عن إخلال جهة التوثيق الإلكتروني بالتزام ناشئ عن العقد والمتمثل في تقديم خدمات التوثيق الإلكتروني، وأن يصيب الضرر المتعاقد الثاني المتمثل في المُوقِّع كصاحب شهادة التصديق الإلكتروني الموصوفة، وبالتالي فإذا شكك هذا الأخير في حدوث اختراق أمني في منظومة أمن إحداث التوقيعات الإلكترونية التي أتاحها له(م.خ.ت.إ) المعتمد أو المرخص له من طرف الجهات الرسمية، ولم يقم المزود بعد إعذاره بجميع الإمكانيات والوسائل المتاحة بإيقاف أو إلغاء شهادة التصديق الإلكتروني، أو عدم قيامه(م.خ.ت.إ) بإخطار الأطراف المعولة على شهادة التصديق بذلك، وقام الغير كطرف ثالث معول بإبرام صفقة تجارية ذات قيمة مالية باهضة باسم صاحب الشهادة، الذي ألحقه أضرار بالغة مَسَّتْ بمصلحته المالية والمعنوية، من جرّاء عدم تنفيذ جهة التوثيق الإلكتروني للالتزام المفروض عليها بموجب العقد، فتُثار عندئذٍ مسؤوليتها العقدية التي لا تتحقق إلاّ بتواجد العلاقة السببية بين الخطأ المرتكب والضرر الذي أُلحق بالمضرور(المُوقِّع) الذي يقع عليه عبئ الإثبات.

**ج- علاقة السببية بين الخطأ والضرر: (Un lien de causalité)**

لا تكفي الأركان السابقة لوحدها لقيام المسؤولية العقدية لجهة التوثيق الإلكتروني ما لم تكون علاقة سببية بين الخطأ العقدي المنسوب إليها والضرر المسبب للمضرور من جرّاء الخطأ العقدي، إلاّ إذا أثبتت جهة التوثيق من عدم تواجد علاقة السببية وذلك بداعي سبب أجنبي خارج عن إرادتها يعود إلى قوة قاهرة أو حادث فجائي متى توافرت شروطه[2].

---

[1] – **العربي بالحاج**، النظرية العامة للالتزام، ديوان المطبوعات الجامعية، الجزائر، 2001، ص ص 17، 18.

[2] – **Art. 1148** du code civil Français : « Il n'y a lieu à aucuns dommages et intérêts lorsque, par suite d'une force majeure ou d'un cas fortuit, le débiteur a été empêché de donner ou de

تجدر الإشارة على أنّه يمكن أن تثار المسؤولية العقدية عن الأضرار الملحقة بالغير وفقا لقواعد الإشتراط لمصلحة الغير(Stipulation pour autrui)، ويتحقق ذلك عندما يشترط المُوقّع كصاحب شهادة التصديق الإلكتروني على(م.خ.ت.إ)، أن يضمن تجاه الغير الأضرار التي تُلحقه نتيجة تعويله على الشهادة، فعندئذ ينشئ العقد إلتزاما قانونيا لصالح الغَيْرْ يتحمله(م.خ.ت.إ)، فآثار العقد وفقا للأصل العام لا تنصرف إلاّ على الأطراف المتعاقدة ولا تنصرف إلى غيرهم، وكاستثناء من ذلك يجوز للمتعاقدين الإتفاق على إفادة شخص ثالث ليس طرفا في العقد من أحكامه، الذي يكتسب(الغير) حقًّا مباشرا من العقد[1].

## 2- المسؤولية التقصيرية لمقدم خدمة التصديق الإلكتروني.

يمكن لـ (م.خ.ت.إ) أن يتحمل المسؤولية التقصيرية من جرّاء الأضرار الملحقة للأطراف التي لا تربطهم علاقة عقدية معه، نتيجة الإخلال بالتزام فرضه القانون وهو عدم الإضرار بالغير، في حين يعتبر الإلتزام القانوني المصدر المباشر والرئيسي لقيام المسؤولية التقصيرية لجهة التوثيق الإلكتروني، التي تتحقق بمجرد توافر أركان الثالوث الشهير المعروفة في الخطأ والضرر والعلاقة السببية بينهما، وبالتالي يُمكن للمسؤولية التقصيرية الإلكترونية أن تُنشأ عن الفعل الشخصي أو عن فعل الغير أو عن الأشياء[2].

---

faire ce à quoi il était obligé, ou a fait ce qui lui était interdit. » http://www.legifrance.gouve.fr/

[1] – إبراهيم الدسوقي أبو الليل، مرجع سابق، ص 1887.

- **Bernard BRUN**, Nature et impacts juridiques de la certification dans le commerce électronique sur Internet, P. 50. Article publié sur : http://www.signelec.comcontentsearticlesarticle_bernard_brun_html

– المادة 113 (أمر رقم58/75 مؤرخ في 26 سبتمبر 1975، معدل ومتمم): "لا يرتب العقد إلتزاما في ذمة الغير، ولكن يجوز أن يكسبه حقا."

[2] – **محمد صبري السعدي**، شرح القانون المدني الجزائري (مصادر الإلتزام – الواقعة القانونية)، الطبعة الثانية، دار الهدى، الجزائر، 2004، ص ص 27، 28.

– **عبد الرزاق السنهوري**، الوسيط (مصادر الإلتزام)، الوسيط في شرح القانون المدني (نظرية الإلتزام- الإثبات)، الطبعة الثالثة، الجزء الثاني، دار النهضة العربية، القاهرة، 1981، ص 1083.

**أولا: المسؤولية عن الفعل الشخصي. (La responsabilité du fait personnel)**

إنّ المسؤولية عن الأعمال الشخصية وفقا لمختلف التشريعات المنظمة للأحكام العامة للمسؤولية المدنية قائمة على أساس إثبات الخطأ، وهذا ما أكدّه المشرع الفرنسي بموجب المادتين 1382 و1383 من القانون المدني التي من خلالها ألزم كل مرتكب لخطأ سبّب في حدوث ضرر للغير بالتعويض، ويتحمل المسؤولية سواءا كان الخطأ عمدي أو بسبب الإهمال وعدم توخي الحذر[1]، بالإضافة إلى ذلك ألزم المشرع الفيدرالي السويسري بدوره بموجب المادة 1/41-2 من قانون الإلتزامات(CO)، الشخص الذي ألحق بطريقة غير مشروعة ضررا للغير بالتعويض سواء كان ذلك عمدا أو بالإهمال أو عدم الاحتياط[2].

كما ألزم المشرع المصري بموجب المادتين 163 و164 من القانون المدني كلّ مرتكب لخطأ سبب ضررا للغير بالتعويض، ويتحمل المسؤولية عن أعماله الغير المشروعة متى صدرت وهو مميز، أمّا المشرع الجزائري فطبق حرفيا نص المادة 1382 من القانون المدني الفرنسي في المادة 124 من القانون المدني التي تنص:" **كل فعل أيّا كان يرتكبه الشخص بخطئه، ويسبب ضررا للغير يلزم من كان سببا في حدوثه بالتعويض.**"

لذا يتعين على جهة التوثيق الإلكتروني أن تلتزم بواجب الحذر أو الحيطة والتبصر في سلوكها المهني تجاه الغير حتى لا تُلحقه أضرارا، والالتزام هنا هو إلتزام ببذل العناية وليس تحقيق النتيجة كأن لا يمارس(م.خ.ت.إ) العناية المعقولة لضمان دقة واكتمال كلّ ما يقدمه من تأكيدات جوهرية ذات صلة بشهادة التصديق الإلكتروني، كتوضيح الطريقة المُستخدمة في تعيين هوية المُوقِّع، أو أية قيود على الغرض أو القيمة التي يجوز أن تُستخدم من أجلها

---

1) – **Art.1382** (code civil français): « Tout fait quelconque de l'homme, qui cause à autrui un dommage, oblige celui par la faute duquel il est arrivé à le réparer. »
- **Art.1383** : « chacun est responsable du dommage qu'il a causé non seulement par son fait, mais encore par sa négligence ou par son imprudence. » http://www.legifrance.gouve.fr

2) – **Art.41-1,2** (Code des Obligations suisse du 30 mars 1911) :
« 1- Celui qui cause, d'une manière illicite, un dommage à autrui, soit intentionnellement, soit par négligence ou imprudence, est tenu de le réparer .
2- Celui qui cause intentionnellement un dommage à autrui par des faits contraires aux mœurs est également tenu de le réparer. » http://www.admin.chopcfrclassified-compilation/

الشهادة أو عدم قيام (م.خ.ت.إ) بتعليق العمل بشهادة التصديق الإلكتروني، أو إلغاءها لأيّ سبب من الأسباب المبررة بالرغم من علمه بذلك، أو عدم توفيره للمُوقِّع للوسائل اللازمة بالإخطار نتيجة تعرض بيانات إحداث توقيعه الإلكتروني لما يثير الشبهة، الشيء الذي ألحق أضرار تِجَاهَ الغير الذي عوّل على الشهادة الخ...، فكل ذلك يستوجب تحمل الجهة المُصدرة لها(الشهادة) للمسؤولية التقصيرية نتيجة تخلفها ببذل العناية اللازمة لمنع وقوع الضرر للغير الذي يقع عليه عبئ إثبات ذلك[1].

يعتبر الضرر الركن الثاني الذي يجب توافره في المسؤولية التقصيرية عن الفعل الشخصي لجهة التوثيق الإلكتروني، وذلك باعتباره كمحور أساسي تدور حوله المسؤولية بوجه عام، في حين يُعرف الضرر بمعناه العام على أنّه الأذى الذي يُصيب الشخص نتيجة المساس بمصلحة مشروعة له أو بحق من حقوقه، وبتعبير آخر الإخلال بمصلحة مشروعة سواءا كانت مادية أم معنوية(أدبية)، فالضرر المادي(Dommage Matériel) يعني الإخلال بمصلحة للمضرور ذات قيمة مالية ويُشترط أن يكون الضرر مُحقّقا فلا يكفي أن يكون مُحتملاً، كأن يعول الغير على شهادة تصديق مُلغاة أو منتهية الصلاحية مما أدى به إلى تفويت الفرصة (Perte d’une chance) في إبرام صفقة تجارية ذات قيمة مالية بالغة الأهمية.

أمّا الضرر المعنوي (Dommage Moral) هو الذي لا يمس المصلحة المالية للشخص المضرور كما هو الحال للضرر المادي، بل يصيبه في شعوره نتيجة المساس بحريته أو كرامته أو بشرفه أو سمعته أو غير ذلك من الأمور المعنوية التي يحرص عليها الإنسان في حياته اليومية، كأن يُسبب الضرر المادي المتعلق بتفويت الفرصة للغير في إبرام صفقة تجارية ذات قيمة مالية باهضة، بالشعور بإحباط نفسي بسبب آلام أدت بالإصابة بتشوهات أو إعاقات جسدية منعته من القيام بمهامه.

---

1) - **Philippe PIERRE**, La place de la responsabilité objective: Notion et rôle de la faute en droit français, pp. 03-06 et 09-11. Article disponible sur : http://grerca.univ-rennes1.fr/digitalAssets/268/268674_ppierre.pdf

– راجع كذلك نص المادة 09 من قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية لعام 2001. http://www.uncitral.org

يجب على الطرف المضرور الذي لا تربطه علاقة عقدية بتقديم خدمة التصديق الإلكتروني، أن يثبت العلاقة السببية بين الخطأ التقصيري المرتكب من طرف جهة التصديق الإلكتروني نتيجة عدم بذلها العناية اللازمة من الحيطة والتبصر لتفاديه، والضرر الذي ألحق بمصلحته المشروعة لقيام مسؤولية(م.خ.ت.إ) عن فعله الشخصي، غير أنّه من الصعب على المستهلك كطرف ثالث معول على شهادة التصديق الإلكتروني، إثبات العلاقة السببية بين الخطأ والضرر في بيئة إلكترونية إفتراضية معقدة ومُتعددة الأطراف[1]، فغالبا ما يكون الضرر ناتجا عن عدة وقائع أو أسباب تشترك في حدوثه، مما يُثير التساؤل عن أيّ سبب من هذه الأسباب التي يمكن إسناد الضرر إليه أم يكون هذا الإسناد إلى جميع الأسباب، لذا أثارت مسألة تعدد الأسباب أبحاث نظرية عميقة أدت إلى انقسام آراء الفقه إلى عدة اتجاهات والتي يُمكن حصرها في ثلاثة نظريات:

**أ- نظرية تعادل الأسباب:** يرى أصحاب هذه النظرية أنّ الضرر يحدث نتيجة مجموعة من الأسباب المتكافئة أو المتساوية التي بدونها لما وقع، فإذا ما ألغينا أحدها فإنّ الضرر لا يحدث، وبالتالي لا يمكن التفريق بين الأسباب بحسب أهميتها في إحداث الضرر، لكون أنّ كل سبب يعتبر كشرط ضروري لحدوثه (الضرر) [2].

**ب- نظرية السبب القريب:** يُقصد بالسبب القريب كل سبب يؤدي في تتابع طبيعي ومُستمر إلى إحداث النتيجة دون أن يقطعه تدخل سبب آخر فعّال، متى ثبت أنّ السبب كان وحده مؤديا إلى الضرر ولولا وقوعه لما حدثت النتيجة، لذا يرى أصحاب هذه النظرية أنّه يجب في إطار المسؤولية المدنية دائما البحث عن معيار للتفرقة بين الأسباب لكونها غير متساوية في إحداث الضرر، لذلك وجب التفريق بينها لمعرفة الأسباب بالمعنى الحقيقي، وبالتالي فالمعيار المُعتمد في ذلك هو معرفة الفترة الفاصلة بين حدوث السبب ووقوع الضرر فإذا كانت تلك الفترة بعيدة فلا يُعتد بالسبب أمّا إذا كانت قريبة فيمكن الأخذ به، لذا فإنّ هذه

---

[1] – **Bernard BRUN**, op.cit., pp. 51, 52.

[2] – **محمد صبري السعدي**، مرجع سابق، ص 96.

النظرية تقوم على أساس نظري من خلالها يتم تتبع الوقائع بعيدا عن فكرة تحديد السبب الحقيقي لها[1].

**ج- نظرية السبب المنتج:** ظهرت هذه النظرية نتيجة الانتقادات الموجهة للنظريتين السابقتين وأساس هذه النظرية أنّ المسؤولية عن الضرر لا تقوم إلاّ إذا كان من شأن الفعل الذي أحدثه في ظروف معينة أن يحدثه وفقا للمجرى العادي للأمور، وبالتالي يجب معرفة منذ البداية جميع الأسباب التي تدخلت في إحداث الضرر للتفريق بين ما هو صالح لإحداثه على الوجه المعتاد، وبين ما لا يُحدِث الضرر على هذا الوجه، فالسبب المنتج هو الذي يعتبر سببا قانونيا يؤدي حسب المألوف إلى إحداث الضرر، لذلك فإنّ السببية المنتجة هي السببية القانونية وليست السببية الطبيعية فهذه الأخيرة تجمع كل العوامل المتصلة بالحادث دون تمييز بين ما يكون منها منتجا من عدمه، أمّا السببية القانونية فتسعى إلى البحث عن السبب المنتج من بين الأسباب المختلفة، لذا نجحت هذه النظرية في حمل الفقه والقضاء على الأخذ بها[2].

**ثانيا: المسؤولية عن فعل الغير. (La responsabilité du fait d'autrui)**

يستعين(م.خ.ت.إ) أثناء قيامه بمهامه بموارد بشرية ذات كفاءات ومؤهلات عالية في ميدان التصديق الإلكتروني جديرة بالثقة للقيام بمسؤولياتهم وواجباتهم، بحيث تربطهم علاقة تبعية بمقدم الخدمة بصفته كمتبوع يمارس السلطة الفعلية في رقابتهم وتوجيههم كتابعين له في إطار المهام التي يمارسونها لحسابه(المتبوع)، لذا نظمت مختلف التشريعات الوطنية الأحكام العامة للمسؤولية عن عمل الغير وبالخصوص مسؤولية المتبوع عن أعمال تابعه على غرار المشرع الفرنسي، الذي ألزم الرؤساء والمتبوعون بموجب المادة 5/1384 من القانون المدني بتحمل مسؤولية الأضرار المرتكبة من طرف خادمهم أو تابعهم في أثناء تأدية وظائفهم[3].

---

[1] – **محمود محمد أبو فروة**، مرجع سابق، ص ص 191-193.

[2] – **عبد الرزاق السنهوري**، مرجع سابق، ص ص 1264، 1265.

[3] – **Art.1384- 5** du Code civil français. http://www.legifrance.gouve.fr/

كما نص القانون المدني المصري على ذلك في المادة 1/174-2 منه[1]:" **يكون المتبوع مسؤولا عن الضرر الذي يُحدثه تابعه بعمله الغير المشروع، متى كان واقعا منه في حال تأدية وظيفته أو بسببها. وتقوم رابطة التبعية، ولو لم يكن المتبوع حرّا في اختيار تابعه، متى كانت عليه سلطة فعلية في رقابته وفي توجيهه**".

أمّا المشرع الجزائري فقد نص على هذه المسؤولية في المادة 136 من القانون المدني[2]:" **يكون المتبوع مسؤولا عن الضرر الذي يحدثه تابعه بفعله الضار متى كان واقعا منه في حالة تأدية وظيفته أو بسببها أو بمناسبتها. وتتحقق علاقة التبعية ولو لم يكن المتبوع حرّا في اختيار تابعه متى كان هذا الأخير يعمل لحساب المتبوع**".

تضيف المادة 137 من نفس القانون على أنّه:" **للمتبوع حق الرجوع على تابعه في حالة ارتكابه خطأ جسيما.**"

فمن خلال أحكام هذه النصوص يتضح لنا أنّ مسؤولية المتبوع عن أعمال تابعيه تتحقق بمجرد توافر شرطين: الأول يتعلق بقيام رابطة التبعية (Lien de préposition) والثاني يتمثل في خطأ التابع (Le Préposé) حال تأدية الوظيفة أو بسببها أو بمناسبتها.

**أ- قيام رابطة التبعية:**

يُقصد بها تواجد رابطة التبعية بين جهة التوثيق الإلكتروني والموظفين أو المستخدمين الذين تمارس عليهم السلطة الفعلية في الرقابة والتوجيه، فعادة ما تنشأ علاقة التبعية عن

---

« On est responsable non seulement du dommage que l'on cause par son propre fait, mais encore de celui qui est causé par le fait des personnes dont on doit répondre, ou des choses que l'on a sous sa garde,[...] Les maîtres et les commettants, du dommage causé par leurs domestiques et préposés dans les fonctions auxquelles ils les ont employés. »

- **Philippe NEAU-LEDUC,** Droit Bancaire, 4e édition, éditions DALLOZ, Paris, 2010, p. 108.

- **Philippe MALINVAUD, Dominique FENOUILLET**, Droit des Obligations, 11e édition, Litec, France, 2010, pp. 462, 463, 474-476, 482-484.

[1] – قانون رقم 131-1948 مؤرخ في 16 جويلية 1948 المتعلق بإصدار القانون المدني، المنشور في الوقائع المصرية عدد 108 مكرر، الصادر في 29 جويلية 1948. http://www.arablaw.org

[2] – أمر رقم 58/75 مؤرخ في 26 سبتمبر 1975 يتضمن القانون المدني، معدل ومتمم.

عقد العمل الذي من خلاله يقوم المتبوع بحرية اختيار موارد بشرية جديرة بالثقة تتمتع بكفاءات وخبرات مهنية مؤهلة للقيام بمسؤولياتهم وواجباتهم المهنية.

**ب- خطأ التابع حال تأدية الوظيفة أو بسببها أو بمناسبتها:**

تتحقق مسؤولية جهة التوثيق الإلكتروني عن أعمال الموظفين أو المستخدمين التابعين لها بمجرد إثبات الأركان الثلاثة لمسؤولية التابع، فإذا انتفت مسؤولية هذا الأخير سواءا بسبب عدم ثبوت الخطأ في حقه أصلا أو وقع لسبب أجنبي لا شأن له(التابع) فيه، فإنّ مسؤولية المتبوع تنتفي بدورها، وبالتالي فقد يرتكب التابع لخطأ أثناء تأديته لوظيفته أو بسببها أو حتى بمناسبتها، كأن يعمل سهواً بإفشاء أو تعديل المعطيات الشخصية المتعلقة بصاحب شهادة تصديق التوقيع الإلكتروني لصاحبها، أو لا يقوم بإجراءات التحقق من هوية صاحب طلب إصدار الشهادة(المُحتال) عند إيداعه للطلب، أو لا يلتزم بالواجبات المفروضة عليه بموجب عقد العمل وبالمعايير والمتطلبات التي يحدّدها(م.خ.ت.إ) الخ...

كما تتحمل جهة التوثيق المسؤولية التقصيرية عن عمل الغير من جراء الأضرار المرتكبة من طرف أحد فروعها التي تعمل لحسابها، كالأخطاء التي يرتكبها المتعامل التقني الذي يقوم بخدمات التصديق الإلكتروني لحسابها، أو سلطة التسجيل التابعة لسلطة التصديق أو سلطة الأرشيف، أو السلطات الفرعية لها التي تؤدي خدمات تصديق لحساب بنك معين الخ...، بمجرد توافر الشَرْطَان المذكوران أعلاه[1]، لذا يجب على سلطة التصديق الإلكتروني أن تحدّد في سياسة التصديق الإلكتروني، مهام والتزامات كلّ فرع أو متعامل تقني يعمل لحسابها(PSCE) على مستوى أدنى درجة في هرم مرفق المفاتيح العمومية[2].

---

1) - **Marc LACOURSIÈRE,** « La responsabilité bancaire à l'ère du commerce électronique : impact des autorités de certification », revue les cahiers de droit, vol. 42, n° 4, 2001, pp. 1001-1004. Article disponible sur : http://www.erudit.org/revue/cd/2001/v42/n4/043684ar/

2) - En regard des services de certification, la **responsabilité de la banque** dépend de la relation juridique entre **celle-ci** et **l'autorité de certification**. La **banque** peut opérer une **autorité de certification** selon diverses structures, soit en vertu de la Loi sur les banques ou en vertu de certaines institutions du droit civil, comme le mandat et le contrat d'entreprise ou de service, La banque peut également n'avoir qu'un lien indirect avec l'autorité de certification. - **Marc LACOURSIÈRE et Édith VÉZINA,** op.cit., pp. 142-151.

**ثالثا: المسؤولية الناشئة عن الأشياء الغير الحيّة. (La responsabilité du fait des choses inanimées)**

تنص المادة 138 من القانون المدني الجزائري على:" **كلّ من تولى حراسة شيء وكانت له قدرة الاستعمال والتسيير، والرقابة، يعتبر مسؤولا عن الضرر الذي يُحدثه ذلك الشيء. ويُعفى من هذه المسؤولية الحارس للشيء إذا أثبت أنّ ذلك الضرر حدث بسبب لم يكن يتوقعه مثل عمل الضحية، أو عمل الغير، أو الحالة الطارئة، أو القوة القاهرة.**"

فمن خلال نص هذه المادة نفهم أنّه يمكن أن تُثار المسؤولية التقصيرية لسلطة التصديق الإلكتروني عن الأشياء الغير الحية الموضوعة تحت حراستها، كالمواقع التجارية التي يعول عليها أطراف التعامل الإلكتروني في البيع والشراء والتبادل أو الدفع الإلكتروني ومعدات وأنظمة أمن المعلومات التي تتيحها للمشتركين، في إحداث توقيعاتهم الإلكترونية والأنظمة المعلوماتية المتعلقة بإصدار أو حفظ أو إلغاء شهادات التصديق الإلكتروني الخ...، وذلك بمجرد توافر شرطان، فالأول يتعلق بتواجد شيء في حراسة شخص يملك السيطرة الفعلية عليه، وأن يتصرف فيه في الاستعمال والتوجيه والرقابة باعتباره أداة لتحقيق غرض معين، وأمّا الشرط الثاني يتعلق في أن يتسبب الشيء المحروس في حدوث ضرر للغير الذي يجب عليه إثبات علاقة السببية بين الضرر وبين تدخل الشيء الإيجابي.

إنطلاقا من ذلك فإنّ أساس المسؤولية عن حراسة الشيء قائم على أساس خطأ مُفترض وقوعه من حارس الشيء افتراضا لا يقبل العكس ناتج عن فقدانه للسيطرة الفعلية على ذلك الشيء، إلاّ إذا أثبت الحارس أنّ وقوع الضرر ناتج عن سبب أجنبي لا يَدَ له فيه كالقوة القاهرة أو خطأ المضرور أو الغير، كأن تُقصّر جهة التوثيق الإلكتروني ببذل العناية اللازمة في إصلاح منظومة إحداث وفحص التوقيعات الإلكترونية التي لا تضمن أحادية مفاتيح التشفير، أو عجز البرامج والمعدات الإلكترونية أو الأنظمة المعلوماتية في الإدراج الفوري والإتاحة اللحظية لقوائم الشهادات الموقوفة أو الملغاة، أو عمل جهة التوثيق بإدراج مَوْقِع

---

- **Eric A. CAPRIOLI**, « De l'authentification à la signature électronique : quel cadre juridique pour la confiance dans les communications électroniques internationales ? », pp. 37-40. Article disponible sur : http://www.caprioli-avocats.com

تجاري(لا يستجيب لمعايير الأمان) ضمن قائمة المواقع الإلكترونية المحمية، مما ألحق أضرارا بالغة لأطراف التعامل الإلكتروني من جرّاء ثقتهم فيه وتعويلهم عليه من خلال عمليات البيع والشراء والدفع الإلكتروني[1] الخ...

### 3- المسؤولية الجزائية لمقدم خدمة التصديق الإلكتروني.

قد يحدث أن يُكيّف الفعل الغير المشروع الذي ارتكبه(م.خ.ت.إ) بصفته كشخص طبيعي أو معنوي على أساس جريمة، يعاقب عليها وفقا للأحكام العامة الواردة في قوانين العقوبات، الشيء الذي يعرضه إلى تحمل المسؤولية الجزائية وفقا لمبدأ الشرعية الجزائية (Principe de Légalité Pénale) المعروف بالعبارة المتداولة، "لا جريمة ولا عقوبة بدون نص" والتي تتحقق(المسؤولية)[2] بمجرد توافر أركانها، لذا فرضت مختلف التشريعات مجموعة من الجزاءات المتعلقة بالتصديق الإلكتروني في قوانين العقوبات(سنراها لاحقا).

تجدر الإشارة أنّ التشريعات الحديثة اعترفت بإسناد المسؤولية الجزائية للشخص المعنوي عن الجرائم المرتكبة لحسابه من طرف أجهزته أو ممثليه، وذلك على غرار المشرع الجزائري الذي نص في المادة 51 مكرر من قانون العقوبات:" **بإستثناء الدولة والجماعات المحلية والأشخاص المعنوية الخاضعة للقانون العام، يكون الشخص المعنوي مسؤولا جزائيا عن**

---

[1] – **عايد رجا الخلايلة**، المسئولية التقصيرية الإلكترونية: المسئولية الناشئة عن إساءة إستخدام أجهزة الحاسوب والإنترنيت (دراسة مقارنة)، دار الثقافة للنشر والتوزيع، عمان، 2009، ص ص 244-252.

[2] – **Art. 111-3** : (code pénal Français) http://www.legifrance.gouve.fr
« Nul ne peut être puni pour un crime ou pour un délit dont les éléments ne sont pas définis par la loi, ou pour une contravention dont les éléments ne sont pas définis par le règlement.
Nul ne peut être puni d'une peine qui n'est pas prévue par la loi, si l'infraction est un crime ou un délit, ou par le règlement, si l'infraction est une contravention. »
- **Art.1** : (code pénal suisse du 21 décembre 1937(état le 1er janvier 2014))
« Une peine ou une mesure ne peuvent être prononcées qu'en raison d'un acte expressément réprimé par la loi. » http://www.admin.chopcfrclassified-compilation/
- أمر رقم 66-156 المؤرخ في 08 جويلية 1966 يتضمن قانون العقوبات، معدل ومتمم.
- المادة 01:" لا جريمة ولا عقوبة أو تدابير أمن بغير قانون."
- **علي جبار الحسيناوي**، جرائم الحاسوب والإنترنيت، دار اليازوري العلمية للنشر والتوزيع، الأردن، 2009، ص ص 37-43.

**الجرائم التي ترتكب لحسابه من طرف أجهزته أو ممثليه عندما ينص القانون على ذلك. إنّ المسؤولية الجزائية للشخص المعنوي لا تمنع مساءلة الشخص الطبيعي كفاعل أصلي أو كشريك في نفس الأفعال."**

يتبين لنا من كلّ ما سبق أنّ تطبيق الأحكام الواردة في القوانين المدنية والجزائية على جهات التوثيق الإلكتروني، لا تكفي لوحدها في تكييف وتحديد نوع المسؤولية التي يجب تحملها في حالة الإخلال بالإلتزامات في إطار مرفق المفاتيح العمومية، كما أنّ معاملات التجارة الإلكترونية التي تعتمد على الوسائل التكنولوجية الحديثة، تستوجب الحاجة إلى الإستعانة بالقواعد الخاصة المنظمة لخدمات التصديق الإلكتروني، التي من شأنها أن تساعد على تحديد طبيعة المسؤولية المترتبة على كلّ طرف تربطه أم لا تربطه علاقة عقدية بـ(م.خ.ت.إ) المعتمد أو المرخص له من طرف الجهات الرسمية بمزاولة نشاطاته.

**ثانيا- مسؤولية مقدم خدمة التصديق الإلكتروني وفقا للقواعد الخاصة.**

أمام عدم كفاية القواعد المدنية والجزائية المنظمة لمسؤولية جهات التوثيق الإلكتروني قامت معظم التشريعات الدولية والوطنية المنظمة للمعاملات الإلكترونية، بوضع قواعد خاصة بالمسؤولية التي سنتطرق إليها على النحو التالي:

**أ- مسؤولية جهات التصديق الإلكتروني وفقا للتشريعات الأجنبية.**

**1- التوجيه الأوروبي رقم 93/99 المتعلق بالتوقيعات الإلكترونية:**

وضع التوجيه الأوروبي المتعلق بالتوقيع الإلكتروني تنظيما قانونيا لمسؤولية(م.خ.ت.إ) عن الأضرار والخسائر الملحقة، بالأطراف المعولة على شهادات التصديق الإلكتروني الموصوفة، بحيث ترك التوجيه مسألة تحديد وتكييف المسؤولية المدنية أو الجزائية للقوانين الداخلية للدول المعنية بالتوجيه، لذا نصت المادة 06 منه على ضرورة قيام الدول الأعضاء بتنظيم القواعد الخاصة بمسؤولية(م.خ.ت.إ) عن الأضرار الملحقة بالطرف المعول(شخص طبيعي أو معنوي)، على شهادة التصديق الإلكتروني الموصوفة الصادرة منه وذلك في حالة عدم صحة المعلومات الواردة فيها وقت صدورها، أو في حالة عدم تطابق منظومة أمن

إحداث التوقيع الإلكتروني مع منظومة فحصه، أو في حالة إغفال(م.خ.ت.إ) تسجيل الشهادات المُلغاة في السجل الخاص بها، أو عدم ذكر القيود المفروضة على الغرض أو القيمة أو نطاق المسؤولية التي تستعمل من أجلها شهادة التصديق الإلكتروني[1].

إنطلاقا من ذلك فإنّ جهة التوثيق الإلكتروني لا تتحمل مسؤوليتها إذا أثبتت عدم إهمالها لأي إلتزام مفروض عليها بموجب العقد أو القانون، كما لا تتحمل الأضرار الناجمة عن الإستعمال التعسفي لشهادة التصديق الإلكتروني الموصوفة، ويجب في كلّ الظروف

---

1) – **Art. 06** (Directive européenne n° 99/93 sur les signatures électroniques) :
« **1-** Les États membres veillent au moins à ce qu'un prestataire de service de certification qui délivre à l'intention du public un certificat présenté comme qualifié ou qui garantit au public un tel certificat soit responsable du préjudice causé à toute entité ou personne physique ou morale qui se fie raisonnablement à ce certificat pour ce qui est de:
a) l'exactitude de toutes les informations contenues dans le certificat qualifié à la date où il a été délivré et la présence, dans ce certificat, de toutes les données prescrites pour un certificat qualifié;
b) l'assurance que, au moment de la délivrance du certificat, le signataire identifié dans le certificat qualifié détenait les données afférentes à la création de signature correspondant aux données afférentes à la vérification de signature fournies ou identifiées dans le certificat;
c) l'assurance que les données afférentes à la création de signature et celles afférentes à la vérification de signature puissent être utilisées de façon complémentaire, dans le cas où le prestataire de service de certification génère ces deux types de données, sauf si le prestataire de service de certification prouve qu'il n'a commis aucune négligence.
**2-** Les États membres veillent au moins à ce qu'un prestataire de service de certification qui a délivré à l'intention du public un certificat présenté comme qualifié soit responsable du préjudice causé à une entité ou personne physique ou morale qui se prévaut raisonnablement du certificat, pour avoir omis de faire enregistrer la révocation du certificat, sauf si le prestataire de service de certification prouve qu'il n'a commis aucune négligence.
**3-** Les États membres veillent à ce qu'un prestataire de service de certification puisse indiquer, dans un certificat qualifié, les limites fixées à son utilisation, à condition que ces limites soient discernables par des tiers. Le prestataire de service de certification ne doit pas être tenu responsable du préjudice résultant de l'usage abusif d'un certificat qualifié qui dépasse les limites fixées à son utilisation.
**4-** Les États membres veillent à ce qu'un prestataire de service de certification puisse indiquer, dans un certificat qualifié, la valeur limite des transactions pour lesquelles le certificat peut être utilisé, à condition que cette limite soit discernable par des **tiers**. Le prestataire de service de certification n'est pas responsable des dommages qui résultent du dépassement de cette limite maximale.
**5-** Les dispositions des paragraphes 1 à 4 s'appliquent sans préjudice de la directive 93/13/CEE du Conseil du 5 avril 1993 concernant les clauses abusives dans les contrats conclus avec les consommateurs. »

الأخذ بعين الإعتبار بأحكام التوجيه الأوروبي رقم 13/93 المؤرخ في 05 أفريل 1993 المتعلق بالبنود التعسفية في العقود المبرمة مع المستهلك.

**2- القانون البلجيكي:**

طبق المشرع البلجيكي نص المادة 06 من التوجيه الأوروبي المتعلق بالتوقيعات الإلكترونية حرفيا، عند صياغته للمادة 14 من القانون الصادر في 09 جويلية2001 المتعلق بالإطار القانوني للتوقيعات الإلكترونية وبخدمات التصديق، التي من خلالها يتحمل(م.خ.ت.إ) مسؤولية الأضرار المسببة للأطراف المعولة على شهادة التصديق الإلكتروني الموصوفة الصادرة منه، وذلك من جراء عدم ضمانه صحة البيانات الواردة فيها أو عدم مطابقة بيانات إحداث التوقيع الإلكتروني الموصوف مع بيانات فحصه، أو في حالة إغفاله تسجيل الشهادة في السجل الخاص بها(LCR)[1]، أو عدم توضيح القيود المتعلقة بالغرض أو القيمة أو بحدود المسؤولية التي تستعمل من أجلها الشهادة، غير أنّه تنتفي مسؤولية(م.خ.ت.إ) عن كلّ إستعمال تعسفي للشهادة تجاوز نطاقها المحدّد فيها، أو إذا أثبت عدم إهماله لأي إلتزام مفروض عليه بموجب العقد أو القانون.

**3- القانون الفرنسي:**

مراعاة لأحكام المادة 06 من التوجيه الأوروبي رقم 93/99 المتعلق بالتوقيعات الإلكترونية قام المشرع الفرنسي بتنظيم القواعد الخاصة بمسؤولية(م.خ.ت.إ) المؤهل، في القانون رقم 2004-575 المؤرخ في 21 جوان 2004 المتعلق بالثقة في الإقتصاد الرقمي فوفقا للمادة 33 منه، يتحمل(م.خ.ت.إ) المسؤولية عن الأضرار الملحقة بالطرف المعول على الشهادة الإلكترونية الموصوفة، في حالة عدم صحة المعلومات الواردة فيها في وقت صدورها، أو عدم احتواءها على البيانات الإلزامية المحددة بموجب القانون المعمول به كذكر حدود استعمالها والقيود المتعلقة بالغرض والقيمة التي تُستعمل من أجلها تلك الشهادة، أو

---

1) – Loi du 09 Juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification. http://www.moniteur.be

عدم مطابقة بيانات إحداث التوقيع الإلكتروني مع بيانات فحصه، أو في حالة إغفاله تسجيل الشهادة الملغاة في السجل الخاص، لذا تنتفي مسؤولية(م.خ.ت.إ) في حالة إثبات عدم ارتكابه لأيّ خطأ أو عند تجاوز حدود إستعمال الشهادة أو قيمة المعاملة المحددة فيها[1].

تجدر الإشارة أنّ المشرع الفرنسي قد نص في القانون رقم 2004-575 المتعلق بالثقة في الإقتصاد الرقمي، على مجموعة من الجزاءات المتعلقة بالتصديق الإلكتروني التي على أساسها يتحمل(م.خ.ت.إ) للمسؤولية الجزائية بمجرد توافر أركانها وفقا لمبدأ الشرعية الجزائية (Principe de Légalité Pénale)(التي سنراها لاحقا).

**ب- مسؤولية مقدم خدمة التصديق الإلكتروني وفقا للتشريعات العربية.**

**1- القانون التونسي:**

وفقا للفصل 22 من قانون رقم 83-2000 المتعلق بالمبادلات والتجارة الإلكترونية يتحمل(م.خ.ت.إ) مسؤولية الأضرار الملحقة بالطرف المعول على شهادة التصديق الإلكتروني، نتيجة إخلاله بالإلتزامات المفروضة عليه بموجب الفصل 18 من نفس القانون المتعلقة بعدم ضمان صحة المعلومات الواردة في الشهادة وقت إصدارها، أو عدم مطابقة

---

1) – **Art. 33** :(loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.)
« Sauf à démontrer qu'ils n'ont commis aucune faute intentionnelle ou négligence, les prestataires de services de certification électronique sont responsables du préjudice causé aux personnes qui se sont fiées raisonnablement aux certificats présentés par eux comme qualifiés dans chacun des cas suivants :
**1**- Les informations contenues dans le certificat, à la date de sa délivrance, étaient inexactes ;
**2**- Les données prescrites pour que le certificat puisse être regardé comme qualifié étaient incomplètes ;
**3**- La délivrance du certificat n'a pas donné lieu à la vérification que le signataire détient la convention privée correspondant à la convention publique de ce certificat ;
**4**- Les prestataires n'ont pas, le cas échéant, fait procéder à l'enregistrement de la révocation du certificat et tenu cette information à la disposition des tiers.
Les prestataires ne sont pas responsables du préjudice causé par un usage du certificat dépassant les limites fixées à son utilisation ou à la valeur des transactions pour lesquelles il peut être utilisé, à condition que ces limites figurent dans le certificat et soient accessibles aux utilisateurs. Ils doivent justifier d'une garantie financière suffisante, spécialement affectée au paiement des sommes qu'ils pourraient devoir aux personnes s'étant fiées raisonnablement aux certificats qualifiés qu'ils délivrent, ou d'une assurance garantissant les conséquences pécuniaires de leur responsabilité civile professionnelle. » http://www.legifrance.gouve.fr/

بيانات إحداث التوقيع الإلكتروني مع بيانات فحصه، أو في حالة عدم التدقيق في المعلومات المقدمة إليها في طلبات إصدار شهادات التصديق الإلكتروني، وهذا ما حدث لسلطة التصديق الإلكتروني(Verisign)[1] عندما قامت بإصدار شهادتي تصديق لشخص مُنتحلا صفة مُسْتَخْدَمْ لدى شركة(Microsoft) من دون فحص سلطة التسجيل لهويته، كما يتحمل المزود كذلك المسؤولية عن الأضرار المسببة للغير نتيجة إخلاله بالتزام تعليق أو إلغاء العمل بالشهادة وفقا للفصلين 19 و20 من نفس القانون، والجدير بالذكر أنّ الباب السابع من نفس القانون نص على مجموعة من الجزاءات المتعلقة بالتصديق الإلكتروني(التي سنراها لاحقا)، التي على أساسها يتحمل(م.خ.ت.إ) مسؤوليته الجزائية.

**2- قانون الإمارات العربية المتحدة:**

نص المشرع الإتحادي بموجب المادة 4/21 من القانون الإتحادي رقم 01-2006 بشأن المعاملات والتجارة الإلكترونية، على تحمل(م.خ.ت.إ) المسؤولية عن الأضرار والخسائر المترتبة للطرف المعول(المُوقّع أو الغير) على شهادة التصديق الإلكتروني نتيجة عدم صحتها أو تواجد أي عيب فيها، وتضيف الفقرة الخامسة من نفس المادة على انتفاء مسؤولية المزود في حالة ما إذا أدرج في الشهادة بيانا يقيد نطاق ومدى مسؤوليته تجاه أي شخص ذي صلة بالشهادة، أو في حالة إثبات المزود بأنّه لم يرتكب أي خطأ أو إهمال أو أنّ الضرر قد نشأ عن سبب أجنبي لا يد له فيه، والجدير بالذكر أنّ الفصل التاسع من نفس القانون نص على مجموعة من الجزاءات المتعلقة بالتصديق الإلكتروني، التي على أساسها يتحمل(م.خ.ت.إ) المسؤولية الجزائية وفقا لمبدأ الشرعية في العقاب (التي سنراها لاحقا).

**3- القانون العماني:**

وفقا للمادة 1/35-2 من قانون المعاملات الإلكترونية العماني تقوم المسؤولية المدنية لـ(م.خ.ت.إ) في حالة ما إذا ألحق ضررا بالطرف الذي تعاقد معه لتقديم الشهادة، أو أيّ

---

1) – Voir le Bulletin d'alerte de CERT-FR, (ANSSI). http://www.cert.ssi.gouv.fr/site/CERTFR-2001-Rec-001.pdf

شخص يكون قد اعتمد بدرجة معقولة على الشهادة، وذلك سواءا نتيجة عدم صحة الشهادة أو لأنّها معيبة نتيجة خطأ أو إهمال من طرفه(م.خ.ت.إ)، ولا يكون هذا الأخير مسؤولا عن أيّ ضرر إذا أثبت أنّه لم يرتكب أي خطأ أو إهمال أو أنّ الضرر كان ناشئا عن سبب خارج عن إرادته، والجدير بالذكر أنّ المشرع العماني نص في الفصل التاسع من نفس القانون[1]، على مجموعة من الجزاءات المتعلقة بالتصديق الإلكتروني والتي على أساسها يتحمل (م.خ.ت.إ) مسؤوليته الجزائية وفقا لمبدأ الشرعية في العقاب (التي سنراها لاحقا).

**4- القانون الجزائري:**

نص المشرع الجزائري بموجب المواد 53 إلى 57 من القانون رقم 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، على تحمل(م.خ.ت.إ) المسؤولية المدنية عن الضرر المسبب للطرف المعول(هيئة أو شخص معنوي أو طبيعي) على شهادة التصديق الإلكتروني الموصوفة، نتيجة عدم صحة البيانات الواردة في الشهادة وقت إصدارها، أو عدم مطابقة بيانات إحداث التوقيع الإلكتروني مع بيانات فحصه، أو إخلاله بالتزام إلغاء الشهادة بعد ثبوت دواعي ذلك، في حين تنتفي مسؤولية(م.خ.ت.إ) في حالة إثبات أنه لم يرتكب أي إهمال، أو في حالة تجاوز حدود إستعمال الشهادة، أو القيمة المحددة فيها، كما يمكن لـ(م.خ.ت.إ) أن يتحمل المسؤولية الجزائية وفقا لمبدأ الشرعية في العقاب على أساس الجزاءات الواردة في الباب الرابع من نفس القانون(التي سنراها لاحقا).

## الفرع الثاني

## مسؤولية الأطراف المُعَوِّلَة على شهادة التصديق الإلكتروني

إنّ صاحب شهادة التصديق الإلكتروني يتحمل المسؤولية المدنية في حالة إخلاله بالإلتزامات العقدية أو القانونية، والمسؤولية الجزائية في حالة ارتكابه لجريمة يعاقب عليها

---

[1] – المرسوم السلطاني رقم 69-2008 مؤرخ في 17 ماي 2008، يتعلق بإصدار قانون المعاملات الإلكترونية.http://www.omanlegal.org/law/search.aspx

بموجب القانون(أولا)، كما أنّ الطرف الثالث المُعوِّل(Tiers) يتحمل بدوره الآثار المترتبة من جرّاء تخلفه عن اتخاذ الإجراءات المعقولة في قابلية التعويل على الشهادة(ثانيا).

**أولا- مسؤولية صاحب شهادة التصديق الإلكتروني.**

يتحمل صاحب شهادة التصديق الإلكتروني المسؤولية المدنية أو الجزائية بمجرد تحقق أركانها، والتي سنتطرق إليها على النحو التالي:

**1- المسؤولية المدنية لصاحب شهادة التصديق الإلكتروني.**

يجب على صاحب التوقيع الإلكتروني الموصوف أن يتحمل الآثار المترتبة من جرّاء إخلاله بالإلتزامات المفروضة عليه بموجب العقد أو القانون، مما يستوجب عليه تحمل المسؤولية العقدية أو التقصيرية.

**أ- المسؤولية العقدية:**

تربط صاحب شهادة التصديق الإلكتروني بـ(م.خ.ت.إ) علاقة عقدية حول تقديم خدمة التوثيق الإلكتروني، التي بموجبها يتحمل المسؤولية العقدية عن الأضرار المسببة لمقدم الخدمة بمجرد تحقق أركانها الثلاثة المعروفة في الخطأ العقدي والضرر والعلاقة السببية بينهما[1]، كأن لا يبذل المُوقِّع العناية اللازمة في إستخدام المعدات الخاصة بآلية أمن إحداث توقيعه الإلكتروني المأذون بها من طرف مقدم خدمة التوثيق الإلكتروني الموثوق به في سياق مرفق المفاتيح العمومية، أو يمتنع عن إبلاغ(م.خ.ت.إ) أو أيّ شخص يتوقع منه على وجه معقول أن يُعوِّلَ على توقيعه الإلكتروني الموصوف، عن كلّ ما يثير الشبهة من تعرض بيانات إنشاء توقيعه الإلكتروني، أو بضياع أو سرقة بطاقة الإئتمان الذكية التي

---

[1] – **محمد حاتم البيات**، المسئولية المدنية عن الخطأ في المعاملات التي تتم عبر الوسائط الإلكترونية، بحث مقدم في مؤتمر المعاملات الإلكترونية (التجارة الإلكترونية- الحكومة الإلكترونية) الذي نظمه مركز الإمارات للدراسات والبحوث الإستراتيجية المنعقد في دبي من 19 إلى 20 ماي 2009، بحوث المجلد الثاني، ص ص 809، 812. http://www.slconf.uaeu.ac.aeslconf17arabic_prev_conf2009.asp

يتواجد فيها المفتاح الخاص بتوقيعه الإلكتروني والشهادة الموصوفة، أو التعنت عن تقديمه للمعلومات الصحيحة المتعلقة بشهادة التصديق الإلكتروني، أو إمتناعه عن إعلام(م.خ.ت.إ) عن أيّ تغيير في المعلومات التي تحتويها تلك الشهادة الخ...

فوفقا للمادتين 61 و62 من القانون رقم 15-04 المتضمن القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، يعتبر صاحب شهادة التصديق الإلكتروني الموصوفة المسؤول الوحيد عن كلّ ما يتعلق بسرية بيانات إنشاء توقيعه الإلكتروني والحفاظ عليها، أو في حالة ما إذا أصبحت هذه البيانات غير مطابقة للمعلومات الواردة في شهادة التصديق الإلكتروني ولم يطلب إلغائها من(م.خ.ت.إ)، أو في حالة قيام صاحب الشهادة المنتهية صلاحيتها أو الملغاة بإستعمال بيانات إنشاء التوقيع الإلكتروني الواردة فيها، للتصديق عليها مرة آخرى من طرف(م.خ.ت.إ) آخر، أو إستعمال الشهادة الإلكترونية الموصوفة خارج الأغراض التي مُنحت من أجلها، وهكذا يبقى وفاء جهة التوثيق الإلكتروني بالتزاماتها العقدية مُتوقف على مدى التعاون القائم بينها وبين المُوقِّع صاحب شهادة التصديق الإلكتروني.

**ب- المسؤولية التقصيرية:**

يتحمل صاحب شهادة التصديق الإلكتروني المسؤولية التقصيرية عن الأضرار الملحقة بالطرف الثالث المعول على الشهادة(Tiers)، نتيجة تقصيره في بذل العناية اللازمة لمنع حدوثها[1]، وبالتالي فإنّ أساس المسؤولية التقصيرية قائم على الإخلال بالتزام فرضه القانون والمتمثل في إلتزام العناية أو الحيطة والتبصر، في سلوك المُوقِّع تجاه الغير حتى لا يضرّه فإذا انحرف عن السلوك الواجب إتباعه، أُعتبر مُخطئا مما يؤدي إلى إمكانية إثارة مسؤوليته التقصيرية عن فعله الشخصي، أو الناشئة عن الأشياء الغير الحية الموضوعة تحت حراسته بما فيها أدوات إحداث التوقيع الإلكتروني المأذون بها من طرف(م.خ.ت.إ)، أو بطاقة الإئتمان الذكية الخ...

---

[1] – **محمد حاتم البيات**، مرجع سابق، ص ص 816، 817.

فلكي تقوم مسؤولية صاحب شهادة التصديق عن فعله الشخصي يستوجب توافر أركانها الثلاثة المتمثلة في الخطأ والضرر والعلاقة السببية بينهما، في حين يتحقق خطأ صاحب الشهادة إذا ثبت من جانبه إهمال في حماية المفتاح الخاص ببيانات إحداث توقيعه الإلكتروني، أو يترك بطاقة الإئتمان الذكية التي تتواجد فيها بيانات إحداث التوقيع الإلكتروني وشهادة التصديق الإلكتروني الموصوفة، تحت تصرف أفراد أسرته أو أحد موظفيه من دون وعيهم بشروط استعمالها والمخاطر التي تجوبها، أو يُهمل المُوقِّع إعتماد إحدى برامج الحماية الإلكترونية المعروفة على صعيد حفظ البيانات والمنزلة على حاسوبه الشخصي، مما قد يُعرضها لعمليات القرصنة الإلكترونية من طرف الغير، كما قد يتعلق الخطأ بإخلال صاحب الشهادة بواجب إعلام أيّ شخص طبيعي أو معنوي يتوقع تعويله على شهادة التصديق الإلكتروني، وذلك في حالة ما إذا علم أو شكك من إمكانية تعرض بيانات إحداث توقيعه الإلكتروني لما يثير الشبهة فيها كقرصنتها من طرف أحد البرامج الخبيثة، مما يُعرض الأطراف المعولة لأضرار من الممكن تفاديها لو أخطرهم صاحب الشهادة بكافة الوسائل المتاحة لديه.

بالإضافة إلى ذلك يجب أن يسبب الخطأ المرتكب من جانب صاحب الشهادة ضررا للطرف الثالث المعوّل على شهادة التصديق الإلكتروني، الذي يُشترط فيه(الضرر) أن يكون محققا أو مؤكد الوقوع في المستقبل(Préjudice futur)، فلا يكفي أن يكون محتملا(Préjudice éventuel) سواءا كان الضرر المتسبب مادي أو معنوي، كأن يعول الغير على شهادة تصديق إلكتروني بناءا على معلومات مزورة في إبرام صفقة تجارية معينة تم إيقاف العمل بها أو إلغاءها، ممّا أدّى إلى إلحاقه بخسارة مالية أو تفويته الفرصة في حالة عدم إبرامه للصفقة، وفي كلتا الحالتين يمكنه أن يتضرر معنويا عن طريق الشعور بإحباط نفسي أو المساس بسمعته التجارية[1] الخ ...

أما المسؤولية عن الأشياء الغير الحيّة تستوجب تواجد شيء يتطلب حراسته من الحارس الذي يملك عليه سلطة الاستعمال والتوجيه والرقابة، كأجهزة الحاسوب وبرامجه وبطاقات

---

[1] – **محمد حاتم البيات**، مرجع سابق، ص ص 814، 815.

الإئتمان الذكية، والوسائل الإلكترونية الآخرى المستعملة في خزن وحفظ شهادات التصديق الإلكتروني، كالحاويات الإلكترونية الأقراص الصلبة أو أدوات إحداث التوقيعات الإلكترونية الموصوفة الموضوعة تحت سيطرة المُوقِّع بشكل قانوني الخ...، كما يجب على صاحب شهادة التصديق الإلكتروني بصفته كحارس، أن تكون لديه السلطة الفعلية على الشيء المتصرف فيه بالاستعمال والتوجيه والرقابة لحساب نفسه دون غيره، وأن يسبب ذلك الشيء في حدوث ضرر كأن تخرج أدوات إنشاء التوقيع الإلكتروني عن سيطرة المُوقِّع، مما يتيح الفرصة للغير بالعبث أو التلاعب بالبيانات الإلكترونية المتعلقة بالتوقيع الإلكتروني واستنباطها بالوسائل التكنولوجية المتوافرة، أو تقصيره في بذل العناية اللازمة في حفظ المفتاح الخاص بتوقيعه الإلكتروني بطريقة آمنة، أو ضياعه لبطاقته الذكية[1] الخ...

إنطلاقا من ذلك فإنّ أساس المسؤولية عن حراسة الشيء وفقا للمادة 138 من القانون المدني الجزائري السالفة الذكر، قائم على أساس خطأ مفترض وقوعه من حارس الشيء افتراضا لا يقبل العكس، ناتج عن فقدانه للسيطرة الفعلية على ذلك الشيء المحروس، إلاّ إذا أثبت الحارس أنّ وقوع الضرر ناتج عن سبب أجنبي لا يد له فيه كالقوة القاهرة أو خطأ المضرور أو الغير، فما يقع على المضرور إلاّ إثبات الضرر الذي حدث له من التدخل الإيجابي للشيء، ولا يكلف بإثبات الخطأ[2].

**2- المسؤولية الجزائية لصاحب شهادة التصديق الإلكتروني.**

قد يحدث أن يُكيَّفَ الفعل الضار الغير المشروع الذي ارتكبه صاحب الشهادة على أساس جريمة يُعاقب عليها بمقتضى الأحكام الجزائية، الواردة سواءا بمقتضى قوانين

---

[1] – **Art.59 (a)** (code des obligations suisse de 30 mars 1911) : « 1- Le titulaire d'une clé de signature répond envers les **tiers** des dommages que ces derniers ont subis parce qu'ils se sont fiés à un **certificat qualifié** valable délivré par un fournisseur de services de certification **reconnu** au sens de la loi du 19 décembre 2003 sur la signature électronique.
2- Le titulaire de la clé de signature est libéré de sa responsabilité s'il peut établir de manière crédible qu'il a pris les mesures de sécurité raisonnablement imposées par les circonstances pour éviter une utilisation abusive de la clé de signature .
3- Le Conseil fédéral arrête les mesures de sécurité à prendre au sens de l'al. 2. »

[2] – **عبد الرزاق السنهوري**، مرجع سابق، ص ص 1540، 1541.

العقوبات أو بموجب القوانين الخاصة المنظمة للمعاملات والتجارة الإلكترونية، الذي على أساسها يتحمل المسؤولية الجزائية وفقا لمبدأ الشرعية الجزائية (التي سنراها لاحقا).

**ثانيا- مسؤولية الغير(Tiers) كطرف ثالث مُعوّل على شهادة التصديق الإلكتروني.**

تنص المادة 11 من قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية لعام 2001 على ما يلي:" **يتحمّل الطرف المعوّل التبعات القانونية الناجمة عن تخلفه عن:**
**(أ) اتخاذ خطوات معقولة للتحقّق من قابلية التعويل على التوقيع الالكتروني؛ أو**
**(ب) اتخاذ خطوات معقولة، إذا كان التوقيع الالكتروني مؤيّدا بشهادة، لأجل:**
**1- التحقّق من صلاحية الشهادة أو وقفها أو إلغائها؛**
**2- مراعاة وجود أي تقييد بخصوص الشهادة.**"

لذا فإنّ الطرف المعول يمكن أن تربطه أم لا تربطه علاقة تعاقدية بصاحب شهادة التصديق الإلكتروني وبـ(م.خ.ت.إ)، ففي كلتا الحالتين يتحمل المسؤولية المترتبة عن عدم إتباع الخطوات المعقولة للتحقق من قابلية التعويل على التوقيع الإلكتروني، وما إذا كان معززا بشهادة تصديق إلكتروني موصوفة من أجل التأكد من صلاحيتها ومن عدم تعليق أو إلغاء العمل بها مع مراعاة القيود المحددة فيها، ففي حالة تواجد علاقة عقدية بين الطرف المعول مع صاحب شهادة التصديق الإلكتروني فالمسؤولية تتوقف على طبيعة المعاملة التجارية المتفق عليها، أمّا إذا لم تربط الطرف المعول أية علاقة عقدية بمقدم الخدمة أو صاحب الشهادة، فيتحمل النتائج المترتبة عن عدم اتخاذ الخطوات المعقولة لتقدير قابلية التعويل على التوقيع الإلكتروني أو بشهادة التصديق الإلكتروني[1]، فمهما تخلف الطرف المعول عن الإمتثال لاشتراطات قابلية التعويل فلا ينبغي منع ذلك الطرف من إستخدام التوقيع أو شهادة التصديق الإلكتروني، وذلك إذا لم يكن التحقق المعقول من شأنه أن يكشف

---

[1] - **كامران الصالحي**، الطبيعة القانونية لمسئولية مزود خدمات التصديق، بحث مقدم في مؤتمر المعاملات الإلكترونية(التجارة الإلكترونية-الحكومة الإلكترونية) الذي نظمه مركز الإمارات للدراسات والبحوث الإستراتيجية المنعقد في دبي من 19 إلى 20 ماي 2009، بحوث المجلد الثاني، ص ص 655-652. http://www.slconf.uaeu.ac.aeslconf17arabic_prev_conf2009.asp

عدم صحة التوقيع أو الشهادة، كما أنّ المفهوم الواسع لعبارة "الطرف المعول" لا ينبغي أن يُؤدي إلى إلقاء إلتزام على عاتق صاحب شهادة التصديق الإلكتروني، بأن يتحقق من صحة الشهادة التي يشتريها من (م.خ.ت.إ) الموثوق به[1].

## الفرع الثالث

## الإعفاء من المسؤولية وتقييدها

إنّ الإتفاق على تعديل أحكام المسؤولية العقدية وفقا لمختلف التشريعات ليس فيه ما يُخالف النظام العام، لأنّه إذا كان العقد وليد حرية المتعاقدين فإنّ لهما الحرية في حق التعديل، وهذا ما نصت عليه المادة 178 من القانون المدني الجزائري: "**يجوز الإتفاق على أن يتحمل المدين تبعية الحادث المفاجئ أو القوة القاهرة. وكذلك يجوز الإتفاق على إعفاء المدين من أيّة مسؤولية تترتب عن عدم تنفيذ التزامه التعاقدي، إلاّ ما ينشأ عن غشه، أو عن خطئه الجسيم غير أنّه يجوز للمدين أن يشترط إعفاءه من المسؤولية الناجمة عن الغش، أو الخطأ الجسيم الذي يقع من أشخاص يستخدمهم في تنفيذ التزامه. ويبطل كل شرط يقضي بالإعفاء من المسؤولية الناجمة عن الفعل الإجرامي.**"

فمن خلال نص المادة يتضح لنا أنّه يمكن لأطراف عقد تقديم خدمة التصديق الإلكتروني الإتفاق على تعديل أحكام المسؤولية العقدية، وفقا لمبدأ الحرية التعاقدية سواءا بتشديدها أو التخفيف منها بَلْ قد يصل الأمر إلى الإعفاء منها، لذا يجوز الإتفاق على إعفاء المدين من أية مسؤولية تترتب على عدم تنفيذ التزامه التعاقدي، إلاّ في حالة الخطأ العمدي أو الجسيم الذي يُرتب مسؤوليته الشخصية، ممّا يؤدي إلى عدم جواز الإتفاق على الإعفاء أو التخفيف منها، كما يمكن للمدين أن يشترط إعفاءه من المسؤولية الناجمة عن الغش أو الخطأ الجسيم الذي يقع من أشخاص يستخدمهم في تنفيذ التزامه، وبالتالي فإذا كان التعديل يمس بأحكام المسؤولية العقدية فإنّ الأمر يختلف في المسؤولية التقصيرية الناجمة

---

[1] – دليل التشريع لقانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية لعام 2001، ص ص 82، 83. http://www.unicitral.org/pdf/Arabic/texts/selectcom/mt-elecsig/

عن العمل الإجرامي أي الفعل الغير المشروع، بحيث أجمع الفقه والقضاء ومختلف التشريعات على اعتبار شرط الإعفاء باطل ومخالف للنظام العام، غير أنّه يجوز الإتفاق على تشديدها لعدم مخالفته للنظام العام[1].

فعادة ما يشترط(م.خ.ت.إ) الإعفاء من المسؤولية التي يتحملها بالنسبة لحالات معينة أو يشترط تقييد هذه المسؤولية بقيود محددة، وبالتالي فإنّ شروط الإعفاء من المسؤولية أو تقييدها تأخذ عدّة صور، كتقييد المسؤولية بمبلغ معين لكل حادث أو عن كلّ مجموعة من الحوادث، أو إشتراط سقف أعلى للمسؤولية لا تتجاوزه سواء بتحديدها بمبلغ معين أو بنسبة محددة، كما يمكن استبعاد المسؤولية في حالة الضرر المتمثل في الكسب الفائت سواءا كان الضرر مباشرا أو غير مباشر أو استبعاد الأضرار العرضية، كما قد يمكن أن تقيد المسؤولية كذلك بحدّ معين من قيمة المعاملة التجارية التي تُستخدم من أجلها شهادة التصديق الإلكتروني، أو يقتصر التقييد على حالات معينة تُستخدم فيها الشهادة مع استبعاد حالات آخرى غير مُتفق عليها.

لذا أثير التساؤل حول أثر شروط تقييد المسؤولية على مضمون الإلتزام العقدي الذي تتحمله جهة التوثيق الإلكتروني، وبالخصوص الشروط التي تضع حدّا أقصى لقيمة التعامل الذي تُستخدم في شأنه شهادة التصديق الإلكتروني، وكذلك بالنسبة للشروط التي تُحدد الغرض من إستعمال الشهادة بقصر استعمالها في أغراض معينة أو استبعاد بعض طرق استعمالها، ففي حالة ما إذا تمثل التقييد في قصر المسؤولية على قيمة معينة للمعاملة المراد إنجازها فإنّ مخالفة هذا الشرط لا تؤدي إلى عدم قيام المسؤولية كُلِيَّةً وإنّما يقتصر أثر المخالفة على تقييد المسؤولية فقط، وعدم شمولها ما جاوز الحدّ المتفق عليه[2] وهذا ما يتفق مع نص المادة 4/06 من التوجيه الأوروبي رقم 99-93، المتعلق بالتوقيعات الإلكترونية

---

1) - **Philippe MALINVAUD, Dominique FENOUILLET**, pp. 581-583.

- **عبد الرزاق السنهوري**، مرجع سابق، ص ص 1370-1374.

2) - **إبراهيم الدسوقي أبو الليل**، مرجع سابق، ص ص 1886، 1887.

أمّا إذا كان الغير(Tiers) قد عوّل على الشهادة بالرغم من علمه بعدم صحة المعلومات التي تتضمنها فلا يكون هناك محل لقيام مسؤولية جهة التوثيق الإلكتروني.

تجدر الإشارة أنّ عقود تقديم خدمات التصديق الإلكتروني تنعدم فيها القدرة على مُساومة شروطها المُعدّة مُسبقا من طرف المُوجِب(م.خ.ت.إ)، الذي يستغل عادة الظروف الإقتصادية كذريعة لفرض بعض الشروط التعسفية على الطرف المعول(الضعيف) على شهادات التصديق الإلكتروني، وبالتالي فإنّ عدم التوازن في العلاقة العقدية يحتاج إلى حماية تشريعية وقضائية للطرف المُذعن من أجل إعادة التوازن العقدي المطلوب، لذا ألزم مشرع الإتحاد الأوروبي بموجب المادة 5/06 من التوجيه الأوروبي رقم 99-93 المتعلق بالتوقيعات الإلكترونية، الدول الأعضاء في الإتحاد الأوروبي على ضرورة الأخذ بعين الإعتبار أحكام التوجيه الأوروبي رقم 13/93 المؤرخ في 05 أفريل 1993 المتعلق بالبنود التعسفية في العقود المبرمة مع المستهلك[1]، كما نص المشرع الجزائري بموجب المادة 110 من القانون المدني الجزائري على أنّه، في حالة ما إذا تم إبرام العقد بطريقة الإذعان مُتضمنا شروطا تعسفية في بنوده، جاز للقاضي أن يُعدل هذه الشروط أو أن يُعفي الطرف المُذعن منها، ويُعد كلّ اتفاق يُخالف ذلك باطلا.

لحظر البنود التعسفية المفروضة على المستهلك كطرف ضعيف في العلاقة العقدية قام المشرع الجزائري بموجب المادة 06 من المرسوم التنفيذي رقم 06-306 المؤرخ في 10 سبتمبر 2006، المحدد للعناصر الأساسية للعقود المبرمة بين الأعوان الإقتصاديين والمستهلكين والبنود التي تعتبر تعسفية، بإنشاء لجنة البنود التعسفية ذات طابع استشاري تابعة لوزارة التجارة، مكلفة بمهمة البحث في كلّ العقود المبرمة بطريقة الإذعان والبنود ذات الطابع التعسفي، كما تقوم بنشر وتبليغ آرائها وتوصياتها بكل الوسائل الملائمة إلى الوزير المكلف بالتجارة عن كلّ دراسة أو خبرة، متعلقة بكيفية تطبيق العقود تجاه المستهلك أو إثر مباشرتها لكلّ عمل يدخل في مجال اختصاصها، والذي(الوزير) يتمتع بالسلطة التقديرية

---

1) – Directive 93/13/CEE du Conseil, du 5 avril 1993, concernant les clauses abusives dans les contrats conclus avec les consommateurs. http://www.eur-lesc.europa.eu

حول الأخذ أو عدم الأخذ بالتوصيات، فمن الضروري على اللجنة أن تبلغ آراءها أو توصياتها إلى السلطة الوطنية للتصديق الإلكتروني بصفتها كمراقب على نشاطات التصديق الإلكتروني في الجزائر، حول كلّ ما يتعلق بالبنود التعسفية الواردة في عقود تقديم خدمات التصديق الإلكتروني التي تُصادق على نماذجها مسبقا هذه السلطة، مع وجوب إضفاء المشرع الجزائري لهذه الآراء أو التوصيات طابع الإلزامية.

## المطلب الثاني

## الجزاءات المتعلقة بالتصديق الإلكتروني

نصت مختلف التشريعات الوطنية المنظمة للمعاملات والتجارة الإلكترونية على مجموعة من العقوبات المفروضة على أطراف التصديق الإلكتروني، والتي سنتطرق من خلالها إلى الجزاءات الإدارية في(الفرع الأول)، ثم إلى جزاء الإخلال بالإلتزامات القانونية والعقدية في (الفرع الثاني)، وأخيرا إلى مختلف الجزاءات العقابية المفروضة بموجب أحكام قوانين العقوبات أو التشريعات الخاصة بالمعاملات الإلكترونية(الفرع الثالث).

### الفرع الأول

### الجزاءات الإدارية

نصت مختلف القوانين الخاصة بتنظيم المعاملات ومبادلات التجارة الإلكترونية في أحكامها، على فرض جزاءات إدارية من جرّاء إرتكاب(م.خ.ت.إ) للمخالفات المتعلقة بالقواعد القانونية والتنظيمية لدفاتر الشروط المحددة لكيفيات وشروط ممارسة خدمات التصديق الإلكتروني، وذلك على غرار المشرع التونسي الذي نص بموجب الفصلين 44 و45 (الباب السابع) من قانون عدد 83-2000 المتعلق بالمبادلات والتجارة الإلكترونية، على جزاءات إدارية بعد معاينة المخالفات المرتكبة من طرف أعوان الضبط القضائي، لذا تقوم الوكالة الوطنية للمصادقة الإلكترونية(ANCE) بعد سماع (م.خ.ت.إ)، بسحب الترخيص منه مع إيقاف نشاطه في حالة إخلاله بواجباته المنصوص عليها بهذا القانون، أو بنصوصه

التطبيقية أو يعاقب بغرامة مالية تقدر بـ 1.000 إلى 10.000 دينار تونسي في حالة عدم مراعاته مقتضيات كراس الشروط المنصوص عليها في الفصل 12 من هذا القانون.

تجدر الإشارة أنّه يمكن للوزير المشرف على (و.و.م.إ) أن يجري الصلح في المخالفات التي يرتكبها المزود بشأن مقتضيات كرّاس الشروط المنصوص عليه في الفصل 12 من قانون المعاملات والمبادلات التجارية، أو المخالفات التي تمت معاينتها بموجب الفصل 49 من نفس القانون، وتكون الطرق والإجراءات المتبعة في الصلح وفقا للنصوص القانونية المنظمة للرقابة الإقتصادية وبالخصوص القانون عدد 64-1991 المتعلق بالمنافسة والأسعار بدون المساس بحقوق الغير، وتنقضي الدعوى العمومية بدفع المبلغ المحدد في عقد الصلح (الفصل 53 من قانون عدد 83-2000).

أمّا بالنسبة للمشرع المصري فقد نص بموجب المادة 26 من القانون رقم 15-2004 المتعلق بالتوقيع الإلكتروني وبإنشاء(هـ.ت.ص.ت.م)، على أنّه يمكن للهيئة(مع عدم الإخلال أحكام المادة 23 من القانون) في حالة ما إذا خالف المرخص له بإصدار شهادات تصديق إلكتروني شروط الترخيص، أو خالف أيّا من أحكام المادة 19 من نفس القانون أن تُلغي الترخيص وأن توقف سريانه إلى غاية زوال أسباب المخالفة، وذلك وفقا للقواعد والإجراءات المحددة بموجب اللائحة التنفيذية.

كما نص المشرع الجزائري هو الأخر بموجب المادة 64 من القانون رقم 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين[1] على جزاءات إدارية متعلقة بالمخالفات المرتكبة من طرف(م.خ.ت.إ)، ففي حالة عدم إحترام هذا الأخير لأحكام دفتر الشروط أو سياسة التصديق الإلكتروني الخاصة به والموافق عليها من طرف السلطة الإقتصادية(ARPT)، تفرض هذه الأخيرة على(م.خ.ت.إ) عقوبة مالية يتراوح مبلغها ما بين 200.000 دج إلى 5.000.000 دج، حسب تصنيف الأخطاء المنصوص عليه في دفتر

[1] – قانون رقم 15-04 مؤرخ في 01 فيفري 2015 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين.

الشروط الخاص بمؤدي الخدمات، وتُعْذِرُهُ بالامتثال لالتزاماته في مدة تتراوح بين ثمانية(8) أيّام وثلاثين(30) يوما حسب الحالة، وتبلّغ القرارات المتخذة ضد مؤدي الخدمات حتى يتسنى له تقديم مبرراته الكتابية ضمن الآجال المذكورة سابقا.

في حالة عدم امتثال مؤدي الخدمات للأعذار، تتخذ ضدّه (س.ض.ب.م) قرار سحب الترخيص الممنوح له وإلغاء شهادته حسب الحالة بعد موافقة السلطة الوطنية للتصديق الإلكتروني، وتحدد كيفيات تحصيل المبالغ المتعلقة بالعقوبة المالية المنصوص عليها في الفقرة الأولى من هذه المادة عن طريق التنظيم، ففي حالة إنتهاك(م.خ.ت.إ) للمقتضيات التي يتطلبها الدفاع الوطني والأمن العمومي تقوم سلطة(ARPT)، بالسحب الفوري للترخيص بعد موافقة السلطة الوطنية للتصديق الإلكتروني، وتكون تجهيزات(م.خ.ت.إ) مَحلّ تدابير تحفظية طبقا للتشريع المعمول به وذلك دون الإخلال بالمتابعات الجزائية(المادة 65 من نفس القانون).

## الفرع الثالث

## التعويض

يُعتبر التعويض الجزاء الذي يترتب على تحقق المسؤولية المدنية وبالتالي فإنّ التشريعات الخاصة بتنظيم المعاملات والتجارة الإلكترونية، قد أشارت فقط إلى ضرورة تعويض الضرر المتسبب للمضرور بفعل المسؤول، الذي أخل بالتزاماته العقدية أو القانونية ولم تتطرق إلى مسألة طرق تحديد وتقدير التعويض(Indemnité) الواجب منحه أو دفعه من طرف المسؤول عن الضرر، التي تركتها لقاضي الحكم الذي يفصل في التعويض وفقا للأحكام العامة للمسؤولية المدنية، ما لم تتفق الأطراف المعنية فيما بينها بتحديد التعويض اللازم مسبقا في العقد، وهذا ما أكدّه المشرع الجزائري في نص المادة 182 من القانون المدني الجزائري:" **إذا لم يكن التعويض مقدرا في العقد، أو في القانون فالقاضي هو الذي يقدره، ويشمل التعويض ما لحق الدائن من خسارة وما فاته من كسب، بشرط أن يكون هذا نتيجة طبيعية لعدم الوفاء بالإلتزام أو للتأخر في الوفاء به، ويعتبر الضرر نتيجة طبيعية إذا لم يكن في استطاعة الدائن أن يتوقاه ببذل جهد معقول، غير أنّه إذا كان**

**الإلتزام مصدره العقد، فلا يلتزم المدين الذي لم يرتكب غشا أو خطأ إلاّ بتعويض الضرر الذي كان يمكن توقعه عادة وقت التعاقد."**

إنطلاقا من ذلك يجوز للمتعاقدين أن يُحددا مقدما قيمة التعويض سواءا بالنص عليها في العقد أو في إتفاق لاحق، مع الأخذ بعين الإعتبار أحكام المواد 176 إلى 181 من القانون المدني، غير أنّه يمكن لقاضي الحكم أن يخفض مبلغ التعويض إذا أثبت المدين أنّ التقدير أو أنّ الإلتزام الأصلي قد نُفذ في جزء منه، كما يجوز له(القاضي) أن يُنقص مقدار التعويض أو لا يحكم بالتعويض إذا كان الدائن بخطئه قد اشترك في إحداث الضرر أو زاد فيه، فإذا جاوز الضرر قيمة التعويض المحدد في الإتفاق فلا يجوز للدائن الذي لم يشترك بخطئه في إحداث ذلك الضرر، أن يُطالب بأكثر من هذه القيمة إلاّ إذا أثبت أنّ المدين قد ارتكب غشا أو خطأ جسيما[1].

لذا اشترطت مختلف التشريعات الأجنبية والعربية أن يكون التعويض عادل ومنصف وهذا ما نصت عليه المادة 1153-1 من التقنين المدني الفرنسي، التي اشترطت في كلّ المواد أن يتضمن حكم التعويض مصلحة عادلة ومنصفة في التقدير حتى في حالة غياب طلب أو حكم خاص بذلك، وباستثناء ما يخالف القانون يبدأ سريان المفعول القانوني للتعويض بإصدار منطوق الحكم إلاّ إذا قرّر القاضي غير ذلك، ففي حالة إثبات قاضي الإستئناف بموجب قرار التعويض الضرر بصفة عادلة ومنصفة، فيسري مفعوله(التعويض) إبتداءا من صدور حُكْمِ المحكمة الابتدائية، فالتعويضات المستحقة بموجب المادة 1149 من نفس القانون تشمل عادة ما لحق الدائن من خسارة وما فاته من كسب، إلاّ إذا نص القانون على غير ذلك[2].

---

[1] – راجع المواد 177، 183-185، من الأمر رقم 58/75 المؤرخ في 26 سبتمبر 1975، المتضمن القانون المدني، المعدل والمتمم.

[2] – **Art.1149** du code civil français. http://www.legifrance.gouve.fr
« - Les dommages et intérêts dus au créancier sont, en général, de la perte qu'il a faite et du gain dont il a été privé, sauf les exceptions et modifications ci-après. »
-**Art.1153-1** : « - En toute matière, la condamnation à une indemnité emporte intérêts au taux légal même en l'absence de demande ou de disposition spéciale du jugement. Sauf disposition

كما نص المشرع الفيدرالي السويسري بموجب المادة 2-1/42 من قانون الإلتزامات السويسري(CO) على أنّه، في حالة عدم إتفاق الأطراف حول تقدير مبلغ التعويض يُحدد هذا الأخير، من طرف القاضي بصفة عادلة ومنصفة مع الأخذ بعين الإعتبار الظروف المحيطة بالطرف المتضرر، كما سمحت المادة 2-1/43 من نفس القانون لقاضي الحكم بتحديد طرق التعويض وفقا للظروف وجسامة الأخطاء، فإذا كانت طريقة التعويض في شكل إيراد مرتبا ألزم القانون الدائن بتقديم تأمينات كافية[1].

بالإضافة إلى ما سبق اشترطت التشريعات العربية بدورها أن تكون طرق تقدير التعويضات عادلة ومنصفة وفقا للأحكام العامة للمسؤولية، لذا سمح المشرع المصري بموجب المادة 170 من القانون المدني للقاضي، إمكانية تقدير مدى التعويض عن الضرر الذي لحق بالمضرور وفقا للمادتين 221 و222 من نفس القانون مع مراعاته في ذلك الظروف الملابسة، فإذا لم يَتَيَّسَرْ له وقت الحكم أن يُعيّن مدى التعويض تعيينا نهائيا، يحق للمضرور أن يُطالبَ خلال مدة معينة بإعادة النظر في تقدير التعويض، وبالتالي فإذا لم يكن التعويض مقدرا في العقد أو بنص في القانون فالقاضي هو الذي يملك السلطة في تقديره ويجب في هذه الحالة، أن يشتمل التعويض ما لحق الدائن من خسارة وما فاته من كسب، بشرط أن يكون الضرر المتسبب نتيجة طبيعية لعدم الوفاء بالإلتزام أو للتأخر في الوفاء به ولم يستطيع الدائن أن يتفاداه ببذل جهدٍ معقول، فإذا كان الإلتزام مصدره العقد فلا

---

contraire de la loi, ces intérêts courent à compter du prononcé du jugement à moins que le juge n'en décide autrement. - En cas de confirmation pure et simple par le juge d'appel d'une décision allouant une indemnité en réparation d'un dommage, celle-ci porte de plein droit intérêt au taux légal à compter du jugement de première instance.
Dans les autres cas, l'indemnité allouée en appel porte intérêt à compter de la décision d'appel. Le juge d'appel peut toujours déroger aux dispositions du présent alinéa. »

[1] – **Art.42** (code des obligations suisse) : « **1-** La preuve du dommage incombe au demandeur.
**2-** Lorsque le montant exact du dommage ne peut être établi, le juge le détermine équitablement en considération du cours ordinaire des choses et des mesures prises par la partie lésée. »
-**Art.43/1-2** : « **1-** Le juge détermine le mode ainsi que l'étendue de la réparation , d'après les circonstances et la gravité de la faute.
**2-** Des dommages-intérêts ne peuvent être alloués sous forme de rente que si le débiteur est en même temps astreint à fournir des sûretés. » http://www.admin.chopcfrclassified-compilation/

يلتزم المدين الذي لم يرتكب غشًّا أو خطأ جسيم إلاّ بتعويض الضرر الذي كان يمكن توقعه عادة وقت التعاقد، ويشمل كذلك التعويض الضرر الأدبي إذا طلب الدائن بذلك أمام القضاء أو إذا تحدد ذلك بمقتضى إتفاق[1].

أما بالنسبة للمشرع الجزائري فقد نقل حرفيا نص المادة 170 من القانون المصري وذلك أثناء صياغته لنص المادة 131 من القانون المدني، التي بموجبها منح للقاضي إمكانية تقدير مدى التعويض عن الضرر الذي لحق المصاب وفقا لأحكام المادتين 182 و182 مكرر مراعيا في ذلك الظروف المُلابسة، فإذا لم يتيسر له وقت الحكم تقدير قابلية التعويض بصفة نهائية، يحق للمضرور في أن يُطالبَ خلال مدة معينة بإعادة تقدير التعويض، ففي حالة ما إذا لم يكن التعويض مقدرا بموجب القانون أو العقد فالقاضي هو الذي يقدره على أن يشمل التعويض ما لحق الدائن من خسارة وما فاتحه من كسب، بشرط أن يكون الضرر المتسبب نتيجة طبيعية لعدم الوفاء بالإلتزام، أو للتأخر في الوفاء به مع عدم إمكانية الدائن أن يتفاداه ببذل جهد معقول، غير أنّه إذا كان الإلتزام مصدره العقد فلا يلتزم المدين الذي لم يرتكب غشًّا أو خطأ جسيم إلاّ بتعويض الضرر الممكن توقعه وقت التعاقد.

تجدر الإشارة أنّ المادتين 171 من القانون المدني المصري و132 من القانون المدني الجزائري، قد سمحتا للقاضي بتحديد طرق تقدير التعويض تبعا للظروف، إذ يَصِحُّ أن يكون التعويض مقسطا أو أن يكون في شكل إيراداً مُرَتَباً مع إلزام المدين في كلتا الحالتين بأن يقدر تأمينا، ويجوز للقاضي أن يُقدر التعويض النقدي تبعا للظروف بناءا على طلب المضرور أو أن يأمر بإعادة الحالة إلى ما كانت عليه، أو أن يحكم ببعض الإعانات التي تتصل بالفعل الغير المشروع.

فمن خلال المواد السابقة يتضح لنا أنّه في حالة ما إذا لم يدرج عقد تقديم خدمة التصديق الإلكتروني لأحكام حول التعويض، يفصل القاضي بإحدى طرق التعويض التي

---

[1] – **عبد الرزاق السنهوري**، مرجع سابق، ص ص 1357–1360.

يراها مناسبة وفقا للظروف التي على إثرها يُقَرَّرْ التعويض العيني أو بمقابل، في حين يعتبر الأول من أفضل طرق التعويض التي تؤدي إلى إصلاح الضرر إصلاحا تاما عن طريق إعادة الحالة إلى ما كانت عليه، وهذا ما نجده خاصة في الإلتزامات العقدية بشرط أن يكون ممكنا وأن يطلبه الدائن أو يتقدم به المدين، أمّا التعويض بالمقابل غالبا ما يكون نقدا كما يجوز أن يكون كذلك غير نقدي إذا كان الضرر أدبي، كأن يعمل القاضي بنشر الحكم الذي قضى بإدانة المدعى عليه في الصحف أو بأداء بعض الإعانات عندما يتعلق الأمر بالعمل الغير المشروع، غير أنّ التعويض النقدي هو الغالب في المسؤولية التقصيرية والأكثر ملائمة لإصلاح الضرر الناتج عن الفعل الغير المشروع فأصبح بمقدور القاضي من تقويم الضرر الأدبي نقدًا[1]، وبالتالي فمن المُمْكِنِ على جهة التوثيق الإلكتروني أن تلتزم بالتعويض المقابل للضرر المسبب للطرف المعول على شهادة التصديق الإلكتروني سواءا كان المُوقِّع بذاته أو الغير، في حالة تأمين مسؤوليتها المدنية لدى شركة التأمين.

من بين إيجابيات التعويض بالمقابل نجد إمكانية المسؤول(المدين) عن الضرر بدفع مبلغ المال دفعة واحدة للمضرور أو يدفعه على أقساط، أو يحكم القاضي بدفع مبلغ التعويض في شكل إيراد مرتب مع إلزام المسؤول بتقديم تأمين، أو يأمر بإيداع المبلغ الكافي لضمان الوفاء بالإيراد المحكوم به، ففي حالة إلتزام شركة التأمين بدفع التعويض اللازم للمضرور(الطرف المعول)، لا يجب على هذا الأخير الذي تحصل على التعويض أن يرجع بعد ذلك على المسؤول(م.خ.ت.إ) بتعويض آخر، إلاّ في حالة عدم تَمَكُّنِهِ من الحصول على تعويض كامل من شركة التأمين فيرجع بالتالي على المسؤول بما يَكْمِلُ التعويض، وفي كلّ الأحوال لا يُلزم الشخص الطبيعي أو المعنوي بتعويض الضرر إذا أثبت أنّ هذا الأخير(الضرر) قد نشأ عن سبب لا يد له فيه، كحادث مفاجئ أو قوة قاهرة أو خطأ صدر من المضرور أو خطأ من الغير، ما لم يوجد نص قانوني أو إتفاق يُخالف ذلك[2].

---

[1] – **عبد الرزاق السنهوري**، مرجع سابق، ص ص 1355، 1356.

[2] – **Art.1148** (Code Civil Français) : « Il n'y a lieu à aucuns dommages et intérêts lorsque, par suite d'une force majeure ou d'un cas fortuit, le débiteur a été empêché de donner ou de faire ce à quoi il était obligé, ou a fait ce qui lui était interdit. »

لذا يسقط حق المضرور في طلب حق التعويض بتقادم دعوى التعويض الناشئة عن العمل الغير المشروع حسب المُدَّة المُقَرَّرَة في كلِّ تشريع، فقد حددتها المادة 60 من قانون الإلتزامات السويسري(CO)، بسنة إبتداءا من التاريخ الذي عَلِمَ فيه الطرف المضرور بالضرر وبالشخص المُسَبِّبِ له، وبعشرة سنوات(10) تبدأ من تاريخ إرتكاب الضرر، فإذا كانت الدعوى ناشئة عن جريمة وكانت الدعوى الجنائية لم تتقادم بَعْدْ بالرغم من سقوط الدعوى المدنية، فدعوى التعويض لا تسقط إلاّ بسقوط الدعوى الجنائية[1]، وتسقط دعوى التعويض وفقا للمادة 133 من القانون المدني الجزائري بإنقضاء خمس عشرة(15) سنة تسري من يوم وقوع الفعل الضار، وتسقط كذلك بسقوط الدعوى الجنائية إذا كانت دعوى التعويض ناشئة عن جريمة (المشرع الجزائري لم يذكر الحالة الأخيرة في نص المادة 133).

## الفرع الرابع

## العقوبات الجزائية

فرضت التشريعات المنظمة للمعاملات الإلكترونية مجموعة من العقوبات التي تُمكِّن الطرف المضرور من تأسيس دعوى المسؤولية الجزائية، عند رفعها أمام الجهة القضائية المختصة ضد الطرف المسؤول عن الضرر(شخصا طبيعيا أم معنويا)، فوفقا لنص المادة

---

– المادة 127 من القانون المدني الجزائري: "إذا أثبت الشخص أنّ الضرر قد نشأ عن سبب لا يد له فيه كحادث مفاجئ، أو قوة قاهرة، أو خطأ صدر من المضرور أو خطأ من الغير، كان غير ملزم بتعويض هذا الضرر، ما لم يوجد نص قانوني أو اتفاق يخالف ذلك."

1) - **Art. 60** du code des obligations suisse : « **1**- L'action en dommages-intérêts ou en paiement d'une somme d'argent à titre de réparation morale se **prescrit par un an à compter du jour où la partie lésée a eu connaissance du dommage ainsi que de la personne qui en est l'auteur,** et, dans tous les cas, par **dix ans dès le jour où le fait dommageable s'est produit** .
**2**- Toutefois, si les dommages-intérêts dérivent d'un acte punissable soumis par les lois pénales à une prescription de plus longue duré, cette prescription s'applique à l'action civile .
**3**- Si l'acte illicite a donné naissance à une créance contre la partie lésée, celle-ci peut en refuser le paiement lors même que son droit d'exiger la réparation du dommage serait atteint par la prescription. » http://www.admin.chopcfrclassified-compilation/
- **voir aussi** l'article 18 du (LFSCSE 2003). http://www.admin.chopcfrclassified-compilation20011277index.html

35-I من القانون الفرنسي رقم 2004-575 المؤرخ في 21 جوان 2004 المتعلق بالثقة في الإقتصاد الرقمي، يُعاقب بعقوبة الحبس لمدة سنة(01) وبغرامة مالية تقدر بـ15000 أورو، كلّ من لم يُراعي الإجراءات المتعلقة بتوريد أو تحويل أو استيراد أو تصدير وسائل أو معدات التشفير، وتُضاعف كلّ من عقوبة الحبس لمدة عامين(02) والغرامة المالية إلى 30000 أورو، في حالة ما إذا تم تصدير أو تحويل هذه المعدات إلى إحدى دول الإتحاد الأوروبي، من دون الحصول على ترخيص مُسبق من طرف الوزير الأول، كما يتحمل الشخص المعنوي بموجب الفقرة(V) من نفس المادة(35) المسؤولية الجزائية وفقا للحالات المذكورة في المادة 121-2 من قانون العقوبات الفرنسي[1].

تضيف المادة 132-79 من قانون العقوبات الفرنسي المعدلة بموجب المادة 37 من قانون الثقة في الإقتصاد الرقمي، على أنّه في حالة إستعمال معدّات أو وسائل التشفير بمفهوم نص المادة 29 من القانون رقم 2004-575 المتعلق بالثقة في الإقتصاد الرقمي[2] لتحضير، أو إرتكاب جناية أو جنحة، أو لتسهيل تحضيرها أو إرتكابها، يُعاقب بإحدى

---

1) – Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique. http://www.legifrance.gouve.fr/

**-Art.35:** « **I.**- Sans préjudice de l'application du code des douanes: **1-** Le fait de ne pas satisfaire à l'obligation de déclaration prévue à **l'article 30** en cas de fourniture, de transfert, d'importation ou d'exportation d'un moyen de cryptologie ou à l'obligation de communication au Premier ministre prévue par ce même article est puni d'un an d'emprisonnement et de 15 000 € d'amende;

**2-** Le fait d'exporter un moyen de cryptologie ou de procéder à son transfert vers un État membre de la Communauté européenne sans avoir préalablement obtenu l'autorisation mentionnée à l'article 30 ou en dehors des conditions de cette autorisation, lorsqu'une telle autorisation est exigée, est puni de deux ans d'emprisonnement et de 30 000 € d'amende. »

**« V.** - Les personnes morales sont responsables pénalement, dans les conditions prévues par l'article 121-2 du code pénal, des infractions prévues au présent article. Les peines encourues par les personnes morales sont : **1-** L'amende, suivant les modalités prévues par l'article 131-38 du code pénal;

**2-** Les peines mentionnées à l'article 131-39 du code pénal. »

2) – **Art.29** (Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique): « On entend par moyen de cryptologie tout matériel ou logiciel conçu ou modifié pour transformer des données, qu'il s'agisse d'informations ou de signaux, à l'aide de conventions secrètes ou pour réaliser l'opération inverse avec ou sans convention secrète. Ces moyens de cryptologie ont principalement pour objet de garantir la sécurité du stockage ou de la transmission de données, en permettant d'assurer leur confidentialité, leur authentification ou le contrôle de leur intégrité. On entend par prestation de cryptologie toute opération visant à la mise en œuvre, pour le compte d'autrui, de moyens de cryptologie. »

العقوبات السالبة للحرية بِحَسَبِ الجريمة المرتكبة، وبالتالي فقد يعاقب إمّا بالسجن المؤبد (إذا كانت الجريمة مُعاقب عليها بالسجن لمدة 30 سنة)؛ أو السجن لمدة 30 سنة (إذا كانت الجريمة مُعاقب عليها بالسجن لمدة 20 سنة)؛ أو بالسجن لمدة 20 سنة (إذا كانت الجريمة مُعاقب عليها بالسجن لمدة 15 سنة)؛ أو بالسجن لمدة 15 سنة (إذا كانت الجريمة مُعاقب عليها بالسجن لمدة 10 سنة)؛ أو بالسجن لمدة 15 سنة (إذا كانت الجريمة مُعاقب عليها بالسجن لمدة 20 سنة)؛ أو بالحبس لمدة 07 سنة (إذا كانت الجريمة مُعاقب عليها بالحبس لمدة 05 سنوات)؛ أو بالحبس لمدة (02) عامين في حالة ما إذا كانت الجريمة مُعاقب عليها بالحبس لمدة 03 سنوات على الأكثر، كما يُعفى كلّ من الفاعل أو الشريك في إرتكاب الجريمة من تطبيق أحكام هذه المادة بطلبٍ من السلطة القضائية أو الإدارية، في حالة ما إذا قاموا بتسليم الرسالة المشفرة بدقة مع الإتفاقات السرية الضرورية لفك التشفير.

كما يعاقب كلّ من يدخل أو يبقى عن طريق الغش في كلّ أو جزء من منظومة المعالجة الآلية للمعطيات، بالحبس لمدة(02)عامين وبغرامة مالية مُقدرة بـ 30000 أورو فإذا قام بحذف أو تغيير المعطيات التي تحتويها المنظومة أو تعطيل نظامها، فيعاقب المجرم بالحبس لمدة ثلاثة(03) سنوات مع غرامة مالية مقدرة بـ 45000 أورو، فإذا أُرتكبت هذه الجرائم على حساب أنظمة المعالجة الآلية للمعطيات تابعة للدولة، فيُعاقب الفاعل بعقوبة الحبس لمدة 05 سنوات وبغرامة مالية تُقدر بـ 75000 أورو(المادة 323-1 من نفس القانون)، ويعاقب بنفس العقوبة وفقا للفقرة الثانية من نفس المادة(323-2) كلّ من عرقل أو غيّر منظومة المعالجة الآلية للمعطيات، وترتفع كلّ من عقوبة الحبس إلى سبعة(07) سنوات والغرامة المالية إلى 100000 أورو، في حالة ما إذا كان نظام المعالجة الآلية للمعطيات تابع للدولة، وكلّ من أدخل بطريق الغش معطيات في نظام المعالجة الآلية للمعطيات أو أزال أو عدّل عن طريق الغش المعطيات التي يتضمنها، يعاقب بموجب الفقرة الثالثة من نفس المادة (323-3) بالحبس لمدة خمسة(05) سنوات وبغرامة مالية تُقدر بـ 75000 أورو، وإذا أُرتكبت تلك الجريمة على حساب نظام المعالجة الآلية للمعطيات تابع للدولة، فتكون عقوبة الحبس لمدة سبعة(07) سنوات وغرامة مالية تقدر بـ100000 أورو[1].

---

1) – **Art. 323-1** du code pénal Français. http://www.legifrance.gouve.fr

أمّا المشرع الفيدرالي السويسري فقد نص هو الأخر في قانون العقوبات المؤرخ في 12 ديسمبر 1937 المعدل والمتمم، على مجموعة من الجزاءات العقابية ذات صلة بخدمات التصديق الإلكتروني، فوفقا لنص المادتين 143 و143 مكرر منه، يُعاقب بالعقوبة السالبة للحرية لمدة ثلاثة(03) سنوات على الأكثر أو بغرامة مالية، كلّ من يستولي على البيانات الإلكترونية المحمية والمسجلة، أو التي تم تبادلها سواءا لخدمة مصالحه الشخصية أو يضعها تحت تصرف الغير، أو يدخل بغير حقّ إلى منظومة إرسال البيانات الإلكترونية لنظام معلوماتي محمي تابع للغير، أو يستعمل أو يكشف عن رقم سرّي محمي أو برنامج أو معطيات إلكترونية، من أجل القيام بارتكاب الجريمة تحت علمه أو عن طريق الشبهة.

بالإضافة إلى ذلك يُعاقب بموجب الفقرة الأولى من المادة 144 مكرر، كلّ من يقوم بطريقة غير شرعية بإزالة أو تعديل أو إتلاف البيانات الإلكترونية المُسجلة أو التي تم تبادلها إلكترونيّاً أو قام بذلك بأية وسيلة مماثلة، بالعقوبة السالبة للحرية لمدة ثلاثة(03) سنوات على الأكثر أو بغرامة مالية، ويُمكن للقاضي أن يحكم بعقوبة سالبة للحرية من سنة(01) إلى خمسة(05) سنوات وذلك في حالة ما إذا تسبب الفاعل بإلحاق أضرار جسيمة أو معتبرة، وكلّ من صنع أو استورد أو وضع حيّز الاستعمال أو منح أو سهّل عملية صنع، أو

---

« Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30000 euros d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45000 euros d'amende.
Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État, la peine est portée à cinq ans d'emprisonnement et à 75 000 € d'amende. »

- **Art. 323-2** : « Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75000 euros d'amende.
Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État, la peine est portée à sept ans d'emprisonnement et à 100 000 € d'amende. »

- **Art. 323-3** : « Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75000 euros d'amende. Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État, la peine est portée à sept ans d'emprisonnement et à 100 000 € d'amende. »

جعل بأيّة طريقة إستخدام البرامج المعلوماتية التي يعلم أو كان يُشكك في استعمالها لغرض إرتكاب الجريمة، يُعاقب بموجب الفقرة الثانية من نفس المادة(144 مكرر2)، بالعقوبة السالبة للحرية لمدة ثلاثة(03) سنوات على الأكثر أو بغرامة مالية، وفي كلّ الظروف يمكن للقاضي أن يحكم بالعقوبة السالبة للحرية من سنة(01) إلى خمسة(05) سنوات في حالة ما إذا جعل الفاعل من هذه الأفعال مهنة له.

كما يعاقب بغرامة مالية كلّ من قام بطريق الغش صناعة أو استيراد أو تصدير أو نقل أو أدخل إلى السوق، أو قام بتثبيت تجهيزات أو برامج معالجة المعطيات من أجل إستخدامها لغرض فكّ شفرات الخدمات المؤمنة،(المادة 150 مكرر من نفس القانون) وكلّ من يَدخُل بطريقة غير شرعية إلى منظومة المعالجة الآلية للمعطيات الشخصية، يُعاقب بموجب المادة 179 مكرر7 بالعقوبة السالبة للحرية لمدة ثلاثة(03) سنوات على الأكثر أو بغرامة مالية[1].

---

1) - Code pénal suisse du 21 décembre 1937 (état le 1er janvier 2014). http://www.admin.chopcfrclassified-compilation/

- **Art.143**: « 1- Celui qui, dans le dessein de se procurer ou de procurer à un tiers un enrichissement illégitime, aura soustrait, pour lui-même ou pour un tiers, des données enregistrées ou transmises électroniquement ou selon un mode similaire, qui ne lui étaient pas destinées et qui étaient spécialement protégées contre tout accès indu de sa part, sera puni d'une peine privative de liberté de cinq ans au plus ou d'une peine pécuniaire.
2- La soustraction de données commise au préjudice des proches ou des familiers ne sera poursuivie que sur plainte. »

- **Art.143 bis** : « 1- Quiconque s'introduit sans droit, au moyen d'un dispositif de transmission de données, dans un système informatique appartenant à autrui et spécialement protégé contre tout accès de sa part est, sur plainte, puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire…
2- Quiconque met en circulation ou rend accessible un mot de passe, un programme ou toute autre donnée dont il sait ou doit présumer qu'ils doivent être utilisés dans le but de commettre une infraction visée à l'al. 1 est puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire. »

- **Art.144 bis** : « 1- Celui qui, sans droit, aura modifié, effacé, ou mis hors d'usage des données enregistrées ou transmises électroniquement ou selon un mode similaire sera, sur plainte, puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire.
Si l'auteur a causé un dommage considérable, le juge pourra prononcer une peine privative de liberté de un à cinq ans. La poursuite aura lieu d'office.
2- Celui qui aura fabriqué, importé, mis en circulation, promu, offert ou d'une quelconque manière rendu accessibles des logiciels dont il savait ou devait présumer qu'ils devaient être utilisés dans le but de commettre une infraction visée au ch. 1, ou qui aura fourni des

نص المشرع التونسي بموجب الباب السابع من قانون عدد 83-2000 المتعلق بالمبادلات والتجارة الإلكترونية، على مجموعة من العقوبات حسب درجة الجريمة (جنحة، جناية) المسلطة على أطراف التصديق الإلكتروني، وبالتالي يُعاقب كلّ من يمارس نشاط (م.خ.ت.إ) بدون الحصول على ترخيص مُسبق طبقا للفصل 11 من هذا القانون بالسجن لمدة تتراوح بين شهرين(02) وثلاثة(03) سنوات، وبغرامة تتراوح بين 1.000 و10.000 دينار تونسي أو بإحدى هاتين العقوبتين(الفصل 46 منه)، ويُعاقب كذلك طبقا للفصل 254 من المجلة الجنائية المزود وأعوانه الذين يفشون أو يحثون أو يشاركون في إفشاء المعلومات التي عُهدت إليهم في إطار ممارسة نشاطهم، بإستثناء تلك التي رخص بها صاحب الشهادة كتابيا أو إلكترونيا في نشرها أو الإعلام بها، أو في الحالات المنصوص عليها في التشريع الجاري به العمل(الفصل 52 منه)، وفي حالة مخالفة المزود لأحكام الفصلين 38 و39 المتعلقين بمعالجة المعطيات الشخصية، يُعاقب بغرامة مالية تتراوح بين 1.000 و10.000 دينار تونسي(الفصل 51 منه).

بالإضافة إلى ذلك يعاقب كلّ من صرّح عمدًا بمُعطيات خاطئة لـ(م.خ.ت.إ) ولكافة الأطراف التي طلب منها أن تثق بتوقيعه الإلكتروني، أو استعمل بصفة غير مشروعة عناصر تشفير شخصية متعلقة بالتوقيع الإلكتروني للغَيْرِ، بالسجن لمدة تتراوح بين ستة(6) أشهر وعامين(02)، وبغرامة تتراوح بين 1.000 و10.000 دينار تونسي أو بإحدى هاتين العقوبتين(الفصل 47 و48 منه)، وكلّ من استغل ضُعْفُ أو جُهْلَ شخص في إطار عمليات البيع الإلكتروني بدفعه للالتزام حاضرا أم آجلا بأيّ شكل من الأشكال، يعاقب بغرامة مالية

---

indication en vue de leur fabrication, sera puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire.
Si l'auteur fait métier de tels actes, le juge pourra prononcer une peine privative de liberté de un à cinq ans. »

**-150 bis** : « **1-** Celui qui aura fabriqué, importé, exporté, transporté, mis sur le marché ou installé des appareils dont les composants ou les programmes de traitement des données servent à décoder frauduleusement des programmes de télévision ou des services de télécommunication cryptés ou sont utilisés à cet effet sera, sur plainte, puni de l'amende.
**2-** La tentative et la complicité sont punissables. »

**-Art.179 novies** : « - Celui qui aura soustrait d'un fichier des données personnelles sensibles ou des profils de la personnalité qui ne sont pas librement accessibles sera, sur plainte, puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire. »

تتراوح بين 1.000 و20.000 دينار تونسي، وذلك إذا تم الإثبات من ظروف الواقعة أنّ هذا الشخص غير قادر على تمييز أبعاد تعهداته أو كشف الحِيل والخِدع المعتمدة بالإلتزام أو إذا كان تحت الضغط مع مراعاة أحكام المجلة الجنائية(الفصل 50 منه) [1].

أما بالنسبة للمشرع المصري فقد نص هو الأخر على مجموعة من العقوبات الجزائية في القانون رقم 15-2004، المتعلق بتنظيم التوقيع الإلكتروني وبإنشاء(هـ.ت.ص.ت.م) وذلك من دون الإخلال بأية عقوبة أشد منصوص عليها في قانون العقوبات أو في أيّ قانون آخر، بحيث نص في المادة 23 منه على عقوبة الحبس وبغرامة لا تقل عن 10000 جنيه لا تتجاوز 100000 جنيه أو بإحدى هاتين العقوبتين، كلٌّ من أصدر شهادة تصديق إلكتروني دون الحصول على ترخيص بمزاولة النشاط من الهيئة، أو أتلف أو عيب توقيعا أو وسيطا أو مُحَرِّرًا إلكترونيا أو زور شيئا من ذلك بطريق الاصطناع، أو التعديل أو التحرير أو بأيّ طريق آخر، أو استعمل توقيعا أو وسيطا أو محررا إلكترونيا معيبا، أو مزورا مع علمه بذلك أو خالف أيًّا من أحكام المادتين 19 و21 من هذا القانون، أو توصل بأية وسيلة إلى الحصول بغير حق على توقيع أو محرّر إلكتروني أو اخترق هذا الوسيط أو اعترضه أو عَطَّلَهُ عن أداء وظيفته.

كما يعاقب كذلك على مخالفة المادة 13 من هذا القانون بغرامة لا تقل عن 5000 جنيه لا تتجاوز عن 50000 جنيه، وفي حالة العود(Récidive) تزاد بمقدار المثل هذه الجرائم في حديها الأدنى والأقصى، وفي جميع الأحوال يُحكم بنشر حكم الإدانة في جريدتين يوميتين واسعتي الانتشار، وعلى شبكات المعلومات الإلكترونية المفتوحة على نفقة المحكوم عليه، كما نصت المادة 24 من نفس القانون على معاقبة المسؤول عن الإدارة الفعلية للشخص الاعتباري المخالف، بذات العقوبات المقررة عن الأفعال التي ترتكب بالمخالفة لأحكام هذا القانون، إذا كان إخلاله بالواجبات التي تفرضها عليه الإدارة قد ساهم في وقوع

---

[1] – قانون عدد 83 لسنة 2000 مُؤرخ في 9 أوت 2000 يتعلق بالمبادلات والتجارة الإلكترونية. http://www.legislation.tn

– **عبد المنعم كيوة**، الإطار القانوني للإمضاء والمصادقة الإلكترونية، ص ص 23-25. مقال منشور على الموقع التالي: http://www.ism-justice.nat.tn

الجريمة مع علمه بذلك، ويكون الشخص المعنوي في هذه الحالة مسؤولا بالتضامن عن الوفاء بما يحكم به من عقوبات مالية وتعويضات، إذا كانت المخالفة قد ارتكبت من أحد العاملين به وباسم ولصالح الشخص المعنوي.

أمّا بالنسبة للمشرع الجزائري فبدوره نص في قانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 66-156 المؤرخ في 08 جويلية 1966 الذي يتضمن قانون العقوبات[1]، وبالخصوص في القسم السابع مكرر منه، على مجموعة من العقوبات الجزائية ذات صلة بخدمات التصديق الإلكتروني، وذلك تماشيا مع التطور التكنولوجي والعلمي في مجال تقنيات المعلومات، والمتمثلة في:

**أ)**- كلّ من يدخل أو يبقى عن طريق الغش في كلّ أو جزء من منظومة المعالجة الآلية للمعطيات أو يُحاول ذلك، يُعاقب بالحبس من ثلاثة(03) أشهر إلى سنة(01)، وبغرامة من 50.000 دج إلى 100.000 دج ، وتُضاعف العقوبة في حالة ما إذا ترتب عن ذلك حذف أو تغيير معطيات المنظومة، وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام تشغيل منظومة المعالجة الآلية للمعطيات، تكون العقوبة الحبس من ستة(06) أشهر إلى سنتين(02) وغرامة مالية من 50.000 دج إلى 150.000 دج(المادة 394 مكرر)؛

**ب)**- كلّ من أدخل بطريق الغش مُعطيات في نظام المعالجة الآلية أو أزال أو عدّل بطريق الغش المعطيات التي يتضمنها، يُعاقب بالحبس من ستة(06) أشهر إلى ثلاثة(03) سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج (المادة 394 مكرر 1)؛

**ج)**- كلّ من يقوم عمداً وعن طريق الغش بتصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مُخزنة أو معالجة، أو مرسلة عن طريق منظومة معلوماتية أو حيازة أو إفشاء أو نشر أو إستعمال لأيّ غرض يُمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم، يعاقب بالحبس من شهرين(02) إلى ثلاثة(03) سنوات وبغرامة من 1.000.000 دج إلى 5.000.000 دج، وتُضاعف العقوبات المنصوص عليها في هذا

---

[1] – أمر رقم 66-156 مؤرخ في 08 جويلية 1966 يتضمن قانون العقوبات، معدل ومتمم.

القسم إذا استهدفت الجريمة الدفاع الوطني أو الهيئات أو المؤسسات الخاضعة للقانون العام دون الإخلال بعقوبات أشدّ(المادتين 394 مكرر2، و394 مكرر3)؛

**د)**- يُعاقب الشخص المعنوي الذي ارتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة مالية تُعادل خمس(05) مرّات الحدّ الأقصى للغرامة المُقررة للشخص الطبيعي(المادة 394 مكرر4)؛

**هـ)**- كلّ من شارك في مجموعة أو في إتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا التحضير مجسدا بفعل أو عِدَّةِ أفعال مادية، يعاقب بالعقوبات المُقررة للجريمة ذاتها(المادة 394 مكرر5)؛

**و)**- يُحكم بمُصادرة الأجهزة والبرامج والوسائل المُستخدمة مع إغلاق المَوَاقِعْ التي تكون محلاً لجريمة من الجرائم المُعاقب عليها وفقا لهذا القسم، مع إغلاق المحلّ أو مكان الإستغلال إذا كانت الجريمة قد أُرتكبت بعلم مالكها، مع الإحتفاظ بحقوق الغير حسن النيّة ويُعاقب على الشروع في إرتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المُقرّرة للجنحة ذاتها. (المادتين 394 مكرر6، و394 مكرر7)

تجدر الإشارة أنّ القانون رقم 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونين قد نص بموجب الفصل الثاني من الباب الرابع منه، على مجموعة من الجزاءات المفروضة على أطراف عملية التصديق الإلكتروني والمتمثلة في:

أ)- يعاقب بالحبس من ثلاثة(03) أشهر إلى ثلاثة(03) سنوات، وبغرامة من 20.000 دج إلى 200.000 دج، أو بإحدى هاتين العقوبتين فقط، كلّ من أدلى بإقرارات كاذبة للحصول على شهادة تصديق إلكتروني موصوفة[1](المادة 66 منه)، ويعاقب بالحبس من شهرين إلى سنة واحدة، وبغرامة من 200.000 دج إلى 1.000.000 دج، أو بإحدى هاتين العقوبتين فقط كلّ(م.خ.ت.إ) أخل بالتزام إعلام(س.ض.ب.م) بالتوقف عن نشاطه في الآجال المحددة في المادتين 58 و 59 من هذا القانون(المادة 67 منه)؛

[1] – راجع كذلك نص المادتين 17 و18 من قانون رقم 15-03 مؤرخ في 01 فيفري 2015 يتعلق بعصرنة العدالة، ج ر عدد 06 الصادر في 10 فيفري 2015.

**ب)**- يعاقب بالحبس من ثلاثة(03) أشهر إلى ثلاثة(03) سنوات، وبغرامة تتراوح من 1.000.000 دج إلى 5.000.000 دج أو بإحدى هاتين العقوبتين فقط، كلّ من يقوم بحيازة أو إفشاء أو إستعمال بيانات إنشاء توقيع إلكتروني موصوف خاصة بالغير(المادة 68 منه)، ويعاقب بالحبس من شهرين إلى ثلاثة سنوات، وبغرامة من 20.000 دج إلى 200.000 دج أو بإحدى هاتين العقوبتين فقط، كلّ من يخلّ عمدا بالتزام تحديد هوية طالب شهادة تصديق إلكتروني موصوفة (المادة 69 منه)؛

**ج)**- يعاقب بالحبس من ثلاثة(03) أشهر إلى سنتين(02) وبغرامة من 200.000 دج إلى 1.000.000 دج أو بإحدى هاتين العقوبتين فقط، كلّ (م.خ.ت.إ) يخلّ بأحكام المادة 42 من هذا القانون(المادة 70منه)، ويعاقب بالحبس من ستة(06) أشهر إلى ثلاثة(03) سنوات، وبغرامة من 200.000 دج إلى 1.000.000 دج أو بإحدى هاتين العقوبتين فقط كلّ(م.خ.ت.إ) يخلّ بأحكام المادة 43 من هذا القانون (المادة 71 منه)؛

**د)**- يعاقب بالحبس من سنة واحدة(01) إلى ثلاثة(03) سنوات وبغرامة من 200.000 دج إلى 2.000.000 دج أو بإحدى هاتين العقوبتين فقط، كلّ من يؤدي خدمات التصديق الإلكتروني للجمهور من دون ترخيص أو كلّ(م.خ.ت.إ) يستأنف أو يواصل نشاطه بالرغم من سحب ترخيصه، وتُصادر التجهيزات التي أُستعملت لارتكاب الجريمة طبقا للتشريع المعمول به(المادة 72 منه)؛

**هـ)**- يعاقب بالحبس من ثلاثة(03) أشهر إلى سنتين(02) وبغرامة من 20.000 دج 200.000 دج أو بإحدى هاتين العقوبتين فقط، كلّ شخص مُكلّف بالتدقيق يقوم بكشف معلومات سرية أطل أثناء قيامه بالتدقيق(المادة 73 منه)، كما يعاقب كذلك بغرامة من 2.000 د ج إلى 200.000، كلّ شخص يستعمل شهادته للتصديق الإلكتروني الموصوفة لغير الأغراض التي مُنحت من أجلها(المادة 74 منه)، ويعاقب الشخص المعنوي الذي ارتكب إحدى الجرائم المنصوص عليها في هذا الفصل، بغرامة تعادل خمسة مرّات الحدّ الأقصى للغرامة المنصوص عليها بالنسبة للشخص الطبيعي(المادة 75 منه).

كما نص المشرع الإماراتي بدوره في مواد الفصل التاسع من القانون الإتحادي بشأن المعاملات والتجارة الإلكترونية لعام 2006، على مجموعة من العقوبات بحسب درجة

الجريمة، لذا يعاقب بالحبس لمدة لا تقل عن سنة(01) وبغرامة مالية لا تقل عن 50.000 درهم ولا تزيد عن 250.000 درهم أو بإحدى العقوبتين، كلّ من أنشأ أو نشر أو وَفَّرَ أو قدّم أية شهادة تصديق إلكتروني تتضمن أو تشير إلى بيانات غير صحيحة مع علمه بذلك (المادة 26 منه)، ويعاقب بالحبس لمدة لا تزيد عن ستة(06) أشهر وبغرامة مالية لا تزيد 100.000 درهم أو بهاتين العقوبتين، كلّ من قدّم عمدا بيانات غير صحيحة لـ (م.خ.ت.إ) بغرض طلب إصدار أو إلغاء أو إيقاف شهادة التصديق الإلكتروني (المادة 27 منه).

زيادة على ذلك يُعاقب بالحبس لمدة لا تقل عن ستة(6) أشهر وبغرامة مالية لا تقل عن 20.000 ولا تزيد عن 100.000 درهم أو بإحدى هاتين العقوبتين، كلّ شخص تمكن بموجب أية سلطات ممنوحة له في هذا القانون من الإطلاع على معلومات أو سجلات أو مستندات أو مراسلات إلكترونية أفشى أيًّا من هذه المعلومات، ويُستثنى من ذلك حالات التصريح بالمعلومات التي تتم لأغراض تنفيذ هذا القانون أو تنفيذا لأيّة إجراءات قضائية (المادة 28 منه)، كما يجوز للمحكمة في حالات الإدانة بموجب أحكام هذا القانون أن تقضي بمصادرة الآلات والأدوات التي أستخدمت في إرتكاب الجريمة وذلك دون الإخلال بحقوق الغير حسن النية، أو تطبق عقوبات أشدّ يُنَصّ عليها في أيّ قانون آخر أو تحكم(المحكمة) بإبعاد الأجنبي في حالة الحكم عليه بالحبس بموجب أحكام هذا القانون (المواد 31 و32 و33 منه) [1].

بالإضافة إلى التشريعات السابقة نص قانون المعاملات الإلكترونية لسلطنة عمان بموجب المادتين 52 و53 من الفصل التاسع منه، على عقوبة السجن لمدة لا تتجاوز سنتين وبغرامة لا تتجاوز 5.000 ريال عماني أو بإحدى هاتين العقوبتين، أو عقوبة السجن لمدة لا تتجاوز سنة واحدة وبغرامة مالية لا تتجاوز 1.500 ريال عماني مع عدم الإخلال بأية عقوبة أشد ينص عليها قانون الجزاء العماني أو أي قانون آخر، كلّ من ارتكب الجرائم المحدّدة على سبيل الحصر بموجب أحكام المادتين أعلاه، وتضيف المادة 54 من نفس

---

[1] – القانون الإتحادي لدولة الإمارات العربية المتحدة رقم 2006/1 بشأن المعاملات والتجارة الإلكترونية الصادر بتاريخ 30 جانفي 2006. http://sbusiness.abudhabi.aeegovPoolPortal/

القانون أنّه في حالة الإدانة بموجب أحكام هذا القانون يمكن للمحكمة أن تحكم بالإضافة إلى عقوبة آخرى بمصادرة الأدوات التي أُسْتُعْمِلَتْ في إرتكاب الجريمة[1].

فمن خلال كلّ ما سبق نصل إلى أنّه مهما اعترفت النظم القانونية بحق أطراف عقد تقديم خدمة التصديق الإلكتروني في اللجوء إلى الحدّ من المسؤولية أو استبعادها، فإنّ هذا الحق يخضع إلى قيود وشروط محدّدة بموجب القواعد المتعلقة بحماية المستهلك التي تفرض عليهم إلتزام حماية مصلحة الطرف الثالث المعول على شهادة التصديق الإلكتروني، وبالتالي فإنّ نجاح عملية التصديق الإلكتروني مرهون بتضافر وتعاون أطراف التعامل الإلكتروني بما فيهم أصحاب الشهادات أو الغير أو جهات التوثيق الإلكتروني، والذي لا يتحقق إلاّ بتحمل كلّ واحد منهم للإلتزامات العقدية والقانونية والمسؤولية المترتبة عن ذلك، مما يزيدهم ثقة وأمان أثناء قيامهم بمعاملات التجارة الإلكترونية.

[1] – مرسوم سلطاني رقم 69-2008 مؤرخ في 17 ماي 2008، يتعلق بإصدار قانون المعاملات الإلكترونية. http://www.omanlegal.org/law/search.aspx

إنّ الدور المهم الذي تلعبه جهة التوثيق الإلكتروني الموثوق بها كطرف محايد عن أطراف التعامل الإلكتروني، في توثيق توقيعاتهم الإلكترونية وتعزيزها بشهادات تصديق إلكتروني موصوفة، تثبت وتشهد على صحة وسلامة البيانات الإلكترونية المتداولة في وقت أو قبل إصدارها(الشهادات) في بيئة إلكترونية إفتراضية، دفع بالتشريعات الدولية والوطنية إلى الإسراع في تنظيم الخدمات المتعلقة بالتصديق الإلكتروني، عن طريق تحديد إلتزامات الجهات المشرفة على خدمات التصديق الإلكتروني المعتمدة، والتزامات الأطراف المعولة على الشهادات الإلكترونية سواءا كان المُوقِّع بصفته كصاحب الشهادة، أو الغير كطرف ثالث معول بغض النظر عن العلاقة العقدية أو القانونية التي تربطه بمقدم خدمة التصديق الإلكتروني، مع تحمل الأطراف النتائج المترتبة عن الإخلال بها.

لذا يعتبر موضوع المسؤولية الإلكترونية من بين أدق المسائل التي يجب على التشريعات الدولية والوطنية من تنظيمها تنظيما كافيا، بالشكل الذي يسمح بإرساء مناخ مؤمن ملائم للقيام بالمعاملات الإلكترونية مهما كانت مجالاتها، وبالتالي فإنّ إعتماد أطراف التصديق الإلكتروني على الأحكام الواردة في القوانين المدنية والجزائية لتحديد طبيعة المسؤولية وتكييفها وفقا لأسس قانونية صحيحة، غير كافية لضمان حقوق كلّ طرف نظرا للوسائل التقنية والتكنولوجية الحديثة المستعملة في معاملاتهم الإلكترونية وبالخصوص التجارة الإلكترونية، كما أنّ القوانين الخاصة بالمعاملات الإلكترونية لم تعطي الأهمية البالغة لموضوع المسؤولية نظرا للثغرات القانونية التي تشوبها، مما يُصَعِّبْ المهمّة لقضاة الموضوع في تحديد طبيعة المسؤولية، وفي تقدير التعويضات المستحقة للطرف المضرور كما أنّ القواعد العامة المتبعة بشأن تعديل أحكام المسؤولية تخدم أكثر جهات التوثيق الإلكتروني بإعتبارها كطرف أقوى في العلاقة العقدية أو القانونية التي تربطها بالأطراف المعولة على خدماتها.

إنطلاقا من ذلك تسعى هذه الجهات إلى وضع شروط وقيود مسبقة لاستعمال شهادات التصديق الإلكتروني، قصد الحدّ أو الإعفاء من مسؤوليتها المترتبة في حالة الإخلال بالتزاماتها العقدية أو القانونية، فما يبقى على الأطراف المعولة بما فيها صاحب شهادة التصديق الإلكتروني أو الغير سوى قبول أو رفض هذه الشروط قبل إبرام العقد النموذجي

بشأن تقديم خدمة التصديق الإلكتروني، ومن ثمّة يسعى مُسبقا أطراف التعامل الإلكتروني وبالخصوص المُوَقِّعِ على فرض إشتراط على جهة التوثيق الإلكتروني المُصدرة لشهادة التصديق الإلكتروني الموصوفة، بأن تضمن تجاه الغير الأضرار التي تُلحقه نتيجة تعويله على الشهادة، وبالتالي ينشئ العقد واجبا قانونيا لصالح الغير تتحمله جهة التوثيق على النحو الذي يؤدي إلى إمكانية مساءلتها عقديا تجاه الغير المتضرر وفقا للقواعد الخاصة بالإشتراط لمصلحة الغير، وذلك كاستثناء من قاعدة نسبية أثر العقد التي تقتصر فيها أحكام العقد والتزاماته على أطرافه فقط، لذا يشترط لاستفادة الغير كطرف معول على شهادة التصديق الإلكتروني أن تتجه نية طرفي عقد تقديم خدمة التصديق الإلكتروني (الموقع وجهة التوثيق الإلكتروني) إلى إفادته(الغير) من العقد، مما يستوجب على جهة التوثيق أن تؤكد وتضمن صحة الإشتراط الوارد في الشهادة التي تصدرها تجاه هذا الغير.

إنّ تحقيق الإشتراط لمصلحة الغير ليس بالفرض العملي في الكثير من الحالات، زيادة على ذلك نجد أنّ القواعد العامة في الإشتراط لمصلحة الغير تتطلب في الكثير من الأحيان أن يكون للمُشترط مصلحة عُليا في هذا الإشتراط، فمهما اتجهت نيّة أطراف عقد تقديم خدمة التصديق الإلكتروني حول الإشتراط لمصلحة الغير، إلاّ أنّه يبقى على هذا الأخير(Tiers) مراعاة الإلتزام المتعلق بتقدير قابلية التعويل على التوقيعات الإلكترونية، ومن مدى تعزيزها بشهادات تصديق إلكتروني موصوفة، فإن كان الأمر بذلك يجب عليه اتخاذ الإجراءات المعقولة اللاّزمة من أجل التحقق من صلاحية الشهادة، وعدم تعرضها للإيقاف أو الإلغاء مع التأكد من وجود القيود الواردة فيها على القيمة أو المسؤولية، ففي حالة تخلف الطرف المعول عن الإمتثال بالتزاماته فإنّه لا ينبغي منع ذلك الطرف(Tiers) من إستخدام التوقيع الإلكتروني أو شهادة التصديق الإلكتروني الموصوفة، إذا لم يكن من شأن التحقق المعقول أن يكشف عدم صحة التوقيع الإلكتروني أو الشهادة، فمهما كانت الظروف لا ينبغي تعريض الإلتزامات الملقاة على الطرف الثالث المُعوِّل(Tiers)، للمستوى ذاته مع الإلتزامات المفروضة على أطراف عقد تقديم خدمة التصديق الإلكتروني(الموقع و(م.خ.ت.إ).

# خـــــاتمـــة

تناولت دراستنا السابقة موضوع رئيسي من الموضوعات المهمة والحديثة التي تُثيرها المعاملات الإلكترونية بصفة عامة والتجارة الإلكترونية بصفة خاصة ألا وهو التوثيق أو التصديق الإلكتروني، الذي أوضحنا من خلاله الأهمية البالغة التي منحتها مختلف التشريعات الدولية والوطنية لتقنيات التوثيق الإلكتروني في مجالات الإقتصاد الرقمي وبالخصوص معاملات التجارة الإلكترونية والعمليات المصرفية، التي شاع اللجوء إليها في وقتنا الحاضر نظرا لسهولتها وسرعتها بالإضافة إلى تقليلها لنفقات إنجازها إلى حدّ كبير.

إنّ معاملات التجارة الإلكترونية تتم عن بُعد في بيئة إلكترونية إفتراضية مملوءة بالمخاطر بين أطراف لا يعرف بعضهم البعض الآخر، الشيء الذي يستدعي ضرورة التأكد مُسبقا قبل إجراء هذه المعاملات من حقيقة ومع من تَتِّمْ ومدى جدّيتها وسلامتها وخلوها من الغش والاحتيال، والعمل على تفادي إنكار عملية البيع والشراء أو إثارة الشبهة في طرق التبادل أو الدفع الإلكتروني عبر الإنترنيت، فالتوثيق الذي يعتمد على الكتابة الخطية والتوقيع اليدوي بشهادة ضابط عمومي أو المكلف بالخدمة العامة (الموثق، المحضر القضائي الخ...)، أصبح لا يتأقلم مع مستجدات وتطورات الوقت الراهن الذي سيطرت فيه تكنولوجيا المعلومات على جميع مختلف القطاعات بما فيها الإقتصادية، مما دفعت الضرورة بأطراف التصرف الإلكتروني إلى البحث عن وسائل وتقنيات إلكترونية موثوق بها يشرف عليها طرف ثالث محايد ومعتمد يقوم بذات الدور الذي يلعبه الموثق العادي.

لذا قامت مختلف التشريعات الدولية والوطنية بإصدار قوانين خاصة بالمعاملات والتجارة الإلكترونية، التي من خلالها تطرقت إلى مسألة تنظيم مرافق المفاتيح العمومية في إطار مخططات الثقة في التصديق الإلكتروني، يمارس من خلالها الموثق الإلكتروني لمهامه نظرا لدوره الفعّال في إرساء مناخ ثقة أمن للمعاملات الإلكترونية، وبالتالي أصبحت الثقة والأمان لدى المتعاملين يأتيان في مقدمة الضمانات التي يجب على(م.خ.ت.إ) توفيرها لأطراف التصرف الإلكتروني، عن طريق إتاحتهم لأدوات إنشاء التوقيعات الإلكترونية المؤمنة التي تكون تحت سيطرتهم، مع تزويد توقيعاتهم بشهادات تصديق إلكتروني موصوفة وفقا للمعايير الدولية المعترف بها، التي من خلالها تؤكد من أنّ المُوقِّع المحددة هويته في الشهادة حائز على بيانات إحداث توقيعه الإلكتروني في وقت أو قبل إصدارها(الشهادة).

انطلاقا من ذلك فإنّ عملية التصديق الإلكتروني بحاجة إلى بنية تحتية لإدارة نظام مرفق المفاتيح العمومية(PKI)، الذي يعتبر كعنصر أساسي من عناصر بناء منظومة التصديق الإلكتروني في معاملات التجارة الإلكترونية والعمليات المصرفية، لكونها(البنية) توفر أعلى مستويات الحماية الأمنية لمحتوى التصرفات الإلكترونية التي تتم عبر شبكة الإنترنت، فالغرض الرئيسي من البِنْيَةِ التحتية للمفتاح العام ينصب حول إصدار شهادات المفاتيح العمومية وإدارتها، بحيث تشمل إدارة مفاتيح التشفير إحداث مفتاحين(خاص وعام) مع إصدار شهادات إلكترونية تصدق بأنّ المفتاح العام لأحد المستعملين يناظر بالفعل المفتاح الخاص لذلك المستعمل، وتخزين وحفظ المفاتيح والشهادات وأرشفتها، وإبطالها عند الحاجة لذلك وإلغاءها عندما تنتهي مُدّتها، كما تعمل سلطات إصدار الشهادات حسب عدد من الإرشادات وسياسات التصديق الموثوق بها من طرف الجهات الرسمية، وفقا للمعايير التقنية الواردة في التوصية(X.509) الصادرة عن الاتحاد الدولي للاتصالات(ITU)، المتعلقة بتنظيم البنية التحتية للمفتاح العمومي وإصدار الشهادات الرقمية.

لذا تَتّبِع سلطة إصدار الشهادات(AC) في ذلك القواعد والإجراءات والسياسات المبينة في سياسة الشهادة(PC) أوفي إعلان ممارسة إصدار الشهادات(CPS)-(DPC)، التي تعتبر من الوثائق الأساسية التي يجب أن تنشرها سلطة التصديق الإلكتروني لكي تكون في متناول عملائها، إذْ تساعد هذه الوثائق في ضمان توفير الأرضية المشتركة لتقدير وتقييم درجة الثقة التي يمكن أن يتوقعها أطراف التعامل الإلكتروني من الشهادات الرقمية التي تصدرها جهات التوثيق الإلكتروني، كما أن هذه الوثائق توفر الإطار القانوني الضروري لبناء الثقة فيما بين مُكوّنات البنية التحتية للمفتاح العام، وباستخدام الشهادات الرقمية المصدرة والمُراقبة من قِبَلِ البنية التحتية للمفتاح العام، يُمكن توفير تقنيات تشفير عالية الوثاقة تُمكّن المتعاملين من التوقيع إلكترونيا على تعاملاتهم الإلكترونية، مع ضمان سلامة وسرية المعلومات والوثائق المتداولة إلكترونيا وعدم القدرة على إنكارها، مما يرفع من مستوى قيمتها القانونية لتعادل قيمة الوثائق الموقعة يدويّا في الإثبات.

انطلاقا من ذلك فإنّ الوظيفة الرئيسية لشهادة التصديق الإلكتروني تتمثل في ربط المفتاح العام بالمفتاح الخاص للموقع اللذين تربطهما معادلة رياضية معقدة، يستحيل

استنباط بيانات إحداث التوقيع الإلكتروني بالوسائل التكنولوجية المتاحة بالرغم من إتاحة المفتاح العام للعموم، وبالتالي تعتبر شهادة التصديق الإلكتروني الموصوفة بمثابة وثيقة إثبات هوية صاحبها(بطاقة التعريف الوطنية أو جواز السفر) التي تسمح بإتاحة توثيق فوري وعاجل لبيانات إحداث التوقيع الإلكتروني الموصوف المتصل بالمحرر الإلكتروني، مع ضمان مطابقتها لبيانات فحصه، ونسبتها للمُوقِّع وعدم إنكارها في وقت إصدار الشهادة.

لذا يستوجب على أطراف التصرف الإلكتروني قبل مباشرتهم لتصرفاتهم اتخاذ الخطوات المعقولة في تقدير قابلية التعويل على خدمات(م.خ.ت.إ)، محايد ومعتمد أو مرخص له من طرف الجهات الرسمية في إطار نماذج الثقة المنتهجة في التصديق الإلكتروني، وذلك عن طريق التأكد من السياسة العامة المتبعة في خدمات التصديق الإلكتروني(PC) وبالخصوص كلّ ما يتعلق بإحداث التوقيع الإلكتروني الموصوف وبإصدار وإيقاف وإلغاء شهادات التصديق الإلكتروني، وكذلك التعرف على الإلتزامات المفروضة على أطراف خدمة التصديق الإلكتروني مع طرق حلّ الخلافات والنزاعات في حالة إثارتها الخ...، وبالتالي يجب على(م.خ.ت.إ) أن يتقيد بالإلتزامات المفروضة عليه بموجب الترخيص أو الإعتماد الممنوح له، وأن يتصرف وفقا للتأكيدات التي يقدمها بخصوص سياسته العامة وممارساته في مجال التصديق الإلكتروني، وأن يولي قدرا معقولا من العناية لضمان دقة واكتمال كلّ ما يقدمه من تأكيدات جوهرية، مُدرجة في شهادات التصديق الإلكتروني الموصوفة طيلة مدة صلاحيتها، وبالمقابل تقع على عاتق الأطراف المعولة على شهادات التصديق الإلكتروني مجموعة من الإلتزامات، المفروضة عليهم بموجب التشريعات والتنظيمات المتعلقة بخدمات التصديق الإلكتروني، التي قد يكون لها تأثيرا على المسؤولية الفردية لكل طرف عند الإخلال بها.

فبالرغم من إتاحة قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية لمجموعة من القواعد المشتركة الأساسية التي تحكم واجبات معينة تقع على عاتق الأطراف المعنية بعملية التصديق الإلكتروني، إلاّ أنّ النص الدولي النموذجي لم يتناول جميع قضايا المسؤولية الناجمة عن إستخدام طرق التوثيق الإلكتروني المؤمنة على الصعيد الدولي، بل ترك مسألة تنظيمها للقوانين الداخلية لكل بلد راغب.

تجدر الإشارة أنّ موضوع المسؤولية الإلكترونية تعتبر من بين أدق المسائل التي تثيرها المعاملات الإلكترونية بالنظر إلى حداثتها، واختلاف التكنولوجيا المستخدمة والبنية التحتية(مرفق المفاتيح العمومية) المتبعة في نماذج التصديق الإلكتروني، والتي قد تثير مسائل معقدة وبالخصوص المشاكل المترتبة في إطار مرفق المفاتيح العمومية الهرمي نتيجة ضعف المفتاح العمومي للسلطة الرئيسية، المستعمل في إصدار شهادات التصديق الإلكتروني، واستحواذه من طرف القراصنة لتزوير شهادات التصديق الإلكتروني مما يؤدي إلى إمكانية انهيار المرفق بأكمله، أو تلك الخلافات أو النزاعات المثارة في إطار اندماج عدة مرافق مفاتيح عمومية بشأن تحديد القانون الواجب التطبيق، والجهة القضائية المختصة بالفصل في النزاع المتعلق بأطراف التصديق الإلكتروني، وهذا ما يستدعي في كلّ الظروف الإستعانة بالأحكام الواردة في القوانين المدنية أو الجزائية المنظمة للمسؤولية، وذلك نظرا لعدم تنظيم القواعد الخاصة بالمعاملات الإلكترونية للمسؤولية الإلكترونية تنظيما كافيا.

تُشكل شهادات التصديق الإلكتروني الموصوفة حجر الزاوية لكلّ المعاملات الإلكترونية بإعتبارها كوسيلة أمان حديثة، يُعول عليها أطراف التصرف الإلكتروني في إثبات تصرفاتهم الإلكترونية وفقا للأغراض التي أُصدرت من أجلها الشهادة، لذا يتعين على جهة التصديق الإلكتروني وأطراف التعامل الإلكتروني القيام بحفظ الشهادة بطريقة مؤمنة، في الشكل الذي أنشئت أو أرسلت أو أستلمت به على أيّ حامل إلكتروني مؤمن، يُتيح إمكانية الإطلاع على مُحتواها كلّما اقتضت الحاجة لذلك، فمن الأفضل على أطراف التصديق الإلكتروني في حالة عدم قدرتهم أو افتقارهم لإمكانيات أو لأنظمة أمن حفظ واسترجاع الشهادات، الإستعانة بخدمات طرف آخر موثوق به لديه من الخدمات ما يحقق إشتراطات القانون في حفظ واسترجاع المحررات الإلكترونية وفقا للمعايير المعمول بها.

في الختام نصل إلى أنّ مصير الثقة والأمان في المعاملات الإلكترونية مرهون بمدى قوة المفتاح العمومي المعول عليه في خدمات التصديق الإلكتروني، وإحترام أطراف التصديق الإلكتروني للإلتزامات المفروضة عليهم بموجب التشريعات والتنظيمات المتعلقة بخدمات التصديق الإلكتروني، ومدى إقرار أطراف التعامل الإلكتروني بقابلية التعويل على خدمات جهة توثيق إلكتروني محايدة ومعتمدة أو مرخص لها بمزاولة نشاطاتها من طرف

جهة ترخيص أو إعتماد رسمية في إطار مرفق المفاتيح العمومية، لذا نهيب بالمشرع الجزائري بمجموعة من الاقتراحات والمتمثلة في:

**1)**- الإسراع في إصدار قانون خاص بالتجارة الإلكترونية مع الأخذ بعين الإعتبار لقوانين الأونسيترال الدولية النموذجية بشأن التجارة الإلكترونية لعام 1996 والتوقيعات الإلكترونية لعام 2001، بحيث يتطرق من خلاله إلى العقود الإلكترونية، وكلّ التصرفات التجارية ذات صلة بخدمات التصديق الإلكتروني؛

**2)**- تحديد الشروط المتعلقة بممارسة نشاط(م.خ.ت.إ) والطرف الثالث الموثوق عن طريق نصوص تنظيمية، والتي بدأ المشرع الجزائري في النص عليها(الشروط) بموجب أحكام القانون رقم 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين؛

**3)**- من المُستحسن وضع إطار قانوني خاص بالتشفير(Cryptographie) عن طريق نص تنظيمي(Texte réglementaire) يتعلق بإستعمال معدات وبرامج التشفير، من خلاله يتطرق إلى تحديد مفهوم التجهيزات وبرامج التشفير، والمواصفات الأمنية والتقنية المتطلبة فيها، إجراءات توثيقها، الخ...؛

**4)**- إصدار قانون خاص بإحداث نظام وطني لاعتماد مراكز تقييم مطابقة معدات وبرامج التشفير وفقا للمعايير المعمول بها في الجزائر، تشرف عليه الهيئة الوطنية المكلفة بالإعتماد التي توضع من المستحسن تحت تصرف سلطة الوزير الأول، مع تحديد مهامها المتعلقة بمنح أو سحب الإعتماد، وتنظيم عمليات التدقيق ومتابعتها وتكوين المدققين وتأهيلهم وفقا للمواصفات الوطنية والدولية المعمول بها في الإعتماد، ومن إمكانية إبرامها لاتفاقيات الإعتراف المتبادل لشهادات المطابقة مع الجهات الأجنبية المثيلة لها، وذلك من أجل تدعيم الإعتراف المتبادل بين مراكز تقييم المطابقة الذين يمارسون مهامهم في الجزائر مع المراكز الأجنبية، كما يجب توضيح إجراءات إعتماد هذه المراكز أو المكاتب أو المصالح المختصة المكلفة بالتدقيق على السلطة الوطنية للتصديق الإلكتروني، والسلطتين الفرعيتين الحكومية والاقتصادية، و(م.خ.ت.إ) والأطراف الثالثة الموثوق بها، التي أشار إليها المشرع الجزائري في المادتين 78 و79 من القانون رقم 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين؛

**5)**- إصدار قانون خاص بالمعالجة الآلية للمعطيات ذات الطابع الشخصي، والقانون الخاص بحماية المستهلك مع تعديل كلّ النصوص القانونية الآخرى ذات صلة بخدمات التصديق الإلكتروني المعتمدة؛

**6)**- استحداث مشغل دفع إلكتروني أمن(SPS) يقبل التشغيل ببطاقات الإئتمان الأجنبية والمحلية، الذي يسمح بإجراء عمليات البيع والشراء أو الدفع أو التبادل الإلكتروني في أيّ منطقة من العالم، مع ضمان عمليات تحويل الأموال فيما بين البنوك، بحيث يشرف عليه طرف ثالث موثوق به تحت رقابة السلطة الوطنية للتصديق الإلكتروني، وكلّ ذلك يسمح بخلق مناخ ثقة أمن للأعمال مع تشجيع الاستثمارات في الجزائر؛

**7)**- توعية القضاة وأعضاء النيابة العامة بالمستجدات الحديثة التي عرفتها مجالات الإقتصاد الرقمي وبالخصوص معاملات التجارة الإلكترونية والعمليات المصرفية، مع الحرص على التكوين الجيّد لقضاة متخصصين في مجالات حلّ النزاعات الناشئة في مجالات المعاملات الإلكترونية، والعمل على تسهيل إجراءات التقاضي بالوسائل والتقنيات التكنولوجية الموثوق بها في إطار خدمات التصديق الإلكتروني، التي بدأ المشرع الجزائري في النص عليها بموجب المواد 14 و15 و16 (الفصل الرابع) من قانون رقم 15-03 مؤرخ في 01 فيفري 2015 المتعلق بعصرنة العدالة.

# قائمة المراجع

# قـــائـمـة الـمـراجـــع

## 1- باللغة العربيـــة.

### أولا- الكتب:


**1- إبراهيم خالد ممدوح**، التوقيع الإلكتروني، دار الجامعية، الإسكندرية، 2010.

**2- خالد مصطفى فهمي**، النظام القانوني للتوقيع الإلكتروني في ضوء الاتفاقيات الدولية والتشريعات العربية، دار الجامعة الجديدة، الإسكندرية، 2007.

**3- رضا متولي وهدان**، النظام القانوني للعقد الإلكتروني والمسئولية عن الإعتداءات الإلكترونية (دراسة مقارنة في القوانين الوطنية وقانون الأونسيترال النموذجي والفقه الإسلامي)، الطبعة الأولى، دار الفكر والقانون للنشر والتوزيع، المنصورة، 2008.

4- **سعيد السيد قنديل**، التوقيع الإلكتروني: ماهيته- صوره- حجيته في الإثبات بين التداول والإقتباس، الطبعة الثانية، دار الجامعة الجديدة للنشر، الإسكندرية، 2006.

**5- سمير حامد عبد العزيز جمال**، التعاقد عبر تقنيات الإتصال الحديثة، الطبعة الأولى، دار النهضة العربية، القاهرة، 2006.

**6- سليمان إيمان مأمون أحمد**، إبرام العقد الإلكتروني وإثباته (الجوانب القانونية لعقد التجارة الالكترونية)، دار الجامعة الجديدة، الإسكندرية، 2008.

**7- طارق إبراهيم الدسوقي عطية**، الأمن المعلوماتي (النظام القانوني للحماية المعلوماتية)، دار الجامعة الجديدة للنشر، الإسكندرية، 2009.

**8- العربي بالحاج**، النظرية العامة للإلتزام، ديوان المطبوعات الجامعية، الجزائر، 2001.

**9- علا محمد عيد نصيرات**، حجية التوقيع الإلكتروني في الإثبات (دراسة مقارنة)، الطبعة الأولى، عمّان، دار الثقافة للنشر والتوزيع، 2005.

**10- عبد الفتاح بيومي حجازي**، التوقيع الإلكتروني في النظم القانونية المقارنة، دار الفكر العربي، الإسكندرية، 2005.

**11 ـــــــــــــــــــــــ**، حماية المستهلك عبر شبكة الإنترنيت، دار الفكر الجامعي، الإسكندرية، 2006.

**12 ـــــــــــــــــــــــ**، التجارة الإلكترونية في القانون العربي النموذجي، الطبعة الأولى، الكتاب الثاني، دار الفكر الجامعي، الإسكندرية، مصر، 2006.

**13- عمر خالد زريقات،** عقود التجارة الإلكترونية: عقد البيع عبر الإنترنيت (دراسة تحليلية)، الطبعة الأولى، دار الحامد للنشر والتوزيع، الأردن، 2007.

**14- عيسى غسان ربضي،** القواعد الخاصة بالتوقيع الإلكتروني، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2009.

**15- عايد رجا الخلايلة،** المسؤولية التقصيرية الإلكترونية: المسؤولية الناشئة عن إساءة إستخدام أجهزة الحاسوب والإنترنيت (دراسة مقارنة)، دار الثقافة للنشر والتوزيع، عمان، 2009.

**16- علي جبار الحسيناوي،** جرائم الحاسوب والإنترنيت، دار اليازوري العلمية للنشر والتوزيع، الأردن، 2009.

**17- عبد الرزاق السنهوري،** الوسيط في شرح القانون المدني (نظرية الإلتزام- الإثبات)، الطبعة الثالثة، الجزء الثاني، دار النهضة العربية، القاهرة، 1981.

**18- لورنس محمد عبيدات،** إثبات المحرر الإلكتروني، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمّان، 2005.

**19- محمد صبري السعدي،** شرح القانون المدني الجزائري (مصادر الإلتزام – الواقعة القانونية)، الطبعة الثانية، دار الهدى، الجزائر، 2004.

**20- محمد خالد جمال رستم،** التنظيم القانوني للتجارة والإثبات الإلكتروني في العالم، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2006.

**21- محمد فواز المطالقة،** الوجيز في عقود التجارة الإلكترونية (أركانها- إثباتها- حمايتها(التشفير)- التوقيع الإلكتروني- القانون الواجب التطبيق)، دار الثقافة للنشر والتوزيع، عمان، 2008.

**22- مناني فرح،** أدلة الإثبات الحديثة في القانون، دار الهدى للطباعة والنشر، الجزائر، 2008.

**23 ــــــــــــ،** العقد الإلكتروني وسيلة إثبات حديثة في القانون المدني الجزائري، دار الهدى للطباعة والنشر، الجزائر، 2009.

**24- محمود محمد أبو فروة،** الخدمات البنكية الإلكترونية عبر الإنترنيت، الطبعة الأولى، دار الثقافة للنشر والتوزيع، الأردن، 2009.

**25- محمد محمد سادات،** حجية المحرّرات الموقعة إلكترونيًّا في الإثبات (دراسة مقارنة)، دار الجامعة الجديدة، مصر، 2011.
**26- ناصر خليل،** التجارة والتسويق الإلكتروني، الطبعة الأولى، دار أسامة للنشر والتوزيع، الأردن، 2009.
**27- نضال سليم برهم،** أحكام عقود التجارة الإلكترونية، دار الثقافة للنشر والتوزيع، عمّان، 2009.
**28- وسيم شفيق الحجار**، الإثبات الإلكتروني، المنشورات الحقوقية، بيروت، 2002.

**ثانيا- الرسائل والمذكرات الجامعية:**

**أ- رسائل الدكتوراه:**

**1- حمودي ناصر**، النظام القانوني لعقد البيع الدولي الإلكتروني المبرم عبر الإنترنيت، رسالة شهادة دكتوراه في العلوم، التخصص القانون، كلية الحقوق، جامعة مولود معمري تيزي وزو، 2009.
**2- عايض راشد المري،** مدى حجية الوسائل التكنولوجية الحديثة في إثبات العقود التجارية، رسالة دكتوراه، جامعة القاهرة، 1998.
**3- مخلوفي عبد الوهاب،** التجارة الإلكترونية عبر الإنترنيت، رسالة دكتوراه في الحقوق، تخصص قانون الأعمال، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر بباتنة، 2012.
**4- إيمان مأمون أحمد سليمان،** الجوانب القانونية لعقد التجارة الإلكترونية، رسالة دكتوراه، جامعة المنصورة، مصر، 2006.

**ب- مذكرات الماجستير:**

**1- زعاتري كريمة،** المركز القانوني لسلطة ضبط البريد والمواصلات السلكية واللاسلكية، مذكرة شهادة الماجستير، تخصص إدارة و مالية، كلية الحقوق والعلوم السياسية، جامعة أمحمد بوقرة بومرداس، 2001.

**2- سمية ديمش**، التجارة الإلكترونية حتميتها وواقعها في الجزائر، مذكرة شهادة الماجستير في العلوم الإقتصادية، تخصص تحليل وإستشراف إقتصادي، كلية العلوم الإقتصادية وعلوم التسيير، جامعة منتوري بقسنطينة، 2011.

**3- العاني إيمان**، البنوك التجارية وتحديات التجارة الإلكترونية، مذكرة شهادة الماجستير في العلوم الإقتصادية، تخصص بنوك وتأمينات، كلية العلوم الإقتصادية وعلوم التسيير، جامعة منتوري قسنطينة، 2007.

**4- واقد يوسف**، النظام القانوني للدفع الإلكتروني، مذكرة ماجستير في القانون العام، تخصص قانون التعاون الدولي، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، 2011.

**ثالثا- المقالات والبحوث العلمية.**

**1- أسامة بن غانم العبيدي**، "التصديق الإلكتروني وتطبيقاته في النظام السعودي"، المجلة القضائية، الرياض، عدد 04، 1433هـ. http://www.adl.moj.gov.saAlqadaeyaattach864.pdfn

**2- إسماعيل عبد النبي شاهين**، أمن المعلومات في الإنترنيت بين الشريعة و القانون، بحث مقدم في مؤتمر القانون و الكمبيوتر والإنترنيت، المنعقد في 1-3 ماي 2000 بجامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، بالتعاون مع مركز الإمارات للدراسات والبحوث الإستراتيجية ومركز تقنية المعلومات بالجامعة، المجلد الثالث، الصفحات 971 إلى 992. http://www.slconf.uaeu.ac.aearabic_prev_conf2000.asp

**3- إبراهيم الدسوقي أبو الليل**، توثيق التعاملات الإلكترونية و مسؤولية جهة التوثيق تجاه الغير المضرور، بحث مقدم في مؤتمر الأعمال المصرفية بين الشريعة والقانون، الذي نظمته جامعة الإمارات العربية المتحدة، بالتعاون مع غرفة التجارة الإلكترونية وصناعة دبي، في الفترة مابين 10 و 12 ماي 2003، المجلد الخامس، الصفحات 1745 إلى 1913. http://www.unue.banque.com/imarat/arab/

**4- بركات كريمة،** "الحماية القانونية للمستهلك في عقود الإذعان"، المجلة النقدية للقانون والعلوم السياسية، عدد 2011/02، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو.

**5- ثروت عبد الحميد،** مدى حجية التوقيع الإلكتروني في الإثبات على ضوء القواعد التقليدية للإثبات، بحث مقدم في مؤتمر الأعمال المصرفية بين الشريعة والقانون، الذي نظمته جامعة الإمارات العربية المتحدة، بالتعاون مع غرفة التجارة الإلكترونية وصناعة دبي، في الفترة مابين 10 و 12 ماي 2003، المجلد الأول، الصفحات 397-425.
http://www.unue.banque.com/imarat/arab/

**6- طارق كميل،** حجية شهادات المصادقة الإلكترونية الأجنبية (دراسة مقارنة)، بحث مقدم في مؤتمر المعاملات الإلكترونية (التجارة الإلكترونية- الحكومة الإلكترونية) الذي نظمه مركز الإمارات للدراسات والبحوث الإستراتيجية المنعقد في دبي من 19 إلى 20 ماي 2009، المجلد الثاني، الصفحات 571-615.
http://slconf.uaeu.ac.aeslconf17arabic_prev_conf2009.asp

**7- عبد المنعم كيوة،** الإطار القانوني للإمضاء والمصادقة الإلكترونية، مقال منشور على الموقع التالي: http://www.ism-justice.nat.tn

**8- كامران الصالحي،** الطبيعة القانونية لمسؤولية مزود خدمات التصديق، بحث مقدم في مؤتمر المعاملات الإلكترونية (التجارة الإلكترونية- الحكومة الإلكترونية) الذي نظمه مركز الإمارات للدراسات والبحوث الإستراتيجية المنعقد في دبي من 19 إلى 20 ماي 2009، المجلد الثاني، الصفحات 617-671.
http://www.slconf.uaeu.ac.aeslconf17arabic_prev_conf2009.asp

**9- محمد عبد الرحيم،** جرائم الإنترنيت والإحتساب عليها، بحث مقدم في مؤتمر القانون والكمبيوتر والإنترنيت، المنعقد في 1-3 ماي 2000 بجامعة الإمارات العربية المتحدة، كلية الشريعة و القانون، بالتعاون مع مركز الإمارات للدراسات والبحوث الإستراتيجية ومركز تقنية المعلومات بالجامعة. المجلد الثالث، الصفحات 871 إلى 886.
http://www.slconf.uaeu.ac.aearabic_prev_conf2000.asp

**10- محمد حاتم البيات،** المسؤولية المدنية عن الخطأ في المعاملات التي تتم عبر الوسائط الإلكترونية، بحث مقدم في مؤتمر المعاملات الإلكترونية (التجارة الإلكترونية-

الحكومة الإلكترونية) الذي نظمه مركز الإمارات للدراسات والبحوث الإستراتيجية المنعقد في دبي من 19 إلى 20 ماي 2009، بحوث المجلد الثاني، الصفحات 809 إلى 815.
http://www.slconf.uaeu.ac.aeslconf17arabic_prev_conf2009.asp

**11- نبيلة إسماعيل رسلان**، التأمين في مجال المعلوماتية والشبكات، بحث مقدم في مؤتمر القانون والكمبيوتر والإنترنيت، المنعقد في 1-3 ماي 2000 بجامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، بالتعاون مع مركز الإمارات للدراسات والبحوث الإستراتيجية ومركز تقنية المعلومات بالجامعة، المجلد الثالث، الصفحات 835 إلى 870.
http://www.slconf.uaeu.ac.aearabic_prev_conf2000.asp

**12- نجوى أبو هيبة**، التوقيع الإلكتروني (تعريفه-مدى حجيته في الإثبات)، بحث مقدم إلى مؤتمر الأعمال المصرفية بين الشريعة والقانون، الذي نظمته كلية الشريعة والقانون في جامعة الإمارات العربية المتحدة، بالتعاون مع غرفة التجارة الإلكترونية وصناعة دبي، في 10 و 12 ماي 2003، المجلد الأول، الصفحات 427 إلى 454.
http://www.unue.banque.com/imarat/arab/

**13- يونس عرب**، قانون تقنية المعلومات والتجارة العالمية. مقال منشور على الموقع التالي: http://www.arablaw.org

**14 ـــــــــــــــ**، العقود الإلكترونية – أنظمة الدفع والسداد الإلكتروني. مقال منشور على الموقع التالي: http://www.arablaw.org

**رابعا- النصوص القانونية:**

**أ- النصوص التشريعية:**

**1-** أمر رقم 156/66 المؤرخ في 8 جويلية 1966، يتضمن قانون العقوبات، معدل ومتمم.

**2-** أمر رقم 58/75 المؤرخ في 26 سبتمبر 1975، يتضمن القانون المدني، معدل ومتمم.

**3-** قانون رقم 2000-03 مؤرخ في 5 أوت 2000، يُحدد القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية، ج ر عدد 48 الصادر في 6 أوت 2000.

**4**- قانون رقم 15-03 مؤرخ في 01 فيفري 2015 يتعلق بعصرنة العدالة، ج ر عدد 06 الصادر في 10 فيفري 2015.
**5**- قانون رقم 15-04 مؤرخ في 01 فيفري 2015 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، ج ر عدد 06 الصادر في 10 فيفري 2015.

**ب- نصوص تنظيمية:**

**1**- مرسوم تنفيذي رقم 06-306 مؤرخ في 2006/09/10، يحدد العناصر الأساسية للعقود المبرمة بين الأعوان الاقتصاديين والمستهلك والبنود التي تعتبر تعسفية، ج ر عدد 56 الصادر في 2006/09/11، معدل ومتمم بموجب مرسوم تنفيذي رقم 44/08 المؤرخ في 2008/02/03، ج ر عدد 07 الصادر في 2008/02/10.
**2**- مرسوم تنفيذي رقم 07-162 مؤرخ 30 ماي 2007 يتعلق بنظام الإستغلال المُطبق على كلّ نوع من أنواع الشبكات بما فيها اللاّسلكية الكهربائية وعلى مُختلف خدمات المواصلات السلكية واللاسلكية، ج ر عدد 37 الصادر في07 جويلية 2007. يعدل ويتمم المرسوم التنفيذي رقم 01-123 المؤرخ في 09 ماي 2001، ج ر عدد 27 الصادر في 13 ماي 2001.
**3**- مرسوم تنفيذي رقم 09-410 مؤرخ في 10 ديسمبر 2009 المحدد لقواعد الأمن المطبقة على النشاطات المنصبة على التجهيزات الحساسة، ج ر عدد 73 الصادر في 13 ديسمبر 2009.

**خامسا- النصوص القانونية الأجنبية.**

**أ- القوانين الدولية النموذجية:**

**1**- قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية لعام 1999، مع دليله التشريعي.
http://www.unicitral.org/pdf/Arabic/texts/selectcom/mt-elecsig/
**2**- قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية لعام2001 مع دليله التشريعي.
http://www.unicitral.org/pdf/Arabic/texts/selectcom/mt-elecsig/

**ب- القوانين الوطنية:**

**1**- قانون عدد 83 لسنة 2000 مُؤرخ في 9 أوت 2000 يتعلق بالمبادلات والتجارة الإلكترونية، المنشور في ر.ر.ج.ت عدد 64، الصادر في 9 أوت 2000(تونس). http://www.legislation.tn

**2**- قانون عدد 92-2005 مؤرخ في 03 أكوبر 2005، يتعلق بتنقيح وإتمام القانون عدد 70-1994 المؤرخ في 20 جوان 1994 المتعلق بإحداث نظام وطني لإعتماد هيئات تقييم المطابقة، المنشور في (ر.ر.ج.ت) عدد 79 الصادر في 04 أكتوبر2005 (تونس). http://www.legislation.tn

**3**- قرار وزير تكنولوجيا الإتصال المؤرخ في 19 جويلية2001 يتعلق بضبط المواصفات التقنية لمنظومة إحداث الإمضاء الإلكتروني، المنشور في ر.ر.ج.ت عدد 60، الصادر في 19 جويلية2001(تونس). http://www.legislation.tn

**4**- قرار وزير تكنولوجيا الإتصال مؤرخ في 19 جويلية2001 يتعلق بضبط المعطيات التقنية المتعلقة بشهادات المصادقة الإلكترونية والوثوق بها، المنشور في ر.ر.ج.ت عدد 60 الصادر في 2001/07/27(تونس). http://www.legislation.tn

**5**- قانون المعاملات الأردني رقم 2001/85 المؤرخ في 11 ديسمبر 2001، الصادر في الجريدة الرسمية للمملكة الأردنية رقم 6010، في 31 ديسمبر 2001. http://www.lob.gov.jouilawsindex.jsp

**6**- أمر عدد 1667-2001 مؤرخ في 17 جويلية2001 المتعلق بالمصادقة على كرّاس الشروط الخاص بممارسة نشاط مُزود خدمات التصديق الإلكتروني، المنشور في ر.ر.ج.ت عدد 60، الصادر في 27 جويلية2001(تونس). http://www.legislation.tn

**7**- أمر عدد 1668-2001 مؤرخ في 17 جويلية2001، يتعلق بضبط إجراءات الحصول على ترخيص لممارسة نشاط مزود خدمات المصادقة الإلكترونية، المنشور في ر.ر.ج.ت عدد 60 الصادر في 17 جويلية2001(تونس). http://www.legislation.tn

**8**- قانون رقم 2004/15 المتعلق بتنظيم التوقيع الإلكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات، المنشور في الجريدة الرسمية عدد 17، الصادر في 22 أفريل 2004(مصر). http://www.ragylaw.com~rplfegimagesfile/

**9**- قرار رقم 2005/109، المؤرخ في 15 ماي 2005، المتعلق بإصدار اللائحة التنفيذية لقانون التوقيع الإلكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات، المنشور بالوقائع المصرية عدد 115 الصادر في 25 ماي 2005(مصر).
http://www.ragylaw.com~rplfegimagesfile/ ou http://www.arablaw.org
**10**- قانون إتحادي لدولة الإمارات العربية المتحدة رقم 2006/1 بشأن المعاملات والتجارة الإلكترونية الصادر بتاريخ 30 جانفي 2006.
http://sbusiness.abudhabi.aeegovPoolPortal/
**11**- مرسوم سلطاني رقم 52-2006 الصادر في 31 ماي 2006 بإنشاء هيئة تقنية المعلومات، الجريدة الرسمية لسلطنة عمّان عدد 816.
http://www.omanlegal.org/law/search.aspx
**12**- أمر عدد 1044-2008 مؤرخ في 14 أفريل 2008 يتعلق بالمصادقة على النظام الأساسي الخاص بأعوان الوكالة الوطنية للمصادقة الإلكترونية، المنشور في ر.ر.ج.ت عدد 32 الصادر في 18 أفريل 2008(تونس). http://www.legislation.tn
**13**- مرسوم سلطاني رقم 69-2008 مؤرخ في 17 ماي 2008، يتعلق بإصدار قانون المعاملات الإلكترونية، الجريدة الرسمية لسلطنة عمان عدد 864، الصادر في 17 ماي 2008. http://www.omanlegal.org/law/search.aspx
**14**- القرار الوزاري رقم (1) لسنة 2008 (الإمارات العربية المتحدة) بشأن إصدار لائحة مزودي خدمات التصديق الإلكتروني. http://www.government.ae
http://www.tra.gov.ae/ ou
**15**- قرار مجلس الوزراء رقم 8-2009 (الإمارات العربية المتحدة) بشأن الرسوم المستحقة على معاملات مزودي خدمات التصديق الإلكتروني، الصادر في 01 فيفري 2009.
http://www.tra.gov.ae/

## 2- باللغة الأجنبية.

**1- Ouvrages :**

**1- Aboudramane OUATTARA**, La preuve électronique (Étude de Droit comparé Afrique, Europe, Canada), Presses Universitaires d'Aix-Marseille, 2011.

**2-Arnaud-F. FAUSSE**, La signature électronique : transaction et confiance sur Internet, DUNOD, Paris, 2001.

**3- Djamel BENABDESSELAM,** Initiation à l'informatique, Edition Diffusion Communication OMEGA, Alger, 1997.

**4- Étienne WÉRY,** Facture, Monnaie et paiement électroniques, édition du Juris-Classeur, Litec, France, 2003.

**5- Lionel BOUCHURBERG**, Internet et commerce électronique (Site web-Contrats- Responsabilité- Contentieux), 2e édition, DELMACE, France, 2001.

**6- Philippe NEAU-LEDUC,** Droit Bancaire, 4e édition, éditions DALLOZ, 2010.

**7- Philippe MALINVAUD, Dominique FENOUILLET**, Droit des Obligations, 11e édition, Litec, France, 2010.

**8- Thierry-PIETTE COUDOl**, La signature électronique (Introduction technique et juridique à la signature électronique sécurisée, preuve et écrit électronique), Edition Litec, Paris, 2001.

**2- Thèses et Mémoire.**

**A- Thèses de Doctorat :**

**1- Duc-PHONG LÊ**, Protocoles Cryptographique (Multi signature et Horodatage), Thèse de doctorat en Informatique, Spécialité Informatique, Université de Pau et des Pays de l'Adour, France, 2009.

**2- Matthieu WIROTIUS**, Authentification par Signature Manuscrite sur Support Nomade, Thèse de doctorat, Discipline: Informatique, École Doctorale, Santé, Sciences et Technologies, Université François Rabelais, Tours, 2005.

**3- Paul Axayacatl FRAUSTO BERNAL,** Infrastructure de Confiance sur des Architectures de Réseaux pour les Services de Signature évoluée, Thèse de doctorat, spécialité Informatique et Réseaux**,** École Nationale Supérieure de Télécommunications, Paris, 2004.

**4- Yousef SHANDI**, la formation du contrat a distance par voie électronique, thèse de doctorat, mention Droit privé, université Robert SCHUMAN Strasbourg III, Faculté de droit, de sciences politiques et de gestion, 2005.

**B- mémoire :**

**1- Laurent GRANIER**, L'authenticité notariale électronique, Mémoire du diplôme supérieure du notariat, Université de Montpelier 1, Faculté de Droit, 2004. http://www.droit-tic.com/

**3- Articles :**

**1- Alain BENSOUSSAN et Charles COPIN**, Le livre blanc de la signature électronique. Article disponible sur : http://www.alain-bensoussan.com

**2- A. Arsenault** et **S. Turner**, X.509 Internet Public Key Infrastructure PKIX Feuille de route, article disponible sur : http://www.ietf.org/internet-drafts/draft-ietf-pkix-roadmap-04.txt

**3- Béatrice FRAENKEL et David PONTILLE**, « l'écrit Juridique à l'épreuve de la signature électronique, approche pragmatique ». Revue Langage et société, 2003/2 n° 104, pp. 83 à 122. Disponible sur le site : http://www.cairn.info/revue-langage-et-societe-2003-2-page-83.htm

**4 ----------,** « La Signature au temps de l'électronique », Revue Politix, vol, 02 n°74, 2006, pp. 103 à 121. Disponible sur : http://www.cairn.info/revue-politix-2006-2-page-103.htm

**5- Bernard BRUN**, Nature et impacts juridiques de la certification dans le commerce électronique sur Internet. Article publié sur : http://www.signelec.comcontentsearticlesarticle_bernard_brun_html

**6- Carole AUBERT**, « La nouvelle loi sur la signature électronique et le droit du bail». Article disponible sur : http://www.unine.chfilescontentsitesbailfilessharedDocumentsSeminaires_precedents2006Aubert

**7- David BOUNIE**, « quelques incidences bancaires et monétaires des systèmes de paiement électronique », Revue économique/ Presses de Sciences Po, 2001/7 vol, 52, pp. 313 à 330. Article disponible sur : http://www.cairn.info/revue-economique-2001-7-page-313.htm

**8- Didier GOBERT**, « Cadre juridique pour les signatures électroniques et les services de certification: analyse de la loi du 9 juillet 2001», Publié in La preuve, Formation permanente CUP, vol, 54, mars 2002, pp. 83 à 172. Disponible sur : http://www.consultandtraining.com

**9- David BOUNIE et Marc BOURREAU**, « Sécurité des Paiements et Développement du Commerce Électronique », Revue économique/ Presses de Sciences Po, vol, 55, n° 04/ 2004, pp. 689 à 714. Disponible sur : http://www.cairn.info/revue-economique-2004-4-page-689.htm

**10- Eric A. CAPRIOLI,** signature et confiance dans les communications électroniques en droits français et européen. Article publié sur : http://www.caprioli-avocats.com

**11- ----------**, De l'authentification à la signature électronique : quel cadre juridique pour la confiance dans les communications électroniques internationales ? Article disponible sur : http://www.caprioli-avocats.com

**12- ----------**, L'archivage des documents électroniques. Article disponible sur : http://www.caprioli-avocat.com

**13- Florence DARQUES et Laurence BIRNBAUM-SARCY**, La signature électronique Comparaison entre les législations française et américaine, Article publié sur Internet. Voir le site : http://www .signelec.com/content/se/articles/comparaison_fr_us_html

**14- Garance MATHIAS et Jean-Michel SAHUT,** le paiement : enjeu du e - commerce. Article disponible sur : http://piae.univ-larochelle.frimg/

**15- Hillarius KLUDZE et W. Glenn Rowe**, « le rôle de la confiance dans le commerce électronique : une analyse stratégique », Revue gestion, 2002/5 vol, 27, pp. 80 à 90. Article disponible sur : http://www.cairn.info/revue-gestion-2002-5-page-80.htm

**16- Hassan BEZZAZI**, Sécuriser les échanges numérique, article publié sur le site : http://www.cours.unjf.frfile/

**17- Jean-Luc ARCHIMBAUD**, « les principes techniques des certificats électroniques », Revue les cahiers du numérique, vol. 4, n° 3-4/2003, pp. 101-110. Disponible sur : http://www.cairn.info/revue-les-cahiers-du-numerique-2003-3-page-101.htm

**18- Louise MARTEL et René ST-GERMAIN,** « la Certification de Conformité des Sites Web », Revue gestion, 2002/5 vol. 27, pp. 91 à 97. Article disponible sur : http://www.cairn.info/revue-gestion-2002-5-page-91.htm

**19- Le Duc BAO**, Authentification des empreintes digitales dans un système BioPKI, Institut de la Francophonie pour l'Informatique (Hanoi), 2007. Disponible sur : http://www.ifi.vnu.edu/

**20- Maxime WACK et AL**, «certification et archivage légal de dossiers numériques», Revue document numérique, vol 6, n°1/2002, pp. 145 à 158. Article disponible sur : http://www.cairn.info/revue-document-numerique-2002-1-page-145.htm

**21- Marc LACOURSIÈRE et Édith VÉZINA**, La sécurité des opérations bancaires par Internet. Article disponible sur : http://www.themis.umontreal.ca

**22- Marc LACOURSIÈRE,** « La responsabilité bancaire à l'ère du commerce électronique : impact des autorités de certification », revue les cahiers de droit, vol. 42, n° 4, 2001, pp. 961-1012. Article disponible sur : http://www.erudit.org/revue/cd/2001/v42/n4/043684ar/

**23- Maximilien AMEGEE**, La signature électronique fragilise-t-elle le contrat. Article disponible sur : http://www.lafrique.free.fra/

**24- Pascal AGOSTI**, Le régime juridique des actes authentiques électroniques. Disponible sur : http://www.caprioli-avocats.com

**25- Patrice JOURDAIN**, La Distinction des responsabilités délictuelle et contractuelle : état du Droit Français. Disponible sur : http://www.grerca.univ-rennes1.fr/

**26- Philippe PIERRE**, La place de la responsabilité objective: Notion et rôle de la faute en droit français. Article disponible sur : http://grerca.univ-rennes1.fr/digitalAssets/268/268674_ppierre.pdf

**27- Renaud HOFFMAN**, Une architecture de certification à l'échelle mondiale, Disponible sur: http://www.01net.com/article/168355.html.

**28- Samarcq (N),** Les actes authentique électronique, une réalité au 1er février, article publié sur : http://www.droit-ntic.

**29- Sedallian (V),** preuve et signature électronique. Article publié sur : http://www.internet-juridique.net

**4- Textes Juridiques** :

**1**- Loi fédérale complétant le Code civil suisse (Livre cinquième: Code des obligations) du 30 mars 1911(Suisse). http://www.admin.chopcfrclassified-compilation/

**2**- Loi Fédérale sur la protection des données (LPD) du 19 juin 1992 (Suisse). http://www.admin.chopcfrclassified-compilation20011277index.html

**3**- Directive 93/13/CEE du Conseil, du 5 avril 1993, concernant les clauses abusives dans les contrats conclus avec les consommateurs. J.O.C.E, n° L 095 du 21/04/1993. http://www.eur-lesc.europa.eu

**4**- Loi Fédéral du 6 octobre 1995 sur les entraves techniques au commerce, LETC (RS 946.51) et les dispositions d'exécution pertinentes(Suisse). http://admin.chopcfrclassified-compilation20011277index.html

**5**- Directive 95/46/CE du Parlement Européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. J.O.C.E, n° L 281/31 du 23/11/1995. http://www.eur-lesc.europa.eu

**6**- Uniform Electronic Transactions Act (1999), Drafted by the National Conference of Commissioners on Uniform State Laws, approved and recommended for enactment in all the states at its annual conference meeting in its one-hundred-and-eighth year in DENVER, COLORADO, july 23 – 30, 1999. http://www.nccusl.org/nccusl/uniformact_ factsheets/uniformacts-fs-ueta.asp

**7**- Directive 1999/93/CE du parlement européen et du conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques. J.O.C.E, n° L 13, du 19 janvier 2000. http://www.ec.europa.eu

**8**- Loi concernant le Cadre Juridique des Technologies de l'Information (Québec). http://www.canlii.ca/

**9**- Public Law 106–229106th Congress June 30, 2000, Electronic Signatures in Global and National Commerce Act. http://www.fdic.govregulationscompliancemanualpdfX-3.1.pdf.

**10**- Loi sur la Protection des Renseignements Personnels et les Documents Électroniques, LC 2000 (Canada). http://www.ulcc.cafrlois-uniformes-fr/

**11**- Loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique (France). J.O.R.F, n° 62 le 14 mars 2000. http://www.legifrance.gouve.fr/

**12**- Loi du 9 Juillet 2001, fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification. MB n° 2699 du 29.09.2001. http://www.moniteur.be

**13**- Loi fédérale sur les services de certification dans le domaine de la signature électronique (Loi sur la signature électronique, SCSE) du 19 décembre

2003(Suisse).http://www.admin.chopcfrclassified-compilation20011277index.html

**14**- Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives. J.O.R.F, n° 286 du 9 décembre 2005. http:// www.legifrance.gouve.fr/

**15**- Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique. J.O.R.F, n° 143 du 22 juin 2004. http:// www.legifrance.gouve.fr/

**16**- Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. J.O.R.F, n° 182 du 07 août 2004. http:// www.legifrance.gouve.fr

**17**- Ordonnance (suisse) sur les services de certification dans le domaine de la signature électronique (Ordonnance sur la signature électronique, OSCSE), du 3 décembre 2004. http://admin.chopcfrclassified-compilation20011277index.html

**18**- Décret n° 2001-272 du 30 mars 2001 relatif à la signature électronique. J.O.R.F, n° 0077 du 30 mars 2001. http://www.legifrance.gouve.fr/

**19**- Décret n° 2001-693 du 31 juillet 2001 créant au secrétariat général de la défense nationale une direction centrale de la sécurité des systèmes d'information. J.O.R.F, n° 177 du 02 août 2001. www.legifrance.gouve.fr/

**20**- Le décret n° 2002-535 du 18 avril 2002, relatif à l'évaluation et la certification de la sécurité offerte par les produits et systèmes des technologies de l'information. J.O.R.F, n° 92. Du 19 avril 2002. http://www.legifrance.gouve.fr/

**21**- Décret n° 2005-973 du 10 août 2005 modifiant le décret n° 71-941 du 26 novembre 1971 relatif aux actes établis par les notaires. J. O.R.F, n° 186 du 11 août 2005. www.legifrance.gouve.fr/

**22**- Décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information ». J.O.R.F, n°156 du 8 juillet 2009. www.legifrance.gouve.fr/

**23**- Décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives. J.O.R.F, n° 0029 du 4 février 2010.

www.legifrance.gouve.fr

**24-** Décret n° 2011-434 du 20 avril 2011 relatif à l'horodatage des courriers expédiés ou reçus par voie électronique pour la conclusion ou l'exécution d'un contrat. J.O.R.F, n° 0094 le 21 avril 2011. www.legifrance.gouve.fr/

**25-** Arrêté de ministre de l'économie et de finance et de l'industrie du 31 mai 2002, relatif à la reconnaissance de qualification des prestataires de services de certification électronique et à l'accréditation des organismes chargés de l'évaluation. J.O.R.F, n° 132 du 08 juin 2002. www.legifrance.gouve.fr/

**26-** Arrêté de ministre délégué à l'industrie, du 26 juillet 2004 relatif à la reconnaissance de qualification des prestataires de services de certification électronique et à l'accréditation des organismes qui procèdent à leur évaluation. J.O.R.F, n° 182 du 07 août 2004. Abrogeant l'Arrêté de ministre de l'économie et de finance et de l'industrie du 31 mai 2002. www.legifrance.gouve.fr/

**27-** Arrêté royal du 6 décembre 2002, organisant le contrôle et l'accréditation des prestataires de service de certification qui délivrent des certificats qualifiés. MB n° 192 du 17.01.2003. http:// www.moniteur.be

**4- Jurisprudences:**

**1**- Cass. Civ, 1ère chambre, du 8 novembre 1989, pourvoi n° 86-16196. Bulletin 1989, I, n° 342. http://www.legifrance.gouve.fr/

**2**- Cass. Civ, 1ère chambre, du 8 novembre 1989, pourvoi n° 86-16197. Bulletin 1989, I, n° 342. www.legifrance.gouve.fr/

**3**- Cass. Civ, 1ère chambre, du 30 septembre 2010, pourvoi n° 09-68555. Bulletin 2010, I, n° 178. www.legifrance.gouve.fr/

**5- Séminaire:**

**1- Ahmed BERBAR,** Certification Électronique en Algérie Situation et Perspectives, (SICE' 2011 ARPT), Alger du 08 et 09 décembre 2009. http://www.arpt.dz

**2- Hadjira BOUDER**, le cadre juridique de la signature et de la certification électronique en Algérie: que reste-t-il à faire? (SICE' 2011 ARPT), Alger du 28 Au 30 Juin 2011. http://www.arpt.dz

**3- Manel ABDELKADER,** La Certification Électronique en Tunisie Expérience et Défis, (SICE' 2011 ARPT), Alger du 08 et 09 décembre 2009. http://www.arpt.dz

**6- Sites Internet:**

http://csrc.nist.gov/publications/PubsSPs.html#800-63-Rev1.
http://www.wikipédia.fr
http://www.itida.gov.eg/E.signature-root-ca.agp
http://www.verisign.com/
http://www.eurochambres.be
http://www.sibtel.com.tn
http://www.clictopay.com

# فهرس الموضوعات

**ملخص**

للتصديق الإلكتروني دور فعال ومهم في معاملات التجارة الإلكترونية والعمليات المصرفية إذ يعمل على خلق مناخ ثقة آمن لأطراف العقد الإلكتروني المبرم عبر شبكة الإنترنيت، في بيئة إلكترونية إفتراضية تُعرضهم إلى مختلف المخاطر كانتحال الهوية، وتلقي الغير للرسائل الإلكترونية الموقعة، وإنكار عقد بيع أو عملية دفع أو تبادل إلكتروني للبيانات، لذا فإنّ الحاجة إلى إرساء بنية مرفق المفاتيح العمومية وفقا لنموذج التصديق الموثوق به تبدو من الضروريات التي تسمح لسلطة التصديق الإلكتروني، بتحديد هوية أطراف الرسائل الإلكترونية وضمان سرية وسلامة البيانات الإلكترونية المتداولة، وعدم إنكارها، وذلك عن طريق قيامها بإصدار شهادات تصديق إلكترونية معتمدة وفقا للمعايير الدولية المعترف بها.

فعن طريق شهادة التصديق الإلكتروني يمكن ضمان الصلة الرسمية بين الشخص والمفتاح العمومي وتسهيل عملية التحقق من سلامة المعلومات التي تحتويها الوثيقة الإلكترونية مع تأكيد صحتها، فشهادة التصديق الإلكتروني الموصوفة تضمن للأطراف المعولة إمكانية إثبات تصرفاتهم الإلكترونية المتداولة في حالة النزاع أمام الجهات القضائية.

**Résumé**

La Certification électronique a un rôle efficace et primordial dans les transactions du commerce électronique et les opérations bancaires, son objectif est d'instaurer un climat de confiance sécurisé entre les parties prenantes d'un contrat électronique conclu, dans un environnement virtuel (Internet) où sont confrontés à un certain nombre de risques tels que, l'interception du message signé électroniquement par un tiers ou l'usurpation d'identité, la répudiation de l'acte de vente ou le paiement et l'échange, néanmoins, la mise en place d'une infrastructure à clé publique (PKI ou ICP) s'avère être une nécessité qui permet à l'autorité de certification électronique, de garantir l'authentification des auteurs des messages, la confidentialité et l'intégrité de données électroniques transmises, et la non-répudiation, en émettant des certificats électroniques qualifiés selon des normes de sécurité des systèmes éditées par des organismes principaux reconnues à l'échelle mondiale, qui sont applicables aux signatures et certificats électroniques.

En effet, le rôle du certificat électronique consiste à garantir un lien formel entre une personne et une clé publique, et faciliter la vérification de l'exactitude de l'information contenue dans le document électronique, et d'en assurer sa validité face à un tiers, c'est ainsi que la présence du certificat électronique qualifié assure la qualité d'une preuve irréfutable qui puisse être acceptée par les parties en cas de litige devant les juridictions.