F – 1 – 02
28 mai 2002

PROJET DE LOI CONCERNANT LES DELITS RELATIFS AUX SYSTEMES D'INFORMATIONS

EXPOSE DES MOTIFS

Parallèlement aux progrès technologiques, à la démocratisation de l'accès à l'informatique, à la globalisation et au développement des réseaux d'informations et du domaine de l'électronique, une nouvelle forme de délinquance, la criminalité informatique, est en constante augmentation.

Cette cybercriminalité s'avère d'autant plus inquiétante et complexe qu'elle touche une population sans cesse croissante et de plus en plus variée, allant de la petite à la grande délinquance. Elle résulte aussi bien du comportement du jeune « pirate » surdoué qui s'introduit dans un système informatique par jeu, par défi, ou simplement pour se faire connaître, en y insérant de fausses données ou en désorganisant ledit système, que de l'organisation criminelle « professionnelle » qui cherche à détourner des milliards en pénétrant frauduleusement les systèmes informatiques d'une grande banque. Les attitudes répréhensibles se multiplient et portent de plus en plus atteinte à la sécurité des réseaux dont l'exploitation, source de richesse économique ou simplement informationnelle, doit être préservée.

Ces actes de piratage ou sabotage d'informations peuvent constituer un frein au développement du commerce électronique, mais aussi une atteinte aux droits des personnes dans leur vie privée, leurs droits d'auteurs, leurs droits de propriété.

Si les infractions constatées sont pour une part d'un type classique et peuvent être réprimées par les textes actuels du droit pénal sanctionnant notamment l'abus de confiance, le faux, l'usage de faux, le vol, l'escroquerie, certaines incriminations s'avèrent insuffisantes pour s'appliquer aux particularismes des nouvelles technologies.

Le présent projet de loi a été élaboré afin de lutter contre ces nouvelles formes de délinquance. Il a pour objet de définir de nouvelles infractions plus spécifiquement adaptées au monde de l'informatique et des réseaux, et plus particulièrement de sanctionner les atteintes irrégulières aux systèmes d'informations et aux données qu'ils contiennent.

Toujours dans un but de protection des données, les dispositions proposées posent le principe d'effacement et d'anonymisation des données de communication dès leur achèvement, sous réserve de deux dérogations qui visent à faciliter les poursuites judiciaires et à permettre le recouvrement des prestations par les opérateurs qui les ont fournies.

Les dispositions présentées permettent ainsi de compléter et renforcer l'action gouvernementale entreprise dans d'autres domaines du droit des nouvelles technologies, comme le commerce électronique, les casinos virtuels, etc..., par la mise en oeuvre d'un ensemble normatif qui procède d'une même préoccupation : garantir des objectifs de défense économique et de protection des investissements, assurer le maintien de la sécurité et la défense de l'ordre public, protéger le droit de chacun à la propriété et au respect de la vie privée.

Sous le bénéfice de ces considérations générales, les dispositions projetées appellent les observations particulières suivantes :

ARTICLE PREMIER : Cet article prévoit l'insertion des infractions susvisées dans la classification typologique et la numérotation actuelle du Code pénal. Ces incriminations concernant des fraudes aux systèmes d'informations répriment des délits contre les biens.

De ce fait, les nouvelles dispositions s'intègrent au Livre III du Code pénal qui traite « Des crimes et délits et de leur répression », et plus particulièrement à son titre II « Crimes et délits contre les personnes, les propriétés et les animaux ». Elles sont regroupées au sein d'une nouvelle Section IV, intitulée : « Des délits relatifs aux systèmes d'informations ».

ARTICLE 2 : Il sanctionne les formes d'intrusions irrégulières dans tout système d'informations, qu'elles résultent d'un accès illicite ou d'un maintien interdit dès lors que le contrevenant a agi frauduleusement. Cet élément moral implique que le contrevenant ait agi non seulement intentionnellement mais encore indûment, c'est-à-dire en ayant conscience d'usurper un droit qu'il n'a pas, d'agir abusivement sans autorisation, et au mépris de la volonté des titulaires, « contre le gré du maître du système ».

Dès lors, l'accès inopiné ou le maintien inconscient ne sont pas poursuivis. En revanche, le seul agissement, le simple fait d'entrer et/ou de se maintenir frauduleusement dans un système d'information peut suffire à constituer l'infraction, sans considération du mobile, du but poursuivi et des conséquences du comportement délictueux.

Le maintien peut donc être considéré comme frauduleux même lorsqu'il est consécutif à un accès licite. Tel est le cas, par exemple, lorsqu'après avoir régulièrement accédé à une base de données payante, le « pirate » déjoue volontairement les systèmes de calcul du prix de la prestation lié à la durée de connexion, ou encore neutralise les systèmes de protection pour espionner des fichier confidentiels.

ARTICLE 3 : Cet article permet de réprimer toutes les formes d'atteintes volontaires au fonctionnement d'un système d'informations, consécutives ou non à un accès ou à un maintien frauduleux, et ce, quelque soit le moyen matériel ou intellectuel utilisé. Il peut s'agir de procédés techniques comme la saturation des capacités d'accès ou l'utilisation d'une carte d'interruption, etc..., dès lors que ces atteintes ont pour conséquence d'empêcher le fonctionnement correct du système et/ou de lui faire produire un résultat autre que ce qu'il aurait dû être.

ARTICLE 4 : L'introduction d'un virus fait l'objet d'une incrimination spécifique aggravée par une pénalité renforcée. Cette disposition se justifie par la nécessité de sanctionner les conséquences particulièrement destructrices du virus, les effets parasitaires qu'il provoque, et les préjudices en chaîne dont il est la cause.

ARTICLE 5 : Il réprime les atteintes volontaires aux données électroniques qui sont contenues dans un système d'informations quelqu'en soit le moyen : altération, falsification, ou même contrefaçon, ce qui s'entend de toutes les formes de dégâts causés à l'intégrité ou à l'authenticité des données.

Celui qui se sera rendu coupable d'utiliser en connaissance de cause, c'est-à-dire en sachant qu'elles ont fait l'objet d'atteintes irrégulières, les données altérées, falsifiées ou contrefaites, sera puni des mêmes peines.

ARTICLE 6 : L'article impose aux opérateurs de communications ainsi qu'à toute personne physique ou morale qui fournit un service de la société de l'information, d'effacer ou de rendre anonyme toute donnée technique de communication dès lors que celle-ci est terminée. Le manquement à cette obligation est sanctionnée d'une peine correctionnelle. Deux exceptions sont prévues à l'effacement des données.

La première est d'ordre judiciaire. Elle se justifie par la nécessité de renforcer les moyens d'enquête lors de la poursuite de crimes et délits commis sur les réseaux ou par leur biais. Les données enregistrées par les opérateurs des réseaux pourront ainsi être exploitées pour faciliter la recherche des preuves et aider à la manifestation de la vérité.

La seconde est d'ordre commercial. Les opérateurs peuvent conserver les données nécessaires à la facturation et au paiement des prestations qu'ils fournissent, sans pouvoir excéder le temps nécessaire aux délais légaux de recouvrement de leur créance.

Les données ainsi conservées ne peuvent en aucune façon porter sur le contenu des correspondances ou informations échangées.

ARTICLE 7 : Il édicte une liste de peines complémentaires facultatives dont le juge pourra disposer afin de mieux adapter les pénalités selon le principe de la personnalisation des peines.

ARTICLES 8 à 10 : Ces articles punissent au même titre que l'infraction, la tentative, l'entente préparatoire et la récidive. Compte tenu de la gravité des faits, ces dispositions permettent de réprimer les comportements délictueux autres que ceux de l'auteur principal et que la seule infraction consommée.

Tel est l'objet du présent projet de loi.

*

* *

PROJET DE LOI

ARTICLE PREMIER.- Il est ajouté une section IV au chapitre II du titre II du Livre III du Code pénal, qui s'intitule : « Des délits relatifs aux systèmes d'informations ».

ARTICLE 2.- Il est inséré à la section IV du chapitre II du titre II du Livre III du Code pénal ainsi créée, un nouvel article n° 389-1, rédigé comme suit :

«Article 389-1.- Quiconque aura accédé ou se sera maintenu frauduleusement dans tout ou partie d'un système d'informations sera puni d'un d'emprisonnement d'un an et de l'amende prévue au chiffre 2 de l'article 26 du Code pénal.

Est qualifié de système d'informations, tout système comprenant des éléments matériels, logiciels, progiciels, de bases de données, de données électroniques et de télécommunications permettant le traitement, le stockage et/ou la transmission de données électroniques.

Lorsque l'accès ou le maintien frauduleux aura causé un dommage au système d'informations lui-même et/ou une suppression ou une modification des données qui y sont contenues, la peine sera portée à un emprisonnement de deux ans et à l'amende prévue au chiffre 3 de l'article 26 du Code pénal.

Est qualifiée d'accès frauduleux, toute action de pénétration ou d'intrusion irrégulière, par quelque moyen que ce soit, dans tout ou partie d'un système d'informations consistant à consulter des données ou des informations, à créer une menace ou à attenter à la sécurité, la confidentialité, l'intégrité, la disponibilité d'un système d'informations ou des données qui y sont intégrées ou stockées.

Est qualifié de maintien frauduleux, tout maintien non autorisé dans un système d'informations qui aurait pour conséquence de porter atteinte à l'intégrité ou à la confidentialité des données ou du système d'informations. »

ARTICLE 3.- Il est inséré à la section IV du chapitre II du titre II du Livre III du Code pénal un nouvel article numéroté 389-2, rédigé comme suit :

«Article 389-2.- Quiconque aura, volontairement, entravé ou altéré le fonctionnement de tout ou partie d'un système d'informations sera puni d'un emprisonnement de trois ans et de l'amende prévue au chiffre 4 de l'article 26 du Code pénal.

Est qualifiée d'entrave du fonctionnement d'un système d'informations, toute action ayant pour effet, objet ou finalité de paralyser un système d'informations par l'introduction, le transfert, la modification, l'endommagement, l'effacement ou la suppression de données électroniques.

Est qualifiée d'altération du fonctionnement d'un système d'informations, toute action consistant à fausser le fonctionnement dudit système pour lui faire produire un résultat autre que celui pour lequel il est normalement conçu et utilisé. »

ARTICLE 4.- Il est inséré à la section IV du chapitre II du titre II du Livre III du Code pénal un nouvel article numéroté 389-3, rédigé comme suit :

« Article 389-3 .- Quiconque aura, volontairement, altéré tout ou partie des données électroniques sera puni d'un emprisonnement de trois ans et de l'amende prévue au chiffre 4 de l'article 26 du Code pénal.

Est qualifiée de donnée électronique, tout ou partie d'une information, quelle qu'en soit la nature, le format et/ou le support initial, contenue dans un système d'informations à quelque fin que ce soit.

Est qualifiée d'altération des données électroniques, toute action visant, de manière volontaire, à supprimer et/ou modifier les données, ainsi que toute action visant à supprimer ou modifier leur mode de traitement ou de transmission.»

ARTICLE 5.- Il est inséré à la section IV du chapitre II du titre II du Livre III du Code pénal un nouvel article numéroté 389-4, rédigé comme suit :

« Article 389-4.- Quiconque aura, volontairement, fait usage de données électroniques volontairement altérées sera puni d'un emprisonnement de quatre ans et de l'amende prévue au chiffre 4 de l'Article 26 du Code pénal. »

ARTICLE 6.- Il est inséré à la section IV du chapitre II du titre II du Livre III du Code pénal un nouvel article numéroté 389-5, rédigé comme suit :

«Article 389-5.- Les opérateurs et les prestataires de services chargés de l'exploitation des réseaux et des services de télécommunications et de communications électroniques sont tenus d'effacer ou de rendre anonyme toute donnée électronique relative à une communication dès que celle-ci est achevée, sous réserve des dispositions des alinéas 2, 3, et 4 ci-après.

Pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales, et dans le seul but de permettre, en tant que de besoin, la mise à disposition d'informations à l'autorité judiciaire, il peut être différé pour une durée maximale d'un an aux opérations tendant à effacer ou à rendre anonymes certaines catégories de données électroniques. Une ordonnance souveraine, prise après avis de la Commission de Contrôle des Informations Nominatives, détermine, dans les limites fixées par l'alinéa 4, ces catégories de données et la durée de leur conservation, selon l'activité des opérateurs et des prestataires de services et la nature des communications.

Pour les besoins de la facturation et du paiement des prestations de communications, les opérateurs et les prestataires de services peuvent, jusqu'à la fin de la période au cours de laquelle la facture peut être légalement contestée ou des poursuites engagées pour en obtenir le paiement, utiliser, conserver et, le cas échéant, transmettre à des tiers concernés directement par la facturation ou le recouvrement, les catégories de données électroniques qui sont déterminées, dans les limites fixées par l'alinéa 4, selon l'activité des opérateurs et des prestataires de services et la nature de la communication, par ordonnance souveraine prise après avis de la Commission de Contrôle des Informations Nominatives. Les opérateurs et les prestataires de services peuvent en outre réaliser un traitement de ces données électroniques en vue de commercialiser leurs propres services de communications, si les usagers y consentent expressément et pour une durée déterminée. Cette durée ne peut, en aucun cas, être supérieure à la période correspondant aux relations contractuelles entre l'usager et l'opérateur ou le prestataire de services.

Les données électroniques conservées et traitées dans les conditions définies aux alinéas 2 et 3 portent exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs et les prestataires de services et sur les caractéristiques techniques des communications assurées par ces derniers. Elles ne peuvent en aucun cas porter sur le contenu dans le cadre de ces communications. La conservation et le traitement de ces données s'effectuent dans le respect des dispositions de la loi du 23 décembre 1993 n° 1.165 réglementant les traitements d'informations nominatives. Les opérateurs et les prestataires de services prennent toutes mesures pour empêcher une utilisation de ces données électroniques à des fins autres que celles prévues au présent article.

Le fait, pour les opérateurs et les prestataires de services chargés de l'exploitation des réseaux et des services de télécommunications électroniques, de ne pas procéder aux opérations tendant à effacer ou à rendre anonymes les données électroniques est puni d'un emprisonnement d'un an et de l'amende prévue au chiffre 4 de l'article 26 du Code pénal.

ARTICLE 7.- Il est inséré à la section IV du chapitre II du titre II du Livre III du Code pénal un nouvel article numéroté 389-6, rédigé comme suit :

« Article 389-6.- Les tribunaux pourront prononcer à l'encontre des personnes reconnues coupables des délits prévus à la présente section les peines complémentaires suivantes :

1°- l'affichage ou la diffusion de la décision prononcée suivant les modalités prévues à l'article 30 du Code pénal ;

2°- l'interdiction des droits civils, civiques et de famille suivant les modalités prévues à l'article 27 du Code pénal ;

3°- l'interdiction, pour une durée de cinq ans au plus, d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise ;

4°- l'interdiction d'émettre des chèques à l'exclusion des chèques certifiés ou de retrait de fonds du tireur auprès du tiré. »

ARTICLE 8.- Il est inséré à la section IV du chapitre II du titre II du Livre III du Code pénal un nouvel article numéroté 389-7, rédigé comme suit :

« Article 389-7.- Quiconque tente de commettre une des infractions prévues aux articles 389-1 à 389-5 est puni des peines prévues pour l'infraction elle-même. »

ARTICLE 9.- Il est inséré à la section IV du chapitre II du titre II du Livre III du Code pénal un nouvel article numéroté 389-8, rédigé comme suit :

« Article 389-8.- Quiconque participe à une association ou à une entente établie en vue de préparer ou de commettre une des infractions prévues par les articles 389-1 à 389-3 est puni des peines prévues pour l'infraction elle-même. »

ARTICLE 10.- Il est ajouté un nouvel alinéa 4 à l'article 40 du Code pénal, relatif « aux peines de la récidive pour crimes et délits », rédigé comme suit :

« Article 40.- Il en sera de même du condamné à un emprisonnement de plus d'une année pour délit, qui, dans le délai de cinq ans, serait reconnu coupable du même délit ou d'un crime n'ayant entraîné qu'une peine d'emprisonnement.

Celui qui, ayant été condamné antérieurement à une peine d'emprisonnement de moindre durée, commettrait le même délit dans les mêmes conditions de temps, sera condamné à une peine d'emprisonnement qui ne pourra être inférieure au double de celle précédemment prononcée, sans toutefois qu'elle puisse dépasser le double du maximum de la peine encourue.

Les délits de vol, d'escroquerie et d'abus de confiance seront considérés comme étant, au point de vue de la récidive, le même délit.

Il en sera de même pour les délits prévus et punis par les articles 362 à 365 inclus.

Il en sera également ainsi pour les délits punis par les articles 389-1 à 389-5 inclus.

Le recel sera considéré, au point de vue de la récidive, comme le délit qui a procuré la chose recelée. »

-:-:-:-:-