LOIS

Loi n° 09-04 du 14 Chaâbane 1430 correspondant au 5 août 2009 portant règles particulières relatives à la prévention et à la lutte contre les infractions liées aux technologies de l'information et de la communication.

———

Le Président de la République,

Vu la Constitution, notamment ses articles 119, 120, 122-7° et 126 ;

Vu l'ordonnance n° 66-155 du 8 juin 1966, modifiée et complétée, portant code de procédure pénale ;

Vu l'ordonnance n° 66-156 du 8 juin 1966, modifiée et complétée, portant code pénal ;

Vu l'ordonnance n° 75-58 du 26 septembre 1975, modifiée et complétée, portant code civil ;

Vu la loi n° 2000-03 du 5 Joumada El Oula 1421 correspondant au 5 août 2000, modifiée et complétée, fixant les règles générales relatives à la poste et aux télécommunications ;

Vu l'ordonnance n° 03-05 du 19 Joumada El Oula 1424 correspondant au 19 juillet 2003 relative aux droits d'auteur et aux droits voisins ;

Vu la loi n° 08-09 du 18 Safar 1429 correspondant au 25 février 2008 portant code de procédure civile et administrative ;

Après avis du Conseil d'Etat,

Après adoption par le Parlement,

Promulgue la loi dont la teneur suit :

CHAPITRE I

DISPOSITIONS GENERALES

Objet

Article 1er. — La présente loi vise à mettre en place des règles particulières de prévention et de lutte contre les infractions liées aux technologies de l'information et de la communication.

Terminologie

Art. 2. — Au sens de la présente loi, on entend par :

a - **Infractions liées aux technologies de l'information et de la communication** : les infractions portant atteinte aux systèmes de traitement automatisé de données telles que définies par le code pénal ainsi que toute autre infraction commise ou dont la commission est facilitée par un système informatique ou un système de communication électronique.

b - **Système informatique** : tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données.

c - **Données informatiques** : toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction.

d - **Fournisseurs de services** :

1 - toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique et/ou d'un système de télécommunication ;

2 - et toute autre entité traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs.

e - **Données relatives au trafic** : toute donnée ayant trait à une communication passant par un système informatique, produite par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ainsi que le type de service.

f - **Communications électroniques** : toute transmission, émission ou réception de signes, de signaux, d'écrits, d'images, de sons ou de renseignements de toute nature, par tout moyen électronique.

CHAMP D'APPLICATION

Art. 3. — Conformément aux règles prévues par le code de procédure pénale et par la présente loi et sous réserve des dispositions légales garantissant le secret des correspondances et des communications, il peut être procédé, pour des impératifs de protection de l'ordre public ou pour les besoins des enquêtes ou des

informations judiciaires en cours, à la mise en place de dispositifs techniques pour effectuer des opérations de surveillance des communications électroniques, de collecte et d'enregistrement en temps réel de leur contenu ainsi qu'à des perquisitions et des saisies dans un système informatique.

CHAPITRE II

SURVEILLANCE DES COMMUNICATIONS ELECTRONIQUES

Cas autorisant le recours à la surveillance électronique

Art. 4. — Les opérations de surveillance prévues par l'article 3 ci-dessus peuvent être effectuées dans les cas suivants :

a) pour prévenir les infractions qualifiées d'actes terroristes ou subversifs et les infractions contre la sûreté de l'Etat.

b) lorsqu' il existe des informations sur une atteinte probable à un système informatique représentant une menace pour l'ordre public, la défense nationale, les institutions de l'Etat ou l'économie nationale ;

c) pour les besoins des enquêtes et des informations judiciaires lorsqu'il est difficile d'aboutir à des résultats intéressant les recherches en cours sans recourir à la surveillance électronique ;

d) dans le cadre de l'exécution des demandes d'entraide judiciaire internationale.

Les opérations de surveillance ci-dessus mentionnées ne peuvent être effectuées que sur autorisation écrite de l'autorité judiciaire compétente.

Lorsqu'il s'agit du cas prévu au paragraphe (a) du présent article, l'autorisation est délivrée aux officiers de police judiciaire relevant de l'organe visé à l'article 13 ci-après, par le procureur général près la Cour d'Alger, pour une durée de six (6) mois renouvelable, sur la base d'un rapport indiquant la nature du procédé technique utilisé et les objectifs qu'il vise.

Sous peine des sanctions prévues par le code pénal en matière d'atteinte à la vie privée d'autrui, les dispositifs techniques mis en place aux fins désignées au paragraphe (a) du présent article doivent être orientés, exclusivement, vers la collecte et l'enregistrement de données en rapport avec la prévention et la lutte contre les actes terroristes et les atteintes à la sûreté de l'Etat.

CHAPITRE III

REGLES DE PROCEDURE

Perquisition des systèmes informatiques

Art. 5. — Les autorités judiciaires compétentes ainsi que les officiers de police judiciaire, agissant dans le cadre du code de procédure pénale et dans les cas prévus par l'article 4 ci-dessus, peuvent, aux fins de perquisition, accéder, y compris à distance :

a) à un système informatique ou à une partie de celui-ci ainsi qu'aux données informatiques qui y sont stockées ;

b) à un système de stockage informatique.

Lorsque, dans le cas prévu par le paragraphe (a) du présent article, l'autorité effectuant la perquisition a des raisons de croire que les données recherchées sont stockées dans un autre système informatique et que ces données sont accessibles à partir du système initial, elle peut étendre, rapidement, la perquisition au système en question ou à une partie de celui-ci après information préalable de l'autorité judiciaire compétente.

S'il est préalablement avéré que les données recherchées, accessibles au moyen du premier système, sont stockées dans un autre système informatique situé en dehors du territoire national, leur obtention se fait avec le concours des autorités étrangères compétentes conformément aux accords internationaux pertinents et suivant le principe de la réciprocité.

Les autorités en charge de la perquisition sont habilitées à réquisitionner toute personne connaissant le fonctionnement du système informatique en question ou les mesures appliquées pour protéger les données informatiques qu'il contient, afin de les assister et leur fournir toutes les informations nécessaires à l'accomplissement de leur mission.

Saisie de données informatiques

Art. 6. — Lorsque l'autorité effectuant la perquisition découvre, dans un système informatique, des données stockées qui sont utiles à la recherche des infractions ou leurs auteurs, et que la saisie de l'intégralité du système n'est pas nécessaire, les données en question de même que celles qui sont nécessaires à leur compréhension, sont copiées sur des supports de stockage informatique pouvant être saisis et placés sous scellés dans les conditions prévues par le code de procédure pénale.

L'autorité effectuant la perquisition et la saisie doit, en tout état de cause, veiller à l'intégrité des données du système informatique en question.

Toutefois, elle peut employer les moyens techniques requis pour mettre en forme ou reconstituer ces données en vue de les rendre exploitables pour les besoins de l'enquête, à la condition que cette reconstitution ou mise en forme des données n'en altère pas le contenu.

Saisie par l'interdiction d'accès aux données

Art. 7. — Si, pour des raisons techniques, l'autorité effectuant la perquisition se trouve dans l'impossibilité de procéder à la saisie conformément à l'article 6 ci-dessus, elle doit utiliser les techniques adéquates pour empêcher l'accès aux données contenues dans le système informatique ou aux copies de ces données qui sont à la disposition des personnes autorisées à utiliser ce système.

Données saisies au contenu incriminé

Art. 8. — L'autorité ayant procédé à la perquisition peut ordonner les mesures nécessaires pour rendre inaccessible les données dont le contenu constitue une infraction, notamment en désignant toute personne qualifiée pour employer les moyens techniques appropriés à cet effet.

Limites à l'utilisation des données collectées

Art. 9. — Sous peine de sanctions édictées par la législation en vigueur, les données obtenues au moyen des opérations de surveillance prévues à la présente loi ne peuvent être utilisées à des fins autres que les enquêtes et les informations judiciaires.

CHAPITRE IV
OBLIGATIONS DES FOURNISSEURS DE SERVICES

Assistance aux autorités

Art. 10. — Dans le cadre de l'application des dispositions de la présente loi, les fournisseurs de services sont tenus de prêter leur assistance aux autorités chargées des enquêtes judiciaires pour la collecte ou l'enregistrement, en temps réel, des données relatives au contenu des communications et de mettre à leur disposition les données qu'ils sont tenus de conserver en vertu de l'article 11 ci-dessous.

Sous peine des sanctions prévues en matière de violation du secret de l'enquête et de l'instruction, les fournisseurs de services sont tenus de garder la confidentialité des opérations qu'ils effectuent sur réquisition des enquêteurs et les informations qui s'y rapportent.

Conservation des données relatives au trafic

Art. 11. — Selon la nature et les types de services, les fournisseurs de services s'engagent à conserver :

a) les données permettant l'identification des utilisateurs du service ;

b) les données relatives aux équipements terminaux des communications utilisées ;

c) les caractéristiques techniques ainsi que la date, le temps et la durée de chaque communication ;

d) les données relatives aux services complémentaires requis ou utilisés et leurs fournisseurs ;

e) les données permettant d'identifier le ou les destinataires de la communication ainsi que les adresses des sites visités.

Pour les activités de téléphonie, l'opérateur conserve les données citées au paragraphe (a) du présent article et celles permettant d'identifier et de localiser l'origine de la communication.

La durée de conservation des données citées au présent article est fixée à une (1) année à compter du jour de l'enregistrement.

Sans préjudice des sanctions administratives découlant du non-respect des obligations prévues par le présent article, la responsabilité pénale des personnes physiques et morales est engagée lorsque cela a eu pour conséquence d'entraver le bon déroulement des enquêtes judiciaires. La peine encourue par la personne physique est l'emprisonnement de six (6) mois à cinq (5) ans et l'amende de 50.000 DA à 500.000 DA.

La personne morale encourt la peine d'amende suivant les modalités prévues par le code pénal.

Les modalités d'application des alinéas 1, 2 et 3 du présent article sont, en tant que de besoin, précisées par voie réglementaire.

Obligations des fournisseurs d'accès à internet

Art. 12. — Outre les obligations prévues par l'article 11 ci-dessus, les fournisseurs d'accès à internet sont tenus :

a) d'intervenir, sans délai, pour retirer les contenus dont ils autorisent l'accès en cas d'infraction aux lois, les stocker ou les rendre inaccessibles dès qu'ils en ont pris connaissance directement ou indirectement ;

b) de mettre en place des dispositifs techniques permettant de limiter l'accessibilité aux distributeurs contenant des informations contraires à l'ordre public ou aux bonnes mœurs et en informer les abonnés.

CHAPITRE V

ORGANE NATIONAL DE PREVENTION ET DE LUTTE CONTRE LES INFRACTIONS LIEES AUX TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Création de l'organe

Art. 13. — Il est créé un organe national de prévention et de lutte contre la criminalité liée aux technologies de l'information et de la communication.

La composition, l'organisation et les modalités de fonctionnement de l'organe sont fixées par voie réglementaire.

Missions de l'organe

Art. 14. — L'organe visé à l'article 13 ci-dessus est chargé notamment de :

a) la dynamisation et la coordination des opérations de prévention et de lutte contre la criminalité liée aux technologies de l'information et de la communication ;

b) l'assistance des autorités judiciaires et des services de police judiciaire en matière de lutte contre la criminalité liée aux technologies de l'information et de la communication, y compris à travers la collecte de l'information et les expertises judiciaires ;

c) l'échange d'informations avec ses interfaces à l'étranger aux fins de réunir toutes données utiles à la localisation et à l'identification des auteurs des infractions liées aux technologies de l'information et de la communication.

CHAPITRE VI

LA COOPERATION ET L'ENTRAIDE JUDICIAIRE INTERNATIONALES

Compétence judiciaire

Art. 15. — Outre les règles de compétence prévues par le code de procédure pénale, les juridictions algériennes sont compétentes pour connaître des infractions liées aux technologies de l'information et de la communication commises en dehors du territoire national, lorsque leur auteur est un étranger et qu'elles ont pour cible les institutions de l'Etat algérien, la défense nationale ou les intérêts stratégiques de l'économie nationale.

Entraide judiciaire internationale

Art. 16. — Dans le cadre des investigations ou des informations judiciaires menées pour la constatation des infractions comprises dans le champ d'application de la présente loi et la recherche de leurs auteurs, les autorités compétentes peuvent recourir à l'entraide judiciaire internationale pour recueillir des preuves sous forme électronique.

En cas d'urgence, et sous réserve des conventions internationales et du principe de réciprocité, les demandes d'entraide judiciaire visées à l'alinéa précédent sont recevables si elles sont formulées par des moyens rapides de communication, tels que la télécopie ou le courrier électronique pour autant que ces moyens offrent des conditions suffisantes de sécurité et d'authentification.

Echange d'informations et les mesures conservatoires

Art. 17. — Les demandes d'entraide tendant à l'échange d'informations ou à prendre toute mesure conservatoire sont satisfaites conformément aux conventions internationales pertinentes, aux accords bilatéraux et en application du principe de réciprocité.

Restrictions aux demandes d'entraide internationale

Art. 18. — L'exécution de la demande d'entraide est refusée si elle est de nature à porter atteinte à la souveraineté nationale ou à l'ordre public.

La satisfaction des demandes d'entraide peut être subordonnée à la condition de conserver la confidentialité des informations communiquées ou à la condition de ne pas les utiliser à des fins autres que celles indiquées dans la demande.

Art. 19. — La présente loi sera publiée au *Journal officiel* de la République algérienne démocratique et populaire.

Fait à Alger, le 14 Chaâbane 1430 correspondant au 5 août 2009

Abdelaziz BOUTEFLIKA.