

« Le cadre juridique de la signature et de la certification électroniques en Algérie après quinze ans de législation »

" الإطار القانوني للتوقيع و التصديق الإلكترونيين في الجزائر بعد خمسة عشر عاما من التشريع "

د.بودر هجيرة

Dr. Hadjira BOUDER

أستاذة بحث قسم ب، مركز البحث في الإعلام العلمي و التقني، الجزائر

Maître de Recherche B, CERIST, Algérie

hbouder@cerist.dz

تاريخ النشر: 2021/06/28

تاريخ القبول: 2021/05/09

تاريخ إرسال المقال: 2021/04/03

ملخص:

يعد اليوم التوقيع الإلكتروني القائم على التصديق الإلكتروني أكثر الوسائل التكنولوجية ضمانا لأمن المبادلات الإلكترونية. و لكن هذا الأمن التقني يجب أن يستكمل بأمن قانوني يضمه إطار قانوني منسجم. و قد قامت الجزائر ببعث العديد من المشاريع في إطار تحولها الرقمي؛ التي أبرزت نقائص النصوص القانونية السارية المفعول، و ضرورة وضع نظام قانوني أكثر انسجاما و ملائمة للتوقيع الإلكتروني الرقمي. و هو ما يفسر اهتمامنا بتطور الإطار القانوني للتوقيع الإلكتروني في بلادنا، من أجل إبراز جوانبه الإيجابية و تسليط الضوء على النقائص التي يجب تصحيحها. و قد توصلنا من خلال هذه الدراسة إلى أن الإطار القانوني للتوقيع الإلكتروني في الجزائر، على الرغم من تطوره البطيء، صار أكثر ملائمة للطبيعة الخاصة لهذه الوسيلة التكنولوجية لحماية المبادلات الإلكترونية، و إن كان لا يزال يحتاج إلى تحسين.

كلمات مفتاحية:

التوقيع الإلكتروني، قانون التكنولوجيات الرقمية، المبادلات الإلكترونية، التوقيع الرقمي، التصديق الإلكتروني.

Résumé:

La signature électronique basée sur la certification électronique est désormais considérée comme le moyen technologique le plus fiable pour la sécurité des échanges électroniques. Mais cette sécurité technique doit être complétée par une sécurité juridique, que seul un cadre juridique cohérent peut garantir. L'Algérie a lancé plusieurs chantiers de dématérialisation des échanges; qui ont mis en exergue les insuffisances des textes juridiques en vigueur et la nécessité de définir un cadre juridique cohérent pour la signature électronique. D'où l'intérêt d'examiner l'évolution de ce cadre juridique, afin de faire ressortir ses avancées et relever les insuffisances qui doivent être corrigées.

Cet examen nous a permis de constater, qu'en dépit de la lenteur de l'évolution du cadre juridique de la signature électronique, le droit algérien appréhende mieux ce procédé technologique de sécurité des échanges, même si il reste à parfaire.

Keywords:

Signature électronique; Droit des technologies numériques; échanges électroniques; signature numérique; certification électronique.

Introduction :

Il est bien établi que le Droit est toujours en retard par rapport aux évolutions rapides des technologies, notamment les technologies numériques. Ce qui explique les incohérences dans les niveaux de connaissances entre les spécialistes de ces deux disciplines scientifiques, mais aussi les incohérences sur l'utilisation de la terminologie¹. Ainsi, certains termes juridiques ont été utilisés par les spécialités en technologies numériques pour désigner des procédés techniques qui n'assure pas forcément les fonctions correspondant à ces termes dans le domaine juridique, et qui diffèrent également selon la tradition juridique de chaque pays. Le terme « Signature électronique » en est l'exemple type.

Ce terme a été adopté par les experts techniques par analogie avec la « signature manuscrite » d'un document papier, dont les fonctions et les caractéristiques ont été définis depuis longtemps par les lois, pour garantir la sécurité juridique des transactions. Cependant, le terme « Signature électronique » désigne l'ensemble des procédés techniques destinés à garantir la sécurité des échanges sur les réseaux numériques, tels que : la Signature manuscrite numérisée, la Signature biométrique, Code secret associé à l'utilisation d'une carte et la Signature numérique ou digitale, etc²; et dont la fiabilité diffère selon la nature et les fonctions assurées par chacun de ces procédés. Aussi, les fonctions de certaines signatures électroniques dépassent de loin celles garanties par la signature manuscrite. Il s'agit notamment de la « signature numérique » basée sur la cryptographie asymétrique dans le cadre d'une infrastructure à clés publique (ICP ou PKI en anglais).

Ce type de signatures électroniques garantit aussi bien les fonctions de la signature manuscrite que des fonctions propres au contexte numérique. Il permet de garantir quatre aspects de la sécurité des échanges électroniques, à savoir : l'authentification, la confidentialité, l'intégrité et la non répudiation³.

C'est pourquoi la signature numérique est désormais considérée comme la meilleure solution pour les différents protagonistes au sujet de la sécurité des échanges via les réseaux de télécommunication au niveau international⁴. Même si au début de son émergence en Droit International, cette signature était envisagée surtout sous l'angle du droit commercial.

C'est du moins ce qui ressort des travaux de la CNUDCI, qui a adopté une loi type sur le commerce électronique et a entamé les travaux visant à uniformiser le régime des signatures électroniques qui ont débouchés sur l'adoption d'une loi type sur les signatures électroniques en 2001; l'OCDE qui travaille sur le sujet depuis le printemps 1997, dans la continuité de ses études précédentes qui ont en juin 2007

Le cadre juridique de la signature et de la certification électroniques en Algérie après quinze ans de législation

Hadjira BOUDER

débouché sur un ensemble de recommandations sur l'authentification électronique et orientations pour l'authentification électronique; et l'OMC, qui a engagé un processus de pré-négociations qui devait comprendre ce sujet parmi beaucoup d'autres abordés sous le terme générique de « commerce électronique ».

N'étant pas en reste de ces évolutions technologiques et juridiques, l'Algérie a dès l'année 2000 pris conscience du rôle que peuvent jouer les Technologies de l'Information et de la Communication (TICs) dans son développement Socio-économique. Cette prise de conscience a été traduite par l'adoption de la première stratégie « e- Algérie 2004-2010); où l'adaptation du cadre juridique occupait une place privilégiée.

Dans ce cadre, le gouvernement avait procédé à la refonte du cadre juridique en vigueur, en vue de l'adapter aux exigences des TICs. Le premier secteur visé par cette refonte fut le secteur des télécommunications, à travers la promulgation de la loi 03- 2000⁵ qui a consacré la libéralisation du marché des télécommunications en Algérie. Cette promulgation a été suivie par l'adoption de nouveaux textes juridiques et l'actualisation de textes en vigueur, dont le code civil qui a été révisé en 2005 pour introduire pour la première fois en droit algérien la reconnaissance de l'écrit et de la signature électronique.

Parallèlement à cette avancée juridique, plusieurs chantiers de dématérialisation des échanges, ayant principalement trait au e-gouvernement, ont été lancé dans notre pays, à l'image du passeport et de la carte d'identité biométriques, la compensation bancaire, les cartes de paiement d'Algérie Poste, la carte Chifa et la télé-TVA. Ces applications de l'administration électroniques ont mis en exergue les faiblesses du dispositif juridique en place, et la nécessité de le redéfinir pour renforcer la sécurité de ces échanges électroniques, garantie en partie par la certification électronique des signatures électroniques sur lesquelles reposent ces applications.

En effet, la révision du code civil de 2005 a été suivie de la promulgation de plusieurs textes réglementaires émanant de différents départements ministériels, et traduisant l'appréhension de chacun de ces département de la signature électronique selon son angle d'attaque (impératif de modernisation du droit, impératif de développement des services de télécommunication, impératif sécuritaire). Cet état de fait a impacté négativement le cadre juridique de la signature électronique numérique en Algérie, et a, par conséquent, ralenti la cadence des chantiers de modernisation entrepris par l'Etat, et retardé le lancement du e-commerce.

Toutefois, l'identification des incohérences et insuffisances des textes qui ont régi la signature et la certification électronique pendant une décennie a permis la mise en place d'un nouveau cadre juridique plus cohérent et mieux adapté aux spécificités de la signature électronique numérique.

D'où l'intérêt de s'interroger sur les principales étapes de l'évolution du cadre juridique de la signature électronique en Algérie? Et est-ce que cette évolution va contribuer au renforcement de la sécurité juridique dans l'environnement numérique pour plus de confiance dans la sécurité des échanges électroniques dans notre pays ?.

Le cadre juridique de la signature et de la certification électroniques en Algérie après quinze ans de législation

Hadjira BOUDER

Afin de répondre à cette problématique, il est nécessaire, en premier lieu, de passer en revue les textes juridiques ayant régi la signature électronique avant l'uniformisation de son cadre juridique (section 1), puis examiner le cadre juridique actuellement en vigueur afin de mettre en exergue ses apports mais aussi ses éventuelles lacunes ou insuffisances (Section 2). A cet effet, nous avons adopté le plan suivant :

Section 1 : Evolution du cadre juridique de la signature depuis la reconnaissance légal de l'écrit et de la signature électroniques

Sous- section 1 : Cadre juridique de la signature électronique avant la promulgation de la loi d'uniformisation de 2015

Sous-section 2 : Cadre juridique de la Signature et de la certification électroniques après la promulgation de la loi de 2015 et de textes connexes

Section 2 : Parachèvement du cadre juridique de la signature électronique par le renforcement du cadre légal de la cryptographie

Sous-section1: Le décret exécutif 16-61 a-t-il modifié le régime juridique des équipements et logiciels d'encryption ?

Sous-section 2 : Mise en place d'un dispositif national de la sécurité des systèmes d'information : une garantie pour la fiabilité de la signature électronique

Section1 : Evolution du cadre juridique de la signature électronique depuis la reconnaissance légal de l'écrit et de la signature électroniques

Le cadre juridique de la signature électronique en Algérie est passé par plusieurs phases, qu'on peut scinder en deux, par rapport à une date clé de son évolution, à savoir l'année 2015.

Cette année a été marquée par la promulgation de la loi 15-04 relative à la signature et la certification électronique⁶, qui est venu uniformiser le cadre juridique de la signature électronique et lever les ambiguïtés qui l'entachaient. Ainsi, nous reviendrons dans cette section sur l'état des textes juridiques relatifs à la signature et la certification électroniques avant 2015 (sous-section1), puis nous présenterons les avancés apportés par la loi 15-04 et ses textes connexes (sous-section 2). Et ce afin de démontrer l'apport de chacun de ces textes dans la promotion de l'utilisation de la signature électronique dans le cadre de ses différentes applications : e-gouvernement, e-finance, e-banking, e-commerce, etc.

Sous-section 1 : Cadre juridique de la signature électronique avant la promulgation de la loi d'uniformisation de 2015

En 2000, l'Algérie avait adopté la déclaration du millénaire des Nations Unis qui a consacré les Technologies de l'Information et de la Communication (TICs) comme vecteur important de développement. Elle a également adopté les résolutions du sommet mondial sur la société de l'information 2003-2005. Et s'était engagée de la sorte à développer les TICs en Algérie au profit de son développement socio-économique. Cet engagement a été traduit par l'adoption de la première stratégie « e-

Le cadre juridique de la signature et de la certification électroniques en Algérie après quinze ans de législation

Hadjira BOUDER

Algérie 2004-2010); ou l'adaptation du cadre juridique occupait une place privilégiée.

Dans ce cadre, le gouvernement avait procédé à la refonte du cadre juridique en vigueur, en vue de l'adapter aux exigences des TICs. Le premier secteur visé par cette refonte fut le secteur des télécommunications, à travers la promulgation de la loi 03- 2000, qui a consacré la libéralisation du marché des télécommunications en Algérie. Cette promulgation a été suivie de l'adoption de nouveaux textes juridiques et l'actualisation de textes en vigueur, dont :

- La loi n°05-02 du 6 février 2005 modifiant et complétant l'ordonnance n°75-59 du 26 septembre 1975 portant code de commerce⁷, qui a consacré pour la première fois la recevabilité des lettres de change et chèques présentés par tout moyen d'échange électronique, défini par la législation et la réglementation en vigueur, à une chambre de compensation, et
- La loi n° 05-10 du 20 juin 2005 modifiant et complétant l'ordonnance n° 75-58 du 26 septembre 1975, modifiée et complétée, portant code civil⁸. Cette loi constitue, en dépit de ses insuffisances, la pierre angulaire du cadre juridique de la signature électronique en Algérie. Elle a été complétée par des textes réglementaires, dont l'apport ne peut être négligé.

1. Code civil de 2005 et réglementation connexe: première esquisse du cadre juridique de la signature électronique en Algérie :

1.1. Apports de la loi n° 05-10 du 20 juin 2005 modifiant et complétant le code civil :

La loi n° 05-10 du 20 juin 2005 a consacré la reconnaissance juridique de l'écrit électronique comme preuve recevable, ainsi que la reconnaissance de la signature électronique :

- **Concernant la reconnaissance de l'écrit électronique comme preuve littérale :**

Cette loi a redéfini la preuve par écrit comme suit : « la preuve par écrit résulte d'une suite de lettres ou de caractères ou de chiffres ou de tout autre signe ou symbole doté d'une signification intelligible, quels que soient leurs supports et leurs modalités de transmission. » (art.323 bis). Elle a également reconnu à l'écrit sur support électronique la même force probante que l'écrit sur support papier à la condition «...que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité » (art.323 ter).

- **Concernant la reconnaissance juridique de la signature électronique :**

Cette reconnaissance a été introduite de manière implicite à travers l'article 323 ter, qui a précisé les conditions de fiabilité de l'écrit sous forme électronique sans faire référence à la signature électronique. Qui d'ailleurs, n'a pas été définie par la loi, ni même la signature de manière générale.

La signature électronique n'a été abordée que dans le dernier paragraphe de l'article 327 relatif à la reconnaissance de l'acte sous seing privée sur support électronique, où il est fait référence aux conditions d'admission de l'écrit sur support

électronique comme preuve littérale: « *l'acte sous-seing privé est réputé émaner de la personne à qui sont attribuées l'écriture, la signature ou l'empreinte digitale y apposées, à moins de désaveu formel de sa part [...]. Est admise la signature électronique conformément aux conditions de l'article 323 ter. ».*

Ceci était dû à une confusion entre les conditions de recevabilité de l'écrit électronique entant que preuve littérale et les conditions de fiabilité d'une signature électronique.

Deux ans après la promulgation de la loi 05-10, un texte réglementaire, cette fois ci proposé par le ministère de la poste et des télécommunications, est venu compléter les dispositions de la loi sus-mentionnée. Il s'agit du décret exécutif n° 07-162 du 30 mai 2007 modifiant et complétant le décret exécutif n° 01-123 du 9 mai 2001 relatif au régime d'exploitation applicable à chaque type de réseaux, y compris radio-électriques et des différents réseaux de télécommunications⁹.

1.2. Apports du Décret Exécutif n° 07-162 du 30 mai 2007 :

Bien qu'adopter dans le cadre de l'application des dispositions de la loi 03-2000 relative aux télécommunications, ce décret exécutif a été d'un grand apport pour le cadre juridique de la signature électronique. Puisque il nous a permis de constater que la signature électronique visée implicitement dans la loi 05-10 n'était autre que la signature numérique basée sur la cryptographie asymétrique. La précision du choix technologique du législateur dans un décret exécutif paraissait très logique, conformément au principe de la neutralité technologique¹⁰ des textes juridiques dans le domaine numérique, mais la teneur de ce décret n'était pas assez claire et précise. Et au lieu de clarifier le cadre juridique de la signature électronique, les dispositions de ce décret l'ont rendu encore plus flou. Parmi les apports de ce texte, nous citons:

- La consécration d'une définition de la signature électronique, qui nous renvoi aux articles 323 bis et 323 ter du la loi 05-10. Ce décret a également définit ce qu'est un certificat électronique et des concepts connexes a la certification, qui indiquent que la signature électronique en question est la signature numérique fondé sur une ICP, même sans faire mention de la cryptographie;
- La soumission de l'activité de fourniture de services de certification électronique à une autorisation assortie d'un cahier des charges, sans précisions concernant le statut juridique des fournisseurs de ces services (article 2 du décret exécutif n° 07-162) ;
- La reconnaissance implicite de l'Autorité de Régulation de la Poste et des télécommunications (ARPT) comme autorité de certification racine, à travers l'article 4 du décret exécutif de 2007, qui indique que le législateur algérien a opté pour le modèle hiérarchique de certification¹¹.

Ainsi, et en dépit de ses insuffisances, ce décret exécutif nous a, comme déjà souligner, dévoilé qu'il s'agit bien de signature numérique basée sur la cryptographie asymétrique. D'où l'intérêt de rechercher le régime juridique de la cryptographie en Algérie, qui est à la base de ce type de signature électronique, et que nous avons retrouvé dans le Décret exécutif n°09-410 du 10 décembre 2009 fixant les règles de sécurité applicables aux activités portant sur les équipements sensibles¹².

1.3. Apports du Décret exécutif n°09-410 du 10 décembre 2009 fixant les règles de sécurité applicables aux activités portant sur les équipements sensibles :

Ce décret exécutif a classé les équipements et logiciels d'encryption (ou de cryptage) dans la catégorie des équipements sensibles de télécommunication. Il est venu renforcer le cadre juridique de la signature électronique en Algérie; vu la place importante qu'occupe la cryptographie dans la sécurité de la signature électronique numérique. A souligner que :

- Avant la promulgation de ce décret, les activités portant sur les équipements sensibles étaient régis par un arrêté interministériel ;
- Ce décret qualifiait les équipements et les logiciels d'encryption d'équipements sensibles en dehors de la liste des matériels classés dans le décret exécutif n° 98-96 du 18/03/1998 fixant les modalités d'application de l'ordonnance n°97-06 du 21/01/1997 relative aux matériels de guerre, armes et munitions (annexe 1, section A, sous-section 3 du décret exécutif 09-410);
- Ce décret a institué un régime unique pour l'ensemble des équipements sensibles, sans tenir compte des spécificités des équipements et logiciels d'encryption pouvant être utilisés pour la sécurisation des échanges électroniques;
- Il réservait également un traitement unique pour l'ensemble des équipements et logiciels d'encryption, sans distinction aucune (qu'ils soient destinés à l'identification et l'intégrité ou à la confidentialité);
- Ce décret traitait essentiellement d'aspects procéduraux.

2. Lacunes et insuffisances des textes relatifs à la Signature électronique avant la loi d'uniformisation de 2015:

L'analyse des textes juridiques relatifs à la signature électronique dans notre pays, cités ci-dessus, nous a permis de dégager les lacunes et les insuffisances de ce dispositif juridique¹³, qui ont, entre autres causes, entravé la promotion des services numériques en Algérie, notamment le e-commerce. On peut les résumer comme suit :

2.1. Au niveau de l'adaptation du droit de la Preuve (la loi 05-10):

Ce que l'on peut relever des dispositions du code civil de 2005 relatives à l'adaptation du droit de la preuve algérien aux TICs, c'est que :

- Aucune précision n'a été donnée quant aux cas de conflit de preuve littérale entre l'écrit papier et l'écrit électronique
- Quant à la reconnaissance implicite de la signature électronique, la loi 05-10 n'a défini ni la signature de manière générale, ni la signature électronique de manière particulière, et ne renvoyait à aucun éventuel texte d'application.
- Outre la confusion entre conditions d'admission de l'écrit électronique comme preuve littérale et les conditions de fiabilité d'une signature électronique.

2.2. Au niveau du dispositif légal relatif à la signature électronique entant que procédé fiable pour la sécurité des échanges électroniques:

Concernant les conditions de fiabilité de la signature électronique basée sur une ICP ou PKI, elles devaient être fixées par le décret exécutif de 2007. Mais ce texte n'a fait que semer davantage la confusion autour du cadre juridique de la signature électronique :

- Le décret exécutif 07-162 Soumettait l'activité de fourniture de services de certification au régime de l'autorisation assortie d'un cahier des charges sans se conformer aux dispositions de la loi 2000-03 relative aux télécommunications ;
- Ce décret exécutif a listé un ensemble de définitions sans clarification de leurs contenus, ni de l'objectif de leur insertion en son sein ;
- En instituant (implicite) l'ARPT autorité de certification racine en Algérie, ce décret aurait assigné de nouvelles missions à cette autorité administrative chargée, conformément à la loi 03-2000 relative à la poste et aux télécommunications, de la régulation du marché de la poste et des télécommunications, par voie réglementaire ;
- Aussi, ce décret n'a donné aucune précision sur le régime juridique de la certification électronique et les fournisseurs de services de certification. Il s'est contenté de les soumettre au cahier des charges élaboré par l'ARPT.

2.3. Au niveau du cadre légal de la cryptographie et de ses différents usages :

Ce que l'on peut relever du décret exécutif n° 09-410 concernant le régime juridique de la cryptographie, c'est que :

- L'insertion de restrictions légales à l'usage de la cryptographie dans un texte général traitant de tous les équipements sensibles a rendu l'accès à ce procédé plus complexe, plus lourd et imprécis ;
- Le décret exécutif de 2009 réservait un traitement différencié fondé sur l'activité portant sur les équipements et logiciels d'encryption (homologation, acquisition et exploitation), et non sur l'objet de ces derniers (authentification ou confidentialité).
- Ce décret soumettait également les activités liées à l'acquisition pour exploitation des équipements et logiciels d'encryption à l'autorisation préalable de l'ARPT.

Après avoir passé en revue les textes régissant la signature électronique avant la promulgation de la loi d'uniformisation de 2015, force est de constater que le cadre juridique de la signature et de la certification électroniques en Algérie était incohérent et imprécis. Ceci est dû au fait que chacun de ces textes traduisait l'approche adoptée par Les différents départements ministériels les ayants proposé. Une approche définie selon l'angle sous lequel est traitée la signature et la certification électronique (impératif de modernisation du droit, impératif de développement des services de télécommunication, impératif sécuritaire).

Suite à ce constat, nous avons formulé un certain nombre de recommandations en vue de mettre en place un dispositif légal plus complet et plus cohérent pour la signature et la certification électroniques en Algérie¹⁴, et de promouvoir la confiance dans l'environnement numérique. On peut résumer ces recommandations comme suit :

- Compléter les dispositions du droit de la preuve relatives à l'écrit et à la signature électroniques, à travers notamment: la définition de la signature de manière général et la signature électronique de manière particulière, et la précision de la force probante de l'écrit électronique par rapport à l'écrit sur support papier notamment en cas de conflit de preuve littérale, ainsi qu'en levant la confusion autour de la valeur juridique de l'acte sous seing privée signé électroniquement, et en précisant la valeur juridique de la copie technologique (documents et actes numérisés).

Le cadre juridique de la signature et de la certification électroniques en Algérie après quinze ans de législation

Hadjira BOUDER

- Fixer les conditions de fiabilité de la signature électronique par voie réglementaire afin de maintenir la neutralité technologique qui doit être également observée dans la définition de la signature électronique.
- Compte tenu des objectifs visés par l'adoption de la signature électronique comme moyen de sécurité des échanges via les réseaux, notamment sur le plan commercial, il est nécessaire d'adopter une loi pour les échanges et le commerce électronique, où serait clairement défini: le régime juridique des contrats, le cadre légal du certificat électronique, le statut juridique des fournisseurs de services de certification, ainsi que les attributions de l'ARPT entant qu'autorité racine ou plutôt attribuer cette mission à une autorité neutre.
- Préciser le niveau des services de sécurité mis en œuvre dans le cadre de la télé-procédure administrative (confidentialité, horodatage, archivage,...).
- Bien définir le régime juridique de la cryptographie à travers l'adoption d'un texte réglementaire spécifique à l'usage des équipements et logiciels d'encryption, définition de ces équipements et logiciels, distinguer entre les moyens de cryptage ayant pour objet l'authentification et l'intégrité des données transmises par voie électronique et les autres moyens de cryptage visant la confidentialité,...).
- Création d'un organe national chargé de la sécurité des systèmes d'information.
- Compléter tous les textes dans la sphère privée et publique ayant trait à la signature électronique (actes authentiques, contrats de travail, code des douanes, code des impôts, protection des données personnelles, la dématérialisation des marchés publics,...).

Presque la totalité de ces recommandations a été prise en compte dans le nouveau cadre juridique de la signature et de la certification électronique, mis en place par la loi 15-04 et des textes connexes, comme nous allons le montrer:

Sous-section 2 : Cadre juridique de la Signature et de la certification électronique après la promulgation de la loi 15-04 et de textes connexes

En Algérie, la fin de la première décennie du millénaire a été marquée par la multiplication des applications de l'e-administration dans plusieurs secteurs, soit par souci de modernisation ou en réponse à des engagements internationaux. Il s'agit notamment : du projet e-passport lancé en 2009 par le ministère de l'intérieur, la préparation du lancement du paiement en ligne via Internet par la SATIM¹⁵ après avoir lancé la première opération de paiement interbancaire en 2005, le lancement de la carte « Chifa » en 2008 dans le secteur de la sécurité sociale, ainsi que plusieurs chantiers de modernisation ouverts par plusieurs ministères tel que le ministère de la justice. La réussite de ces projets de dématérialisation dépendait principalement de la confiance des usagers dans la sécurité des services qu'ils proposent. D'où le recours à la signature numérique basée sur une infrastructure de confiance (ICP ou PKI).

Mais le début de la généralisation de ce moyen fiable de sécurité des échanges électroniques dans notre pays a mis en exergue les lacunes et les insuffisances du cadre juridique en vigueur, tel que déjà souligner. Puisque chacun de ces secteurs s'est doté de sa propre PKI, mais le choix du modèle de certification des signatures électroniques adopté par l'Algérie n'apparaissait pas clairement dans les textes en

vigueur, cités en sus. Même si en désignant implicitement l'ARPT comme autorité racine de certification électronique, le décret exécutif n° 07-162 du 30 mai 2007 modifiant et complétant le décret exécutif n° 01-123 du 9 mai 2001 aurait consacré le modèle hiérarchique de certification électronique.

1. 2015, année de l'uniformisation du cadre juridique de la signature et de la certification électronique en Algérie:

En s'acquittant de ses missions d'autorité racine de certification électronique, conformément au Décret exécutif n° 07-162 sus-mentionné, l'ARPT s'était retrouvé confronter à des problèmes techniques, organisationnels mais surtout juridiques.

En effet, l'imprécision et l'incohérence du dispositif juridique relatif à la signature électronique était à l'origine des démarches entreprises par les représentants de cette autorité autonome auprès des autorités suprêmes, pour la redéfinition du cadre juridique de la signature et de la certification électroniques. Ces démarches ont débouché sur la création en 2013 d'une commission ad-hoc rattachée directement au service du premier ministre, qui a rédigé la loi n° 15-04 du 11 Rabie Ethani 1436 correspondant au 1er février 2015 fixant les règles générales relatives à la signature et à la certification électroniques et ses textes d'application promulgués l'année suivante.

Ce que l'on peut relever de ce texte de loi, c'est que ses rédacteurs ont finalement opté pour un texte unique qui traite de presque tous les aspects de la signature et de la certification électroniques, pour garantir la cohérence de son cadre juridique, et pallier ainsi toutes les lacunes et insuffisances enregistrées dans le dispositif antérieur à son adoption.

1.1. Concernant la valeur juridique de la signature électronique

- Afin de pallier l'imprécision des termes définis dans le décret 07-162 sus-cité et les mettre dans leur juste contexte, le législateur de 2015 a défini sans ambiguïté ce qu'il entend de 15 termes liés à la signature et la certification électroniques, tels que : signature électronique, données de création de signature électronique, données de vérification de signature électronique, certificat électronique, clé cryptographique, etc.(art.2).
- Quant à la valeur probante de la signature électronique, la loi 15-04 est venue compléter et clarifier les dispositions du code civil de 2005 relatives à l'écrit et à la signature électronique; en rappelant que la signature électronique visée assure les mêmes fonctions que la signature manuscrite, à savoir : l'authentification du signataire et la manifestation de son adhésion au contenu de l'écrit sous forme électronique (article 6).

Cette loi reconnaît deux types de signature électronique : « la signature électronique simple » et « la signature électronique qualifiée », cette dernière doit satisfaire aux exigences prescrites par l'article 7 pour être assimilée à une signature manuscrite, et bénéficier ainsi de la même valeur probante (art. 8). Cette signature doit être créée par un dispositif sécurisé et vérifiée par un dispositif fiable de vérification, conformément aux articles 11 et 13 de la loi 15-04, dont la conformité

est attestée par l'entité nationale en charge de l'homologation des dispositifs de création et de vérification de la signature électronique (art.14).

Quant à la « signature électronique simple », elle couvre l'ensemble des procédés de signature électronique ne reposant pas sur un certificat électronique qualifié; et bien qu'elle ne puisse être assimilée à une signature manuscrite, elle ne peut être privée de valeur juridique et ne peut être refusée comme preuve en justice au seul motif qu'elle se présente sous forme électronique, ou ne repose pas sur un certificat électronique qualifié, ou n'est pas créé par un dispositif sécurisé de création de signature électronique (art. 9), mais sa valeur juridique sera déterminée selon son degré de fiabilité par le juge.

- Concernant la certification électronique visée par la loi 15-04, elle ne concerne que la signature électronique qualifiée. Elle consiste en la délivrance d'un certificat électronique qualifié par un tiers de confiance ou un prestataire de services de certification, et doit satisfaire aux exigences fixés par l'article 15 de la loi 15-04. Ce certificat est au cœur du processus de la signature électronique, il fait foie de carte d'identité numérique attestant la relation entre le signataire et les données de signature.

1.2. Concernant le Modèle de certification électronique adopté par l'Algérie :

Le modèle de certification électronique ou le schéma national de certification électronique en Algérie est désormais mieux défini grâce à la loi 15-04. Cette dernière a déchargé l'ARPT des missions de l'autorité racine de certification électronique, comme déjà soulevé, en mettant en place une autorité racine nationale et deux autorités subordonnées, une dédiée à la branche gouvernementale et l'autre dédiée à la branche économique. Il s'agit des autorités suivantes :

- L'« Autorité Nationale de Certification Electronique (ANCE) », qui est une autorité administrative indépendante créée auprès du premier ministre (art.16). Cette autorité est chargée de promouvoir l'utilisation et le développement de la signature électronique, en assumant les missions qui lui sont assignées à travers l'article 18 de la loi 15-04. Cette autorité est également chargée de conclure les conventions de reconnaissance mutuelle avec ses homologues étrangers conformément à l'article 63, ce qui confirme son statut d'autorité racine dans le schéma national de la certification électronique.

L'organisation, le fonctionnement et les missions des services techniques et administratifs de cette autorité sont définis dans le décret exécutif n° 16-134 du 17 Rajab 1437 correspondant au 25 avril 2016¹⁶.

- L'« Autorité Gouvernementale de Certification Electronique », qui est une autorité administrative jouissant de la personnalité morale et de l'autonomie financière, créée auprès du Ministre chargé de la Poste et des Technologies de l'Information et de la communication (art.26). Cette autorité est chargée du suivi et du contrôle de l'activité de certification électronique des tiers de confiance ainsi que la fourniture de services de certification électronique au profit des intervenants dans la branche gouvernementale définis dans l'article 2 de la loi 15-04, comme suit : « institutions et administrations publiques, établissements publics tels que définis par

Le cadre juridique de la signature et de la certification électroniques en Algérie après quinze ans de législation

Hadjira BOUDER

la législation en vigueur, institutions nationales autonomes, autorités de régulation, intervenants dans les échanges interbancaires, ainsi que toute personne ou entité qui de par sa nature ou mission fait partie de la branche gouvernementale. ».

Conformément à l'article 28, cette autorité a plusieurs missions, dont : l'élaboration de sa politique de certification qui doit être approuvée par l'autorité nationale, l'approbation des politiques de certification émises par les tiers de confiance, la publication du certificat électronique de l'Autorité nationale et l'audit des tiers de confiance à travers l'entité gouvernementale chargée de l'audit, conformément à la politique de certification (art.28).

La nature, la composition, l'organisation et le fonctionnement de cette autorité ont été fixés, conformément au premier paragraphe de l'article 28 de la loi 15-04, par le Décret exécutif n° 16-135 du 17 Rajab 1437 correspondant au 25 avril 2016¹⁷.

- L'« Autorité Economique de Certification Electronique (AECE) », cette autorité est confiée conformément à l'article 29 de la loi 15-04 à l'autorité de régulation de la Poste et des télécommunications. Elle est chargée du suivi et du contrôle des prestataires de services de certification électronique qui fournissent les services de signature et de certification électroniques au profit du public, et qui sont définis dans l'article 2 comme suit : « personne physique ou morale qui délivre des certificats électroniques qualifiés et fournissent éventuellement d'autres services en matière de certification électronique ».

Selon l'article 30, cette autorité a pour missions, notamment : l'élaboration et la soumission pour approbation à l'autorité nationale sa politique de certification électronique, la délivrance des autorisation aux prestataires de services de certification après avis favorable de l'autorité nationale, de prendre les mesures nécessaires pour assurer la continuité de services en cas d'incapacité du prestataire de services de fournir ses services, d'auditer les demandeurs d'autorisation, de veiller à l'existence d'une concurrence effective et loyale entre les prestataires, d'arbitrer les litiges qui opposent les prestataires entre eux ou avec les utilisateurs, d'élaborer le cahier des charges fixant les conditions et modalités de la prestation des services et les soumettre à l'autorité nationale pour approbation, etc.

Les décisions prises par l'AECE peuvent faire l'objet de recours auprès de l'autorité nationale. Les décisions de cette dernière peuvent également faire objet de recours auprès du Conseil d'Etat.

A noter que l'Autorité Gouvernementale de Certification Électronique n'a été mise en place qu'en janvier 2018. Elle a été chargée de la mise en œuvre du schéma national de certification électronique dans le cadre d'un Groupement de Commandes AGCE-ARPCE dans lequel l'AGCE agissait pour son compte et pour le compte de l'Autorité Nationale de Certification Électronique. Les Autorités Nationales et Gouvernementales de Certification Électronique ne sont opérationnelles que depuis le 15 novembre 2020, date d'obtention du Rapport d'Audit Point in Time – WebTrust¹⁸.

A préciser que les trois autorités de certifications instituées par la loi 15-04 sont assujetties à l'audit WebTrust tout au long de leur activité; et ce à des fins de reconnaissance internationale.

L'Audit WebTrust est un programme qui correspond à des principes et critères décrits dans la norme WebTrust Principles And Criteria For Certification Authorities V2.2 auxquels une autorité de certification électronique doit se conformer. Cette norme est élaborée et est maintenue par l'American Institute of Certified Public Accountants (AICPA) et l'Institut Canadien des Comptables (CPA)¹⁹

1.3. Concernant le régime juridique de la prestation de services de certification électronique :

Ce fut l'une des principales lacunes du cadre juridique de la signature électronique avant l'adoption de la loi 15-04. Puisque la définition du régime juridique de la prestation de services de certification électronique était confiée à l'ARPT à travers le cahier des charges qu'elle devait élaborer conformément au décret exécutif n° 07-162, sus-mentionné. La prestation de services de certification électronique est toujours soumise au régime de « l'autorisation », qui est d'ailleurs toujours délivrée par l'autorité chargée de la régulation de la poste et des télécommunications, sauf qu'actuellement cette dernière agit comme autorité économique de certification électronique conformément aux dispositions du chapitre 3 du Titre III de la loi 15-04.

Dans ce chapitre sont définis : les conditions d'éligibilité à la prestation de services de certification électronique (art.34); préalablement à l'octroi de l'autorisation l'AECE délivre au demandeur une attestation d'éligibilité pour une période d'une année renouvelable une seule fois pour la mise en place des moyens nécessaires à l'activité de certification électronique, l'autorisation n'est octroyer qu'après un audit d'évaluation réalisé par l'autorité économique ou par un cabinet d'audit accrédité (articles de 35 à 40 et 51); les obligations du prestataire de services de certification (articles de 41 à 50) ; la responsabilité du titulaire d'un certificat électronique (articles 61 à 62). Les contrevenants au cahier des charges ou aux dispositions de la loi 15-04 sont passibles de sanctions administratives et/ou pénales conformément au Titre IV de la loi.

Ce qu'on peut constater de la loi 15-04, c'est qu'elle a remédié à une bonne partie des insuffisances relevées dans le cadre juridique de la signature en vigueur avant sa promulgation, à l'exception du cadre légal de la cryptographie comme nous l'avons soulevé plus haut. Sachant que la signature électronique qualifiée visée par la loi 15-04 et en pratique celle reposant sur la cryptographie asymétrique.

Section 2 : Parachèvement du cadre juridique de la signature électronique par le renforcement du cadre légal de la cryptographie:

Comme nous pouvons l'observer, le législateur algérien a redéfini le cadre juridique de la signature électronique sur la base d'une bonne partie des recommandations proposées, pour remédier aux lacunes et insuffisances enregistrées dans le dispositif en vigueur avant la loi de 2015, à l'exception du régime juridique de la cryptographie. En effet, la loi 15-04 ne traite pas du régime juridique de ce procédé technique qui est à la base de la signature électronique qualifiée telle que définie dans cette loi. Ce qui indique que le législateur algérien a choisi de maintenir

la soumission des équipements et logiciels d'encryption au décret exécutif 09-410 relatif aux équipements sensibles.

Ce choix nous paraît judicieux, dans la mesure où les usages de la cryptographie sont multiples et dépassent le cadre de la signature électronique. Mais il était tout de même nécessaire de lever les ambiguïtés et les incohérences enregistrées dans les dispositions du décret exécutif de 2009, relatives aux équipements et logiciels d'encryption, comme nous l'avons déjà soulevé. C'est pourquoi le législateur a procédé par ailleurs à la révision du décret exécutif 09-410, à travers le Décret exécutif n° 16-61 du 11 février 2016 modifiant et complétant le Décret exécutif n° 09-410 du 10 décembre 2009 fixant les règles de sécurité applicables aux activités portant sur les équipements sensibles²⁰ (Sous-section 1). Même si il n'est nullement fait référence à ce décret, ni dans la loi 15-04, ni dans le décret présidentiel n° 20-05 du 20 janvier 2020 portant mise en place d'un dispositif national de la sécurité des systèmes d'information²¹ (Sous-section 2).

Sous-section 1: Le décret exécutif 16-61 a-t-il modifié le régime juridique des équipements et logiciels d'encryption ? :

Comme déjà souligné, hormis le décret exécutif n°09-410 du 10 décembre 2009 fixant les règles de sécurité applicables aux activités portant sur les équipements sensibles, aucun des textes objet de notre étude ne permet d'établir un quelconque lien entre la signature électronique qualifiée, telle que définie dans la loi 15-04, et la cryptographie qui est à la base de cette signature. Ce décret exécutif a été modifié et complété par le décret exécutif n° 16-61 du 11 février 2016, qui a modifié et complété les dispositions du décret exécutif 09-410 relatives aux équipements et logiciels d'encryption comme suit. Il s'agit notamment des articles 7, 14 et 17 qui ont été modifiés, et les articles 17bis, 17 ter et 17 quater qui ont complété le décret exécutif 09-410:

1. Dispositions modifiées par le décret 16-61 :

- La Soumission de l'exercice des activités de commercialisation et de prestation de services des équipements sensibles, dont les équipements et logiciels d'encryption, au régime d'agrément préalable a été maintenue; sauf que l'article 3 du décret 16-61 a modifié l'article 7 du décret exécutif 09-410, qui désormais a uniformisé la procédure de délivrance des agréments de Type I et II prévus à l'article 6 du décret exécutif 09-410²². Ces derniers sont délivrés indépendamment de l'activité portant sur les équipements et logiciels d'encryption par les services du ministère chargé de l'intérieur après avis du ministère chargé des technologies de l'information et de la communication (MPTIC) et le ministère de la défense nationale.

A travers cette modification le législateur aurait substitué les ministères chargés respectivement des technologies de l'information et de la communication et de la défense nationale à l'autorité habilitée chargée de l'homologation des équipements et logiciels d'encryption, citée pour la première fois dans les articles 7, 8, 20 et 35 du décret exécutif 09-410, et visant exclusivement les activités portant sur les équipements et logiciels d'encryption. Et ce afin de répondre au souci relatif à l'opacité qui entoure cette entité.

Le cadre juridique de la signature et de la certification électroniques en Algérie après quinze ans de législation

Hadjira BOUDER

- Concernant la procédure d'acquisition, de vente et d'installation (chapitre III du décret exécutif 09-410), le décret exécutif 16-61 a modifié l'article 14 du décret exécutif 09-410, relatif à l'acquisition sur le marché extérieur des équipements sensibles. Cette activité était soumise à un visa établi par le ministère des PTIC après accord préalable des services des ministères de la défense et de l'intérieur (et dont les conditions et modalités d'application ont été précisées dans l'arrêté interministériel de 2011²³), lorsque elle porte sur des équipements et logiciels d'encryption.

L'article 14 traitait de l'acquisition du marché extérieur des équipements sensibles sans définir les fins ni la qualité de l'acquéreur. Mais depuis 2016, l'acquisition sur le marché extérieur des équipements et logiciels d'encryption par les opérateurs et les personnes physiques ou morales, aux fins de détention et d'utilisation, est soumise à une autorisation préalable délivré par les services du ministère chargé des technologies de l'information et de la communication, après avis préalable des services des ministères chargés de la défense nationale et de l'intérieur; et la demande y relative doit être accompagnée d'une copie de l'autorisation d'exploitation de ces équipements, établie conformément à l'article 20 du décret 09-410 qui n'a pas été modifié, et qui stipule que : « L'exploitation des équipements sensibles classés dans les sous-sections 1, 2 et 3 de la section A, la sous-section 1 de la section B et la sous-section 1 de la section C de l'annexe I, est subordonnée à une autorisation préalable délivrée par les services :

- du ministère chargé des technologies de l'information et de la communication ou de l'autorité de régulation de la poste et des télécommunications, selon le cas, conformément aux dispositions législatives et règlementaires en vigueur, en ce qui concerne les équipements sensibles classés dans les sous-sections 1, 2 et 3 de la section A de l'annexe I, après avis favorable des services du ministère de la défense nationale et du ministère chargé de l'intérieur et de l'autorité visée au 2ème tiret de l'article 7 ci-dessus pour les équipements classés dans la sous-section 3 de la section A précitée ».

À rappeler que l'article 7, auquel renvoi cet article, a été modifié par ce même décret et ne comporte plus aucune mention de l'autorité d'homologation des équipements et logiciels d'encryption (visée au 2ème tiret de l'article 7).

L'article 14 a également été complété par un deuxième paragraphe qui stipule que : « Dans tous les cas cités ci-dessus, une copie de l'autorisation d'acquisition est transmise aux services du ministère de la défense nationale. Une copie de l'autorisation est également transmise aux services du ministère chargé de l'intérieur lorsqu'elle est délivrée par les autorités citées aux tirets 1^{er} et 2 ci-dessus ». Le tiret 1^{er} étant réservé aux équipements et logiciels d'encryption.

L'article 13 du décret exécutif 09-410, relatif à l'acquisition, au niveau national, d'équipements sensibles par les opérateurs dûment agréés n'a pas été modifié, mais l'article 17 du décret 09-410 a été complété par d'autres dispositions.

- En ce qui concerne l'acquisition des équipements et logiciels d'encryption, au niveau national par les personnes physiques ou morales, aux fins de détention ou

d'utilisation, elle est toujours soumise à l'autorisation délivrée par l'ARPT au vu de l'autorisation d'exploitation visée à l'article 20; mais lorsque la demande d'autorisation émane d'une entreprise publique relevant du secteur de l'énergie, cette autorisation d'acquisition est délivrée par le ministère chargé des technologies de l'information et de la communication après avis préalable des services des ministères chargés de la défense nationale et de l'intérieur, conformément au nouveau article 17.

2. Dispositions complétées par le décret exécutif n°16-61 :

L'article 4 du décret 16-61 a complété le décret exécutif 09-410 par trois nouveaux articles 17 bis, 17 ter et 17 quater. Ces articles contiennent tous des dispositions visant les équipements et logiciels d'encryption et concernent respectivement :

- L'article 17 bis est venu ajouter à la procédure d'acquisition au niveau national, d'équipement et logiciels d'encryption, la présentation d'une demande accompagnée d'une copie de l'autorisation d'exploitation de ces équipements.
- L'article 17 ter concerne quant à lui l'admission temporaire (au lieu d'exportation temporaire) sur le territoire national d'équipements sensibles, dont les équipements et les logiciels d'encryption; qui est soumise à une autorisation préalable délivrée par les services du ministère chargé des technologies de l'information et de la communication, après avis préalable des services des ministères chargés de la défense nationale et de l'intérieur. Et la réexportation de ces équipements et logiciels, qui est soumise à une déclaration auprès des services du ministère chargé des technologies de l'information et de la communication (la définition des modalités d'application de cette article étant laissé à la réglementation).
- L'article 17 quater concerne l'exportation temporaire et la réimportation d'équipements sensibles dûment autorisés, qui sont soumises, dans le cas des équipements et logiciels d'encryption, à autorisations délivrées par le ministère chargé des technologies de l'information et de la communication, mais sans préciser si cette autorisation est aussi délivrée après avis préalable des services des ministères chargés de la défense et de l'intérieur. Cette remarque est également valable pour l'article 17 ter.

Nous estimons que l'ajout de ces trois articles est judicieux, puisque il intervient pour combler les lacunes relevées précédemment dans le décret exécutif 09-410, concernant l'importation et l'exportation des équipements et logiciels d'encryption.

Les modalités d'application des dispositions du décret exécutif 09-410 relatives à d'importation ont été définies dans l'arrêté interministériel de 2011 et des textes internes aux services des douanes, mais sans aborder l'importation temporaire de ces équipements et logiciels.

Quant à l'activité d'exportation des équipements sensibles, elle est en principe régit par le décret exécutif 09-410 modifié et complété par le décret exécutif 16-61, comme l'indique son article 6, mais nous n'avons relevé aucune disposition dans ce décret qui traite de cette activité, à l'exception des article 17 ter et 17 quater qui traitent respectivement de la réexportation d'équipements sensibles importés temporairement, et d'exportation temporaire d'équipement dûment autorisés.

A noter, qu'en novembre 2011 un Décret présidentiel fixant les règles et procédures régissant l'exportation des matériels, équipements et produits sensibles²⁴ a été promulgué, suivi d'un texte d'application paru en 2012. Ce décret présidentiel cite explicitement, dans son article 2 : « les équipements sensibles cités dans la sous-section 3 de la section A de l'annexe 1 du décret exécutif 09-410 », c'est-à-dire les équipements et logiciels d'encryption.

Sans rentrer dans les détails de ce décret présidentiel, il faut noter que les procédures qu'il préconise pour l'exportation de ces équipements et logiciels sont rigides. Il soumet cette activité au régime d'autorisation préalable délivrée par le MPTIC, mais ce dernier doit envoyer cette demande au ministre de la défense qui se charge de la soumettre au comité interministériel consultatif cité à l'article 4, ce comité est composé de représentants permanents des ministères chargés de la défense, des affaires étrangères, de l'intérieur, des finances et du commerce, et des membres non permanents selon la nature des équipements ou du produit en question; et pour les équipements et logiciels d'encryption, les représentants en question sont: deux représentants du MPTIC et un représentant de *l'autorité habilitée chargée de l'homologation des équipements et logiciels d'encryption* cité dans les articles 7, 8, 20 et 35 du décret exécutif 09-410, qui n'apparaît plus dans le décret exécutif 16-61.

Mais ce qu'il faut souligner, c'est qu'en dépit de l'importance de ce décret présidentiel dans le cadre juridique de la cryptographie, aucun des textes postérieurs relatifs à la sécurité des échanges électronique, ni même le décret exécutif 16-61 ne fait référence à ce décret présidentiel.

En conclusion, le législateur algérien a tenté à travers la révision du décret exécutif 09-410 de palier les incohérences qui l'entachaient, notamment en ce qui concerne les équipements et logiciels d'encryption, mais il a maintenu l'esprit de ce texte, en se limitant aux aspects procéduraux, et en réservant un régime unique pour l'ensemble des équipements sensibles, où il n'est toujours pas fait de distinction entre la cryptographie utilisée aux fins d'authentification et celle utilisée aux fins de confidentialité. Le décret 16-61 qui ne permet toujours pas, également, d'établir un quelconque lien entre ses dispositions et les dispositions de la loi 15-04 relative à la signature électronique, ne contient plus aucune mention de *l'autorité habilitée chargée de l'homologation des équipements et logiciels d'encryption* citée pour la première fois dans l'article 7 du décret 09-410. Toutefois, la mission de cette autorité a été attribuée conformément à la loi 15-04 à une autre entité; qui a été défini 5 ans plus tard dans le décret présidentiel n° 20-05 du 20 janvier 2020 portant mise en place d'un dispositif national de la sécurité des systèmes d'information.

Sous-section 2 : Mise en place d'un dispositif national de la sécurité des systèmes d'information : une garantie pour la fiabilité de la signature électronique qualifiée

La création d'une agence nationale de sécurité des systèmes d'information faisait partie des recommandations faites à l'endroit du Groupe de Travail Chargé du Rôle de l'Autorité Racine Autonome en matière de Certification Electronique relevant des Services du Premier Ministre en 2013, comme déjà signaler. Cette

recommandation a été finalement concrétisée mais dans un cadre plus large, qui est le dispositif national de la sécurité des systèmes d'information, mis en place par le décret présidentiel n° 20-05.

En effet, le flou qui entourait *l'autorité habilitée chargée de l'homologation des équipements et logiciels d'encryption*, qui a été cité pour la première fois dans le décret exécutif 09-410 sans aucune précision sur sa nature, sa composition, ou son fonctionnement, fut dissipé grâce à la loi 15-04.

1. L'entité en charge des missions d'homologation, d'approbation et d'audit énoncés par la loi 15-04 :

On peut déduire que la suppression de la mention de *l'autorité habilitée chargée de l'homologation des équipements et logiciels d'encryption* dans le décret 16-61, comme déjà souligner, est intervenue suite à l'énoncé de l'article 14 de la loi 15-04, qui attribue la mission de vérification de la conformité du dispositif sécurisé de création de signature électronique qualifiée aux exigences édictées aux articles 11 et 13 de ladite loi à « l'entité nationale en charge de l'homologation des dispositifs de création et de vérification de la signature électronique ».

Aussi, le point 1 de l'article 18 de la loi 15-04 relatif aux missions de « l'autorité nationale de certification électronique », soumet l'approbation de sa politique de certification électronique à l'avis favorable de l'entité en charge de l'approbation.

Ces deux missions, attribuées par la loi 15-04 à cette entité nationale, étaient assurées pour une période transitoire, jusqu'à la création de cette dernière, par : les services compétents en matière d'homologation conformément à l'article 78; et par le conseil de l'autorité nationale de certification en ce qui concerne l'approbation de sa politique de certification conformément à l'article 80.

La missions d'audit de l'autorité nationale de certification électronique, des autorités économique et gouvernementale, des tiers de confiance et des prestataires de services de certification électronique sont également attribuées, conformément à l'article 79 de la loi 15-04, à « l'entité en charge de cette missions », mais elles étaient assurées par les services compétents en matière d'audit, déterminés par voie réglementaire pour une période transitoire jusqu'à la création de cette entité.

La période de transition cité dans les articles 78,79 et 80 ne devant pas dépasser cinq ans à partir de la date de publication de la loi 15-04. Cette échéance a, effectivement, été respectée, puisque l'entité nationale en question a été instituée quelques jours avant la fin de la cinquième année de publication de la loi sur la signature et la certification électronique, à travers le décret présidentiel n° 20-05 du 20 janvier 2020 portant mise en place d'un dispositif national de la sécurité des systèmes d'information.

2. Quelle est « l'entité en charge de l'homologation, de l'approbation et de l'audit » en Algérie? :

Selon l'article 2 du décret présidentiel n° 20-05 du 20 janvier 2020 portant mise en place d'un dispositif national de la sécurité des systèmes d'information, ce dispositif national est : « l'instrument de l'Etat en matière de sécurité des systèmes d'information. Il constitue le cadre organisationnel pour l'élaboration de la stratégie

Le cadre juridique de la signature et de la certification électroniques en Algérie après quinze ans de législation

Hadjira BOUDER

nationale de la sécurité des systèmes d'information et la coordination de sa mise en œuvre ». Il est placé auprès du ministère de la défense nationale, et comprend :

- Un conseil national de la sécurité des systèmes d'information, chargé d'élaborer, d'approuver et d'orienter la stratégie nationale de sécurité de systèmes d'information;
- Une agence de la sécurité des systèmes d'information, chargée de la coordination de la mise en œuvre de la stratégie nationale de sécurité des systèmes d'information.
- Les structures du ministère de la défense nationale compétentes en matière de sécurité des systèmes d'information.

Le conseil national de la sécurité des systèmes d'information, qui est présidé par le ministre de la défense nationale ou de son représentant, est composé de représentants de la présidence de la république, du premier ministre et des ministres chargés des affaires étrangères, de l'intérieur, de la justice, des finances, de l'énergie, des télécommunications et de l'enseignement supérieur. Il est chargé, conformément à l'article 4 du décret présidentiel, de plusieurs missions, dont : « - d'approuver la politique de certification électronique de l'autorité nationale de certification électronique ; ».

Quant à l'agence de la sécurité des systèmes d'information, qui est un établissement public à caractère administratif, doté de la personnalité morale et de l'autonomie financière, elle est administrée par un comité d'orientation et dotée d'un comité scientifique. Le comité d'orientation est présidé par un président nommé au sein du ministère de la défense; et il est composé des représentants des ministères chargés de la défense, des affaires étrangères, de l'intérieur, de la justice, des finances, de l'énergie, de l'enseignement supérieur, de l'industrie, des télécommunications, du commerce, ainsi que des représentants des services de sécurité, de l'autorité de régulation de la poste et des communications électroniques²⁵, de l'autorité nationale de certification électronique, de l'autorité nationale de protection des données à caractère personnel et de l'autorité gouvernementale de certification électronique.

Ainsi toutes les autorités de certification électronique créées par la loi 15-04 sont représentées dans le comité d'orientation de l'agence. Qui est chargée, conformément à l'article 18 du décret présidentiel, de plusieurs missions, dont :

«[...] - de proposer les modalités d'accréditation des prestataires de service d'audit en matière de sécurité des systèmes d'information ;

[...]– de suivre les opérations d'audit de la sécurité des systèmes d'information ;

[...]– d'homologuer et de certifier les produits de la sécurité des systèmes d'information ;

- d'homologuer les dispositifs de création et de vérification de la signature électronique ;

- de fixer les critères et les procédures de labellisation, certification et/ou d'accréditation, conformément à la législation en vigueur, des produits et prestataires en matière de sécurité des systèmes d'information ; [...] »

Il est à présent clair, qu'hormis l'approbation de la politique de certification électronique de l'autorité nationale de certification électronique qui relève des

prérogatives du conseil national de la sécurité des systèmes d'information, les missions d'homologation et d'audit énoncées par la loi 15-04 sont confiées à l'agence de la sécurité des systèmes d'information.

Conclusion :

Après avoir examiné et analysé les multiples textes juridiques ayant régi la signature et la certification électroniques dans notre pays, depuis la reconnaissance de l'écrit électronique en 2005 jusqu'à la mise en place du dispositif national de sécurité des systèmes d'information en 2020, on peut constater que le cadre juridique de la signature électronique en Algérie est passé par deux étapes clés:

- La première étape c'est celle qui a précédé la promulgation de la loi de 2015 sur la signature et la certification électroniques. Celle-ci était marquée par la promulgation de trois textes importants, ayant respectivement trait à : l'adaptation du droit de la Preuve; les conditions de fiabilité de la signature électronique basée sur la certification électronique; et le cadre légal de la cryptographie. Mais en dépit de l'importance de ces textes, le cadre juridique de la signature électronique numérique en Algérie était flou et incomplet, à cause de l'imprécision et des incohérences de ces textes, qui était principalement dû au fait que chacun de ces derniers traduisait l'appréhension du département ministériel l'ayant proposé de la signature électronique (impératif de modernisation du droit, impératif de développement des services de télécommunication, impératif sécuritaire). Mais cet état de fait n'était pas sans conséquences sur la promotion des services numériques dans notre pays, notamment l'e-gouvernement.
- La multiplication des applications de l'e-administration dans notre pays durant la première décennie du millénaire a mis en exergue les lacunes et les insuffisances du cadre juridique de la signature électronique entant que moyen fiable de sécurité des échanges électroniques. D'où la promulgation de la loi de 2015 sur la signature et la certification électroniques, qui a marqué le début de la deuxième étape clé dans l'évolution du cadre juridique de la signature électronique en Algérie. Cette loi a permis de remédier à une bonne partie des lacunes et insuffisances enregistrées dans le dispositif antérieur à son adoption, en précisant la valeur juridique de la signature électronique, définissant le schéma national de certification électronique et le régime juridique de la prestation de services de certification en Algérie. Mais cette loi ne contient pas de dispositions relatives à la cryptographie, qui pourtant est à la base de la signature électronique qualifiée, telle que définie dans la loi de 2015. C'est pourquoi il était nécessaire de parachever ce chantier de redéfinition du cadre juridique de la signature électronique, en révisant le cadre légal de la cryptographie et en mettant en place un dispositif national pour la sécurité des systèmes d'information; même si il est toujours difficile d'établir le lien entre la signature électronique qualifiée et le dispositif national de sécurité des système d'information, d'une part, et le cadre légal de la cryptographie, d'une autre part.

Ainsi on peut conclure que le cadre juridique de la signature et de la certification électroniques dans notre pays a, certes, évolué doucement, mais cette lenteur dans son évolution a permis au législateur de mieux appréhender ce moyen technologique de sécurisation des échanges électroniques, qui fait appel à plusieurs procédés techniques relevant de régimes juridiques distincts, à savoir : la cryptographie et la certification électronique. Et grâce à cette évolution l'Algérie dispose désormais d'un cadre juridique plus clair et cohérent en matière de signature et de certifications électroniques. Ceci ne peut que contribuer à l'accélération de la transformation numérique dans notre pays, notamment après la promulgation de la loi sur le e-commerce et la loi sur la protection des données à caractère personnel en 2018.

Par ailleurs, et en dépit de ces satisfaisantes avancées juridiques, il est nécessaire de revenir sur certains points négatifs relevés lors dans notre présent travail, qui risquent de compromettre la mise en œuvre de ce cadre juridique, et par voie de conséquence entraver la croissance des services numériques dans notre pays, et que nous recommandons d'observer. Il s'agit notamment de :

- Le décalage, d'une part, entre la date de promulgation de la loi de 2015 et de ses textes d'application, telle que l'entité en charge de l'approbation , l'homologation et l'audit énoncés par la loi de 2015, qui a été créée par le décret présidentiel n° 20-05, soit cinq ans après la promulgation de la loi. Et d'une autre par, le décalage entre la promulgation des textes et leur mise en œuvre effective, comme pour Les Autorités Nationales et Gouvernementales de Certification Électronique, qui n'ont été mises en place qu'en janvier 2018, et ne sont opérationnelles que depuis le 15 novembre 2020, soit quatre ans après la promulgation de leur textes de création en 2016. C'est pourquoi nous recommandons d'accélérer la mise en œuvre du dispositif juridique de la signature et de la certification électronique à travers notamment ; la création de la l'agence de la sécurité des systèmes d'information et l'élaboration et la mise en œuvre de la stratégie nationale en la matière prévue par le décret présidentiel n° 20-05. Et ce afin de garantir la fiabilité de la signature électronique basée sur la certification et assurer son effectivité.
- Outre ses aspects juridiques, la sécurité des échanges électroniques fait appel à des technologies très avancées en perpétuelle évolution, qui requièrent une grande maîtrise et une ressource humaine très qualifiée. D'où la nécessité d'élaborer des programmes nationaux de formation adaptés à ces besoins, et d'encourager la recherche et développement dans le domaine de la sécurité des systèmes d'information. Et ce afin de maîtriser notre dépendance numérique dans ce domaine, voire la réduire.

Bibliographie :

I-Textes juridiques :

- Loi n° 2000-03, fixant les règles générales relatives à la poste et aux télécommunications, du 5 août 2000, Journal Officiel de la République Algérienne Démocratique et Populaire n° 48, du 6 août 2000.
- Loi n° 05-02, modifiant et complétant l'ordonnance n° 75-59 du 26 septembre 1975 portant code de commerce, du 6 février 2005, Journal Officiel de la République Algérienne Démocratique et Populaire n° 11, du 9 février 2005,
- Loi n° 05-10, modifiant et complétant l'ordonnance n° 75-58 du 26 septembre 1975 portant code civil, du 20 juin 2005, Journal Officiel de la République Algérienne Démocratique et Populaire n° 44, du 26 juin 2005.
- Loi n° 15-04, fixant les règles générales relatives à la signature et à la certification électroniques, du 1er février 2015, Journal Officiel de la République Algérienne Démocratique et Populaire n° 6, du 10 février 2015.
- Décret présidentiel n° 2011-383, fixant les règles et procédures régissant l'exportation des matériels, équipements et produits sensibles, du 23 novembre 2011, Journal Officiel de la République Algérienne Démocratique et Populaire n° 64, du 27 novembre 2011.
- Décret présidentiel n° 20-05, portant mise en place d'un dispositif national de la sécurité des systèmes d'information, du 20 janvier 2020, Journal Officiel de la République Algérienne Démocratique et Populaire n° 04, du 26 janvier 2020.
- Décret exécutif n° 07-162, modifiant et complétant le décret exécutif n° 01-123 du 15 Safar 1422 correspondant au 9 mai 2001 relatif au régime d'exploitation applicable à chaque type de réseaux, y compris radio-électriques et aux différents services de télécommunications, du 30 mai 2007, Journal Officiel de la République Algérienne Démocratique et Populaire n° 37, du 7 juin 2007.
- Décret exécutif n° 09-410, fixant les règles de sécurité applicables aux activités portant sur les équipements sensibles, du 10 décembre 2009, Journal Officiel de la République Algérienne Démocratique et Populaire n° 73, du 13 décembre 2009.
- Décret exécutif n° 16-134, fixant l'organisation, le fonctionnement et les missions des services techniques et administratifs de l'Autorité Nationale de Certification Electronique, du 25 avril 2016, Journal Officiel de la République Algérienne Démocratique et Populaire n° 26, du 28 avril 2016.
- Décret exécutif n° 16-135, fixant la nature, la composition, l'organisation et le fonctionnement de l'Autorité Gouvernementale de Certification Électronique, du 25 avril 2016, Journal Officiel de la République Algérienne Démocratique et Populaire n° 26, du 28 avril 2016.
- Décret exécutif n° 16-61, modifiant et complétant le Décret exécutif n° 09-410 du 10 décembre 2009 fixant les règles de sécurité applicables aux activités portant sur les équipements sensibles, du 11 février 2016, Journal Officiel de la République Algérienne Démocratique et Populaire n° 09, du 17 février 2016.

Le cadre juridique de la signature et de la certification électroniques en Algérie après quinze ans de législation

Hadjira BOUDER

- Arrêté interministériel, fixant les conditions et modalités d'acquisition, de détention, d'exploitation, d'utilisation et de cession des équipements sensibles, du 13 octobre 2011, Journal Officiel de la République Algérienne Démocratique et Populaire n°63, du 23 novembre 2011.

II- Ouvrages :

- Commission des Nations Unies pour le Droit Commercial International (CNUDCI), « Promouvoir la confiance dans le commerce électronique: questions juridiques relatives à l'utilisation internationale des méthodes d'authentification et de signature électroniques, Publications des Nations Unies, viennes, 2009, https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/fr/08-55699_ebook.pdf (Consulté le : 26-02-2021)
- Claudine GUERRIER et Marie-christine MONGET, « Droit et Sécurité des Télécommunications », Collection technique et scientifique des télécommunications, Springer-Verlag France et CENT France Télécom, Paris, 2000.

III- Communications scientifiques:

- Ahmed BERBAR, « Certification Electronique en Algérie: Situation et Perspectives », Séminaire international sur la certification électronique, les 08 et 09 décembre 2009, ARPT, Algérie.
- Hadjira BOUDER, « Le cadre juridique de la signature et de la certification électronique en Algérie », faite en réponse à l'invitation du Groupe de Travail Chargé du Rôle de l'Autorité Racine Autonome en matière de Certification Electronique relevant des Services du Premier Ministre, le 11 juin 2013, ARPT, Alger.

IV- Sites web :

- Site officiel de l'autorité gouvernementale de la certification électronique, <https://agce.dz/presentation-de-lagce/> (consulté le 02-01-2021)
- Site officiel de l'autorité économique de la certification électronique, <https://aece.dz/webtrust.html> (consulté le 02-01-2021).

Notes de fin de page

¹ Commission des Nations Unies pour le Droit Commercial International (CNUDCI), « Promouvoir la confiance dans le commerce électronique: questions juridiques relatives à l'utilisation internationale des méthodes d'authentification et de signature électroniques, Publications des Nations Unies, viennes, 2009, p.14, https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/fr/08-55699_ebook.pdf (Consulté le : 26-02-2021)

² Commission des Nations Unies pour le Droit Commercial International (CNUDCI), Ibid, p.17.

Le cadre juridique de la signature et de la certification électroniques en Algérie après quinze ans de législation

Hadjira BOUDER

³ Ahmed BERBAR, « Certification Electronique en Algérie: Situation et Perspectives », Séminaire international sur la certification électronique, les 08 et 09 décembre 2009, ARPT, Algérie.

⁴ Claudine GUERRIER et Marie-christine MONGET, « Droit et Sécurité des Télécommunications », Collection technique et scientifique des télécommunications, Springer-Verlag France et CENT France Télécom, Paris, 2000.

⁵ Loi n° 2000-03, fixant les règles générales relatives à la poste et aux télécommunications, du 5 août 2000, Journal Officiel de la République Algérienne Démocratique et Populaire n° 48, du 6 août 2000, p.p.3-21.

⁶ Loi n° 15-04, fixant les règles générales relatives à la signature et à la certification électroniques, du 1er février 2015, Journal Officiel de la République Algérienne Démocratique et Populaire n° 6, du 10 février 2015, p.p.6-14

⁷ Loi n°05-02, modifiant et complétant l'ordonnance n°75-59 du 26 septembre 1975 portant code de commerce, du 6 février 2005, Journal Officiel de la République Algérienne Démocratique et Populaire n°11, du 9 février 2005, p.p.7-9

⁸ Loi n° 05-10, modifiant et complétant l'ordonnance n° 75-58 du 26 septembre 1975 portant code civil, du 20 juin 2005, Journal Officiel de la République Algérienne Démocratique et Populaire n°44, du 26 juin 2005, p.p.19-20

⁹ Décret exécutif n° 07-162, modifiant et complétant le décret exécutif n° 01-123 du 15 Safar 1422 correspondant au 9 mai 2001 relatif au régime d'exploitation applicable à chaque type de réseaux, y compris radio-électriques et aux différents services de télécommunications, du 30 mai 2007, Journal Officiel de la République Algérienne Démocratique et Populaire n°37, du 7 juin 2007, p.p.12-13

¹⁰ Sur le principe de la neutralité technologique voir : Commission des Nations Unies pour le Droit Commercial International (CNUDCI), « Promouvoir la confiance dans le commerce électronique: questions juridiques relatives à l'utilisation internationale des méthodes d'authentification et de signature électroniques », op-cit, p.38.

¹¹ Sur les Modèles de certification électronique voir : Ahmed BERBAR, « Certification Electronique en Algérie: Situation et Perspectives », op-cit.

¹² Décret exécutif n° 09-410, fixant les règles de sécurité applicables aux activités portant sur les équipements sensibles, du 10 décembre 2009, Journal Officiel de la République Algérienne Démocratique et Populaire n°73, du 13 décembre 2009, p.p.4-14.

¹³ Hadjira BOUDER, « Le cadre juridique de la signature et de la certification électronique en Algérie », faite en réponse à l'invitation du Groupe de Travail Chargé du Rôle de l'Autorité Racine Autonome en matière de Certification Electronique relevant des Services du Premier Ministre, le 11 juin 2013, ARPT, Alger.

¹⁴ Hadjira BOUDER, Ibid

¹⁵ Société d'Automatisation des Transactions Interbancaires et de Monétique , créée par un consortium de banques publiques en 1995, et chargée de la promotion et la prestation de services en rapport avec la modernisation, la normalisation et les transactions monétiques interbancaires.

¹⁶ Décret exécutif n° 16-134, fixant l'organisation, le fonctionnement et les missions des services techniques et administratifs de l'Autorité Nationale de Certification Electronique, du 25 avril 2016, Journal Officiel de la République Algérienne Démocratique et Populaire n°26, du 28 avril 2016, p.p. 5-8.

¹⁷ Décret exécutif n° 16-135, fixant la nature, la composition, l'organisation et le fonctionnement de l'Autorité Gouvernementale de Certification Électronique, du 25 avril 2016, Journal Officiel de la République Algérienne Démocratique et Populaire n°26, du 28 avril 2016, p.p.9-14.

¹⁸ Site officiel de l'autorité gouvernementale de la certification électronique, <https://agce.dz/presentation-de-lagce/> (consulté le 02-01-2021)

Le cadre juridique de la signature et de la certification électroniques en Algérie après quinze ans de législation

Hadjira BOUDER

¹⁹ Site officiel de l'autorité économique de la certification électronique, <https://aece.dz/webtrust.html> (consulté le 02-01-2021).

²⁰ Décret exécutif n° 16-61, modifiant et complétant le Décret exécutif n° 09-410 du 10 décembre 2009 fixant les règles de sécurité applicables aux activités portant sur les équipements sensibles, du 11 février 2016, Journal Officiel de la République Algérienne Démocratique et Populaire n° 09, du 17 février 2016, p.p.7-13.

²¹ Décret présidentiel n° 20-05, portant mise en place d'un dispositif national de la sécurité des systèmes d'information, du 20 janvier 2020, Journal Officiel de la République Algérienne Démocratique et Populaire n°04, du 26 janvier 2020, p.p.5-9.

²² L'article 8 étant abrogé par l'article 9 du décret exécutif 16-61

²³ Arrêté interministériel, fixant les conditions et modalités d'acquisition, de détention, d'exploitation, d'utilisation et de cession des équipements sensibles, du 13 octobre 2011, Journal Officiel de la République Algérienne Démocratique et Populaire n°63, du 23 novembre 2011, p.p. 22-29

²⁴ Décret présidentiel n° 2011-383, fixant les règles et procédures régissant l'exportation des matériels, équipements et produits sensibles, du 23 novembre 2011, Journal Officiel de la République Algérienne Démocratique et Populaire n° 64, du 27 novembre 2011, p.p.9-11

²⁵ C'est la nouvelle appellation de l'autorité de régulation de la poste et des télécommunications (ARPT), depuis la publication de la loi [n° 18-04 du 10 mai 2018](#) fixant les règles générales relatives à la poste et aux communications électroniques.