Dahir n° 1-07-129 du 19 kaada 1428 (30 novembre 2007) portant promulgation de la loi n° 53-05 relative à l'échange électronique de données juridiques.

LOUANGE A DIEU SEUL !

(Grand Sceau de Sa Majesté Mohammed VI)

Que l'on sache par les présentes – puisse Dieu en élever et en fortifier la teneur !

Que Notre Majesté Chérifienne,

Vu la Constitution, notamment ses articles 26 et 58,

A DÉCIDÉ CE QUI SUIT :

Est promulguée et sera publiée au *Bulletin officiel*, à la suite du présent dahir, la loi n° 53-05 relative à l'échange électronique de données juridiques, telle qu'adoptée par la Chambre des représentants et la Chambre des conseillers.

Fait à Guelmim , le 19 kaada 1428 (30 novembre 2007).

Pour contreseing :

Le Premier ministre,

ABBAS EL FASSI.

*

* *

Loi n° 53-05
relative à l'échange électronique
de données juridiques

CHAPITRE PRELIMINAIRE

ARTICLE PREMIER

La présente loi fixe le régime applicable aux données juridiques échangées par voie électronique, à l'équivalence des documents établis sur papier et sur support électronique et à la signature électronique.

Elle détermine également le cadre juridique applicable aux opérations effectuées par les prestataires de service de certification électronique, ainsi que les règles à respecter par ces derniers et les titulaires des certificats électroniques délivrés.

TITRE PREMIER

DE LA VALIDITE DES ACTES ETABLIS SOUS FORME ELECTRONIQUE OU TRANSMIS PAR VOIE ELECTRONIQUE

Article 2

Le chapitre premier du titre premier du livre premier du dahir formant code des obligations et des contrats est complété par un article 2-1 ainsi conçu :

« *Article 2-1.* – Lorsqu'un écrit est exigé pour la validité « d'un acte juridique, il peut être établi et conservé sous forme « électronique dans les conditions prévues aux articles 417-1 « et 417-2 ci-dessous.

« Lorsqu'une mention écrite est exigée de la main même de « celui qui s'oblige, ce dernier peut l'apposer sous forme « électronique, si les conditions de cette apposition sont de nature « à garantir qu'elle ne peut être effectuée que par lui-même.

« Toutefois, les actes relatifs à l'application des « dispositions du code de la famille et les actes sous seing privé « relatifs à des sûretés personnelles ou réelles, de nature civile ou « commerciale, ne sont pas soumis aux dispositions de la « présente loi, à l'exception des actes établis par une personne « pour les besoins de sa profession. »

Article 3

Le titre premier du livre premier du dahir formant Code des obligations et des contrats est complété par un chapitre premier *bis* conçu ainsi qu'il suit :

***« Chapitre premier* bis**

« Du contrat conclu sous forme électronique
« ou transmis par voie électronique.

« Section I. – **Dispositions générales**

« Article 65-1. – Sous réserve des dispositions du présent « chapitre, la validité du contrat conclu sous forme électronique « ou transmis par voie électronique est régie par les dispositions « du chapitre premier du présent titre.

« *Article 65-2.* – Les dispositions des articles 23 à 30 et 32 « ci-dessus ne sont pas applicables au présent chapitre.

« Section II. **– De l'offre**

« *Article 65-3.* – La voie électronique peut être utilisée pour « mettre à disposition du public des offres contractuelles ou des « informations sur des biens ou services en vue de la conclusion « d'un contrat.

« Les informations qui sont demandées en vue de la « conclusion d'un contrat ou celles qui sont adressées au cours de « son exécution peuvent être transmises par courrier électronique « si leur destinataire a accepté expressément l'usage de ce moyen.

« Les informations destinées à des professionnels peuvent « leur être transmises par courrier électronique, dès lors qu'ils ont « communiqué leur adresse électronique.

« Lorsque les informations doivent être portées sur un « formulaire, celui-ci est mis, par voie électronique, à la « disposition de la personne qui doit le remplir.

« *Article 65-4.* – Quiconque propose, à titre professionnel, « par voie électronique, la fourniture de biens, la prestation « de services ou la cession de fonds de commerce ou l'un de « leurs éléments met à disposition du public les conditions « contractuelles applicables d'une manière permettant leur « conservation et leur reproduction.

« Sans préjudice des conditions de validité prévues dans « l'offre, son auteur reste engagé par celle-ci, soit pendant la « durée précisée dans ladite offre, soit, à défaut, tant qu'elle est « accessible par voie électronique de son fait.

« L'offre comporte, en outre :

« 1 - les principales caractéristiques du bien, du service « proposé ou du fonds de commerce concerné ou l'un de ses « éléments ;

« 2 - les conditions de vente du bien ou du service ou celles de « cession du fonds de commerce ou l'un de ses éléments ;

« 3 - les différentes étapes à suive pour conclure le contrat « par voie électronique et notamment les modalités selon « lesquelles les parties se libèrent de leurs obligations réciproques ;

« 4 - les moyens techniques permettant au futur utilisateur, « avant la conclusion du contrat, d'identifier les erreurs « commises dans la saisie des données et de les corriger ;

« 5 - les langues proposées pour la conclusion du contrat ;

« 6 - les modalités d'archivage du contrat par l'auteur de « l'offre et les conditions d'accès au contrat archivé, si la nature « ou l'objet du contrat le justifie ;

« 7- les moyens de consulter, par voie électronique, les « règles professionnelles et commerciales auxquelles l'auteur de « l'offre entend, le cas échéant, se soumettre.

« Toute proposition qui ne contient pas l'ensemble des « énonciations indiquées au présent article ne peut être « considérée comme une offre et demeure une simple publicité « et n'engage pas son auteur.

« Section III . – **De la conclusion d'un contrat sous forme électronique**

« *Article 65-5.* – Pour que le contrat soit valablement « conclu, le destinataire de l'offre doit avoir eu la possibilité de « vérifier le détail de son ordre et son prix total et de corriger « d'éventuelles erreurs, et ce avant de confirmer ledit ordre pour « exprimer son acceptation.

« L'auteur de l'offre doit accuser réception, sans délai « injustifié et par voie électronique, de l'acceptation de l'offre qui « lui a été adressée.

« Le destinataire est irrévocablement lié à l'offre dès sa « réception.

« L'acceptation de l'offre, sa confirmation et l'accusé de « réception sont réputés reçus lorsque les parties auxquelles ils « sont adressés peuvent y avoir accès.

« Section IV. – **Dispositions diverses**

« Articles 65-6. - L'exigence d'un formulaire détachable est « satisfaite lorsque, par un procédé électronique spécifique, il est « permis d'accéder au formulaire, de le remplir et de le renvoyer « par la même voie.

« Article 65-7. – Lorsqu'une pluralité d'originaux est « exigée, cette exigence est réputée satisfaite, pour les actes « établis sous forme électronique, si l'acte concerné est établi et « conservé conformément aux dispositions des articles 417-1, 417-2 « et 417-3 ci-dessous et que le procédé utilisé permet à chacune des « parties intéressées de disposer d'un exemplaire ou d'y avoir « accès. »

Article 4

La section II du chapitre premier, du titre septième, du livre premier du dahir formant Code des obligations et des contrats est complétée par les articles 417-1, 417-2 et 417-3 ainsi conçus :

« Section II**. – De la preuve littérale**

« *Article 417-1.* – L'écrit sur support électronique a la « même force probante que l'écrit sur support papier.

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

« *Article 417-2.* – La signature nécessaire à la perfection « d'un acte juridique identifie celui qui l'appose et exprime son « consentement aux obligations qui découlent de cet acte.

« Lorsque la signature est apposée par devant un officier « public habilité à certifier, elle confère l'authenticité à l'acte.

« Lorsqu'elle est électronique, il convient d'utiliser un « procédé fiable d'identification garantissant son lien avec l'acte « auquel elle s'attache.

« Article 417-3. – La fiabilité d'un procédé de signature « électronique est présumée, jusqu'à preuve contraire, lorsque ce « procédé met en œuvre une signature électronique sécurisée.

« Une signature électronique est considérée comme « sécurisée lorsqu'elle est créée, l'identité du signataire assurée « et l'intégrité de l'acte juridique garantie, conformément à la « législation et la réglementation en vigueur en la matière.

« Tout acte sur lequel est apposée une signature électronique « sécurisée et qui est horodaté a la même force probante que l'acte « dont la signature est légalisée et de date certaine. »

Article 5

Les dispositions des articles 417, 425, 426, 440 et 443 du dahir formant Code des obligations et des contrats sont modifiées et complétées ainsi qu'il suit :

« Article 417. – La preuve littérale ……. « sous seing privé.

« Elle peut résulter également……et « documents privés ou de tous autres signes ou symboles dotés « d'une signification intelligible, quels que soient leur support et « leurs modalités de transmission.

« Lorsque la loi n'a pas fixé d'autres règles et, à défaut de « convention valable entre les parties, la juridiction statue sur les « conflits de preuve littérale par tous moyens, quel que soit le « support utilisé.

« Article 425. – Les actes sous seings privés……. « ……au nom de leur débiteur.

« Ils n'ont de date contre les tiers que :

« 1°……

« …… ……

« 6°- lorsque la date résulte de la signature électronique « sécurisée authentifiant l'acte et son signataire conformément à « la législation en vigueur.

« Les ayants cause et successeurs…… au nom de leur « débiteur.

« *Article 426.* – L'acte……..par elle.

« La signature ……..au bas de « l'acte ; un timbre ou cachet ne peuvent y suppléer et sont « considérés comme non apposés.

« Lorsqu'il s'agit d'une signature électronique sécurisée, il « convient de l'introduire dans l'acte, dans les conditions prévues « par la législation et la réglementation applicables en la matière.

« Article 440. – Les copies ……originaux.

« Les copies d'un acte juridique établi sous forme « électronique sont admises en preuve dès lors que l'acte répond « aux conditions visées aux articles 417-1 et 417-2 et que le « procédé de conservation de l'acte permet à chaque partie de « disposer d'un exemplaire ou d'y avoir accès.

« *Article 443.* – Les conventions et autres faits juridiques.... « ….....…….....et excédant « la somme ou la valeur de dix mille dirhams ne peuvent être « prouvés par témoins. Il doit en être passé acte authentique ou « sous seing privé, éventuellement établi sous forme électronique « ou transmis par voie électronique. »

TITRE II

DU REGIME JURIDIQUE APPLICABLE A LA SIGNATURE ELECTRONIQUE SECURISEE, A LA CRYPTOGRAPHIE ET A LA CERTIFICATION ELECTRONIQUE

Chapitre premier

De la signature électronique sécurisée et de la cryptographie

Section 1. – **De la signature électronique sécurisée**

Article 6

La signature électronique sécurisée, prévue par les dispositions de l'article 417-3 du dahir formant Code des obligations et des contrats, doit satisfaire aux conditions suivantes :

– être propre au signataire ;

– être créée par des moyens que le signataire puisse garder sous son contrôle exclusif ;

– garantir avec l'acte auquel elle s'attache un lien tel que toute modification ultérieure dudit acte soit détectable.

Elle doit être produite par un dispositif de création de signature électronique, attesté par un certificat de conformité.

Les données de vérification de la signature électronique sécurisée doivent être mentionnées dans le certificat électronique sécurisé prévu à l'article 10 de la présente loi.

Article 7

Le signataire, visé à l'article 6 ci-dessus, est la personne physique, agissant pour son propre compte ou pour celui de la personne physique ou morale qu'elle représente, qui met en œuvre un dispositif de création de signature électronique.

Article 8

Le dispositif de création de signature électronique consiste en un matériel et/ou un logiciel destiné(s) à mettre en application les données de création de signature électronique, comportant les éléments distinctifs caractérisant le signataire, tels que la clé cryptographique privée, utilisée par lui pour créer une signature électronique.

Article 9

Le certificat de conformité, prévu à l'alinéa 2 de l'article 6 ci-dessus, est délivré par l'autorité nationale d'agrément et de surveillance de la certification électronique, prévue à l'article 15 de la présente loi, lorsque le dispositif de création de signature électronique satisfait aux exigences ci-après :

1) garantir par des moyens techniques et des procédures appropriés que les données de création de signature électronique :

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

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

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

2) n'entraîner aucune altération ou modification du contenu de l'acte à signer et ne pas faire obstacle à ce que le signataire en ait une connaissance exacte avant de le signer.

Article 10

Le lien entre les données de vérification de signature électronique et le signataire est attesté par un certificat électronique, qui consiste en un document établi sous forme électronique.

Ce certificat électronique peut être simple ou sécurisé.

Article 11

Le certificat électronique, prévu à l'article 10 ci-dessus, est un certificat électronique sécurisé, lorsqu'il est délivré par un prestataire de services de certification électronique agréé par l'Autorité nationale d'agrément et de surveillance de la certification électronique et qu'il comporte les données ci-après :

a) une mention indiquant que ce certificat est délivré à titre de certificat électronique sécurisé ;

b) l'identité du prestataire de services de certification électronique, ainsi que la dénomination de l'Etat dans lequel il est établi ;

c) le nom du signataire ou un pseudonyme lorsqu'il existe, celui-ci devant alors être identifié comme tel, titulaire du certificat électronique sécurisé ;

d) le cas échéant, l'indication de la qualité du signataire en fonction de l'usage auquel le certificat électronique est destiné ;

e) les données qui permettent la vérification de la signature électronique sécurisée ;

f) l'identification du début et de la fin de la durée de validité du certificat électronique ;

g) le code d'identité du certificat électronique ;

h) la signature électronique sécurisée du prestataire de services de certification électronique qui délivre le certificat électronique ;

i) le cas échéant, les conditions d'utilisation du certificat électronique, notamment le montant maximum des transactions pour lesquelles ce certificat peut être utilisé.

Section 2. – **De la cryptographie**

Article 12

Les moyens de cryptographie ont notamment pour objet de garantir la sécurité de l'échange et/ou du stockage de données juridiques par voie électronique, de manière qui permet d'assurer leur confidentialité, leur authentification et le contrôle de leur intégrité.

On entend par moyen de cryptographie 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.

On entend par prestation de cryptographie toute opération visant l'utilisation, pour le compte d'autrui, de moyens de cryptographie.

Article 13

Afin de prévenir l'usage à des fins illégales et pour préserver les intérêts de la défense nationale et de la sécurité intérieure ou extérieure de l'Etat, l'importation, l'exportation, la fourniture, l'exploitation ou l'utilisation de moyens ou de prestations de cryptographie sont soumises :

a) à déclaration préalable, lorsque ce moyen ou cette prestation a pour unique objet d'authentifier une transmission ou d'assurer l'intégralité des données transmises par voie électronique;

b) à autorisation préalable de l'administration, lorsqu'il s'agit d'un autre objet que celui visé au paragraphe *a)* ci-dessus.

Le gouvernement fixe :

1. les moyens ou prestations répondant aux critères visés au paragraphe *a)* ci-dessus ;

2. les modalités selon lesquelles est souscrite la déclaration et délivrée l'autorisation, visées à l'alinéa précédent.

Le gouvernement peut prévoir un régime simplifié de déclaration ou d'autorisation ou la dispense de la déclaration ou de l'autorisation pour certains types de moyens ou de prestations de cryptographie ou pour certaines catégories d'utilisateurs.

Article 14

La fourniture de moyens ou de prestations de cryptographie soumises à autorisation est réservée aux prestataires de services de certification électronique, agréés à cette fin conformément aux dispositions de l'article 21 de la présente loi. A défaut, les personnes qui entendent fournir des prestations de cryptographie soumises à autorisation, doivent être agréées à cette fin par l'administration.

Chapitre II

De la certification de la signature électronique

Secion 1. – **De l'Autorité nationale d'agrément et de surveillance de la certification électronique**

Article 15

L'Autorité nationale d'agrément et de surveillance de la certification électronique, désignée ci-après par l'autorité nationale, a pour mission, outre les compétences qui lui sont dévolues en vertu d'autres articles de la présente loi :

– de proposer au gouvernement les normes du système d'agrément et de prendre les mesures nécessaires à sa mise en œuvre ;

– d'agréer les prestataires de services de certification électronique et de contrôler leurs activités.

Article 16

L'autorité nationale publie un extrait de la décision d'agrément au « Bulletin officiel » et tient un registre des prestataires de services de certification électronique agréés, qui fait l'objet, à la fin de chaque année, d'une publication au « Bulletin officiel ».

Article 17

L'autorité nationale s'assure du respect, par les prestataires de services de certification électronique délivrant des certificats électroniques sécurisés, des engagements prévus par les dispositions de la présente loi et des textes pris pour son application.

Article 18

L'autorité nationale peut, soit d'office, soit à la demande de toute personne intéressée, vérifier ou faire vérifier la conformité des activités d'un prestataire de services de certification électronique délivrant des certificats électroniques sécurisés aux dispositions de la présente loi ou des textes pris pour son application. Elle peut avoir recours à des experts pour la réalisation de ses missions de contrôle.

Article 19

Dans l'accomplissement de leur mission de vérification, visée à l'article 18 ci-dessus, les agents de l'autorité nationale, ainsi que les experts désignés par elle ont, sur justification de leurs qualités, le droit d'accéder à tout établissement et de prendre connaissance de tous mécanismes et moyens techniques relatifs aux services de certification électronique sécurisée qu'ils estimeront utiles ou nécessaires à l'accomplissement de leur mission.

Section 2. – **Des prestataires de services de certification électronique**

Article 20

Seuls les prestataires de service de certification électronique agréés dans les conditions fixées par la présente loi et les textes pris pour son application peuvent émettre et délivrer les certificats électroniques sécurisés et gérer les services qui y sont afférents.

Article 21

Pour pouvoir être agréé en qualité de prestataire de services de certification électronique, le demandeur de l'agrément doit être constitué sous forme de société ayant son siège social sur le territoire du Royaume et :

1 – remplir des conditions techniques garantissant :

a – la fiabilité des services de certification électronique qu'il fournit, notamment la sécurité technique et cryptographique des fonctions qu'assurent les systèmes et les moyens cryptographiques qu'il propose ;

b – la confidentialité des données de création de signature électronique qu'il fournit au signataire ;

c – la disponibilité d'un personnel ayant les qualifications nécessaires à la fourniture de services de certification électronique ;

d – la possibilité, pour la personne à qui le certificat électronique a été délivré, de révoquer, sans délai et avec certitude, ce certificat ;

e – la détermination, avec précision, de la date et l'heure de délivrance et de révocation d'un certificat électronique ;

f – l'existence d'un système de sécurité propre à prévenir la falsification des certificats électroniques et à s'assurer que les données de création de la signature électronique correspondent aux données de sa vérification lorsque sont fournies à la fois des données de création et des données de vérification de la signature électronique.

2 – être en mesure de conserver, éventuellement sous forme électronique, toutes les informations relatives au certificat électronique qui pourraient s'avérer nécessaires pour faire la preuve en justice de la certification électronique, sous réserve que les systèmes de conservation des certificats électronique garantissent que :

a – l'introduction et la modification des données sont réservées aux seules personnes autorisées à cet effet par le prestataire ;

b – l'accès du public à un certificat électronique ne peut avoir lieu sans le consentement préalable du titulaire du certificat ;

c – toute modification de nature à compromettre la sécurité du système peut être détectée ;

3 – s'engager à :

3-1 – vérifier, d'une part, l'identité de la personne à laquelle un certificat électronique est délivré, en exigeant d'elle la présentation d'un document officiel d'identité pour s'assurer que la personne a la capacité légale de s'engager, d'autre part, la qualité dont cette personne se prévaut et conserver les caractéristiques et références des documents présentés pour justifier de cette identité et de cette qualité ;

3-2 – s'assurer au moment de la délivrance du certificat électronique :

a) que les informations qu'il contient sont exactes ;

b) que le signataire qui y est identifié détient les données de création de signature électronique correspondant aux données de vérification de signature électronique contenues dans le certificat ;

3-3 – informer, par écrit, la personne demandant la délivrance d'un certificat électronique préalablement à la conclusion d'un contrat de prestation de services de certification électronique :

a) des modalités et des conditions d'utilisation du certificat ;

b) des modalités de contestation et de règlement des litiges ;

3-4 – fournir aux personnes qui se fondent sur un certificat électronique les éléments de l'information prévue au point précédent qui leur sont utiles ;

3-5 – informer les titulaires du certificat sécurisé au moins soixante (60) jours avant la date d'expiration de la validité de leur certificat, de l'échéance de celui-ci et les inviter à le renouveler ou à demander sa révocation ;

3-6 – souscrire une assurance afin de couvrir les dommages résultant de leurs fautes professionnelles ;

3-7 – révoquer un certificat électronique, lorsque :

a) il s'avère qu'il a été délivré sur la base d'informations erronées ou falsifiées, que les informations contenues dans ledit certificat ne sont plus conformes à la réalité ou que la confidentialité des données afférentes à la création de signature a été violée ;

b) les autorités judiciaires lui enjoignent d'informer immédiatement les titulaires des certificats sécurisés délivrés par lui de leur non conformité aux dispositions de la présente loi et des textes pris pour son application.

Article 22

Par dérogation aux dispositions des articles 20 et 21 ci-dessus :

1 – les certificats délivrés par un prestataire de services de certification électronique, établi dans un pays étranger ont la même valeur juridique que ceux délivrés par un prestataire de certification électronique établi au Maroc si le certificat ou le prestataire de service de certification est reconnu dans le cadre d'un accord multilatéral auquel le Maroc est partie ou d'un accord bilatéral de reconnaissance réciproque entre le Maroc et le pays d'établissement du prestataire ;

2 – peuvent être agréés les prestataires de services de certification électronique dont le siège social est établi à l'étranger, sous réserve que l'Etat sur le territoire duquel ils exercent leur activité ait conclu avec le Royaume du Maroc une convention de reconnaissance réciproque des prestataires de services de certification électronique.

Article 23

Le prestataire de services de certification de signature électronique qui émet, délivre et gère les certificats électroniques informe l'administration à l'avance, dans un délai maximum de deux mois, de sa volonté de mettre fin à ses activités.

Auquel cas, il doit s'assurer de la reprise de celles-ci par un prestataire de service de certification électronique garantissant un même niveau de qualité et de sécurité ou, à défaut, révoque les certificats dans un délai maximum de deux mois après en avoir averti les titulaires.

Il informe également l'autorité nationale, sans délai, de l'arrêt de ses activités en cas de liquidation judiciaire.

Article 24

Les prestataires de services de certification électronique sont astreints, pour eux-mêmes et pour leurs employés, au respect du secret professionnel, sous peine des sanctions prévues par la législation en vigueur.

Ils sont responsables, dans les termes du droit commun, de leur négligence, impéritie ou insuffisance professionnelle tant vis-à-vis de leurs cocontractants que des tiers.

Les prestataires de services de certification électronique doivent conserver les données de création du certificat et sont tenus, sur ordre du Procureur du Roi, de les communiquer aux autorités judiciaires et ce, dans les conditions prévues par la législation en vigueur. Dans ce cas, et nonobstant toute disposition législative contraire, les prestataires de services de certification électronique en informent, sans délai, les utilisateurs concernés.

L'obligation de secret professionnel, visée au premier alinéa ci-dessus, n'est pas applicable :

– à l'égard des autorités administratives, dûment habilitées conformément à la législation en vigueur ;

– à l'égard des agents et experts de l'Autorité nationale et agents et officiers visés à l'article 41 ci-dessous dans l'exercice des pouvoirs prévus aux articles 19 et 41 de la présente loi ;

– si le titulaire de la signature électronique a consenti à la publication ou à la communication des renseignements fournis au prestataire de services de certification électronique.

Section 3. – **De l'obligation du titulaire de certificat électronique**

Article 25

Dès le moment de la création des données afférentes à la création de signature, le titulaire du certificat électronique est seul responsable de la confidentialité et de l'intégrité des données afférentes à la création de signature qu'il utilise. Toute utilisation de celles-ci est réputée, sauf preuve contraire, être son fait.

Article 26

Le titulaire du certificat électronique est tenu, dans les meilleurs délais, de notifier au prestataire de services de certification toute modification des informations contenues dans celui-ci.

Article 27

En cas de doute quant au maintien de la confidentialité des données afférentes à la création de signature ou de perte de conformité à la réalité des informations contenues dans le certificat, son titulaire est tenu de le faire révoquer immédiatement conformément aux dispositions de l'article 21 de la présente loi.

Article 28

Lorsqu'un certificat électronique est arrivé à échéance ou a été révoqué, son titulaire ne peut plus utiliser les données afférentes à la création de signature correspondantes pour signer ou faire certifier ces données par un autre prestataire de services de certification électronique.

Chapitre III

Des sanctions, des mesures préventives et de la constatation des infractions

Article 29

Est puni d'une amende de 10.000 à 100.000 DH et d'un emprisonnement de trois mois à un an, quiconque aura fourni des prestations de services de certification électronique sécurisée sans être agréé dans les conditions prévues à l'article 21 ci-dessus ou aura continué son activité malgré le retrait de son agrément ou aura émis, délivré ou géré des certificats électroniques sécurisés en violation des dispositions de l'article 20 ci-dessus.

Article 30

Sans préjudice de dispositions pénales plus sévères, est puni d'un emprisonnement d'un mois à six mois et d'une amende de 20.000 DH à 50.000 DH quiconque divulgue, incite ou participe à divulguer les informations qui lui sont confiées dans le cadre de l'exercice de ses activités ou fonctions.

Toutefois, les dispositions du présent article ne sont pas applicables à la publication ou à la communication autorisée, par écrit sur support papier ou par voie électronique, par le titulaire du certificat électronique ou à la publication ou à la communication autorisée par la législation en vigueur.

Article 31

Sans préjudice de dispositions pénales plus sévères, est puni d'un emprisonnement d'un an à cinq ans et d'une amende de 100.000 DH à 500.000 DH, quiconque a fait sciemment de fausses déclarations ou remis de faux documents au prestataire de services de certification électronique.

Article 32

Est puni d'un an d'emprisonnement et d'une amende de 100.000 DH, quiconque aura importé, exporté, fourni, exploité ou utilisé l'un des moyens ou une prestation de cryptographie sans la déclaration ou l'autorisation exigée aux articles 13 et 14 ci-dessus.

Le tribunal pourra, en outre, prononcer la confiscation des moyens de cryptographie concernés.

Article 33

Lorsqu'un moyen de cryptographie, au sens de l'article 14 ci-dessus, a été utilisé pour préparer ou commettre un crime ou un délit ou pour en faciliter la préparation ou la commission, le maximum de la peine privative de liberté encourue est relevé ainsi qu'il suit :

– il est porté à la réclusion criminelle à perpétuité, lorsque l'infraction est punie de trente ans de réclusion criminelle ;

– il est porté à trente ans de réclusion criminelle, lorsque l'infraction est punie de vingt ans de réclusion criminelle ;

– il est porté à vingt ans de réclusion criminelle, lorsque l'infraction est punie de quinze ans de réclusion criminelle ;

– il est porté à quinze ans de réclusion criminelle, lorsque l'infraction est punie de dix ans de réclusion criminelle ;

– il est porté à dix ans de réclusion criminelle, lorsque l'infraction est punie de cinq ans de réclusion criminelle ;

– il est porté au double, lorsque l'infraction est punie de trois ans d'emprisonnement au plus.

Toutefois, les dispositions du présent article ne sont pas applicables à l'auteur ou au complice de l'infraction qui, à la demande des autorités judiciaires ou administratives, leur a remis la version en clair des messages chiffrés, ainsi que les conventions secrètes nécessaires au déchiffrement.

Article 34

Sauf à démontrer qu'elles n'ont commis aucune faute intentionnelle ou négligence, les personnes fournissant des prestations de cryptographie à des fins de confidentialité sont responsables, au titre de ces prestations, du préjudice causé aux personnes leur confiant la gestion de leurs conventions secrètes en cas d'atteintes à l'intégrité, à la confidentialité ou à la disponibilité des données transformées à l'aide de ces conventions.

Article 35

Est puni d'un emprisonnement d'un an à cinq ans et d'une amende de 10.000 DH à 100.000 DH, quiconque utilise, de manière illégale, les éléments de création de signature personnels relatifs à la signature d'autrui.

Article 36

Est puni d'une amende de 10.000 DH à 100.000 DH et d'un emprisonnement de trois mois à six mois, tout prestataire de services de certification électronique qui ne respecte pas l'obligation d'information de l'autorité nationale prévue à l'article 23 ci-dessus.

En outre, le coupable peut être frappé, pour une durée de cinq ans, de l'interdiction de l'exercice de toute activité de prestation de services de certification électronique.

Article 37

Est puni d'une amende de 10.000 DH à 100.000 DH et d'un emprisonnement de six mois à deux ans, tout titulaire d'un certificat électronique qui continue à utiliser ledit certificat arrivé à échéance ou révoqué.

Article 38

Sans préjudice de dispositions pénales plus sévères, est puni d'une amende de 50.000 à 500.000 DH quiconque utilise indûment, une raison sociale, une publicité et, de manière générale, toute expression faisant croire qu'il est agréé conformément aux dispositions de l'article 21 ci-dessus.

Article 39

Lorsque, sur le rapport de ses agents ou d'experts, l'autorité nationale constate que le prestataire de services de certification électronique délivrant des certificats sécurisés ne répond plus à l'une des conditions prévues à l'article 21 ci-dessus ou que ses activités ne sont pas conformes aux dispositions de la présente loi ou des règlements pris pour son application, elle l'invite à se conformer auxdites conditions ou dispositions, dans le délai qu'elle détermine.

Passé ce délai, si le prestataire ne s'y est pas conformé, l'autorité nationale retire l'agrément délivré, procède à la radiation du prestataire du registre des prestataires agréés et à la publication au « Bulletin officiel » d'un extrait de la décision de retrait de l'agrément.

Lorsque les activités du contrevenant sont de nature à porter atteinte aux exigences de la défense nationale ou de la sécurité intérieure ou extérieure de l'Etat, l'autorité nationale est habilitée à prendre toutes mesures conservatoires nécessaires pour faire cesser lesdites activités, sans préjudice des poursuites pénales qu'elles appellent.

Article 40

Lorsque l'auteur de l'infraction est une personne morale, et sans préjudice des peines qui peuvent être appliquées à ses dirigeants, auteurs de l'une des infractions prévues ci-dessus, les amendes prévues par le présent chapitre sont portées au double.

En outre, la personne morale peut être punie de l'une des peines suivantes :

– la confiscation partielle de ses biens ;

– la confiscation prévue à l'article 89 du code pénal ;

– la fermeture de ou des établissements de la personne morale ayant servi à commettre les infractions.

Article 41

Outre les officiers et agents de police judiciaire et les agents des douanes dans leur domaine de compétence, les agents de l'autorité nationale habilités à cet effet et assermentés dans les formes du droit commun peuvent rechercher et constater, par procès-verbal, les infractions aux dispositions de la présente loi et des textes pris pour son application. Leurs procès-verbaux sont transmis dans les cinq jours au Procureur du Roi.

Les agents et officiers, visés à l'alinéa précédent, peuvent accéder aux locaux, terrains ou moyens de transport à usage professionnel, demander la communication de tous documents professionnels et en prendre copie, recueillir, sur convocation ou sur place, les renseignements et justifications.

Ils peuvent procéder, dans ces mêmes lieux, à la saisie des moyens visés à l'article 12 ci-dessus sur ordre du Procureur du Roi ou du juge d'instruction.

Les moyens saisis figurent au procès-verbal dressé sur les lieux. Les originaux du procès-verbal et de l'inventaire sont transmis à l'autorité judiciaire qui a ordonné la saisie.

Chapitre VI

Dispositions finales

Article 42

Les conditions et modalités d'application des dispositions de la présente loi aux droits réels sont fixées par décret.

Article 43

Par dérogation aux dispositions du premier alinéa de l'article 21 ci-dessus, le gouvernement peut, sur proposition de l'autorité nationale visée à l'article 15, et sous réserve de l'intérêt du service public, agréer les personnes morales de droit public pour émettre et délivrer des certificats électroniques sécurisés et gérer les services qui y sont afférents, dans les conditions fixées par la présente loi et les textes pris pour son application.