Revue Internationale des Sciences de Gestion
ISSN: 2665-7473
Numéro 6 / Volume 3 : numéro 1

La sécurité des échanges électroniques : Cas du gouvernement électronique

The security of electronic exchanges : Case of E-government

GHOULY Mehdi
Docteur en économie et gestion
FSJES Mohammedia
Université Hassan II Ain Chock – Casablanca
Laboratoire Intelligence Stratégique (LIS)
mehdighouly@hotmail.com

FASLY Hakima
Enseignante chercheuse
FSJES Mohammedia
Université Hassan II Ain Chock – Casablanca
Laboratoire Intelligence Stratégique (LIS)
faslyhakima@gmail.com

Date de soumission : 09/12/2019
Date d'acceptation : 21/01/2020
Pour citer cet article :
GHOULY. M & FASLY H. (2019) « La sécurité des échanges électroniques : Cas du gouvernement électronique », Revue Internationale des Sciences de Gestion « « Numéro 6 / Volume 3 : numéro 1 » pp : 869 – 889

Digital Object Identifier : https://doi.org/10.5281/zenodo.3664949

Résumé

Pour passer d'une administration publique traditionnelle qui se caractérise par la bureaucratie et la complexité des procédures, à une administration en ligne, ou encore à un gouvernement électronique, le recours à la technologie internet est plus qu'une nécessité c'est une obligation. Ce réseau géant, permet de mettre en liaison ; instantanément ; plusieurs groupes de réseaux, afin de faciliter la communication, le partage d'information et l'échange de données, avec les particuliers, les entreprises et même parfois entre les administrations elles-mêmes.

Par conséquent, pour profiter pleinement de ce gouvernement électronique, une sécurité technique soutenue par un arsenal juridique solide et adapté à cet environnement virtuel s'avère absolument indispensable. Cette dite sécurité constitue un outil incontournable pour la protection des données et des informations ainsi que le système dans lequel elles se traitent et se logent.

Dans le présent travail nous avons abordé les différentes techniques de sécurité informatique, qui en plus de la protection technique, elles procurent une valeur juridique et administrative appropriée au domaine numérique.

Mots clés : Gouvernement électronique ; ICP « Infrastructure à Clé Publique » ; cryptographie ; certification électronique ; signature électronique.

Abstract

To transit from a traditional public administration characterized by the bureaucracy and the complexity of procedures, to an online administration, or even to an electronic government, the use of internet technology is more than a necessity it is an obligation. This giant network makes it possible to connect; instantly; several groups of networks, in order to facilitate communication, information sharing and data exchange, with individuals, businesses and even sometimes between administrations themselves.

Therefore, to take full advantage of this electronic government, technical security supported by a solid legal arsenal and adapted to this virtual environment is absolutely essential. This so-called security constitutes an essential tool for the protection of data and information as well as the system in which they are processed and housed. In this work we have addressed the various IT security techniques, which in addition to technical protection, they provide a legal and administrative value appropriate to the digital domain.

Keywords: E-government; PKI "Public Key Infrastructure"; cryptography; electronic certification; electronic signature.

Introduction

Aujourd'hui, les moyens de diffusion des informations et les techniques de communications ne sont pas les mêmes que ceux qui existaient dans les années 80 et 90. Les TIC ont profondément modifié notre mode de vie et ne cessent de s'imposer, jours après jours, pratiquement dans tous les domaines d'activité humaine (Tamer H, 2019), chose qui a remis en question la fiabilité et l'efficacité des méthodes classiques de sécurité des informations et des communications. Autrement, l'insécurité des échanges électroniques, constitue un obstacle majeur qui peut entraver la réussite d'un projet aussi ambitieux que le gouvernement électronique.

C'est pour cette raison qu'il est fondamental de tenir compte de toute une série d'enjeux, qui dépasse largement le cadre exigu de la technologie, pour s'étendre aux enjeux juridiques, humains et surtout sécuritaires. Il s'agit d'un mix qu'il faudra réussir, afin d'aboutir aux objectifs escomptés par le gouvernement électronique. Cela nous amène à poser les questions suivantes :

- Quelles sont les évolutions en matière de sécurité des échanges électroniques ?
- Qu'en est-il du cadre juridique marocain, régissant les échanges électronique ?

Pour répondre à ces questions, nous présenterons en premier lieu quelques définitions de l'e-gouvernement, ensuite nous allons donner un aperçu sur la technologie PKI, comme étant l'une des solutions les plus efficaces qui permet de procurer les éléments de réponse aux impératifs de sécurité et d'établir la confiance dans les échanges électroniques en générale et chez les opérateurs de l'e-gouvernement en particulier. En deuxième lieu, nous nous attacherons à mettre en lumière les différentes techniques de sécurité informatique, qui en plus de la protection technique, elles procurent une valeur juridique et administrative appropriée au domaine numérique. Il s'agit en l'occurrence de la cryptographie, la signature électronique et la certification électronique.

1. LE GOUVERNEMENT ELECTRONIQUE

Avant de nous pencher sur la question de la sécurité des échanges électroniques, il nous parait important de situer ce que nous entendons par « le gouvernement électronique », tel qu'il a été étudié et traité par plusieurs auteurs.

1.1 Définition

Le gouvernement électronique, aussi connu sous l'appellation du « E-gouvernement », ou encore « Le gouvernement en ligne », est un domaine qui désigne l'application des règles et des principes du commerce électronique dans la sphère publique. Ainsi, le «e » dans l'e-gouvernement fait référence à l'infrastructure technologique et à la plate-forme informatique et électronique qui permettent le déploiement du réseau internet pour interconnecter les administrations, les entreprises et les citoyens.

Pour certains auteurs, le terme gouvernement électronique *« implique l'automatisation ou l'informatisation des procédures existantes non-informatisées, ce qui conduit à de nouveaux styles de leadership, de nouvelles façons de débattre et de décider des stratégies, d'interagir avec les sociétés commerciales, d'écouter les citoyens et les communautés, d'organiser et de livrer l'information, donc essentiellement à de nouvelles façons de gouverner*. » (Driss Kettani & Bernard Moulin, 2014).

Pour d'autres, le gouvernement électronique est considéré comme étant « *un processus de développement institutionnel par lequel les technologies de l'information et des communications (TIC) sont utilisées ou mises à contribution afin d'orienter plus efficacement l'action du gouvernement et de mieux répondre aux besoins du citoyen, de l'entreprise et des membres de la société civile* » (Henri-François Gautrin, 2004).

Egalement l'OCDE a mis l'accent sur les TIC dans sa définition de l'e-gov, en le considérant comme : « *L'usage que les gouvernements font des TI, en particulier d'internet, pour améliorer leur fonctionnement* » (Réjean Roy, 2006). Cette définition a été retenue, lors d'une conférence qui a eu lieu en mai 2005, à l'occasion du colloque international du CEFRIO sur l'egov, par Mer Edwin Lau, le chef de l'unité du gouvernement électronique de l'OCDE (Réjean Roy, 2006).

Ainsi, en traduisant la définition anglaise qui a été mise en avant par la banque mondiale, le gouvernement électronique désigne : « *L'utilisation par les agences gouvernementales des technologies de l'information (telles les réseaux à large spectre (Wide Area Networks), l'Internet, et l'informatique) qui ont la capacité de transformer les relations avec les citoyens, avec les entreprises et les autres branches du gouvernement. Ces technologies peuvent servir plusieurs objectifs différents : une meilleure fourniture des services gouvernementaux aux citoyens, une*

amélioration des interactions avec les entreprises et les industries, l'habilitation des citoyens grâce à l'accès à l'information ou encore une meilleure gestion des affaires administratives. Les bénéfices attendus peuvent être moins de corruption, davantage de transparence, plus de commodités, l'augmentation des revenus et/ou la réduction des coûts »[1].

D'après ce qui précède, nous pouvons considérer qu'on a affaire à trois acceptions de la notion de l'e-gouvernement, qui se répartissent comme suit :

- L'e-gouvernement renvoi à l'utilisation des TIC dans l'administration afin de répondre aux attentes des usagers et d'offrir un service public de meilleure qualité ;
- L'e-gouvernement est assimilé la fourniture des services publics sur internet ;
- L'e-gouvernement désigne la capacité de transformer et de moderniser l'administration publique, moyennant les NTIC et plus particulièrement internet.

Même si certains définitions sont restreintes et d'autres sont plus extensives, la majorité des auteurs, s'accordent sur le fait que le gouvernement électronique est un concept qui consiste à intégrer de façon optimale, les NTIC dans le fonctionnement interne et externe des organismes gouvernementaux, afin de renforcer les processus démocratiques et de favoriser le développement qualitatif et quantitatif des services publics, tout en réduisant les délais d'attente et en offrant un service en ligne, personnalisé et transparent. Il s'agit d'une nouvelle approche, plus interactives qui vise à combler le fossé entre le gouvernement et les différents usagers des services publics.

2. L'INFRASTRUCTURE A CLE PUBLIQUE (ICP)

Pour relever le défi de la modernisation des services publiques et passer d'une administration traditionnelle ; caractérisée par la lourdeur et la complexité des procédures ; vers une administration en ligne, flexible, moderne et rapide, l'investissement dans une infrastructure technologique développée est plus qu'un luxe, c'est une obligation. Au Maroc, la technologie ICP ou encore la PKI « public key infrastructure », a connu un succès remarquable, surtout avec la mise en vigueur du cadre juridique régissant les échanges électroniques de données. Sachant que « *80% de la sécurité des transactions électroniques dépend de l'existence d'un cadre juridique souple et conforme aux conventions internationales* » (Mohamed Hammoumi, 2014)

[1] Disponible sur le site internet de la banque mondiale : http://www.worldbank.org/en/topic/ict/brief/e-government, consulté en mai 2015.

La PKI a été définit par l'IEFT (Internet Engineering Task Force)[2] comme étant « *un ensemble de moyens matériels, de logiciels, de composants cryptographiques, mis en œuvre par des personnes, combinés par des politiques, des pratiques et des procédures requises, qui permettent de créer, gérer, conserver, distribuer et révoquer des certificats basés sur la cryptographie asymétrique* ».

Cette combinaison de moyens humains, documentaires et techniques, contribue à la sécurisation des bi-clés en générant, et en garantissant la gestion de certificats de clés publiques. Finalement, la PKI n'est qu'un logiciel, qui fait appel à des techniques cryptographiques par clé publique pour contrôler, vérifier et authentifier les différentes entités engagées dans le cadre d'une transaction électronique.

3. LA CRYPTOGRAPHIE, LA SIGNATURE ELECTRONIQUE ET LA CERTIFICATION ELECTRONIQUE

A travers ce paragraphe, nous essaierons de mettre en exergue les différentes solutions techniques qui réduisent, voire même éliminent, les risques de fraude, de criminalité et de la manipulation des données échangées par voie électronique. Nous présentons dans un premier temps le principe de la cryptographie, comme étant le procédé de sécurité le plus répondu depuis longtemps. Ensuite, nous examinons les autres dispositifs de sécurité à savoir la signature électronique et la certification électronique, en tant que deux procédés fondamentaux de la cryptographie.

3.1 La cryptographie

La cryptographie est un art qui converge un certain nombre de méthodes mathématique et logique pour brouiller un message et le rendre par la suite incompréhensible, sauf pour les personnes qui détiennent les outils nécessaires pour le décrypter.

Ainsi, le texte original est appelé " Texte En clair " et le texte codé ou modifié est appelé " Texte Chiffré ", d'où la notion de chiffrement[3] qui est « *Un procédé de transcription d'une information intelligible en une information inintelligible par l'utilisation d'algorithmes* » (M.

[2] Disponible sur : http://www.ietf.org. Consulté en juillet 2016.
[3] La conversion de texte clair en texte chiffré est appelée aussi « codage » et l'opération inverse s'appelle « Décodage ». Et si vous essayez de lire un message, alors que vous n'êtes pas le destinataire légitime, là on assiste à un « Craquage ».

Jean-Baptiste, 1998). La norme ISO 8730, considère le chiffrement comme une « transformation cryptographique des données en vue de produire un texte chiffré ».

Le chiffrement consiste à traiter une information par un algorithme mathématique, de sorte que seule la personne qui possède la clé appropriée puisse accéder à l'information et la traiter. Le principe consiste à utiliser un code pour chiffrer les messages et un autre pour les déchiffrer (Jean-François CARPENTIER, 2009).

En d'autre terme, la cryptologie est la science qui traite de la communication en présence d'adversaires. Ainsi, le rôle d'un système cryptologique est de chiffrer un texte clair en le transformant à un cryptogramme au moyen d'une clé. Ce cryptogramme est transmis à son destinataire sur le canal approprié. Ensuite le destinataire légitime doit pouvoir déchiffrer le cryptogramme à l'aide de la clé pour obtenir le texte clair (Bruno Martin, 2004).

Toutefois, plusieurs méthodes de chiffrement ont été envisagées depuis longtemps, pour faire face à la malveillance ou tout simplement pour cacher le sens des messages :

3.1.1 Les méthodes classiques

Avant l'invention des ordinateurs, les premiers cryptographes ont utilisé des méthodes très simples pour crypter les informations, il s'agit en l'occurrence, de la méthode de substitution et celle de la transposition.

- **La méthode de substitution**

Dans ce procédé, à chaque lettre du message ou groupe de lettres on substitue une autre lettre ou un autre groupe de lettres. C'est une sorte de dérivation pour distinguer les caractères du message chiffré aux caractères du message en claire. Le destinataire légitime de sa part, inverse la dérivée pour obtenir le message initial.

Cette substitution peut être mono alphabétique, comme elle peut être poly-alphabétique[4]. Pour la première, on se donne pour chaque lettre de l'alphabet de base, une autre lettre utilisée dans le texte chiffré. Tandis que pour la deuxième, le principe est le même, mais au lieu d'utiliser un seul alphabet, on utilise une suite d'alphabet pour remplacer le texte claire.

[4] Il existe d'autres méthodes de substitutions qui n'ont pas été évoquées, justement parce qu'ils ont un caractère scientifique, à savoir : les substitutions homophoniques et les substitutions de poly-grammes.

❖ **La méthode de Transposition**

C'est une technique qui permet d'assurer la confidentialité d'un message, sans changer ou remplacer les lettres. C'est un procédé mathématique, basé sur la réorganisation de l'ordre des lettres dans un cadre particulier, tout en gardant l'ensemble des lettres.

3.1.2 Les méthodes modernes :

L'arrivée de l'informatique a explosé un besoin énorme en matière de sécurité, mais également, a beaucoup contribué à l'évolution et au perfectionnement des systèmes de chiffrage. Aujourd'hui, deux méthodes s'imposent dans le domaine électronique. La cryptographie symétrique et la cryptographie asymétrique.

❖ **La Cryptographie symétrique**

Aussi appelée, chiffrement à clé privée, ce système permet à deux personnes ou deux entités de communiquer en toute sécurité, bien sûre en possédant une clé secrète, dite privée, qui sert à la fois au chiffrement et au déchiffrement des messages. En pratique, le processus commence chez l'émetteur qui chiffre le message via la clé secrète, avant de l'envoyer au destinataire, tout en repérant le moyen d'échange le plus sûr de la dite clé privée. Ensuite, quand le destinataire reçoit le message chiffré et la clé de déchiffrement, il procède au décryptage pour obtenir le message en claire.

Son avantage majeur, réside dans sa rapidité à transmettre une très grande quantité de donnée. Par contre, la transmission de la clé, qui fait la faiblesse de cette méthode.

Ça veut dire que, le transfert de la clé à son destinataire légitime, doit être effectué en toute confidentialité, faute de quoi, son interception, engendrera le risque de modification et de falsification des données chiffrées avec cette clé.

Donc « Le risque lié à l'utilisation d'une clé unique repose sur sa divulgation à un tiers et à la nécessaire multiplicité des clés détenues par un individu » (H.Bitan, 2006). De plus, lors de l'utilisation de la cryptographie à clé privée, une personne recevant des messages de vingt personnes différentes devra utiliser vingt clés différentes, ce qui pose le problème de la gestion de ces clés (Toulmlilt, 2008).

❖ **La Cryptographie asymétrique**

Avec l'invention du système asymétrique, une grande avancée s'est produite dans le domaine de la cryptographie. Étant donné qu'elle permet de régler les problèmes de la distribution des clés secrètes entre les utilisateurs. Ainsi, « *Cette nouvelle technique permet non*

seulement d'expédier des messages confidentiels dans de meilleures conditions de sécurité, mais aussi de réaliser des signatures numériques» (Fouad BENSEGHIR, 2011).

Le principe est simple, un émetteur utilise la clé publique du destinataire pour convertir un texte clair au texte chiffré, la clé utilisée pour cette opération est largement connue. Le texte chiffré est envoyé ensuite au destinataire qui utilise sa clé privée pour récupérer le texte en clair. Seule la personne qui possède cette clé privée qui correspond à la clé publique, peut déchiffrer le message. Autrement dit, « *le processus n'est pas réversible, car la clé utilisée pour chiffrer le message ne peut pas être utilisée pour le déchiffrer* » (Fusaro, et al., 2002).

Avec ce procédé, de nombreuses personnes peuvent utiliser la même clé publique pour vous envoyer des données chiffrés en toute confiance, à un destinataire, et uniquement lui; qui possède la clé secrète ; a la possibilité de déchiffrer les données. En effet, plus cette clé publique est longue, plus elle est difficile à déchiffrer.

A cet égard, pour renforcer la sécurité technique et juridique de l'opération, l'expéditeur du message peut faire certifier sa clé publique par une autorité de certification avant la transmission de celle-ci aux tiers.

Précisons par ailleurs, que ce système asymétrique, n'est pas complètement infaillible, et le destinataire doit vérifier que la clé publique est bien celle de l'expéditeur du message, ce qui justifie l'intervention de l'autorité de certification.

Bien que, la cryptographie consiste à protéger les systèmes d'information contre toutes les faiblesses de la sécurité, cette science peut cependant être aussi utilisée par les auteurs de virus afin de renforcer leur caractère nocif (Cédric Llorens, et al., 2010). Dans cette optique, la cryptologie a toujours fait l'objet de la bataille entre les cryptographes ; qui s'occupent de la création des chiffres incassables ; et les cryptanalystes ; qui cherchent ; à travers des études approfondies ; à briser ces chiffres.

Dans ce contexte, une infrastructure technique sûre, telle que la cryptographie, et un cadre juridique prévisible pour leur servir d'appui, seront à la base de l'instauration de la confiance chez toutes les parties prenantes, qui participent de près ou de loin dans les transactions électroniques (Rapport OCDE, 1998).

3.1.3 L'aspect juridique

Avant d'entamer l'analyse relative aux textes juridiques régissant le domaine de la cryptographie au Maroc, il nous paraît évident de préciser que, juridiquement depuis janvier

2014 ; et pour des raisons de sécurité nationale ; tout ce qu'a un rapport avec l'homologation de certification des signatures électroniques et la cryptographie, n'est plus l'affaire de l'ANRT (L'Agence Nationale de Réglementation des Télécommunications).

Cette dernière, qui a été ; dans un passé récent ; l'organisme public chargé de proposer au gouvernement la réglementation applicable à la cryptographie et à son contrôle, devait transférer ; progressivement ; ces prérogatives en la matière, à la Direction Générale de la Sécurité des Systèmes d'Information (DGSSI) relevant de l'Administration de la Défense Nationale, qui a vu le jour, le 21 septembre 2011.

Mais pour des raisons purement techniques et organisationnelles, cette passation a tardé un an, avant qu'elle soit opérationnelle. D'ailleurs, c'est pourquoi le décret n° 2-13-881 modifiant et complétant le décret 2-08-518 du 21 mai 2009 pris pour l'application des articles 13,14,15, 21 et 23 de la loi n° 53-05 relative à l'échange électronique de données juridiques ;qui vient d'être publié au bulletin officiel du 05 février 2015 ; sera applicable à compter du 03 janvier 2014(Avec effet rétroactif) .

Cette réforme a été initiée par l'adoption de la loi n° 93-12 modifiant la loi n° 24-96 relative à la poste et aux télécommunications, promulguée par le dahir n°1-13- 57 du 17 juin 2013, publiée au Bulletin officiel le 04 juillet 2013. Suite à laquelle, un délai de six mois ; a compter de la date de la publication ; a été accordé à la DGSSI pour prendre en charge les prérogatives susmentionnées de l'ANRT.

A cet effet, bien que les textes de base n'ont subi aucun changement significatif, le décret n° 2-13-881 du 28 rabii I 1436 (20 janvier 2015), a fait l'objet d'un certain nombre de modification, portant d'abord sur l'intitulé du décret n° 2-08-518 du 25 joumada I 1430 (21 mai 2009), où l'expression « Des articles 13, 14, 15, 21 et 23 », a été supprimé. Egalement la modification a touché les articles 4, 10, 16 (troisième alinéa), 21 (deuxième alinéa) et 25 (paragraphe a), du même décret, en remplaçant l'expression « Autorité gouvernementale chargée des nouvelles technologies » par « Autorité gouvernementale chargée de l'Administration de la défense nationale ».

La même chose se reproduit pour les articles 3, 5, 8, 16 (deuxième alinéa), 18, 19, 20 (premier alinéa), où l'expression «autorité gouvernementale chargée des nouvelles technologies », est remplacée par l'expression «autorité gouvernementale chargée de l'Administration de la défense nationale (Direction générale de la sécurité des systèmes d'information) ». Dans le

même sens, l'expression «Agence nationale de réglementation des télécommunications », a été remplacé par «autorité gouvernementale chargée de l'Administration de la défense nationale (Direction générale de la sécurité des systèmes d'information) », dans les articles 21 (premier alinéa), 23, 24 et 25 (paragraphe b)) du même décret.

En outre, il faut souligner que désormais ; au terme de l'article 3 du décret n° 2-13-881 ; On entend par «l'autorité nationale » ; prévue par la loi n° 53-05 relative à l'échange électronique de données juridiques ; l'autorité gouvernementale chargée de l'Administration de la défense nationale (Direction générale de la sécurité des systèmes d'information).

Revenons maintenant au concept de la cryptographie ; qui d'ailleurs ne fait l'objet d'aucune définition juridique dans le droit marocain ; l'article 12 de la loi n° 53-05, distingue entre deux aspects essentiels de la cryptographie, à savoir, le moyen de cryptographie et la prestation de cryptographie.

Quant au moyen de cryptographie, il désigne tout matériel et/ou logiciel conçu(s) ou modifié(s) pour transformer des données, qu'il s'agisse d'informations, de signaux ou de symboles, à l'aide de conventions secrètes ou pour réaliser l'opération inverse, avec ou sans convention secrète.

A noter que l'objectif principal de ce moyen, est d'assurer la sécurité des données juridiques échangées par voie électronique, de manière qui permet de garantir leur confidentialité, leur authentification et la vérification de leur intégrité.

En effet, toutes les opérations qui font appel, pour le compte d'autrui, à des outils de cryptographie, peuvent être considérées comme des prestations de cryptographie.

Après l'étude technique et l'analyse du cadre juridique de la cryptographie, logiquement, il faut se poser la question sur l'exploitation effective de cette science ; basée sur des méthodes purement mathématiques ; dans la protection de la sécurité informatique. Chose qui nous a conduit ; dans le prochain paragraphe ; à mettre en évidence le procédé de la signature électronique, qui fait appel ; lors de son fonctionnement ; aux différentes techniques de la cryptographie.

3.2 La signature électronique :

Dans le monde du numérique ; caractérisé de plus en plus par la dématérialisation des documents ; la signature manuscrite ; devenue inadaptée à ce contexte immatériel ; a cédé la place à une nouvelle forme de signature, dite électronique. Cette dernière, dès lors que certaines

fonctions sont remplies, aura la même valeur juridique que la signature traditionnelle « manuscrite ».

L'avènement de Cette nouvelle forme de signature, a contribué considérablement à la réduction de la consommation du papier et ; automatiquement ; des coûts inhérents, à savoir, les coûts d'archivage, de déplacement ainsi que la perte du temps et de productivité.

3.2.1 Définition de la signature électronique :

Le concept de la signature, découle du mot latin « signum » c'est-à-dire mettre un signe. Selon le Dictionnaire Robert, la signature manuscrite se définit comme étant « *une inscription qu'une personne fait de son nom (sous une forme particulière et constante) pour affirmer l'exactitude, la sincérité d'un écrit ou en assumer la responsabilité.* ». Egalement une signature peut être définie comme « *le signe par lequel le signataire s'affirme comme l'auteur de ce qu'il signe, marque personnelle intentionnelle qui manifeste son identité et concentre sur sa tête les effets attachés à son initiative*» (Gérard. CORNU, 2007).

Partons de là, on peut dire que la signature ; en générale ; est un outil qui permet d'identifier un acte ainsi que son auteur et donc sa volonté d'adhérer à cet acte. Toutefois, en signant un document, le signataire exprime son consentement et son engagement envers le document signé.

Or, une signature électronique ; qui apporte éventuellement une rupture par rapport au support papier ; n'a pas le même procédé que celle manuscrite. Cette dernière, n'est qu'un simple dessin modifiable sans aucune sécurité. Il en va de même pour la signature numérisée ; appelée aussi signature scannée ; qui ne demande aucune procédure juridique lors de sa création. Il suffit de scanner la signature manuscrite pour obtenir un signe sous forme d'image numérique, qui ne garantit ni l'adhésion de l'auteur à l'acte signé, ni l'intégrité du message.

C'est la raison pour laquelle, « *Une signature manuscrite peut être remise en cause dans la mesure où la graphologie n'est pas une science certaine. Il y a donc toujours une possibilité de contestation d'une signature frauduleuse* » (Alain Bensoussan, 1998).

Précisons par ailleurs que, l'expression de signature numérisée ne doit pas être confondue avec celle de la signature numérique qui fait appel ; lors de son processus de création ; aux mécanismes cryptographiques, qui ont été développés dans le cadre du paragraphe précédent.

Cependant, les avancées dans ce domaine, sont extrêmement rapides et donnant lieu chaque jour à la naissance d'un nouveau procédé et pourtant, aucun d'entre eux, n'a pu atteindre le niveau de fiabilité technique ainsi que la validité juridique, qu'offre la signature numérique.

Il convient de noter que la signature électronique est l'appellation qui englobe pratiquement toutes les techniques d'identification électronique existant actuellement sur le marché, abstraction faite de la technologie utilisée.

3.2.2 L'aspect technique de la signature électronique :

Au moment où la signature manuscrite peut être dessiné par la main ; via une technique très simple, qui n'a pas besoin d'être organisé et qui se résume dans quelque signes plus ou moins artistiques ; la signature électronique est basée sur un procédé qui laisse présager une certaine complexité technique.

Ce procédé est fondé en principe sur un ensemble de données numériques chiffrées, différentes du message initial, de telle sorte à ce que la relation entre le texte et la signature, devient logique plus que physique.

A cet effet, le fonctionnement technique de la signature électronique [5] repose essentiellement sur la combinaison de la cryptographie asymétrique ; déjà traitée en détail dans le paragraphe consacré à la cryptographie ; ainsi que la fonction de hachage. Cette dernière, constitue la solution idéale pour renforcer le principe d'intégrité, dans la mesure où, elle nous permet de convertir un message en une suite numérique, via des formules mathématiques, fournissant ainsi l'assurance que le message n'a subi aucune altération depuis qu'il a été signé électroniquement.

Autrement dit « *une fonction de hachage sert à produire une empreinte courte d'un message indépendamment de sa longueur. Elle permettra par exemple de contrôler l'intégrité des données. On peut aussi imaginer, pour signer un message, de signer un haché bien choisi (pour avoir une signature courte des messages*» (Alain Yger & Jacques-Arthur Weil, 2009).

Il va sans dire que l'utilisation de la signature électronique, revêt une importance capitale, dans la mesure où, elle contribue considérablement à l'optimisation de la sécurité des transactions à distance, tout en garantissant les deux services de sécurité indispensables à la

[5] Cette signature peut être envoyée au destinataire avec le document original ou bien stocké dans un document séparé.

réussite de ce nouveau mode de communication, à savoir l'identification des parties et l'intégrité des messages.

On comprend de ce qui précède que, la signature électronique ; axée sur des procédures cryptographiques ; représente un symbole de modernité et constitue le moyen de preuve le plus proche de la signature traditionnelle « manuscrite » quant à sa fiabilité technique et sa valeur juridique (F. Benseghir, 2011).

3.2.3 Typologies des signatures électroniques:

Dans le cadre de ce travail nous distinguons entre trois types de signature électronique, compte tenu de la fiabilité technique et du niveau de validité juridique ; de chacune d'entre elles.

- **La signature électronique simple**

La signature électronique simple peut être défini comme étant une donnée sous forme électronique, qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification[6].

Autrement dit, tout procédé de signature électronique est dit « simple » dès lors qu'il permet l'identification du signataire et son adhésion au document signé, alors que le contenu du message, reste exposé à toute modification.

Ce qui fait que la signature électronique simple, même si elle est considérée comme un véritable moyen de traçabilité, elle n'est pas présumée fiable jusqu'à preuve de contraire, étant donné que sa création ne fait l'objet d'aucune formalité administrative. En d'autre terme, elle n'a pas la même valeur que la signature manuscrite, ce qui fait qu'en cas de litige, il faut prouver la fiabilité de la procédure mis en œuvre par celui qui veut se prévaloir des effets juridiques de la signature.

- **La signature électronique sécurisée (avancée)**

En plus des mesures d'authentification précitées ; la signature avancée a pu remédier aux limites de la procédure simple, en détectant toute éventuelle manipulation ou modification des données (Article 2.n°2 de la directive 1999 93).

La signature électronique avancée ; par rapport à la simple signature ; elle a un degré de reconnaissance juridique très fort, du fait qu'elle est étroitement liée au concept de certification, qui se base essentiellement sur la garantie d'un tiers de confiance, dont la principale mission est

[6] L'article 2 de la directive européenne du 13 décembre 1999.

notamment de rendre les contrats et les transactions électroniques ; faisant appel à ce type de signature; plus crédible, en terme d'identification des signataires ainsi qu'en terme d'intégrité des données.

Signalons par ailleurs, que la signature électronique pour qu'elle soit avancée et pour qu'elle acquière sa force probante, elle doit obligatoirement se conformer aux exigences légales suivantes (Article 2.n°2 de la directive 1999 93): Être liée uniquement au signataire, permettre d'identifier le signataire, être créée par des moyens que le signataire puisse garder sous son contrôle exclusif et être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectée.

❖ **La signature électronique parfaite**

C'est une signature électronique qui a les mêmes caractéristiques que celle avancée, à moins que sa création repose sur un certificat dit « qualifié », attestant ainsi, du lien entre les données de vérification de la signature électronique et le signataire, afin de vérifier que la clé publique est utilisée par la bonne personne. En effet, la signature électronique parfaite, par rapport aux autres types de signatures, assure un niveau optimal de protection tout en répondant aux attentes des parties impliquées dans les transactions électroniques.

Pour le cas du Maroc, la délivrance de ce type de certificat, est du ressort de Barid Al-Maghrib, le seul prestataire de service de certification électronique (PSCE), qui s'est procuré l'agrément pour exercer cette activité, suite à la décision n° 02-11 du 2 joumada I 1432(6 avril 2011) du directeur général de l'ANRT, publiée dans le bulletin officielle N° 5940- 1er joumada II (5-mai 2011).

3.2.4 L'aspect juridique de la signature électronique

Au-delà des aspects techniques que nous venons d'évoquer, la signature électronique sécurisée est devenue l'équivalent fonctionnel[7] de la signature manuscrite. Cependant, cette signature électronique[8] agit comme un instrument de preuve quant à l'authenticité du document électronique de la même manière que la signature manuscrite vis-à-vis du document sur papier. On assiste à la naissance d'un nouveau moyen de traçabilité plus sûre techniquement, qui en sus de son caractère moderne, il est valable juridiquement.

[7] La notion d'équivalent fonctionnel désigne la méthode qui consiste à se référer aux notions déjà connues dans le droit classique pour donner des solutions visant à les transposer au monde des nouvelles technologies.
[8] La signature électronique doit être distinguée de la signature numérisée (image d'une signature manuscrite qui a été scannée). Ce type de signature n'a aucune valeur juridique.

C'est dans ce contexte que notre pays a adopté depuis le 30 novembre 2007, la loi ; N°53-05[9]; sur l'échange électronique de données juridiques. Cette loi reprend pratiquement la plupart des principes de la directive 1999/93/CE du 13 décembre 1999.

Ainsi, le législateur marocain confère à l'écrit électronique, la même force probante que l'écrit[10] sous forme papier. Egalement, il peut être accepté comme un instrument de preuve, à condition qu'il permette à la personne dont il émane d'être identifiée et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité (Article 417-1, Loi n° 53-05).

Conformément à la réglementation en vigueur, l'authenticité de l'acte juridique est conditionnée par la fiabilité du procédé de la signature électronique ; qui doit être apposée devant un officier public habilité à certifier ; ainsi que sa capacité à garantir, d'une part l'identification de l'auteur et son adhésion au contenu du document, et d'autre part, le lien entre la signature et l'acte signé (Article 417-2, Loi n° 53-05). Ainsi, l'article 417-3 stipule que, le procédé de signature électronique est présumé fiable dès lors qu'il est sécurisé. Et au moment où cet acte est horodaté[11], il acquiert la même force qu'un acte légalisé ayant une date certaine.

Cependant, pour avoir la qualité d'une signature électronique sécurisée, il suffit de garantir (Article 417-3, Loi n°53-05): Sa création, l'identité du signataire et l'intégrité de l'acte juridique ;

Par conséquent, le dispositif précité doit garantir (Article 9, Loi n°53-05) ; moyennant les techniques et procédures appropriées ; que les données utilisées pour la création de la signature ne peuvent être établies qu'une seule fois tout en assurant sa confidentialité, qu'elles ne peuvent pas être trouvées par déduction, que la protection de la signature électronique contre toute manipulation est assurée, et en dernier lieu, que les dites données sont suffisamment protégées contre toute utilisation illégale.

La deuxième exigence à garantir, c'est que ce dispositif ne provoque aucune modification ou altération du contenu de l'acte objet de la signature.

[9] Promulguée et publiée au Bulletin Officiel n° 5584 du Décembre 2007, à la suite du Dahir n°1-07-129 du 19 Kaada 1428 (30 novembre 2007).
[10] Malgré l'importance de l'écrit en matière de preuve, ce dernier n'a fait l'objet d'aucune définition de la part du législateur. Cité dans (Mohamed Diyaâ TOUMLILIT, 2008).
[11] L'horodatage est l'instrument de traçabilité le plus adapté aux échanges électroniques. Il consiste à la validation de la date et de l'heure des opérations électroniques en temps réel ; par un prestataire de services d'horodatage électronique ; moyennant des techniques cryptographiques.

En outre, pour avoir une identification plus fiable et pour donner plus de crédibilité à la signature électronique, le prestataire de service de certification électronique (PSCE) est en mesure de vérifier la liaison (Article 10, Loi n°53-05) entre les données de vérification de la signature électronique et le signataire en collectant les informations à caractère personnel directement auprès de la personne concernée ou ; via son accord écrit ou électronique ; auprès des tiers (Abderraouf ELLOUMI, 2011).

Toutefois, conformément aux dispositions de l'article 11 de la loi n° 53-05, ce certificat électronique, ne peut être considéré comme sécurisé que s'il est délivré par un prestataire de services de certification électronique agréé par, l'autorité gouvernementale chargée de l'Administration de la défense nationale (Direction générale de la sécurité des systèmes d'information).

L'objectif de la loi 53-05, est d'abord de mettre en place un cadre réglementaire solide capable, de rassurer les différents acteurs qui interviennent dans le domaine du numérique et qui utilisent la signature électronique, ainsi que la certification électronique ; qui fera l'objet du paragraphe suivant ; comme des instruments de preuve. Egalement cette loi permet de résoudre les conflits résultants des transactions électroniques, ce qui contribuera sans aucun doute à la réussite du projet e-gouvernement au Maroc.

3.3 La certification électronique

L'identification a été toujours un aspect très demandé dans les transactions électroniques. De ce fait ; et pour plus de fiabilité et d'efficacité ; le dispositif de création de la signature électronique doit obligatoirement faire l'objet d'une certification électronique auprès d'un tiers de confiance qui atteste de la liaison entre les signataires et les signatures électroniques, donnant ainsi la certitude que la clé publique appartienne réellement à son utilisateur. Ce mécanisme de sécurité, permet d'éviter qu'un pirate puisse pénétrer illégalement dans le réseau Internet pour altérer ou détruire un message électronique, moyennant une fausse clé publique (F. Benseghir, 2011).

Cependant, un certificat électronique, est un document numérique, crée à la demande, qui sert à associer l'identité d'une personne à une clé publique, qui sera utilisée pour décoder des données numériques, ce qui permet d'authentifier de façon unique le propriétaire revendiqué et de vérifier que la personne présentée, est vraiment celui qu'il ou qu'elle prétend être. C'est un

peu comme un passeport ou une carte d'identité virtuelle, qui existe en un seul exemplaire et qui contient des informations personnelles sur son propriétaire.

3.3.1 L'aspect juridique

Ä l'instar de La cryptographie, la loi relative à l'échange électronique de données juridiques n'a pas donné une définition du certificat électronique ni du Prestataire de Service de Certification Electronique. Chose qui nous amène à se référer encore une fois à la législation française ; dont le système juridique est le plus proche de celui du Maroc ; dans l'article premier, alinéa 9 du décret français n°2001-272 du 30 Mars 2001, qui définit le certificat électronique comme étant « *Un document sous forme électronique attestant d'un lien entre les données de vérification de signature électronique et un signataire* ». Dans le même article, à l'alinéa 11, le Prestataire de Service de Certification Electronique est considéré comme « *toute personne qui délivre des certificats électroniques ou fournit d'autres services en matière de signature électronique* ».

En effet, d'après l'article 16 de la même loi, l'autorité gouvernementale chargée de l'Administration de la défense nationale (Direction générale de la sécurité des systèmes d'information) est chargée de publier au « Bulletin officiel », chaque année, une copie de la décision d'agrément et le registre des prestataires de services de certification électronique agréés. Ces derniers, sont ainsi tenus de respecter tous les engagements (Article 17, Loi n°53-05) prévus par la présente loi.

CONCLUSION

A l'issue de cet article, on peut dire que la réussite du gouvernement électronique est conditionnée par la mise en œuvre d'une politique de sécurité solide et rigoureuse.

Nous avons montré que ; malgré le développement spectaculaire des techniques et des moyens de piratage ; les spécialistes dans le domaine de la sécurité informatique ne cessent de mettre en place les contre-mesures, susceptibles d'installer le climat de confiance et de protéger le monde du numérique contre tous les actes frauduleux. Nous avons vu comment la cryptographie ; qui a été dans un passé récent réservé au domaine militaire ; a

contribué considérablement à la sécurité des échanges électroniques, tout en se basant sur un système de chiffrement efficace, qui permet de bloquer toute sorte de malveillance électronique.

En sus de la cryptographie ; qui n'est qu'un instrument parmi d'autres qui s'intègre dans le schéma globale de la sécurité ; nous avons mis en évidence les aspects techniques et juridiques de la signature électronique, comme étant la solution la plus adaptée à ce type de transaction, marqué par la dématérialisation des documents ainsi que l'éloignement géographique des signataires.

En dernier lieu, nous avons jugé utile d'introduire le concept de la certification électronique, étant donné que le dispositif de création de la signature électronique doit faire l'objet d'un certificat électronique, délivré par un tiers de confiance qui atteste de la liaison entre les signataires et les signatures électroniques. Ainsi, cette certification électronique constitue l'ensemble des procédures permettant la délivrance et la gestion des certificats électroniques, mais également la révocation en cas de défaillance.

Nous pouvons conclure que les concepts de : La PKI, la cryptographie, la signature électronique et la certification électronique, sont étroitement liés et convergent tous dans le même objectif, qui se résume en l'optimisation de la confiance et de la sécurité des échanges électroniques. Chose qui ne peut être envisageable, qu'à travers la mise en place d'une réglementation appropriée, qui constitue le cœur même de tous les procédés de la sécurité numérique.

A travers cet article nous avons essayé d'apporter un éclairage quant à question de la sécurité des échanges électroniques, tout en mettant l'accent sur les principales évolutions techniques en la matière. Egalement, parmi les principaux apports de ce travail, c'est l'étude du cadre juridique régissant les échanges électroniques, qui constitue un facteur clé permettant d'instaurer la confiance chez tous les acteurs qui opèrent dans le domaine du numérique et plus particulièrement le gouvernement électronique. Car plus ils sont conscients des aspects techniques et juridiques, plus la probabilité de la réussite de ce projet sera élevée.

Notons ainsi que la sécurité des échanges électronique est un chantier à peine ouvert, surtout dans le contexte marocain. Ce qui fait que nous avons travaillé sur un sujet peu documenté et un terrain émergent. Pourtant, en plus de la technologie et de la réglementation, nous aurons dû mettre en évidence l'aspect humain, qui constitue un facteur fondamentale pour

relever le défi de la modernisation ; en toute sécurité ; de l'administration publique. Cela nous conduit à poser les questions suivantes :

Est-ce que les fonctionnaires des établissements publics sont suffisamment formés pour garantir la sécurité des échanges électroniques dans le cadre du gouvernement électronique ?

Est-ce que les usagers de ce type de service ; dirigeants d'entreprises et particuliers ; sont suffisamment informés du cadre juridique régissant les échanges électroniques ?

Finalement, plusieurs pistes de recherches s'imposent pour éclairer d'avantage, la connaissance ; aussi bien théorique qu'empirique ; dans un domaine en perpétuel mutation.

Bibliographie

- Abderraouf ELLOUMI. (2011). Le formalisme électronique ». Centre de publication universitaire. P 440.
- Alain Bensoussan. (1998). Le commerce électronique, aspects juridiques ». Edition HERMES. P 42.
- Alain Yger & Jacques-Arthur Weil. (2009). Mathématiques appliquées L3. Edition PEARSON EDUCATION. P 462.
- Bruno Martin. (2004). Codage, Cryptologie et applications. Presses polytechniques et universitaires romandes. Première édition. P 149.
- Cédric Llorens, Laurent Levier, Denis Valois, Benjamain Morin. 2010. TABLEAUX DE BORD de la sécurité réseaux. EYROLLES 3em édition. P 93.
- Driss Kettani & Bernard Moulin. 2014. L'e-gouvernement pour la bonne gouvernance dans les pays en développement : l'expérience du Projet eFez. Edition Presses de l'Université de Laval. P : 59.
- F. Benseghir. (2011). Certification électronique. Future Objectif. P.2.
- F. Benseghir. (2011). Signature électronique. Future Objectif. P. 7-12.
- Fouad BENSEGHIR. (2011). Cryptographie. Future Objectif. .P8.
- Gérard.CORNU. (2007). Vocabulaire juridique. 8em édition. Paris. Presses universitaires de France. P. 866.
- H.Bitan. (2006). Protection et contrefaçon des logiciels et des bases de données. Lamy. p232.
- Henri-François Gautrin, Rapport sur le Gouvernement en ligne. (2004). Vers un Québec branché pour ses citoyens. Bibliothèque nationale du Québec. P 7.
- Jean-François CARPENTIER. (2009) « La sécurité informatique dans la petite entreprise Etat de l'art et Bonnes Pratiques ». Editions ENI. P107.

- M. Jean-Baptiste, (1998). Créer et exploiter un commerce électronique. Litec. P.144
- Magda Fusaro, avec la collaboration de Yves Théorêt et de Claude-Yves Charron. (2002). Commerce électronique : Comment crée la confiance. AGMV. MARQUIS. P46.
- Mohamed Diyaâ TOULMLILT. (2008). Le commerce électronique au Maroc Aspects juridiques .Imprimerie les éditions maghrébines. P 117.
- Mohamed Diyaâ TOUMLILIT. (2008). Le commerce électronique au Maroc ‘’Aspects juridiques’’. Imprimerie les éditions maghrébines. P 443.
- Mohamed HAMMOUMI. (2014). Le e-gouvernement et la réforme de l’administration : quelle articulation ?. Dar Nachr Al Maârifa. P 143.
- Réjean Roy. (2006). Vers une nouvelle relation entre le gouvernement et les citoyens : guide sur le gouvernement électronique. Bibliothèque national du Québec.P12.
- Réjean Roy. (2006). Vers une nouvelle relation entre le gouvernement et les citoyens : guide sur le gouvernement électronique. Bibliothèque national du Québec. P 12 et p17.
- TAMER H. (2019). L’impact de la digitalisation des universités sur la motivation des usagers : Revue de littérature. Revue Internationale des Sciences de Gestion. Numéro 4 : Juillet 2019 / Volume 2 : numéro 3 » p :267.

ARTICLES ET RAPPORTS

- Article 10, Loi n°53-05
- Article 17, Loi n°53-05
- Article 2 de la directive européenne du 13 décembre 1999.
- Article 2.n°2 de la directive 1999 93. Cité in Alain Bensoussan, 1998, « Le commerce électronique, aspects juridiques » Edition HERMES. P125.
- Article 2.n°2 de la directive 1999 93. Cité in Alain Bensoussan. Edition HERMES. P43.
- Article 417-1, Loi n° 53-05 relative à l’échange électronique de données juridiques.
- Article 417-2, Loi n° 53-05 relative à l’échange électronique de données juridiques.
- Article 417-3, Loi n°53-05
- Article 6, Loi n°53-05
- Article 9, Loi n°53-05
- Rapport OCDE, 1998 «Un monde sans frontières : Concrétiser le potentiel du commerce électronique mondial», p.13.

Sites :

- http://www.worldbank.org/en/topic/ict/brief/e-government, (Date de consultation : Mai 2015).
- http://www.ietf.org (Date de consultation : Juin 2016)