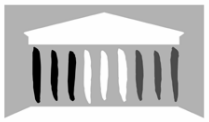

N° 3412

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

TREIZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 11 mai 2011.

PROPOSITION DE LOI

pour **renforcer** *l'***efficience** *de la* **lutte** *contre les* **attaques informatiques**, *pour un monde numérique plus civilisé et donc plus fort,*

(Renvoyée à la commission des lois constitutionnelles, de la législation et de l'administration générale de la République, à défaut de constitution d'une commission spéciale dans les délais prévus par les articles 30 et 31 du Règlement.)

présentée par Mesdames et Messieurs

Muriel MARLAND-MILITELLO, Alfred ALMONT, Patrick BEAUDOUIN, Jacques Alain BÉNISTI, Étienne BLANC, Patrice CALMÉJANE, Bernard CARAYON, Joëlle CECCALDI-RAYNAUD, Dino CINIERI, Alain COUSIN, Marie-Christine DALLOZ, Daniel FASQUELLE, Jean-Michel FERRAND, Daniel FIDELIN, Jean-Claude FLORY, Philippe FOLLIOT, Claude GATIGNOL, François-Michel GONNOT, Michel GRALL, François GROSDIDIER, Arlette GROSSKOST, Louis GUÉDON, Jean-Claude GUIBAL, Christophe GUILLOTEAU, Françoise HOSTALIER, Jacqueline IRLES, Maryse JOISSAINS-MASINI, Patrick LABAUNE, Marguerite LAMOUR, Thierry LAZARO, Jean-Louis LÉONARD, Guy MALHERBE, Jean-Philippe MAURER, Christian MÉNARD, Gérard MENUEL, Georges MOTHRON, Alain MOYNE-BRESSAND, Jean-Marc NESME, Didier QUENTIN, Frédéric REISS, Jean ROATTA, Francis SAINT-LÉGER, Jean-Marie SERMIER, Fernand SIRÉ, Jean-Charles TAUGOURDEAU, Guy TEISSIER, Michel TERROT, Yves VANDEWALLE, Jean-Sébastien VIALATTE, Michel VOISIN, Jean-Pierre DUPONT, Jacques REMILLER, Philippe VITEL et Dominique LE MÈNER,

députés.

EXPOSÉ DES MOTIFS

MESDAMES, MESSIEURS,

Dans une société de la connaissance, à l'ère du numérique, les systèmes informatiques sont des éléments particulièrement stratégiques. Il n'est donc pas étonnant que des personnes fort mal intentionnées les prennent pour cible.

Souvent ces attaques sont menées à distance, depuis des machines situées hors de notre territoire national. Ce n'est pas une raison pour rester passifs devant ces phénomènes, cédant au fatalisme technologique.

Ces armes du monde numérique, utilisées contre tel ou tel système d'information, ne sont pas compatibles avec le monde numérique civilisé que nous appelons de nos voeux, un monde numérique respectueux des droits et libertés de chacun, un monde numérique où chacun est en sécurité.

Or l'arsenal juridique actuel n'est pas suffisant : il mérite d'être amélioré sur deux points.

– Premièrement, le champ d'application des sanctions, actuellement limité aux *systèmes de traitement automatisé de données*, doit être élargi aux atteintes portées aux *services de communication au public en ligne* (qui incluent les sites internet).

– Deuxièmement, il est nécessaire de renforcer les sanctions lorsque les attaques sont dirigées contre les systèmes d'information d'une personne morale de droit public ou d'une personne morale de droit privé chargée d’une mission de service public.

1) La situation actuelle

Notre code pénal, dans son chapitre III du titre II du livre III, couvre les diverses attaques qui peuvent être menées contre les *systèmes de traitement automatisé de données.*

L'article 323-1 du code pénal vise les intrusions dans un système de traitement automatisé de données. Il les rend passibles de 3 ans d'emprisonnement et de 45000 euros d'amende.

L'**article 323-2** quant à lui vise la perturbation du fonctionnement d'un système de traitement automatisé de données qui est passible de cinq ans d'emprisonnement et de 75000 euros d'amende.

L'**article 323-3** vise la modification frauduleuse de données, par exemple dans une base de données. Elle est passible de 5 ans d'emprisonnement et de 75 000 euros d'amende.

L'article **323-3-1** vise quant à lui les moyens qui permettent ces attaques et punit des mêmes peines l'importation, la détention, l'offre, la cession et la mise à disposition de ces moyens techniques, matériels ou logiciels.

Enfin, la tentative de commission de tous les délits sus-mentionnés est punie des mêmes peines (**article 323-7** du code pénal).

2) Qu'est-ce qu'un *système de traitement automatisé de données ?*

Une question reste assez floue : la notion de *systèmes de traitement automatisé de données* s'applique-t-elle à la fois aux *services de communication au public en ligne* que sont les sites internet, dont les données sont publiques, et aux systèmes de traitement automatisé dont les données ont un caractère personnel et/ou confidentiel ?

Ce que l'on peut en revanche affirmer est que la jurisprudence a qualifié de *systèmes de traitement automatisé de données* :

– le disque dur d'un ordinateur contenant le logiciel de comptabilité et les données d'un cabinet d'expertise comptable (cour d'appel de Douai, 7 octobre 1992) ;

– le radiotéléphone (cour d'appel de Paris, 18 novembre 1992) ;

– des systèmes d'exploitation de données au sein d'entreprises (cour d'appel de Paris, 15 mars 1994 ; cour d'appel de Paris, 5 octobre 1994 ; tribunal de grande instance de Paris, 1er juin 2007) ;

– un service télématique (cour d'appel de Paris, 5 avril 1994 – jugeant, contrairement à la définition du Sénat, qu'« il n'est pas nécessaire pour que l'infraction existe que l'accès soit limité par un dispositif de protection », mais qu'il suffit « que le maître du système ait manifesté l'intention d'en restreindre l'accès aux seules personnes autorisées ») ;

– l'annuaire électronique de France Télécom (tribunal correctionnel de Brest, 14 mars 1995) ;

– le réseau cartes France Télécom (tribunal correctionnel de Paris, 26 juin 1995) ;

– le réseau Carte bancaire (tribunal correctionnel de Paris, 25 février 2000)

3) La nécessité d'étendre les sanctions aux attaques contre tous les services de communication au public en ligne

La « délinquance astucieuse » dans le monde numérique, qui est une véritable violence électronique, ne se restreint pas aux *systèmes de traitement automatisé de données,* elle frappe l'ensemble du champ de la *communication au public par voie électronique* qui recouvre à la fois la c*ommunication au public en ligne* et la *communication audiovisuelle.*

Diverses techniques visent à perturber l'accès aux sites internet, sans nécessairement causer de pertes de données. Sans rentrer dans les détails techniques, une méthode en vogue pour attaquer certains sites internet est le déni de service (DoS - *denial of service* en anglais) : attaques par *TCP/SYN flooding, UDP flooding, packet fragmentation, smurfing,* etc. Ces attaques visent à saturer les serveurs pour rendre les données inaccessibles. Ces attaques peuvent même être menées à une échelle bien plus plus massive dans le cas d'attaques DoS distribuées (DDoS - *distributed denial of service* en anglais), en prenant le contrôle à distance de machines zombies sans que l'utilisateur ne le sache.

Les sites internet peuvent également être victimes de défacement, ou défaçage, (*defacing* en anglais). Ce type d'attaque consiste pour un *hacker* à modifier, de manière plus ou moins substantielle, la présentation d'un site sur le réseau internet.

Or, les articles du code pénal ne visent que les atteintes aux *systèmes de traitement automatisé de données*. **Eu égard à l'objectif de sanctionner les attaques informatiques au sens le plus large du terme et ainsi protéger la liberté d'expression et de communication, dont l'exercice est une condition de la démocratie et l'une des garanties du respect des autres droits et libertés**, il convient d'étendre les dispositions du code pénal aux atteintes portées aux *services de communication au public en ligne* (qui incluent les sites internet).

Il est donc proposé, dans l'**article 1er**, de compléter le code pénal en rendant passible de cinq ans d'emprisonnement et de 75000 euros d'amende le fait d'entraver ou de fausser le fonctionnement d'un site internet.

4) La nécessité de renforcer les sanctions lorsque les faits prennent pour cible une institution

Les attaques informatiques, quelles qu'elles soient, ont une portée encore plus grave lorsqu'elles sont dirigées contre une institution publique ou une personne morale de droit privé investie d'une mission de service public.

S'agissant des attaques DDOS, un exemple parmi d'autres s'est produit en mars 2009 et a pris pour cible le site *jaimelesartistes.fr*, site dont le but était de donner des informations sur le projet de loi « Création et Internet ». Les attaques DDOS, en saturant les équipements de l'hébergeur du site, ont contraint le site jaimelesartistes.fr à fermer, privant par là même l'ensemble des internautes des informations utiles qui avaient été mises à leur disposition par le Ministère de la Culture et de la Communication.

Outre les institutions publiques, les attaques informatiques peuvent viser des personnes morales de droit privé chargées d'une mission de service public ou des établissements publics industriels et commerciaux, comme la société nationale des chemins de fer français (SNCF), dont les systèmes de traitement automatisé de données ont été affectés en mars 2010. Les premières victimes ont été les clients de la SNCF, entravés dans leur utilisation d'un service public auquel ils ont pourtant droit.

De telles attaques constituent des atteintes envers notre République et ces principes fondamentaux et partant, doivent être sévèrement réprimées. C'est la raison pour laquelle l'**article 2** de la présente proposition de loi propose de **doubler les peines prévues lorsque ces attaques prennent pour cible une personne morale de droit public ou une personne morale de droit privé chargée d'une mission de service public**.

5) L'instauration d'une nouvelle peine complémentaire dans le respect du principe de proportionnalité des peines

L'**article 3** de la présente proposition de loi vise à **donner un outil supplémentaire au juge en lui permettant de prononcer à titre de peine complémentaire la suspension de la connexion internet et l'interdiction de souscrire un abonnement auprès d'un fournisseur d'accès internet pendant une durée maximale de 2 ans**. S'agissant de la constitutionnalité

d'une telle sanction prononcée par le juge, le Conseil constitutionnel s'est exprimé sur d'autres faits répréhensibles dans sa décision n° 2009-590 DC du 22 octobre 2009 sur la loi relative à la protection pénale de la propriété littéraire et artistique sur internet (HADOPI 2) : « l'instauration d'une peine complémentaire destinée à réprimer les délits de contrefaçon commis au moyen d'un service de communication au public en ligne et consistant dans la suspension de l'accès à un tel service pour une durée maximale d'un an, assortie de l'interdiction de souscrire pendant la même période un autre contrat portant sur un service de même nature auprès de tout opérateur, ne méconnaît pas le principe de nécessité des peines » (considérant n° 21). Vu la gravité des délits que constituent les attaques informatiques intentionnées contre des moyens informatiques d'institutions publiques ou investies d'une mission de service public, il est proposé de doubler ce quantum.

*

Nous devons continuer à lutter le plus efficacement possible contre toutes les formes de délinquance, notamment sur les réseaux de communication électronique, afin de faire progresser la sécurité informatique, la confiance en l'économie numérique, le respect de la vie privée et la liberté de communiquer, pour construire ensemble un monde numérique plus civilisé et donc plus fort.

PROPOSITION DE LOI

Article 1er

① I. – À l'article 323-2 du code pénal, après le mot : « données », sont insérés les mots : « ou un service de communication au public en ligne »

② II. – En conséquence le chapitre III du titre II du livre III du code pénal est renommé ainsi : « Des atteintes aux systèmes informatiques ».

Article 2

① Après l'article 323-3-1 du code pénal, est inséré un article 323-3-2 ainsi rédigé :

② « *Art. 323-3-2.* – Les peines prévues aux articles 323-1 à 323-3-1 sont doublées lorsque le système de traitement automatisé de données est celui d'une personne morale de droit public ou d'une personne morale de droit privé chargée d'une mission de service public, ou lorsque est visé un service de communication au public en ligne dont une personne morale de droit public ou une personne morale de droit privé chargée d'une mission de service public est l'éditeur ou l'hébergeur. »

Article 3

① L'article 323-5 du même code est complété par un alinéa ainsi rédigé :

② « 8° La suspension de l'accès au service pour une durée de deux ans au plus assortie de l'impossibilité, pour l'abonné, de souscrire pendant la même période un autre contrat portant sur l'accès à un service de communication au public en ligne auprès de tout opérateur. »