N° 818 Le 5 novembre 2008

RAPPORT

SUR LE PROJET DE LOI, N° 818, CONCERNANT LES DELITS RELATIFS AUX SYSTEMES D'INFORMATION

(Rapporteur au nom de la Commission des Finances et de l'Economie Nationale : Monsieur Philippe CLERISSI)

Le projet de loi, n° 818, concernant les délits relatifs aux systèmes d'information a été transmis au Conseil National le 9 août 2006. Ce texte a été officiellement déposé au cours de la séance publique du 10 octobre 2006 et renvoyé le même jour pour examen devant la Commission de Législation. Compte tenu de la considérable charge de travail à laquelle cette dernière doit faire face, le présent projet de loi ainsi que son pendant, le projet de loi, n° 817, sur le commerce et la preuve électroniques, ont été, au vu de leur objet *« économique »,* transférés devant la Commission des Finances et de l'Economie Nationale lors de la séance publique du 3 avril 2007.

Sans revenir sur l'historique de l'examen de ce projet de loi, celui-ci venant d'être longuement détaillé dans le rapport établi sur le projet de loi n° 817, votre Rapporteur tient à rappeler que ce double dispositif législatif est destiné à constituer, avec les textes applicables à la protection des informations nominatives et aux jeux de hasard, un *« Code de l'économie numérique »*.

La révolution des technologies de l'information a changé radicalement la société et continuera vraisemblablement de le faire dans un avenir prévisible. Cette révolution a simplifié bien des tâches. Alors qu'initialement, seuls certains secteurs de la société avaient rationalisé leurs méthodes de travail en s'appuyant sur les technologies de l'information, il ne reste pour ainsi dire plus aucun secteur qu'elles

n'aient marqué de leur empreinte. Les technologies de l'information se sont immiscées, d'une manière ou d'une autre, dans tous les aspects des activités humaines.

Les technologies de l'information se singularisent notamment par l'impact qu'elles ont eu et continueront d'avoir sur l'évolution des technologies des télécommunications. La téléphonie classique, qui a pour objet de transmettre la parole, a été gagnée de vitesse par l'échange de vastes quantités de données, qui peuvent être vocales, documentaires, musicales, photographiques et cinématographiques. Cet échange ne se déroule plus uniquement entre les êtres humains mais intervient également entre êtres humains et ordinateurs ainsi qu'entre ordinateurs.

La généralisation de l'utilisation du courrier électronique et de l'accès à une multitude de sites Web par l'Internet sont des exemples de cette évolution qui a révolutionné la société.

La facilité avec laquelle on peut avoir accès à l'information contenue dans les systèmes informatiques, couplée aux possibilités pratiquement illimitées d'échange et de diffusion de cette information, par delà les distances géographiques, a déclenché une explosion de l'information disponible et des connaissances que l'on peut en tirer.

Instrument d'une puissance inouïe et source de valeurs nouvelles, l'informatique ne pouvait qu'intéresser le monde du crime.

Sous l'impulsion du droit international, l'informatique se voit dès lors progressivement encadrée dans les législations nationales par un droit soucieux de maîtriser les incidences et les éventuels dangers de cette technologie. On rappellera pour mémoire, entres autres instruments internationaux, la Convention des Nations-Unies relative aux droits des enfants, visant notamment à lutter contre la pédopornographie sur Internet, et, au niveau européen, la Convention du Conseil de l'Europe sur la cybercriminalité, signée à Budapest le 23 novembre 2001, premier texte à traiter des infractions pénales commises contre les réseaux informatiques ou à

l'aide de ceux-ci et qui vise à harmoniser les législations nationales pour lutter efficacement contre la criminalité dans le *« cyberespace »*.

Le projet de loi n° 818 s'inscrit dans ce mouvement en suivant les préconisations du Conseil de l'Europe, tout en s'inspirant des dispositions françaises prises en ce domaine. Le droit pénal monégasque devait en effet suivre le rythme des évolutions techniques, qui offrent des moyens extrêmement perfectionnés d'employer à mauvais escient les services du *« cyberespace »* et de porter ainsi atteinte à des intérêts légitimes. Le texte qui nous est soumis introduit donc dans notre Code pénal de nouvelles infractions, spécifiques aux nouvelles technologies, qui englobent les infractions informatiques les plus essentielles, à savoir les infractions contre la confidentialité, l'intégrité et la disponibilité des données et des systèmes informatiques, qui représentent les principales menaces. Il modifie également certains articles du Code de procédure pénale afin d'adapter les procédures d'investigation judiciaires aux nouvelles technologies.

Après ces quelques considérations d'ordre général, votre Rapporteur va s'attacher à rappeler les commentaires exprimés par la Commission des Finances et de l'Economie Nationale lors de l'examen de ce projet de loi.

* *
*

L'article premier du projet de loi insère une nouvelle Section IV au sein du Chapitre II du Titre II du Livre III du Code pénal, composée de nouveaux articles numérotés 389-1 à 389-12 relatifs aux infractions informatiques.

L'article 389-1 sanctionne les formes d'intrusions irrégulières dans tout ou partie d'un système d'information, que celles-ci résultent d'un accès ou d'un maintien illégal.

La nécessité d'une protection correspond à l'intérêt des organisations comme des particuliers de pouvoir diriger, exploiter et contrôler leurs systèmes sans

perturbation et entrave d'aucune sorte. La simple intrusion non autorisée, à savoir le *« piratage »*, le *« craquage »* ou l' *« intrusion illicite dans un système informatique »* peut créer des obstacles pour les utilisateurs légitimes des systèmes et des données et entraîner des dommages et des coûts élevés de reconstruction.

Ces intrusions peuvent en outre donner accès à des données confidentielles (mots de passe, informations sur le système cible, secrets), permettre d'utiliser le système gratuitement, voire encourager les pirates à commettre des types plus dangereux d'infractions en relation avec l'ordinateur, telles que la fraude informatique ou la falsification informatique.

Si le moyen le plus efficace de prévenir l'accès ou le maintien illégal est, naturellement, d'adopter et de mettre en place des mesures de sécurité efficaces, la parade ne saurait toutefois être complète sans la menace et l'application de mesures de droit pénal. L'interdiction pénale de l'accès non autorisé permet d'accorder au système et aux données une protection supplémentaire contre les risques susvisés.

L'acte répréhensible – délits d'accès ou de maintien – doit être commis *« sans droit »*, ce qui suppose que l'accédant ne respecte pas la *« règle du jeu »*, que celle-ci procède de la loi, du contrat ou de la volonté du *« maître du système »*. Il n'y a donc pas de pénalisation de l'accès autorisé par le propriétaire du système ou d'une partie de ce système ou par le détenteur d'un droit sur celui-ci (aux fins, par exemple, d'essai autorisé). Il n'y a pas non plus d'incrimination de l'accès à un système informatique lorsque cet accès est libre et public, puisqu'on y accède *« avec droit »*.

La question a été débattue de savoir si le système devait être nécessairement protégé par un dispositif de sécurité pour que l'acte d'accès tombe sous le coup de la loi pénale. La Commission a, après réflexion, opté pour que l'article répressif n'exige pas la violation délibérée d'un dispositif de sécurité dans la mesure où la détermination d'un seuil de sécurité, par ailleurs voué à une rapide obsolescence, serait délicate. En conséquence, il n'est pas nécessaire pour que l'infraction existe que l'accès soit limité par un dispositif de protection.

Votre Rapporteur rappelle que la présence d'un tel dispositif est néanmoins capitale. Elle manifeste à l'évidence que le système n'est pas librement accessible ; le fait de le forcer établit sans conteste le caractère irrégulier et délibéré de l'intrusion.

Les délits d'accès ou de maintien supposent naturellement un élément moral, l'intention. Il ne fait aucun doute en effet qu'un accès inopiné ou qu'un maintien inconscient ne saurait tomber sous le coup de la loi pénale.

La Commission tient en outre à rappeler que dans la loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives, une section spécifique est consacrée à la sécurité et à la confidentialité des traitements de données à caractère personnel. Les responsables de traitements sont ainsi tenus, sous peine de sanctions pénales, je cite, « *de prévoir des mesures techniques et d'organisation appropriées pour protéger les informations nominatives contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions d'informations dans un réseau, ainsi que contre toute autre forme de traitement illicite* ».

Il convient enfin de préciser que, conformément aux dispositions du cinquième alinéa du futur article 389-1, la peine est aggravée lorsqu'il résulte de l'accès ou du maintien irrégulier un dommage (suppression, modification des données informatiques, altération du fonctionnement du système). La Commission estime que le délit aggravé est ici un délit dans lequel le résultat de l'acte dépasse les prévisions de l'individu équivalant, pour schématiser, *« aux coups et blessures volontaires ayant entrainé la mort sans intention de la donner »*. Le dommage n'est en effet pas recherché. Le délit est donc non intentionnel car il y aurait sinon matière à application des articles suivants, qui incriminent les atteintes volontaires au fonctionnement du système (article 389-2) et aux données (article 389-3).

En ce qui concerne plus particulièrement la rédaction de l'article 389-1, la Commission a préféré la notion de *« frauduleusement »*, qui implique à la fois le

caractère volontaire de l'intrusion ou du maintien et la conscience de l'absence de droit, aux termes « *intentionnel et sans droit* ». Votre Rapporteur rappelle que depuis le vote de la loi, n° 1.349, du 25 juin 2008 modifiant le livre Premier du Code pénal, tous les crimes et les délits sont des infractions intentionnelles, sauf mention expresse contraire (imprudence, négligence) ; toute référence à l'élément moral devient donc inutile.

Compte tenu de ce qui précède, l'article 389-1 serait donc modifié comme suit :

« Quiconque aura accédé ou se sera maintenu, ~~intentionnellement et sans droit~~ ***frauduleusement****, dans tout ou partie d'un système d'information sera puni d'un emprisonnement de deux ans et de l'amende prévue au chiffre 3 de l'article 26.*

Est qualifié de système d'information, 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.

Est qualifié d'accès ~~intentionnel et sans droit~~ ***frauduleux****, toute action de pénétration ou d'intrusion irrégulière, par quelque moyen que ce soit, dans tout ou partie d'un système d'information 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'information ou des données qui y sont intégrées ou stockées.*

Est qualifié de maintien ~~intentionnel et sans droit~~ ***frauduleux****, tout maintien non autorisé dans un système d'information qui aurait pour conséquence de porter atteinte à l'intégrité ou à la confidentialité des données ou du système d'information.*

Lorsque l'accès ou le maintien ~~intentionnel et sans droit~~ ***frauduleux****, dans tout ou partie du système d'information, auront soit endommagé, effacé, détérioré, modifié, altéré ou supprimé des données informatiques contenues dans le système, soit entravé ou altéré le fonctionnement de tout ou partie de ce système, la peine sera*

portée à un emprisonnement de trois ans et à l'amende prévue au chiffre 3 de l'article 26.

Est qualifiée de données informatiques toute ou partie d'une information, quels qu'en soient la nature, le format et/ou le support initial, contenue dans un système d'information à quelque fin que ce soit. »

Afin d'harmoniser la rédaction de l'ensemble du texte, la Commission a également amendé le premier alinéa de l'article 389-2, les articles 389-3 à 389-5, le premier alinéa de l'article 389-6 ainsi que les articles 389-7 et 389-8 afin d'exiger un comportement frauduleux et supprimer, par voie de conséquence, l'expression *« intentionnellement et sans droit »*.

L'article 389-2 incrimine les atteintes volontaires au fonctionnement de tout ou partie d'un système d'information.

Afin d'éviter une redondance inutile dans la rédaction de l'article projeté, la Commission préconise de supprimer les précisions apportées dans le premier alinéa concernant les notions d'« *entrave* » et d'« *altération* », définies par ailleurs au sein des deux alinéas suivants.

Si la Commission a préféré éviter toute équivoque en exigeant que l'auteur de l'atteinte au fonctionnement du système ait agi frauduleusement, elle rappelle que l'entrave ou l'altération sont des actes intrinsèquement interdits, contrairement à l'accès ou au maintien (article 389-1), qui est un acte en lui-même régulier. Il en est de même pour l'introduction, la suppression et la modification de données (article 389-3), qui sont des actes inhérents à tout travail informatique.

Le premier alinéa de l'article 389-2 se lirait ainsi qu'il suit :

« Quiconque aura, ~~intentionnellement et sans droit~~ ***frauduleusement****, entravé ou altéré le fonctionnement de tout ou partie d'un système d'information~~, par l'introduction, la transmission, l'endommagement, l'effacement, la modification,~~*

~~*l'altération ou la suppression de données informatiques,*~~ *sera puni d'un emprisonnement de cinq ans et de l'amende prévue au chiffre 4 de l'article 26. »*

Par ailleurs, et contrairement à ce qui est énoncé dans l'exposé des motifs, la Commission considère que le nouvel article 389-2 du Code pénal ne peut viser le téléchargement illicite, qui ne peut être, selon elle, sanctionné que sur le fondement du délit de contrefaçon, conformément aux dispositions de la loi, n° 491, du 24 novembre 1948 sur la protection des œuvres littéraires et artistiques.

L'article 389-3 incrimine les actions sur les données. Cette disposition vise à assurer aux données informatiques une protection analogue à celle dont jouissent les biens corporels à l'encontre des dommages occasionnés délibérément. En l'occurrence, les intérêts juridiques protégés sont l'intégrité et le bon fonctionnement ou le bon usage de données informatiques enregistrées. Comme déjà indiqué, la Commission a, dans un souci d'harmonisation, remplacé l'expression *« intentionnellement et sans droit »* par l'adverbe *« frauduleusement »*. Outre que la suppression du terme *« intentionnellement »* est logique puisque le Code pénal tel que récemment modifié ne connaît de délits qu'intentionnels, sauf mention contraire expresse, l'exigence d'un comportement frauduleux se justifie car l'introduction, la suppression, la modification de données sont des actes en eux-mêmes normaux, inhérents à tout travail informatique. Ils ne doivent donc être punissables que s'ils sont commis avec fraude, ce qui suppose que l'auteur ait agi en sachant que l'acte n'était pas autorisé et en souhaitant obtenir ce résultat.

Reste cependant à souligner la difficulté qui réside dans la coexistence des deux infractions qu'ont pour objet de mettre en place les futurs articles 389-2 et 389-3, compte tenu de la proximité des agissements incriminés. Pour la Commission, lorsque l'action critiquable vise les données, la sagesse voudrait alors que le texte sanctionnant le fait de fausser le fonctionnement d'un système soit écarté, même si l'atteinte à l'intégrité des données se traduit par une altération du fonctionnement du système.

Sous le bénéfice de ces observations, l'article 389-3 serait donc modifié comme suit :

« Quiconque aura, ~~intentionnellement et sans droit~~ ***frauduleusement****, introduit, endommagé, effacé, détérioré, modifié, altéré ou supprimé des données informatiques ou agit* ***frauduleusement*** *de manière à modifier ou à supprimer leur mode de traitement ou de transmission sera puni d'un emprisonnement de cinq ans et de l'amende prévue au chiffre 4 de l'article 26. »*

Au sein de l'article 389-8, qui sanctionne l'escroquerie informatique, la Commission a souhaité supprimer les termes « *frauduleuse ou délictueuse* » afin d'éviter une redondance dans la rédaction. Le comportement frauduleux est en effet déjà exigé dans la formulation employée, à savoir l'*« intention d'obtenir sans droit un bénéfice économique »*. Cet article serait donc modifié comme suit :

« Quiconque aura, ~~intentionnellement et sans droit~~ ***frauduleusement****, causé un préjudice patrimonial à autrui par l'introduction, l'altération, l'effacement ou la suppression de données informatiques ou par toute forme d'atteinte au fonctionnement d'un système d'information, dans l'intention~~, frauduleuse ou délictueuse,~~ d'obtenir sans droit un bénéfice économique pour soi-même ou pour autrui sera puni d'une peine d'emprisonnement de cinq ans et de l'amende prévue au chiffre 4 de l'article 26. »*

La Commission a procédé à des modifications de pure forme au sein de l'article 389-11. Afin d'en faciliter la lecture et d'éviter qu'il y ait des erreurs de renvoi, elle propose de numéroter certains alinéas. En outre, dans un but d'harmonisation avec les dispositions notamment constitutionnelles, l'expression *« autorité judiciaire »* est remplacée par celle de *« pouvoir judiciaire »*.

Cet article deviendrait le suivant :

« Article 389-11 : 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 relative au trafic, sous réserve des dispositions des ***II, III, IV et V*** ~~*deuxième, troisième, quatrième et cinquième alinéas*~~*.*

Sont qualifiées de « données relatives au trafic » toutes données ayant trait à une communication passant par un système d'information, produites 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, la durée de la communication ou le type de service sous-jacent.

II - *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* ***du pouvoir*** ~~*de l'autorité*~~ *judiciaire d'informations, il peut être différé pour une durée maximale d'un an aux opérations tendant à effacer ou à rendre anonymes certaines catégories de données techniques. Une ordonnance souveraine, prise après avis de la Commission de contrôle des informations nominatives, détermine, dans les limites fixées par le* ***V*** ~~*cinquième alinéa*~~*, 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.*

III - *Pour les besoins de la facturation et du paiement des prestations de communications électroniques, 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 techniques qui sont déterminées, dans les limites fixées par le* ***V*** ~~*cinquième alinéa*~~*, 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.*

IV - *Sans préjudice des dispositions* ***du II et du III*** ~~*des deuxième et troisième alinéas*~~ *et sous réserves des nécessités des enquêtes judiciaires, les données*

permettant de localiser l'équipement terminal de l'usager ne peuvent ni être utilisées pendant la communication à des fins autres que son acheminement, ni être conservées et traitées après l'achèvement de la communication que moyennant le consentement de l'abonné, dûment informé des catégories de données en cause, de la durée du traitement, de ses fins et du fait que ces données seront ou non transmises à des fournisseurs de services tiers. L'abonné peut retirer à tout moment et gratuitement, hormis les coûts liés à la transmission du retrait, son consentement. L'utilisateur peut suspendre le consentement donné, par un moyen simple et gratuit, hormis les coûts liés à la transmission de cette suspension. Tout appel destiné à un service d'urgence vaut consentement de l'utilisateur jusqu'à l'aboutissement de l'opération de secours qu'il déclenche et seulement pour en permettre la réalisation.

***V -** Les données conservées et traitées dans les conditions définies aux **II, III, et IV** ~~troisième et quatrième alinéas~~ portent exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs et les prestataires de services, sur les caractéristiques techniques des communications assurées par ces derniers et sur la localisation des équipements terminaux. Elles ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications. La conservation et le traitement de ces données s'effectuent dans le respect des dispositions de la loi n° 1.l65 du 23 décembre 1993 ».*

Le reste sans changement.

Afin de tenir compte des nouvelles dispositions du Code pénal issues de la loi n° 1.349 du 25 juin 2008 modifiant le Livre premier du Code pénal, qui a introduit un principe général de responsabilité pénale des personnes morales, il a été procédé à une nouvelle formulation de l'article 389-12, qui se lirait comme suit :

« Article 389-12 : Les ***personnes morales peuvent être déclarées responsables pénalement, dans les conditions prévues par l'article 4-4, des délits prévus à la présente section.***

Les peines encourues par les personnes morales sont ~~*tribunaux pourront*~~

~~*prononcer, à l'encontre des personnes reconnues coupables des délits prévus à la présente section, les peines complémentaires suivantes*~~ *:*

1°) ***l'amende, suivant les modalités prévues par l'article 29-2 ;*** ~~*l'affichage ou la diffusion de la décision prononcée suivant les modalités prévues à l'article 30,*~~

2°) ***les peines mentionnées aux articles 29-3 et 29-4*** ~~*l'interdiction des droits civils, civiques et de famille suivant les modalités prévues à l'article 27,*~~

~~*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*~~ ».

———

Les articles 3 et 4 du projet de loi, qui introduisent respectivement dans le Code pénal deux nouveaux articles numérotés 294-3 et 294-4, n'ont plus lieu d'être compte tenu de la loi, n° 1.344, du 26 décembre 2007 relative au renforcement de la répression des crimes et délits contre l'enfant, votée en séance publique le 18 décembre 2007. En conséquence, les articles 3 et 4 du projet de loi sont purement et simplement supprimés. La numérotation des articles subséquents s'en trouve, par conséquent, décalée.

———

L'article 6 sanctionne pénalement la menace comportant une motivation raciste et xénophobe. Ainsi qu'indiqué dans l'exposé des motifs, la formulation employée est comparable à celle utilisée dans le cadre des diffamations et injures publiques, telles qu'incriminées respectivement par les articles 24 et 25 de la loi n° 1.299 du 15 juillet 2005 sur la liberté d'expression publique. La Commission a souhaité reprendre l'intégralité de la rédaction usitée dans la loi précitée afin que puisse être pénalement sanctionnée la menace proférée à raison de l'orientation

sexuelle, réelle ou supposée de la personne, sans qu'il soit nécessaire qu'elle soit proférée en public pour tomber sous le coup de la loi pénale. L'article 234-1 serait rédigé comme suit :

« *Article 234-1* : *Lorsqu'elles sont commises envers une personne ou un groupe de personnes à raison de leur origine ou de leur appartenance, réelle ou supposée, ou de leur non-appartenance à une ethnie, une nation, une race ou une religion déterminée*~~,~~ ***ou à raison de leur orientation sexuelle, réelle ou supposée****, les menaces prévues à l'article 230 sont punies d'un emprisonnement de deux à cinq ans et de l'amende prévue au chiffre 4 de l'article 26, celles prévues aux articles 231 et 232 sont punies d'un emprisonnement de un à cinq ans et de l'amende prévue au chiffre 4 de l'article 26, celles prévues à l'article 233 sont punies d'un emprisonnement de six mois à trois ans et de l'amende prévue au chiffre 3 de l'article 26, et celles prévues à l'article 234 sont punies d'un emprisonnement de six mois à trois ans et de l'amende prévue au chiffre 3 de l'article 26* ».

———

L'article 11, qui modifie la rédaction de l'actuel article 255 du Code de procédure pénale, vise à renforcer les attributions du Procureur Général en cas de flagrance, en lui permettant de procéder à la saisie des données informatiques dans le cadre de perquisitions.

La Commission s'est étonnée que le texte maintienne la référence obsolète « *à l'administration des télégraphes* ». La Poste étant aujourd'hui en charge des missions anciennement dévolues à l'administration des télégraphes, la Commission propose donc de modifier légèrement le troisième alinéa de l'article 255 du Code de procédure pénale qui se lirait comme suit :

« *Le procureur général peut rechercher et saisir à la poste les lettres et* ***lui*** *interdire* ~~*à l'administration des télégraphes*~~ *de délivrer au destinataire des télégrammes émanant de l'inculpé ou à lui adressés* ».

———

L'article 17 introduit un titre VIII nouveau au Livre I du Code de procédure pénale aux fins notamment de permettre à l'autorité judiciaire de faire appel aux services de toute personne apte à déchiffrer des données cryptées qui s'avèrent nécessaires à la manifestation de la vérité. Les auteurs du projet de loi semblent s'être inspirés des dispositions du Code de procédure pénale français, introduites par les lois n° 2001-1062 du 15 novembre 2001 et n° 2003-239 du 18 mars 2003 relatives à la sécurité quotidienne et à la sécurité intérieure.

Hormis une erreur de rédaction relevée au sein du premier alinéa du nouvel article 268-3, la future Section I du Titre VIII n'a fait l'objet d'aucune observation.

Le premier alinéa de l'article 268-3 serait modifié comme suit :

*« Dès l'achèvement des opérations ou dès qu'il apparaît que ces opérations sont techniquement impossibles ou à l'expiration du ~~délit~~ **délai** prescrit ou à la réception de l'ordre d'interruption émanant de l'autorité judiciaire requérante, les résultats obtenus et les pièces reçues sont retournés par la personne désignée pour procéder à la mise au clair des données chiffrées à l'autorité judiciaire requérante. Les résultats sont accompagnés des indications techniques utiles à la compréhension et à leur exploitation ainsi que d'une attestation visée par la personne désignée certifiant la sincérité des résultats transmis ».*

La future Section II, intitulée *« Des enquêtes »*, a quant à elle fait l'objet de plusieurs modifications.

La première, de pure forme, a été apportée au dernier alinéa de l'article 268-6, qui se lirait comme suit :

*« Le fait de refuser de répondre sans motif légitime à ces réquisitions est puni d'une peine d'emprisonnement d'un an prévue à l'article 25 **du Code pénal** et de l'amende prévue au chiffre 4 de l'article 26 **dudit Code ».***

La deuxième a pour objet de pouvoir rechercher la responsabilité pénale des personnes morales qui refuseraient de répondre sans motif légitime à toute réquisition de l'officier de police judiciaire prise sur le fondement de ces dispositions. S'il ne fait aucun doute, à la lecture de l'exposé des motifs, que le contrevenant peut être une personne morale, les peines prévues par le texte ne sauraient être prononcées qu'à l'égard d'une personne physique.

Enfin, la Commission des Finances et de l'Economie Nationale a souhaité que la Commission de contrôle des informations nominatives (CCIN) intervienne dans la détermination des garanties nécessaires à l'équilibre du dispositif. Elle propose donc qu'un texte d'application, pris après avis de la CCIN, détermine les catégories d'organismes susceptibles de faire l'objet de réquisitions télématiques ou informatiques et fixe les modalités précises d'interrogation, de transmission et de traitement des informations requises.

Au vu de ces observations, il est proposé d'introduire *in fine* de l'article 268-6 deux alinéas nouveaux rédigés comme suit :

« Les personnes morales peuvent être déclarées responsables pénalement, dans les conditions prévues par l'article 4-4 du Code pénal, de l'infraction prévue à l'alinéa précédent. La peine encourue par les personnes morales est l'amende suivant les modalités prévues par l'article 29-2 du Code pénal. »

« Une ordonnance souveraine, prise après avis de la Commission de contrôle des informations nominatives, détermine les catégories d'organismes visés au premier alinéa ainsi que les modalités d'interrogation, de transmission et de traitement des informations requises. »

* *
*

Ce projet de loi, qui tient compte de la problématique des nouvelles technologies en droit pénal, introduit dans notre Code pénal de nouvelles infractions plus spécifiquement adaptées au monde de l'informatique et des réseaux. Il tend également à modifier certains articles du Code de procédure pénale afin d'adapter les procédures d'investigation judiciaires aux nouvelles technologies. Votre Rapporteur vous invite donc à voter en faveur de ce projet de loi, tel qu'amendé par la Commission des Finances et de l'Economie Nationale.