موثوقية التوقيـــع الإلكتروني فـــي العمل الإداري

أ/ سردوك هيبة
جامعة عنابة

الملخص :

الثقة و الأمان ضالة أعضاء ورواد المجتمع الافتراضي. أين توجد حياة غير ملموسة موازية لحياتنا التقليدية بكل جوانبها و مجالاتها، و لم تفوت الحكومات المعاصرة مواكبة ركب النهضة الرقمية لتقدم خدماتها في مختلف القطاعات عبر بواباتها الإلكترونية، وساعدها على ذلك ما قدمته التقنيات الحديثة من موثوقية بتطوير آليات التشفير و ابتكار أجهزة التصديق الإلكتروني و ما تقدمه من خدمات عملت على توطيد علاقات هذا المجتمع غير المحسوس بتدقيق هوية الأشخاص.

و هو ما سنحاول الحديث عنه من خلال بيان طرق توثيق التوقيع الإلكتروني، لنيل الموثوقية المنشودة في روابط الحكومة الإلكترونية بغيرها من اعضاء المجتمع الإفتراضي.

Résumé :

L'évolution technologique en matière d'informatique et de communication a permis la création d'un monde numérique multi facettes où plusieurs acteurs publics ou privés interagissent.

Les gouvernements ne sont pas resté en marge de cette révolution digitale en proposant leurs services par les moyens de ces techniques d'informatique et de communication.

La confiance et la crédibilité sont des caractères recherché dans le monde matériel qu'immatériel à un point où les gouvernements cherchent à les garantir dans ce dernier, en établissant une certification stricte et fiable pour identifier toute personne agissant dans ce monde virtuel.

C'est pour cela que l'objet de cette étude est l'authentification de la signature électronique, ses méthodes (le chiffrement, la certification), ses critères, pour sécuriser et protéger les liens dématérialisés de l'administration avec les tiers .

مقدمة:

بما أن الإدارة العامة فكرة معنوية مستقلة عن كيان الأشخاص الطبيعيين القائمين على تسييرها و إدارة مختلف جوانب نشاطها، لذلك توجّب إنشاء ذاكرة ورقية تفرغ فيها كل الأعمال الإدارية في شكل مكتوب (حتى و لو كانت القاعدة العامة في مختلف هذه الأعمال القانونية هي عدم وجوب الكتابة ما لم ينص القانون صراحة على خلاف ذلك).

و بتطوير مفهوم الكتابة بمقتضى تعديل أحكام القانون المدني سنة 2005، حيث ساوى المشرع بين الكتابة التقليدية (حبر و ورق) و بين الكتابة الإلكترونية(وسائط الكترونية)، أصبح من المستساغ أن تعتمد الإدارة العامة على مستخرجات الحاسب الآلي في تحرير أوراقها الإدارية و حفظ أرشيفها.

وبعد أن بدأت الإدارة العامة بتقديم خدماتها بالاعتماد على وسائل التكنولوجيا الحديثة، اصطدمت بإشكالية اللاماديات لأن الأشخاص طالبي الخدمة العمومية هم شخصيات غير محسوسة لا يعرفون إلا بإمضاءاتهم الإلكترونية، هذا من جهة. ومن جهة أخرى شكل مبدأ سيادة الدولة و ضرورة تحصين المرافق العامة من اختراق الأشخاص غير المرغوب فيهم هاجس الحكومة الإلكترونية.

إلا أن اجتهاد الأدمغة الخلاقة توصّل إلى توفير درجة لا يستهان بها من الأمان في الحفظ و الاسترجاع و مواجهة مخاطر اللاماديات و القرصنة و جرائم المعلوماتية، و وضع حد لفرص انتحال الشخصيات.

فما هي الطرق التقنية، والقانونية التي تبنتها التشريعات لتحديد الهوية الحقيقية لطالب الخدمة العمومية ومقدّمها بشكل يقي من المخاطر التي تنتقص من مزايا التكنولوجيا الحديثة و ما توفره من وقت وجهد و سرعة و دقة و تميّز في الأداء الحكومي؟

لا شك في أنّ أنجع وسيلتين تم التوصل إليهما في الوقت الراهن ونظمتهما قوانين الدول المقتبسة عن قانون الأونسترال النموذجي المتعلق بالتوقيعات الإلكترونية لسنة 2001، هما تقنية التشفير(المطلب الأول) و تنصيب أجهزة مختصة بمنح شهادات تثبت هوية صاحب التوقيع الإلكتروني(المطلب الثاني)

المطلب الأول: التشفير

تبرز أهمية تقنية التشفير من خلال حماية الأعمال و البيانات التي يتم تداولها عبر شبكات الإتصال الحديثة، فهي تكفل سرية أعمال الإدارة الإلكترونية سواء ما تعلق منها بتنظيمها الداخلي و علاقتها بموظفيها و عمالها، او ما يخص وظيفتها الأساسية في تقديم خدماتها للجمهور و ما تستلزمه من استصدار قرارات على اختلاف أنواعها و إبرام عقود وصفقات أو تخليص مسائلها المالية في مجال المعاملات البنكية

و تتطلب عملية التشفير و فك التشفير استخدام بعض التعليمات السرية التي يشار إليها عادة بمفاتيح خاصة، و هو ما سيأتي تفصيله بعد عرض مفهوم التشفير.

الفرع الأول: مفهوم التشفير

على الرغم من أهمية التشفير، إلا أن معظم القوانين المقارنة المتعلقة بالمعاملات الإلكترونية لم تعنى بإعطاء تعريف محدد لهذا المصطلح بما فيها التشريع الوطني، وذلك على خلاف القانون التونسي الخاص بالمبادلات التجارية الإلكترونية رقم 83 لسنة 2000، الذي عرفه بموجب نص الفصل 2 منه بأنه:"التشفير إما استعمال رموز أو إشارات غير متداولة تصبح بمقتضاها المعلومات المرغوب تمريرها أو إرسالها غير قابلة للفهم من قبل الغير أو استعمال رموز أو إشارات لا يمكن الوصول إلى المعلومة بدونها". وفي ظل غياب التعريف القانوني للتشفير سنحاول عرض بعض التعريفات الفقهية.

I- تعريف التشفير:

أشتق مصطلح "التشفير" من الكلمة اليونانية "KIUPTOS" التي تعني مخفي "فالتشفير هو الآلية التي تحمي معلوماتك القيمة، مثل المستندات أو الصور أو المعاملات الإلكترونية داخل الانترنت من الأشخاص غير المرغوب فيهم للحيلولة دون الوصول إليها أو تغييرها.

ويعمل التشفير باستخدام "شفرة" (صيغة رياضية) و مفتاح لتحويل البيانات المقروءة ("نص عادي")، إلى شكل لا يستطيع الآخرون فهمه ("نص مشفر"). و المفتاح الخاص بك يجعل البيانات المشفرة فريدة من نوعها، يمكن فك تشفيرها حصريا بواسطة من يعرف المفتاح.

و عادة ما تكون المفاتيح سلسلة طويلة من الأرقام التي تحميها آليات المصادقة المشتركة مثل: كلمات المرور، أو الرموز، أو القياسات الحيوية مثل بصمة الإصبع".[1]

"و لذلك يعد التشفير من وسائل حفظ و سرية المعلومات في نطاق الأنظمة الإلكترونية، لاسيما في الحكومة الإلكترونية و تطبيقاتها. كما في التجارة الإلكترونية، و التي تتطلب الحفاظ على بيانات و معلومات الأطراف و حجم الصفقات و نوعها و كذلك حماية النقود المتداولة في نطاق هذه التجارة". [2]

II- مستويات التشفير:

إن الأجهزة الإلكترونية الحديثة المستعملة للولوج إلى مكاتب المرافق العامة الإلكترونية التي تقوم بالنشاط الإداري ليست في حقيقة الأمر مجرد وسيلة لنقل و تبادل البيانات و الحصول على الخدمات العامة المتوفرة الكترونيا فقط، و إنما هي بمثابة مستودعات حفظ و أرشفة الكترونية سواء بالنسبة للإدارة الإلكترونية في حد ذاتها أو بالنسبة للفرد الذي طلب هذه الخدمة العامة.

و لما كان الأمر كذلك، فلابد أن يشمل التشفير المعلومات المخزنة على مستوى هذه الإدارات العامة وكذلك البيانات و الرسائل الإلكترونية المتداولة إلكترونيا.

1- تشفير المعلومات المحفوظة:

يتم تشفير المعلومات و البيانات المحفوظة على أجهزة الحاسب الآلي و غيره من وسائل الحفظ الإلكتروني (كالمخزنات العلمية usb flash أو الأقراص المدمجة و الممغنطة أو الأجهزة اللوحية و الهاتف الذكي)، و يتم على مستويين:

أ- **التشفير على مستوى الملفات:** حيث تشفر ملفات معينة أو مجلدات بأكملها. و من تطبيقاته "نظام تورتل انترست" و نظام "نيل زيمرمان للخصوصية"[3]:

ب- **تشفير القرص الثابت:** يتم التشفير على مستوى القرص الثابت كإستخدام نظام (إف دي إي F.D.E) الذي يعمل على تشفير كل محتويات القرص الثابت تلقائيا بما فيها الملفات المؤقتة[4].

2- تشفير المعلومات المتبادلة و المتدفقة عبر شبكة الإدارة الإلكترونية:

و يتم التشفير في هذه الحالة على عدة مستويات و تتلخص بالأساس فيما يلي:

أ- تشفير وصلات الإتصال:

يستخدم هذا النوع من التشفير لتأمين كل ما يمر عبر وصلات الاتصال عند نقطة الإرسال و تفك الشفرة عند نقطة الاستقبال. و يعتبر بروتوكول "نظام أمن الاتصالات" المعروف بـــ (SSL) أحد أهم التطبيقات المستخدمة، و كذلك نظام "الشبكات الخاصة

المؤمنة" (VPN) و هو ما يتفق مع مقتضيات تأمين شبكة الإدارة الإلكترونية.

ب- تشفير مستوى التصفح:

تشفر البيانات المتداولة بين المتصفح و بين الموقع الذي يجري تصفح المعلومات عبره. بحيث تدعّم مواقع و بوابات الإدارة الإلكترونية بخيار التشفير التلقائي بشكل افتراضي ويعتبر نظام التصفح الآمن أو بروتوكول (HTTPS) الأكثر شيوعا، وكذلك بروتوكول (WPA2) الذي يعتبر أحد أقوى آليات التشفير عند الاتصال بشبكة (واي فاي Wi-Fi) العامة.

الفرع الثاني: طرق التشفير:

بما أن التشفير هو عملية التغيير في البيانات على نحو يتعذر معه قراءتها إلا من طرف الشخص الذي يعرف مفتاح فك التشفير. ومن هنا تظهر العلاقة بين التوقيع الرقمي والتشفير، " فالتوقيع الرقمي هو ختم رقمي مشفر يضمن عدم تعرض الرسالة للتعديل والاختراق"[5]

وتستخدم التوقيعات الالكترونية ما يعرف بنظام شفرة المفتاح العام الذي يقوم على منهج معين بالاستعانة بمفتاحين مختلفين ولكنهما مترابطان حسابيا. احدهما لتحويل البيانات الى اشكال غير مفهومة وغير مقروءة والثاني وظيفته التحقق من صحة التوقيع وإعادة الرسالة الى شكلها المقروء.

وقد يعتمد في التشفير على الاسلوب الذي يقوم على مفتاح واحد للتشفير ولفك التشفير. وبالإضافة إلى ذلك يوجد أسلوب ثالث يقوم على الدمج بين النظامين وهو ما سنحاول ايجازه.

I- التشفير المتماثل:

وهو من التقنيات التي يعتمد فيها على مفتاح واحد للتشفير وفك التشفير، وينتج هذا النوع من التشفير بناء على خوارزمية (لوسيفر)[6]. بحيث لا يمكن الإطلاع على محتوى الرسالة المشفرة الا باستخدام المفتاح ذاته الذي استعمله المرسل.

هذا المفتاح يمكن ان يتضمن حروفا كبيرة او صغيرة وأرقاما عديدة ورموزا اخرى، وذلك بحسب ما ينتج عن الخوارزمية التي تم انشاؤها بين الطرفين للتشفير. وفي حال ادخال كلمة المرور المعدة بالاتفاق بين الطرفين تتحول الى عدد ثنائي يفهمه جهاز الكمبيوتر ثم تضاف إليه رموز اخرى لزيادة طوله. هذا العدد الثنائي هو "مفتاح التشفير" الذي يصعب تزويره بفعل تعقيده.

وتشكل كيفية تبادل هذا المفتاح بين المرسل والمرسل اليه الصعوبة الحقيقية التي تواجه هذه الطريقة لإمكانية سرقته من قبل الغير اثناء تبادله عبر شبكة الانترنت، وهو ما يشكل اهم المآخذ على هذا الاسلوب. ويمكن تفادي هذا العيب بتوفر وسيلة اخرى للتبادل بالاتفاق بين الطرفين بما يكفل سلامته وسريته[7] في مواجهة المتطفلين.

II- التشفير اللامتماثل:

يعد التشفير اللامتماثل من اهم الوسائل التي تضمن سلامة المحرر الالكتروني من كل تبديل او تغيير باستخدام تقنية شفرة المفتاحين العام والخاص[8]، بحيث يتم التشفير بمفتاح وفك التشفير يكون بمفتاح آخر. فيكون لكل شخص (طبيعيا كان او معنويا) نوعين من المفاتيح احدهما "عام" ويكون معروف من أكثر من جهة لأنه يكون متاحا الكترونيا. أما الثاني فهو "المفتاح الخاص" يحتفظ به الشخص وينفرد بمعرفته.

ويتم إصدار رقم الأساس عن طريق البرنامج المتخصص أو احد الهيئات المستقلة المتخصصة في اصدار هذه الارقام. وهو ما يعرف بشهادة المصادقة بحيث يكون لكل مستخدم رقم اساس مثلا (A) ويتم تقسيمه الى مجموعتين: المجموعة (B) وهي ما يعرف بالمفتاح العام و(C) وهي تشكل المفتاح الخاص. بحيث اذا ضربنا(B) في (C) يكون الناتج (A) وهو الرقم الأساس وهو الرقم اللازم لإعادة الملفات والمعلومات إلى وضعها الأصلي قبل التشفير وطبعا هذا الرقم محمي ومشفر بقوة ولا يمكن الوصول اليه.

كما يمكن الكشف عن كل تغيير او تبديل في البيانات الالكترونية من خلال الاستعانة بخدمات سلطة التصديق وشهادات التصديق الالكتروني التي تصدرها. والتي تؤدي الى توفير الأمان والثقة في التوقيع الالكتروني وتضمن صحته وسلامته وتؤكد حجتيه في الإثبات

"إن المفاتيح التكميلية في نظام الشفرة اللاتماثلية تدعى عشوائيا المفتاح الخاص والذي يعرفه فقط الموقع ويستخدم لإنشاء التوقيع الالكتروني. والمفتاح الشفري العام معروف على نطاق أوسع يستخدم من قبل شخص موثوق به للتثبت من صحة التوقيع وفي حال استدعت الظروف الى ان اكثر من جهة بحاجة للتثبت من صحة التوقيع الالكتروني فان المفتاح الشفري العام يجب ان يكون متوفرا لتلك الجهات، على ان يوزع عليهم او ينشر في ملف الاتصال كي يتم الوصول اليه بسهولة . رغم ذلك فان لكل وسيلة من هذه الوسائل ثغراتها وهو ما استتبع اللجوء لفكرة الشخص الوسيط"[9]

وتتم عملية التشفير اللامتماثل على النحو التالي:

أ- التشفير باستخدام المفتاح العام:

يستطيع أي شخص أو جهة تشفير البيانات التي يستقبلها المرسل اليه وذلك باستعمال المفتاح العام، الخاص بالمرسل إليه.

يستقبل المرسل إليه الرسالة المشفرة ليفك شفرتها ويعيدها إلى صيغتها المقروءة باستعمال المفتاح الخاص.

ب- التشفير باستخدام المفتاح الخاص:

يستخدم المرسل في هذه الصورة مفتاحه الخاص لتشفير الرسالة التي يستقبلها المرسل اليه والتي تعاد الى صورتها العادية باستعمال المفتاح العام للمرسل ذاته. وبالرغم من تحديد صاحب الرسالة الالكترونية بدقة لانفراده باستخدام المفتاح الخاص إلا ان سهولة اختراق الرسالة تحبط هذه الطريقة لانتشار المفتاح العام الذي تعلمه اكثر من جهة بالرغم من بقاءه سرا بالنسبة للجمهور. وبهذا لا يوفر السرية والأمان المرجوان من عملية التشفير.

ج- التشفير بمفتاحين (المزج بين نظامي المفتاح المتماثل والمفتاح العام):

يتم التشفير مرتين، المرة الأولى تكون باستخدام المفتاح العام للمرسل اليه ثم تشفر باستخدام المفتاح الخاص للمرسل فيتأكد المرسل اليه من صدورها من المرسل فعلا.

ترسل الرسالة المشفرة باستخدام المفتاح العام والمفتاح المشفر بأي طريقة ليقوم المرسل اليه بفك الشفرة على مرحلتين. الأولى باستخدام المفتاح العام للمرسل فيحصل على رسالة مشفرة بمفتاحه العام ثم يقرأ الرسالة بواسطة مفتاحه الخاص فيتحقق بذلك سرية الرسالة والتأكد من صدورها من صاحبها.[10]

ولضمان فاعلية تقنية التشفير في تأمين معاملات شبكة الحكومة الالكترونية لابد من ان تأخذ جملة من الاحتياطات والإجراءات لتأمين تدفق المعلومات والبيانات وتضمن فاعلية التشفير كجعل عملية فك التشفير من الاختصاصات الشخصية لموظفين محددين بذواتهم بحيث لا يجوز التفويض بشأنها. مع توزيعها طبقا لمعيار التخصص في العمل، فتزود كل وحدة إدارية من المنظمة الإدارية بالمعلومات المتصلة بمجال عملها فقط.[11]

المطلب الثاني : أجهزة التصديق الالكتروني:

بما أن التوقيع الالكتروني من طبيعة غير ملموسة، ويتم إنشاؤه وتداوله في بيئة محررة من كل الشكليات والماديات، فإن إمكانية تحريفه أو تزويره واردة جدا. ولذلك ذهبت

معظم القوانين إلى إدخال شخص وسيط محايد مهمته السهر على صحة التوقيع الالكتروني بإصدار شهادات تؤكد هوية الموقّع وصحة المعلومات التّي دوّنها، وحقيقة طلبه الخدمة المتوفرة عبر الأنترنت. هذا الطرف يطلق عليه تسمية "جهات التصديق " أو "جهات توثيق التوقيع الالكتروني " أو " مقدم خدمات التصديق " أو "مورد خدمات التصديق".

وحرصت هذه التشريعات بما فيها التشريع الجزائري على بيان كيفية تشكيل هذه الجهات وآليات عملها، فقد تكون شخصا طبيعيا أو معنويا وقد تكون هيئة عامة أو خاصة وطنية أو أجنبية على أن تتوفر في هذه الجهة الشروط المحددة قانونا والمتعلقة عادة بأهلية وجنسية مقدم الخدمة، وما يجب أن يقدمه هذا الجهاز من ضمانات. وهو ما سنبينه في الفرعين التاليين.

الفرع الأول: أسلوب الموظف العام المختص بالتصديق الإلكتروني:

اعتمد المشرع الإماراتي بموجب نص المادة (23) من القانون رقم 02 لسنة 2002 الخاص بالمعاملات والتجارة الالكترونية لإمارة دبي على أسلوب الموظف العام الذي يختص بالتصديق الإلكتروني، بحيث يتم تعيين مراقب لخدمات التصديق بموجب قرار صادر عن رئيس سلطة منطقة دبي الحرة للتكنولوجيا و التجارة الإلكترونية و الإعلام يضطلع خاصة بمهمة ترخيص و تصديق و مراقبة أنشطة مزودي خدمات التصديق و الإشراف عليها.

في حين يسهر مزودو خدمات التصديق المرخص لهم بمزاولة النشاط على التقيد بالاشتراطات والواجبات القانونية المذكورة في نص المادة 24 من قانون رقم 2 لسنة 2002 الخاص بالمعاملات والتجارة الالكترونية لإمارة دبي.

I- واجبات مراقب خدمات التصديق ومفوضه:

يجوز للمراقب الذي يعينه رئيس سلطة منطقة دبي الحرة للتكنولوجيا والتجارة الإلكترونية والإعلام أن يقوم بتفويض جزء من مسؤولياته كتابة، ويتخذ المراقب ومفوضه صفة الموظف العام.

يتولى المراقب ضبط قواعد تنظيم وترخيص عمل مزودي خدمات التصديق الذين يعملون في الإمارة، ويرفعها لرئيس سلطة منطقة دبي الحرة للتكنولوجيا والتجارة الالكترونية والإعلام لإعتمادها، ومن بين إختصاصاته نذكر:

الفصل في طلبات منح أو تجديد تراخيص مزودي خدمات التصديق- بيان المعايير المناسبة فيما يتعلق بمؤهلات وخبرة مقدمي خدمات التصديق وتدريب موظفيهم- تحديد شكل ومحتوى أي شهادة أو مفتاح رقمي- وضع اللوائح اللازمة لتنظيم التفتيش والتدقيق في أعمال مزودي خدمات التصديق- تحديد شروط انشاء وتنظيم أي نظام الكتروني بواسطة مزود خدمات تصديق[12].

II- واجبات مزودي خدمات التصديق:

حدد قانون امارة دبي جملة من القيود والواجبات التي يجب أن يلتزم بها مزودو خدمات التصديق الذين يمارسون نشاطهم في الإمارة أو الأجانب، هي كالآتي:

- أن يمارس مزود خدمات التصديق عناية معقولة لضمان دقة واكتمال كل ما يقدمه من بيانات جوهرية ذات صلة بالشهادة أو مدرجة فيها طوال سريانها.
- أن يوفر وسائل يكون من المعقول الوصول اليها وتمكن الطرف الذي يعتمد على خدماته من التأكد مما يلي:
  - هوية مزود الخدمات
  - أن الشخص المعين هويته في الشهادة لديه السيطرة في الوقت المعني على أداة التوقيع المشار اليها في الشهادة.

الفرع الثاني: أسلوب هيئات التصديق الإلكتروني:

على غرار قانون الأونسترال النموذجي المتعلق بالتوقيعات الإلكترونية، فإن أغلب القوانين المتعلقة بتنظيم المعاملات الإلكترونية لم تتضمن أي تعريف لجهات التصديق و لكنها اكتفت ببيان طريقة تشكيلها و كيفية تسييرها لتسهيل المهام المنوطة بها و رتبت مسؤوليتها في حال إخلالها بالتزاماتها الواقعة على عاتقها.

حيث اكتفى نص المدة 09 من قانون الأونسترال النموذجي بشأن التوقيعات الإلكترونية ببيان الإلتزامات الواقعة على عاتق مقدم خدمات التصديق دون تعريفه أو تحديد تشكيلته أو كيفية أدائه وظيفته. وسنعرض موقف التشريعات المقارنة والتشريع الوطني بخصوص تنظيم هذه الهيئة.

I- تنظيم هيئات وطنية للتصديق الإكتروني في القوانين المقارنة:

أنشأت بعض القوانين المقارنة أجهزة وهيئات مختصة بالتصديق، هذه الهيئات يكسبها القانون شخصية معنوية مستقلة و قد تكون من أشخاص القانون العام، أو من أشخاص

القانون الخاص. و النوعان يخضعان لإشراف السلطة التنفيذية، و يتم تنظيمها طبقا للتدرج السلمي على ثلاث مستويات:

1- جهة التصديق على المستوى المركزي:

تتولى مهمة المحافظة على محتوى الرسائل المتبادلة من التغيير و الحذف أو الإضافة بتحديد شروط و مواصفات إنشاء منظومة إحداث الإمضاء و التدقيق، و تمنح تراخيص مزاولة وظيفة مزودي خدمات التصديق أو أي نشاط له علاقة بهذا المجال.

كما تتولى توفير التكنولوجيا الآمنة التي تسمح باستعمال المفاتيح العامة و الخاصة، و كذا ابرام اتفاقيات الاعتراف المتبادل مع الأطراف الأجنبية، ودعم البحوث و الدراسات في مجال تكنولوجيا المعلومات و الاتصالات، و تشجيع الاستفادة بنتائجها و تنظيم نشاطات خدمات التوقيع الالكتروني و غيرها من الأنشطة في مجال المعاملات الالكترونية و صناعة تكنولوجيا المعلومات.

ففي مصر، أنشأ قانون التوقيع الالكتروني "هيئة تنمية صناعة تكنولوجيا المعلومات"[13] التي تتمتع بالشخصية الاعتبارية العامة و تتبع الوزير المختص بشؤون الاتصالات و المعلومات، مقرها الرئيسي محافظة الجيزة، و تنشأ لها فروع في جميع أنحاء الجمهورية بحيث تتولى سلطة اصدار و تجديد التراخيص اللازمة لمزاولة أنشطة خدمات التوقيع الإلكتروني. والترخيص بمزاولة نشاط إصدار شهادات التصديق الإلكتروني.[14] ويبقى اللجوء إلى توثيق التوقيع الإلكتروني اختياريا بالنسبة لأطراف المعاملة الإلكترونية.

و أما المشرع التونسي، فقد أنشأ مؤسسة عمومية لا تكتسي صبغة إدارية تتمتع بالشخصية المعنوية وبالاستقلال المالي أطلق عليها اسم "الوكالة الوطنية للمصادقة الإلكترونية" و تخضع في علاقاتها للقانون التجاري تتخذ مقرا بتونس العاصمة و تخضع لإشراف الوزارة المكلفة بالقطاع[15].

2- سلطة التصديق الجهوية:

تختص على مستوى جهوي أو مستوى أقل من مجال عمل السلطة الرئيسية بالتأكد من ضمان ارتباط المفتاح العام و الخاص لأحد المستخدمين في إطار عمليات إنشاء التواقيع الإلكترونية.

3- سلطة التصديق المحلية:

و مهمتها تلقي الطلبات من الأشخاص الراغبين في الحصول على زوج من مفاتيح التشفير- المفتاح العام و المفتاح الخاص- و التأكد من هوية و شخصية هؤلاء المستخدمين و منح شهادات تصديق تفيد صحة توقيع العملاء.

II- أجهزة التصديق الإلكتروني في الجزائر:

أدرك المشرع الجزائري أهمية و ضرورة المحافظة على سرية البيانات الشخصية و المعلومات المتدفقة عبر شبكات الإتصال و التكنولوجيا الحديثة و جعلها أحد أهم التزامات مزودي الخدمات[16]، كما استحدث بموجب أحكام القانون رقم (2000-03) المؤرخ في 5 غشت 2000 الذي يحدد القواعد العامة المتعلقة بالبريد و بالمواصلات السلكية و اللاسلكية، هيئة جديدة تسمى "سلطة ضبط البريد و المواصلات السلكية و اللاسلكية" ، التي يستشيرها وزير البريد و تكنولوجيات الاعلام و الاتصال" بصدد مراقبة نشاط متعاملي البريد و المواصلات السلكية و اللاسلكية و مزودي النفاد و الخدمات الى الانترنات المرخص لهم قانونا، وطنيين كانوا أو أجانب.

1- سلطة ضبط البريد و المواصلات السلكية و اللاسلكية:

أنشأ نص المادة (10) من القانون رقم (2000-03) المتعلق بالقواعد العامة المتعلقة بالبريد و بالمواصلات السلكية و اللاسلكية سلطة ضبط مستقلة تتمتع بالشخصية المعنوية و الاستقلال المالي، يقع مقرها في الجزائر العاصمة.

أ- تشكيلة سلطة ضبط البريد:

تتشكل سلطة الضبط من مجلس و مدير عام

مجلس سلطة الضبط: يتكون من سبعة أعضاء من بينهم الرئيس، يعينون من قبل رئيس الجمهورية، و تتنافى العضوية في المجلس مع أي نشاط مهني أو وظيفة عامة أخرى.

كما لا يجوز لعضو المجلس امتلاك مصالح مباشرة أو غير مباشرة في مؤسسة تابعة لقطاعات البريد و المواصلات السلكية و اللاسلكية و السمعي البصري و المعلوماتية.

ويشترط لصحة مداولات مجلس سلطة الضبط حضور (5) خمسة أعضاء على الأقل على أن تتخذ قراراته بأغلبية الأعضاء الحاضرين مع ترجيح صوت الرئيس في حال التساوي.

مدير عام سلطة الضبط: يتولى مهمة تسيير و ادارة سلطة الضبط، يتم تعيينه من طرف رئيس الجمهورية و يحضر اجتماعات مجلس سلطة الضبط برأي استشاري و يتولى فيها الأمانة التقنية.

ب- اختصاصات سلطة الضبط:

تضطلع سلطة الضبط باختصاصات متعددة في مجال اتخاذ كل التدابير الضرورية لترقية و تطوير مجال البريد و المواصلات السلكية و اللاسلكية و منح تراخيص استغلال و اعتماد تجهيزات البريد و المواصلات السلكية و اللاسلكية، و التحكيم في النزاعات القائمة بين المتعاملين أو مع المستعملين.(17)

هذا بالإضافة إلى دورها الاستشاري و إبداء الرأي في العديد من المجالات التي تدخل في صميم صلاحيات الوزير المكلف بالبريد و المواصلات السلكية و اللاسلكية.

2- مؤدي خدمات التصديق الإلكتروني الوطنيين:

تم تعريف مؤدي خدمات التصديق الإلكتروني الوطنيين بموجب نص المادة (3) من المرسوم التنفيذي رقم (07-162) المؤرخ في 28 ماي 2007 المعدل و المتمم للمرسوم التنفيذي رقم (01-123) المتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية و على مختلف خدمات المواصلات السلكية و اللاسلكية بأنهم: "كل شخص في مفهوم المادة 8/8 من القانون رقم 2000-03 يسلم شهادات إلكترونية أو يقدم خدمات أخرى في مجال التوقيع الإلكتروني."

و عليه يدخل في مفهوم مؤدي خدمات التصديق الإلكتروني كل شخص طبيعي أو معنوي مرخص له من سلطة ضبط البريد و المواصلات السلكية و اللاسلكية إنشاء و استغلال خدمات التصديق الإلكتروني.(18)

و لم يبين المشرع الشروط الواجب توفرها في مؤدي خدمات التصديق الإلكتروني و اكتفى بتوضيح المقصود بأهلية مؤدي خدمات التصديق، حيث اعتبرها وثيقة تثبت مطابقة الخدمات التي يؤمنها مؤدي خدمات التصديق لمتطلبات من نوعية خاصة. (19)

هذا و قد بين نص المادة (2) من المرسوم التنفيذي رقم 07-162 المؤرخ في 30 ماي 2007 المتعلق بنظام الإستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية، بأن ترخيص

مصالح التصديق يكون مرفقا بدفتر شروط يحدد حقوق و واجبات مؤدي الخدمات و المستعمل.

و لحد ساعة تحرير هذه الأسطر لم يصدر دفتر الشروط الذي من شأنه أن يبين شروط مزاولة التصديق الإلكتروني بالرغم من تصريح الحكومة في أكثر من مناسبة بتحديد تاريخ تلزم نفسها خلاله بحسم الموضوع.

و لقد تقدمت ثماني شركات بعروضها إلى سلطة الضبط التي لم تفصل فيها قبولا و لا رفضا منذ سنة 2009[20]. وبذلك يبقى موضوع مزودي خدمات التصديق الإلكتروني الوطنيين مجرد نصوص مبتورة متناثرة بين التشريع و التنظيم، الأمر الذي من شانه "تجميد مشروع الجزائر الإلكترونية". [21]

3- مؤدي خدمات التصديق الإلكتروني الأجانب:

بالرغم من حرص المشرع الجزائري على اشتراط الجنسية الجزائرية في مقدمي الخدمات في المادة (4) من المرسوم التنفيذي رقم (98-257) المؤرخ في 25 غشت 1998 و المتعلق بضبط شروط و كيفيات إقامة خدمات "انترنات" و استغلالها التي نصت على أنه: "لا يرخص بإقامة خدمات "انترنات" و استغلالها لأغراض تجارية ضمن الشروط المحددة أدناه لا للأشخاص المعنويين الخاضعين للقانون الجزائري، المدعوين أدناه "مقدموا الخدمات" و برأسمال يملكه فقط أشخاص معنويون خاضعون للقانون العام و/أو أشخاص طبيعيون من جنسية جزائرية".

إلا أنه عدل عن ذلك و اعتد بالشهادات التي يسلمها مؤدي خدمات تصديق الكتروني مقيم في بلد أجنبي، ومنحها نفس قيمة الشهادات المسلمة من مؤدي خدمات تصديق الكتروني جزائري، بشرط وجود اتفاقية للاعتراف المتبادل بين البلدين ابرمتها سلطة ضبط البريد و المواصلات السلكية و اللاسلكية. [22]

خاتمة:

إن اقامة أجهزة التصديق الإلكتروني التي تسهر على حماية بيانات انشاء التوقيع الإلكتروني و استمرارية سلامته و حفظه من شأنه ان يدعم نتائج تقنية التشفير و سرية المفاتيح الخاصة.

لذلك نناشد المشرع الجزائري بسرعة اتخاذ الخطوات الجدية لتحويل النصوص القانونية المتعلقة بسلطة ضبط البريد و المواصلات السلكية و اللاسلكية إلى واقع ملموس مع وضع النظام القانوني الكفيل بضبط شروط و واجبات مقدمي خدمات التصديق الإلكتروني، لأن هذه الاجراءات هي جسر العبور إلى "الجزائر الرقمية".

الهوامش:

1- أفريد كيربي، فهم عملية التشفير، النشرة الشهرية حول الوعي الأمني لمستخدمي الحاسب الآلي (! OUCH)، معهد (SANS)، يوليو (تموز) 2011، منشور عبر الموقع الإلكتروني: http://www.securingthehuman.org

2- د. عبد الفتاح بيومي حجازي، النظام القانوني لحماية الحكومة الإلكترونية، الكتاب الثاني، الحماية الجنائية و المعلوماتية لنظام الحكومة الإلكترونية، دار الفكر الجامعي، الطبعة الأولى،2003، ص 141.

3- د. عبد الفتاح بيومي حجازي، مرجع سابق، ص 144.

4- "قد تحتوي أجهزة التخزين المحمولة مثل المخزنات القلمية على خيار لتشفير المعلومات المخزنة عليها، كما يمكن تشفير المعلومات عن طريق برنامج يتم تثبيته على جهاز الحاسب الآلي، و تتضمن كذلك بعض الهواتف الذكية و الأجهزة اللوحية خاصية التشفير. و يمكنك لحصول على برامج لتشفير البيانات عن طريق مصنع جهازك أو عن طريق الموقع الإلكتروني لتطبيقات الأجهزة اللوحية": أفريد كيربي، مرجع سابق.

5- زينب بنعومر، الحجية القانونية للمستندات الإلكترونية في التشريع المغربي، محكمة الإستئناف التجارية بمراكش، 2011/01/27، ص34

6- د. لورنس محمد عبيدات، إثبات المحرر الإلكتروني، دار الثقافة للنشر والتوزيع، 2009، ص141

7- د. لورنس محمد عبيدات، مرجع سابق، ص 145؛ د. عبد الفتاح بيومي حجازي، مرجع سابق، ص 153.

8- وهو ما يسمى بنظام(RSA)، ويستخدم هذا النظام زوجا من المفاتيح: مفتاح عام(PUBLIC Key) ومفتاح خاص(private key) عوضا عن استخدام مفتاح واحد فقط. ورغم أن هذا النظام كان ملائما جدا لأجهزة الكومبيوتر المعقدة، إلا أنه قد تم إختراقه فيما بعد. وبقي الحال كذلك إلى أن قام " فيل زيمرمان" PHIL ZIMMERMAN بتطوير نظام تشفير يعتمد نظام RSA سنة 1986، ولكنه يتميز باستخدام مفتاح بطول 128 بت، ويدعى برنامج الخصوصية المتفوقة، ويتوفر من هذا البرنامج نسخة تجارية نسخة مجانية. وهو من أكثر برامج التشفير إنتشارا في وقتنا الحالي.

انظر: زينب بنعومر، مرجع سابق، ص .34

9- عبد الله مسفر الحيان وحسن عبد الله عباس، التوقيع الالكتروني، دراسة نقدية، مقال منشور في مجلة العلوم الاقتصادية والإدارية، جامعة بغداد، العدد الأول، سنة 2003، ص 98.

10- انظر: د. لورنس محمد عبيدات، مرجع سابق، ص147؛ د. خالد ممدوح ابراهيم، حجية البريد الإلكتروني في الإثبات، دراسة مقارنة، دار الفكر الجامعي، 2008، ص215.

11- انظر: د. عبد الفتاح بيومي حجازي، مرجع سابق، ص 164

12- انظر نص المادة 25 من قانون إمارة دبي رقم 2 لسنة 2002 بشأن المعاملات والتجارة الإلكترونية.

13- أنظر نص المادة (2) من القانون المصري رقم (15) لسنة (2004) المتعلق بتنظيم التوقيع الالكتروني و إنشاء هيئة تنمية صناعة تكنولوجيا المعلومات.

14- انظر نص المادة (19) من اللائحة التنفيذية لقانون التوقيع الإلكتروني وانشاء هيئة تنمية صناعة تكنولوجيا المعلومات.

15- أنظر نص الفصل (8) من القانون التونسي الخاص بالتجارة الإلكترونية رقم (83) المتعلق بالمبادلات التجارية الإلكترونية.

16- جاء في نص المادة (14) من المرسوم التنفيذي رقم (98-257) المؤرخ في 25 غشت 1998 المتعلق بضبط شروط و كيفيات إقامة خدمات "انترنات" و استغلالها ما يلي: "يلتزم مقدم خدمات "انترنات" خلال ممارسة نشاطاته بما يأتي:

المحافظة على سرية كل المعلومات المتعلقة بحياة مشتركيه الخاصة و عدم الادلاء بها إلا في الحالات المنصوص عليها في القانون".

17- انظر نص المادة (13) من القانون رقم (2000-03) المؤرخ في 5 غشت 2000 الذي يحدد القواعد العامة المتعلقة بالبريد و بالمواصلات السلكية و اللاسلكية، ج ر عدد 48، 2000.

18- انظر نص المادة (2) من المرسوم التنفيذي رقم (07-162) المؤرخ في 30 ماي 2007 المعدلة و المتممة لأحكام المادة (3) من المرسوم التنفيذي رقم (01-123) المتعلق بنظام الاستغلال المطبق على كل نوع من انواع الشبكات بما فيها اللاسلكية الكهربائية و على مختلف خدمات المواصلات السلكية و اللاسلكية – و للإشارة فقد استعمل المشرع مصطلح "موفر الخدمات" في أكثر من قانون. فمثلا: جاء في مضمون نص المادة (8) من القانون رقم (2000-03) المتعلق بتحديد القواعد العامة المتعلقة بالبريد و بالمواصلات السلكية و اللاسلكية بما يلي: "يقصد في مفهوم هذا القانون" بـــ:

8-موفر الخدمات: كل شخص معنوي أو طبيعي يقدم خدمات مستعملا وسائل المواصلات السلكية و اللاسلكية". كما ورد مصطلح مقدموا الخدمات ضمن تعريف المصطلحات الذي حمله نص المادة (2) من القانون رقم (09-04) المؤرخ في 5 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتعلقة بتكنولوجيات الاعلام و الاتصال و مكافحتها بقوله: "مقدموا الخدمات: (1)أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية و/أو نظام للاتصالات.

(2) و أي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو مستعمليها".

19- أنظر نص المادة (3) من المرسوم التنفيذي رقم (07-162) المعدل و المتمم لأحكام المرسوم التنفيذي رقم (01-123) المتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية و على مختلف خدمات المواصلات السلكية و اللاسلكية.

20- أنظر: زروق يوسف، حجية وسائل الاثبات الحديثة، رسالة دكتوراه في القانون الخاص، جامعة أبو بكر بلقايد تلمسان، كلية الحقوق و العلوم السياسية، 02-2013 ، ص 69.

21- انظر نص المادة (2) من المرسوم التنفيذي رقم (12-12) المؤرخ في 9 جانفي 2012 يحدد صلاحيات وزير البريد و تكنولوجيات الاعلام و الاتصال.

22- انظر نص المادة (4) من المرسوم التنفيذي رقم (07-162) المعدل و المتمم للمرسوم التنفيذي رقم (01-123) المتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية و على مختلف خدمات المواصلات السلكية و اللاسلكية.