

LOI N° 2008 - 41 DU 20 AOUT 2008 SUR LA CRYPTOLOGIE

EXPOSÉ DES MOTIFS

Le développement de la société de l'information ne peut se réaliser sans la confiance des utilisateurs. Pour y parvenir, une maîtrise globale de la sécurité des systèmes d'information et des données est indispensable.

La cryptologie est à l'heure actuelle la solution technique incontournable pour protéger les échanges et les systèmes d'information sur les nouvelles technologies contre d'éventuelles violations de leur intégrité. A cet effet, elle vise à garantir la confidentialité des systèmes, des données stockées, échangées ou circulant sur l'Internet, sur l'Intranet voire sur un simple réseau privé.

Au Sénégal, la cryptologie est utilisée dans plusieurs secteurs notamment l'administration, les télécommunications et l'informatique, plus précisément au niveau des centres d'appels, des sociétés de transfert d'argent, ainsi que pour les paiements électroniques.

Sur le plan juridique, l'article 37 de la loi n°2001-15 du 27 décembre 2001 portant Code des télécommunications, qui prévoit le régime de la cryptologie, ne prend pas en compte certains aspects fondamentaux notamment, la fourniture, le transfert et les conditions d'homologation liées à l'importation ou l'exportation de moyens ou de prestations de cryptologie.

Par ailleurs, la portée de l'article 67 du même Code, qui prévoit les peines applicables en cas de violation des règles sur la cryptologie est très restrictive car les sanctions envisagées ne portent que sur les exportations ou les importations de moyens de cryptologie sans autorisation.

C'est pourquoi, face à ces insuffisances, il est prévu, d'une part, l'abrogation de ces dispositions et d'autre part, la mise en place d'une loi portant sur la cryptologie.

L'objectif de ce projet de loi, qui comprend huit chapitres, est donc de définir les conditions générales d'utilisation, de fourniture, d'importation et d'exportation des moyens et des prestations de cryptologie.

Telle est l'économie du présent projet de loi.

L'assemblée nationale a adopté, en sa séance du lundi 28 juillet 2008 ;

Le Sénat a adopté, en sa séance du lundi 11 août 2008 ;

Le Président de la République promulgue la loi dont la teneur suit :

CHAPITRE PREMIER : DISPOSITIONS GENERALES

Article Premier :

La présente loi a pour objet de fixer les règles applicables aux moyens, modalités et systèmes de cryptologie.

La cryptologie, composée de la cryptographie et de la cryptanalyse, tend à assurer la protection et la sécurité des informations notamment pour la confidentialité, l'authentification, l'intégrité et la non répudiation des données transmises.

Article 2 :

Les dispositions de la présente loi ne s'appliquent pas aux moyens de cryptologie utilisés par les missions diplomatiques et consulaires visées par la Convention de Vienne sur les relations diplomatiques ainsi que ceux relatifs à la sécurité de l'Etat.

Article 3 :

Au sens de la présente loi, les expressions et termes ci-dessous sont définis comme suit :

1. **Accès dérobé** : mécanisme permettant de dissimuler un accès à des données ou à un système informatique sans l'autorisation de l'utilisateur légitime ;
2. **Activité de cryptologie** : activité ayant pour but la production, l'utilisation, la fourniture, l'importation ou l'exportation des moyens de cryptologie ;
3. **Agrément d'un produit ou d'un système** : reconnaissance formelle que le produit ou le système évalué peut protéger jusqu'à un niveau spécifié par un organisme agréé conformément à l'article 16 de la présente loi ;
4. **Algorithme cryptologique** : procédé permettant, avec l'aide d'une clé, de chiffrer et de déchiffrer des messages ou des documents ;
5. **Authentification** : procédure dont le but est de s'assurer de l'identité d'une personne pour contrôler l'accès à un logiciel ou à un système d'information ou de vérifier l'origine d'une information ;
6. **Bi-clé** : couple clé publique/clé privée utilisé dans des algorithmes de cryptographie asymétrique ;
7. **Clé** : ensemble de caractères, de chiffres, avec une longueur spécifiée, destiné à chiffrer, à déchiffrer, à signer et à authentifier une signature. Une fois générée et

chiffrée avec un système d'identification, la clé est unique dans le système d'information et appartient exclusivement à une personne désignée ;

8. **Chiffrement** : opération qui consiste à rendre des données numériques inintelligibles à des tiers en employant la cryptographie définie au point 18 du présent article ;
9. **Chiffrement par bloc** : chiffrement opérant sur des blocs d'informations claires et sur des informations chiffrées ;
10. **Chiffrer** : action visant à assurer la confidentialité d'une information, à l'aide de codes secrets, pour la rendre inintelligible à des tiers, en utilisant des mécanismes offerts en cryptographie ;
11. **Clé de chiffrement** : série de symboles commandant les opérations de chiffrement et de déchiffrement ;
12. **Clé privée** : clé non publiable utilisée en cryptographie asymétrique et associée à une clé publique pour former une bi-clé définie au point 6 du présent article ;
13. **Clé publique** : clé utilisée en cryptographie asymétrique publiable et nécessaire à la mise en œuvre d'un moyen ou d'une prestation de cryptologie pour des opérations de chiffrement et de déchiffrement ;
14. **Clé secrète** : clé non publiée mais utilisée uniquement en cryptographie symétrique et nécessaire à la mise en œuvre d'un moyen ou d'une prestation de cryptologie pour des opérations de chiffrement ou de déchiffrement.
15. **Conventions secrètes** : accord de volontés portant sur des clés non publiées nécessaires à la mise en oeuvre d'un moyen ou d'une prestation de cryptologie pour les opérations de chiffrement ou de déchiffrement ;
16. **Cryptanalyse** : opération qui vise à rétablir une information inintelligible en information claire sans connaître la clé de chiffrement qui a été utilisée ;
17. **Cryptographie** : l'étude des moyens et produits de chiffrement permettant de rendre illisible des informations afin de garantir l'accès à un seul destinataire authentifié ;
18. **Cryptologie** : science relative à la protection et à la sécurité des informations notamment pour la confidentialité, l'authentification, l'intégrité et la non répudiation des données transmises. Elle est composée de la cryptanalyse et de la cryptographie.
19. **Cryptographie asymétrique** : système de chiffrement et de déchiffrement utilisant deux clés, une clé privée gardée secrète et une clé publique distribuée ;
20. **Cryptographie symétrique** : système de chiffrement et de déchiffrement utilisant la même clé dite clé secrète ;
21. **Déchiffrement** : opération inverse du chiffrement ;
22. **Information** : élément de connaissance, exprimé sous forme écrite, visuelle, sonore ou numérique, susceptible d'être représenté à l'aide de conventions pour être utilisé, conservé, traité ou communiqué.
23. **Intégrité** : propriété qui assure que des données n'ont pas été modifiées ou détruites de façon non autorisée lors de leur traitement, conservation et transmission ;

- 24. Moyens de cryptologie** : l'ensemble des outils scientifiques et techniques (matériel ou logiciel) qui permettent de chiffrer et/ou de déchiffrer ;
- 25. Non répudiation** : mécanisme permettant de garantir que la signature apposée sur un acte électronique est réalisée effectivement par l'une des parties sans aucune possibilité de le nier.
- 26. Prestation de cryptologie** : prestation visant à transformer à l'aide de codes secrets des informations ou des signaux clairs en informations ou signaux inintelligibles pour des tiers ou à réaliser l'opération inverse, grâce à des moyens, matériels ou logiciels conçus à cet effet ;
- 27. Prestataire de services de cryptologie** : personne, physique ou morale, qui fournit une prestation de cryptologie.

CHAPITRE II : COMMISSION NATIONALE DE CRYPTOLOGIE

Article 4 :

Il est créé une Commission nationale de cryptologie rattachée au Secrétariat Général de la Présidence de la République.

Article 5 :

La Commission nationale de cryptologie est chargée de statuer sur :

- 1) toute question relative au développement des moyens ou prestations de cryptologie au Sénégal ;
- 2) les projets de textes législatifs et réglementaires en matière de cryptologie ;
- 3) les normes techniques adoptées dans le domaine de la sécurité des systèmes d'information en général et celui de la cryptologie en particulier.

Elle est compétente pour :

- 1) recevoir les déclarations prévues à l'article 14 de la présente loi ;
- 2) délivrer des autorisations prévues à l'article 15 de la présente loi ;
- 3) délivrer des agréments aux prestataires de services de cryptologie conformément à l'article 16 de la présente loi ;
- 4) demander la communication des descriptions des caractéristiques techniques des moyens de cryptologie ;
- 5) mener des enquêtes et procéder à des contrôles sur les prestataires de services de cryptologie ainsi que sur les produits fournis ;
- 6) prononcer des sanctions administratives à l'encontre des contrevenants aux dispositions de la présente loi ;

- 7) défendre les intérêts du Sénégal dans les instances et organismes régionaux et internationaux traitant de la cryptologie.

Article 6 :

La Commission nationale de cryptologie est composée de quatorze membres choisis, en raison de leur compétence juridique, scientifique et/ou technique en matière de cryptologie.

Sont membres de droit de la Commission :

- 1) le Secrétaire Général de la Présidence de la République ;
- 2) le Chef du Service Technique Central des Chiffres et de Sécurité des Télécommunications ;
- 3) le Directeur général de l'Agence de Régulation des Télécommunications et des Postes (ARTP) ;
- 4) le Directeur de l'Agence De l'Informatique de l'Etat (ADIE) ;
- 5) le Directeur de l'Agence Nationale de la Sécurité.

Sont en outre membres de la Commission :

- 6) le représentant du Premier Ministre ;
- 7) le représentant du Ministre des Affaires Etrangères ;
- 8) le représentant du Ministre de la Justice ;
- 9) le représentant du Ministre chargé de l'Intérieur ;
- 10) le représentant du Ministre chargé des Forces Armées ;
- 11) le représentant du Ministre chargé de l'Economie et des Finances ;
- 12) le représentant du Ministre chargé de l'Education;
- 13) le représentant du Ministre chargé des Télécommunications, des Postes et des Nouvelles Technologies de l'information et de la Communication ;
- 14) le représentant du ministre chargé de la recherche scientifique.

Les membres de la Commission nationale de cryptologie ou leurs suppléants sont désignés, par les structures qu'ils représentent.

Ils sont ensuite nommés par Arrêté du Président de la République.

La qualité de membre de la Commission nationale de cryptologie est incompatible avec l'exercice des fonctions de dirigeant d'entreprise privée et la détention de participation dans les entreprises du secteur de l'informatique ou de télécommunications.

Les membres de la Commission nationale de cryptologie sont tenus à l'obligation de probité, d'intégrité et d'impartialité.

Article 7 :

La Commission nationale de cryptologie est présidée par le Secrétaire Général de la Présidence de la République ou son représentant. Les membres de la Commission se réunissent sur convocation du Président.

Le Secrétariat de la Commission nationale de cryptologie est assuré par le Service Technique Central des Chiffres et de la Sécurité des télécommunications.

Article 8 :

Les dépenses afférentes au fonctionnement de la Commission nationale de cryptologie ainsi que les indemnités dues à ses membres sont couvertes par une subvention allouée par l'Agence de Régulation des Télécommunications et des Postes.

Article 9 :

La Commission nationale de cryptologie peut créer en son sein des sous-commissions techniques.

Le Président de la Commission nationale de cryptologie peut inviter, à titre consultatif, aux travaux de la Commission, toute personne dont la contribution est jugée utile.

Article 10 :

Les membres de la Commission nationale de cryptologie sont soumis au secret professionnel conformément aux textes en vigueur.

Article 11 :

Les décisions prises par la Commission nationale de cryptologie peuvent faire l'objet d'un recours pour excès de pouvoir devant la haute autorité administrative compétente.

CHAPITRE III : RÉGIMES JURIDIQUES DES MOYENS ET PRESTATIONS DE CRYPTOLOGIE

Article 12 :

L'utilisation des moyens et prestations de cryptologie est libre.

Toutefois, lorsque les moyens ou des prestations de cryptologie permettent d'assurer des fonctions de confidentialité, le principe de libre utilisation ne s'applique que s'ils s'appuient sur des conventions secrètes gérées par un organisme agréé conformément à l'article 16 de la présente loi.

La fourniture, l'importation et l'exportation des moyens de cryptologie assurant exclusivement des fonctions d'authentification ou de contrôle d'intégrité sont également libres.

Article 13 :

Nonobstant les dispositions de l'article 12 de la présente loi, les modalités d'utilisation de la taille de certaines clés sont fixées par décret.

Article 14 :

La fourniture ou l'importation d'un moyen de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité est soumise à une déclaration préalable auprès de la commission nationale de cryptologie.

Le prestataire ou la personne procédant à la fourniture ou à l'importation d'un service de cryptologie tient à la disposition de la Commission nationale de cryptologie une description des caractéristiques techniques de ce moyen de cryptologie.

Les prestataires de services de cryptologie sont assujettis au secret professionnel.

Un décret définit les conditions dans lesquelles est effectuée la déclaration visée à l'alinéa premier du présent article.

Article 15 :

Sauf dispositions contraires, l'exportation d'un moyen de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité est soumise à autorisation de la Commission nationale de Cryptologie.

CHAPITRE IV : AGREMENT DES ORGANISMES EXERCANT DES PRESTATIONS DE CRYPTOLOGIE

Article 16 :

Les organismes exerçant des prestations de cryptologie doivent être agréés par la Commission nationale de cryptologie.

Article 17 :

Les conditions de délivrance de l'agrément aux organismes exerçant des prestations de cryptologie ainsi que leurs obligations sont définies par décret.

CHAPITRE V : RESPONSABILITE DES PRESTATAIRES DE SERVICES DE CRYPTOLOGIE

Article 18 :

Les prestataires de services de cryptologie à des fins de confidentialité sont responsables du préjudice causé dans le cadre desdites prestations aux personnes leur confiant la gestion de leurs conventions secrètes, en cas d'atteinte à l'intégrité, à la confidentialité ou à la disponibilité des données transformées à l'aide de ces conventions.

Toute clause contraire est réputée non écrite.

Les prestataires de services de cryptologie sont responsables vis-à-vis des personnes qui se sont raisonnablement fiées à leur produit, du préjudice résultant de leur faute intentionnelle ou de leur négligence.

Les prestataires de services de cryptologie sont exonérés de toute responsabilité à l'égard des personnes qui font un usage non autorisé de leur produit.

CHAPITRE VI : SANCTIONS ADMINISTRATIVES

Article 19 :

Lorsqu'un prestataire de services de cryptologie, même à titre gratuit, ne respecte pas les obligations auxquelles il est assujéti en application de la présente loi, la commission nationale de cryptologie peut, après audition de l'intéressé, prononcer :

- 1) l'interdiction d'utiliser ou de mettre en circulation le moyen de cryptologie concerné ;

- 2) le retrait provisoire de l'autorisation accordée, pour une durée de trois (3) mois ;
- 3) le retrait définitif de l'autorisation ;
- 4) des amendes dont le montant est fixé en fonction de la gravité des manquements commis et en relation avec les avantages ou les profits tirés de ces manquements.

CHAPITRE VII : SANCTIONS PENALES

Article 20 :

Il est créé une Annexe III dans le Code pénal intitulée « Les infractions pénales en matière de cryptologie » ainsi rédigée :

« Article Premier :

Quiconque n'aura pas satisfait à l'obligation de communication à la Commission nationale de cryptologie d'une description des caractéristiques techniques du moyen de cryptologie dans les conditions prévues à l'article 9 de la loi sur la cryptologie sera puni d'un emprisonnement de six (6) mois à deux (2) ans et d'une amende de 400 000 Francs à 2 000 000 Francs ou de l'une de ces deux peines seulement.

Article 2 :

1) Quiconque aura fourni ou importé un moyen de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité sans satisfaire à l'obligation de déclaration préalable auprès de la Commission nationale de cryptologie prévue à l'article 14 de la loi sur la cryptologie, sera puni d'un emprisonnement de six (6) mois à cinq (5) ans et d'une amende de 400 000 Francs à 5 000 000 Francs ou de l'une de ces deux peines seulement.

2) Quiconque aura fourni des prestations de cryptologie sans avoir obtenu préalablement l'agrément de la Commission nationale de cryptologie prévu à l'article 16 de la loi sur la cryptologie, sera puni d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende de 1.000.000 Francs à 20.000.000 Francs ou de l'une de ces deux peines seulement.

Article 3 :

Quiconque aura exporté un moyen de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité sans avoir obtenu préalablement l'autorisation de la Commission nationale de cryptologie prévue à l'article 15 de la loi sur la cryptologie, sera puni d'un emprisonnement d'un (1) an à cinq (5) ans et d'une

amende de 1 000 000 Francs à 20 000 000 Francs ou de l'une de ces deux peines seulement.

Article 4 :

Quiconque aura mis à la disposition d'autrui un moyen de cryptologie ayant fait l'objet d'une interdiction d'utilisation et de mise en circulation en application de l'article 19 de la loi sur la cryptologie sera puni d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende de 1.000.000 Francs à 20.000.000 Francs ou de l'une de ces deux peines seulement.

Article 5 :

Quiconque aura fait obstacle au déroulement des enquêtes prévues à l'article 5 de la loi sur la cryptologie ou refusé de fournir des informations ou documents y afférents sera puni d'emprisonnement d'un (1) an à cinq (5) ans et d'une amende de 1 000 000 Francs à 20 000 000 Francs ou de l'une de ces deux peines seulement.

Article 6 :

Quiconque aura mis en place un accès dérobé à des données ou à un système informatique sans l'autorisation de l'utilisateur légitime, sera puni d'un emprisonnement de deux (2) ans à cinq (5) ans et d'une amende de 2 000 000 Francs à 30 000 000 Francs ou de l'une de ces deux peines seulement.

Article 7 :

Peuvent en outre être prononcées, les peines complémentaires suivantes :

- 1) la confiscation des outils qui ont servi à commettre l'infraction ou qui en sont le produit ;
- 2) l'interdiction d'exercer une fonction publique ou une activité professionnelle liée à la cryptologie pour une durée de cinq (5) ans au plus ;
- 3) la fermeture de l'un ou des établissements de l'entreprise ayant servi à commettre les faits incriminés pour une durée de (5) cinq ans au plus ;
- 4) l'exclusion des marchés publics pour une durée de cinq (5) ans au plus.

Les peines complémentaires s'appliquent à toute personne physique ou morale coupable de l'une des infractions prévues par la présente loi.

Article 8 :

Toute infraction liée à la cryptologie sera constatée sur procès verbal dressé par les officiers de police judiciaire, les agents de l'Administration des Douanes, les agents

assermentés de l'Agence de Régulation des Télécommunications et des Postes ou ceux du Service Technique Central des Chiffres et de la Sécurité des télécommunications. »

CHAPITRE VIII : DISPOSITIONS TRANSITOIRES ET FINALES

Article 21 :

Les personnes assurant des prestations de cryptologie ou exerçant des activités de cryptologie disposent d'un délai de six (6) mois à compter de la date d'entrée en vigueur de la présente loi, pour régulariser leur situation auprès de la Commission nationale de cryptologie.

Article 22 :

Les modalités d'application de la présente loi sont définies par décret.

Article 23 :

Sont abrogées toutes dispositions contraires à la présente loi et notamment les articles 37 et 67 du code des télécommunications sont abrogés.

La présente loi sera exécutée comme loi de l'Etat.

Fait à Dakar, le **20 Août 2008**

Par le Président de la République
Le Premier Ministre

Abdoulaye WADE

Cheikh Hadjibou SOUMARE