F-1-02
15 mai 2006

Reçu au Conseil National
le 9 août 2006
Pdl n° 818

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

EXPOSE DES MOTIFS

L'économie mondiale est aujourd'hui marquée par l'apparition d'une nouvelle composante majeure : l'économie numérique. Toutefois, le développement des activités qui s'y rapportent, fondé sur la mondialisation de la communication électronique, est consubstantiel à l'émergence de formes nouvelles et spécifiques de criminalité. Tombant sous la dénomination générique de cybercriminalité, l'une de leurs manifestations les plus insupportables consiste notamment dans les atteintes à caractère sexuel visant les enfants et commises au moyen des nouvelles technologies.

Il ne peut être admis, dans un État constitutionnellement attaché au respect des libertés et des droits fondamentaux comme la Principauté, que le progrès technologique et la recherche de l'intérêt économique s'opèrent au détriment de ces droits naturels et essentiels. Tel est également le sentiment de la communauté internationale organisée qui s'est rapidement dotée de normes et d'instruments propres à faire face à ce péril des temps modernes.

C'est ainsi que pour ce qui est de l'Organisation des Nations Unies, peuvent être citées avec intérêt : la Convention relative aux droits de l'enfants de New-York du 26 janvier 1990, le protocole additionnel à la Convention de Palerme des Nations-Unies contre la criminalité transnationale organisée visant à prévenir réprimer et punir la traite des personnes, en particulier des femmes et des enfants.

En ce qui concerne l'Union européenne, il convient également de rappeler : les Résolutions du Parlement européen en 1996, 1997 et 1998 ; la Conférence internationale sur la lutte contre la pédopornographie sur Internet (Vienne, 29 septembre – 1er octobre 1999) ; la Décision du Conseil relative à la lutte contre la pédopornographie sur Internet du 29 mai 2000. Il importe également de mentionner la décision 276/1999CE du parlement Européen et du Conseil du 25 janvier 1999, qui adopte un plan d'action communautaire pluriannuel visant à promouvoir une utilisation plus sûre d'Internet par la lutte contre les messages à contenus illicites et préjudiciables diffusés sur les réseaux mondiaux. Sont ainsi encouragés l'auto-réglementation de l'industrie d'*Internet*, le développement de dispositifs de filtrage et enfin la création d'un réseau européen de *hotlines*.

Quant au Conseil de l'Europe, peuvent être mentionnées avec pertinence : la Recommandation 91-11 sur l'exploitation sexuelle, la pornographie, la prostitution, le trafic d'enfants et de jeunes adultes ; la Recommandation sur la lutte contre la traite des êtres humains aux fins d'exploitation sexuelle adoptée par le Comité des Ministres en mai 2000.

Enfin, au titre des textes dont la précellence est avérée dans la lutte contre ces nouvelles formes de délinquance, il convient de faire état de la Convention du Conseil de l'Europe sur la cybercriminalité. Ce texte constitue le premier traité international sur les infractions pénales commises contre les réseaux informatiques ou à l'aide de ceux-ci. Ce texte permet un traitement efficace des agissements des auteurs d'infractions commises sur la toile. Cette convention, signée à Budapest le 23 novembre 2001 par 30 états vise à harmoniser les législations nationales pour mieux lutter contre la cybercriminalité.

Le Gouvernement Princier a souhaité inscrire la législation monégasque dans ce mouvement mondial.

Ainsi le présent projet de loi figure-t-il au cœur d'un triptyque – constitutif *de facto* d'un « *Code du numérique* » – en complément de projets de lois parallèles et relatifs au traitement des informations nominatives ainsi qu'à la protection renforcée des opérateurs économiques du secteur numérique.

Il sera rappelé, pour mémoire, que le présent projet de loi a fait l'objet d'un premier dépôt sur le bureau du Conseil National, le 21 juin 2002, suivi d'un retrait justifié d'une part aux fins d'adaptation du texte, en particulier du fait du développement exponentiel des normes européennes et internationales visant à appréhender et juguler le phénomène de la cybercriminalité et, d'autre part, dans le sillon de l'adhésion de la Principauté au Conseil de l'Europe et de l'engagement subséquemment pris d'adhérer à la convention –précitée – de Budapest dans les cinq ans.

La problématique des nouvelles technologies en droit pénal s'articule autour de deux axes complémentaires qui permettent, dans un premier temps, de cerner les caractéristiques criminelles nécessaires à la compréhension du phénomène délictuel à juguler, et dans un second temps, de configurer la répression y afférente.

Cibles nouvelles de délinquance, les nouvelles technologies elles apparaissent d'abord comme l'objet de l'infraction. Il est donc impératif de pourvoir à leur protection, notamment au regard des les enjeux majeurs qu'elles représentent.

Moyens nouveaux de délinquance, elles portent, en tant que *modus operandi* moderne au service d'infractions classiques, une dangerosité significative, qui se mesure aux facilités qu'elles procurent aux délinquants et à la gravité des infractions dont elles peuvent être le vecteur. Le primat d'une répression opérationnelle doit par conséquent conduire à la mise en place d'une réponse pénale adaptée.

Ainsi le Gouvernement Princier s'est-t-il attaché, par le truchement du présent projet de loi, à la mise en œuvre d'une répression efficiente et efficicace, tendant ainsi à la combinaison de ces deux lignes directrices. La réponse pénale est donc duale.

Le phénomène criminel à combattre est quant à lui éminemment étendu et protéiforme. La criminalité en cause est en effet à la fois spécifique par son ampleur, par sa diversité et par la pluralité des agents pénaux.

De fait, en contrepoint d'une démocratisation de l'accès à l'informatique et de la globalisation de l'interconnexion aux réseaux, les comportements délictueux commis par le biais des systèmes d'information se multiplient, se propagent, dépassant les frontières, conférant ainsi à la cybercriminalité une ampleur sans équivalence. De tels actes de piratage ou sabotage informatique peuvent donc constituer un frein au développement du commerce électronique. De tels agissements sont également susceptibles de constituer une atteinte aux droits des personnes dans leur vie privée, leurs droits d'auteur, leurs droits de propriété.

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 d'information 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 qui cherche à détourner des milliards en pénétrant frauduleusement les systèmes d'information d'une grande banque.

Aussi Importe-t-il d'indiquer d'ores et déjà, avant que de passer à l'explicitation détaillée des articles, les différentes manifestations de délinquance envisagées et les réponses auxquelles tend le présent projet de loi.

En outre, force est aujourd'hui de constater que Internet est de plus en plus utilisé comme un moyen d'offrir et de diffuser de la pornographie enfantine. S'en infère la nécessité, pour la protection de l'enfance, de prendre les mesures qui permettent d'enrayer ce phénomène, dit de « pédopornographie ».

Le projet de loi présente donc d'importantes dispositions relatives à la lutte contre la pornographie enfantine, notamment celle commise ou facilitée par les réseaux de communication comme Internet, afin de renforcer les mesures de protection des mineurs contre l'exploitation et les abus sexuels de toutes sortes commis à leur encontre.

Si les dispositions projetées procèdent du contexte international de lutte contre la pédopornographie, à l'appui des textes cités à titre liminaire, il importe à cet égard de mentionner que lesdites dispositions s'inscrivent dans le sillage des actions menées par l'Association Mondiale des Amis de l'Enfance (A.M.A.D.E.), laquelle, sous la présidence de Son Altesse Royale la Princesse Caroline de Hanovre, a initié une campagne juridique pour obtenir la qualification des crimes les plus graves commis contre les enfants, comme crimes contre l'humanité.

Lors de la tenue récente en Principauté – en date des 4 et 5 avril dernier – d'une conférence du Conseil de l'Europe, Son Altesse Royale la Princesse Caroline de Hanovre a en effet souligné « *l'éminente nécessité d'une amélioration de la défense des droits des enfants* » ceci, dans le cadre d' « *un projet du Conseil de l'Europe destiné à lutter contre les risques d'abus sexuel contre les risques d'abus sexuel par le biais des courriers électronique* ». En outre, ces orientations font écho à la réunion de la Commission permanente de l'Assemblée Parlementaire du Conseil de l'Europe – tenue en Principauté au mois de septembre dernier – à l'occasion de laquelle Elle avait souligné le nécessaire « *besoin d'un outil juridique commun sur les questions de cybercriminalité* ».

Si la répression de la cyberciminalité dirigée à l'encontre des enfants – et plus spécifiquement de la pédopornographie – est d'ores et déjà intégrée au cœur du présent projet de loi, il convient au demeurant d'indiquer que le renforcement de la répression de l'ensemble des comportements criminels utilisant ou visant les enfants a récemment fait l'objet d'une proposition de loi, n° 184, en date du 28 mars 2006.

Au titre des atteintes plus générales aux droits de l'homme, ill convient de mentionner, dans une perspective d'intelligibilité et de lisibilité du processus législatif, que dans sa version initiale, les infractions pouvant être commises par voie de communication au public faisaient l'objet de plusieurs articles projetés, lesquels, d'une part, intègraient *expressis verbis* le nouveau vecteur des communications électroniques et, d'autre part, infèraient certaines modifications du droit positif consacré à la liberté de la presse et d'expression publique.

Or, ces dispositions ne pouvaient être maintenues en l'état, dans la mesure où la matière spécifique est désormais régie par la loi n° 1.299 du 15 juillet 2005 sur la liberté d'expression publique, laquelle a concomitamment conduit à l'abrogation de l'Ordonnance du 3 juin 1910.

D’un point de vue substantiel, il importait donc de supprimer les dispositions qui érigeaient en infraction plusieurs comportements commis par le truchement des communications électroniques : diffusion et/ou mise à disposition du public de matériel raciste et xénophobe, injure et/ou diffamation xénophobe(s), etc. Dans la mesure où ces comportements délictueux ont d’ores et déjà été appréhendés par la législation désormais en vigueur en Principauté, à travers la loi n° 1.299 du 15 juillet 2005, les dispositions prévues *ab initio* ne pouvaient être conservées.

Pour ce qui est des atteintes à la vie privée des personnes au moyen des nouvelles technologies, les dispositions protectrices 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.

En matière d’atteintes aux biens, 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. Aussi, à l’effet de renforcer la sécurité juridique des réseaux, le présent projet de loi incrimine les diverses formes de fraude informatique parmi lesquelles, à titre d'exemple, l'accès et le maintien intentionnel et sans droit dans un système d'information, l'entrave ou l'altération du fonctionnement de ce système, ou bien encore l'atteinte aux données informatiques.

En outre, si certaines 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, d'autres, en revanche, s'avèrent insuffisantes pour s’appliquer aux nouvelles technologies.

Le présent projet de loi a donc 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, outre les contenus illicites, les atteintes irrégulières aux systèmes d'information et aux données qu'ils contiennent.

Enfin, de nombreuses dispositions du projet de loi tendent à une modification substantielle du Code de procédure pénale, dans la perspective d'une adaptation des procédures d'investigations judiciaires aux nouvelles technologies. Tel est notamment le cas des dispositions relatives aux saisies pouvant être effectuées par le juge d'instruction, modifiées aux fins de permettre la mise sous main de justice des supports informatiques et données électroniques.

Il apparaît pertinent de souligner que ces dispositions figurent également au sein du projet de loi portant nouveau Code de procédure pénale. Si ce projet opère la refonte intégrale de l'actuelle codification, la reprise prospective des dispositions sus-mentionnées sera de nature à permettre, dans un souci de cohérence législative, la pérennisation de tout acquis et modifications normatives jusqu'à son entrée en vigueur.

En conclusion, les dispositions présentées permettent ainsi de compléter et renforcer l'action gouvernementale entreprise dans d'autres domaines du droit des nouvelles technologies, tels que, par exemple, le commerce électronique, ou les casinos virtuels, 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 :

L'article premier prévoit l'insertion des infractions relatives aux systèmes d'information dans la classification typologique et la numérotation actuelle du Code pénal.

Ces incriminations concernant des fraudes aux systèmes d'information répriment des délits contre les biens.

De ce fait, les nouvelles dispositions s'intègrent au Livre III du Code pénal qui traitent « *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'information* », laquelle comporte les articles 389-1 à 389-12, projetés, du Code pénal.

L'article 389-1 projeté, introduit par l'article premier du projet de loi, sanctionne les formes d'intrusions irrégulières dans tout ou partie d'un système d'information, qu'elles résultent d'un accès intentionnel et sans droit ou d'un maintien intentionnel et sans droit.

Ces délits différents peuvent, le plus souvent, être commis concomitamment mais pas obligatoirement. Il est en effet parfaitement envisageable qu'en dépit d'un accès autorisé, une personne se maintienne néanmoins frauduleusement dans tout ou partie d'un système d'information.

L' accès intentionnel et sans droit dans tout ou partie d'un système d'information vise toute forme de pénétration matérielle et active dans un système.

Ainsi, il suffit d'établir une communication avec le système pour que le délit soit consommé, peu importe que l'accédant ne parvienne pas à ses fins, par exemple la captation d'éléments du système, ou n'utilise pas effectivement ce système, par une opération de manipulation informatique ou de toute autre manœuvre permettant de communiquer avec le système, y compris à distance.

Sont donc visés tous les modes de pénétrations irréguliers d'un système tels que, par exemple, la composition d'un code d'accès obtenu irrégulièrement, le déplombage d'un code d'accès, son décryptage, toute autre manipulation tendant à le « casser », l'utilisation des faiblesses du système de contrôle d'accès, l'insertion d'un cheval de Troie ou d'une bombe logique. Il est remarquable que ces deux derniers modes de pénétrations peuvent s'avérer extrêmement préjudiciables au système, de par leur mode même de fonctionnement. Ainsi peut-il être indiqué, au titre d'explicitations techniques, que le « *cheval de Troie* » est un programme caché dans un autre qui exécute des commandes, donnant généralement un accès à la machine sur laquelle il est exécuté en ouvrant une porte dérobée (fréquemment traduit en anglais par *backdoor*). Les « *bombes logiques* » quant à elles désignent des dispositifs programmés dont le déclenchement s'effectue à un moment déterminé en exploitant la date du système, le lancement d'une commande, ou n'importe quel appel au système.

Par ailleurs, l'accès à certaines composantes du système, telles qu'un matériel, un logiciel, certaines données, suffit à constituer l'infraction.

En outre, l'accès doit être sans droit c'est-à-dire par une personne qui n'a pas le droit d'accéder au système ou en tout cas pas de la manière dont elle y a accédé.

Cet élément moral implique que le contrevenant ait agi intentionnellement, savoir 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* ».

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

Cet article sanctionne donc les formes d'intrusions irrégulières et de maintien irrégulier dans tout système d'information, qu'ils résultent d'un accès illicite ou d'un maintien interdit dès lors que le contrevenant a agi frauduleusement. Dès lors, l'accès inopiné ou le maintien inconscient ne sont pas poursuivis.

En revanche, le seul agissement, le seul 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.

De même, l'intention de nuire, même si elle peut se rencontrer, n'est pas indispensable à la réalisation de l'infraction. La conscience de transgresser un interdit suffit à caractériser l'élément moral.

Lorsque l'accès et/ou le maintien intentionnels et sans droit causent un dommage au système, le délit est alors plus sévèrement réprimé. Le dommage s'entend de manière large : il peut s'agir d'une atteinte aux données ou d'une altération du fonctionnement du système.

Enfin, pour une meilleure interprétation du présent projet de loi, cet article donne une définition du système d'information et des données informatiques qui se veulent les plus larges possibles.

L'article 389-2 du Code pénal, introduit par l'article premier du projet de loi, permet de réprimer toutes les formes d'atteinte volontaire au fonctionnement d'un système d'information, consécutives ou non à un accès ou à un maintien frauduleux, et ce, quel que soit le moyen matériel ou intellectuel utilisé.

L'emploi du terme « *fonctionnement* » signifie que ce sont toutes les fonctions du système qui sont ainsi visées par ce texte.

La notion d'entrave peut recouvrir les situations les plus diverses comme par exemple :

l'impossibilité totale d'utiliser un système : blocage d'un code d'accès, paralysie du fonctionnement d'un système à cause d'un virus ;

le ralentissement ou une diminution de la capacité d'un système ;

le dysfonctionnement peut se produire à intervalle régulier comme par exemple à cause de l'introduction d'une bombe logique ;

l'entrave peut ne concerner que quelques utilisateurs seulement et non leur totalité.

La notion d'altération du système vise, quant à elle, l'hypothèse selon laquelle le résultat produit par le système est différent de ce qu'il aurait dû être. L'exemple du téléchargement illicite peut à cet égard être donné.

Les techniques qui permettent ainsi d'aboutir à un résultat différent de celui auquel le maître du système est en droit de s'attendre sont très variées et rejoignent celles qui peuvent également être employées dans le cas de l'entrave au fonctionnement ci-dessus décrite : il s'agit par exemple des chevaux de Troie, des virus, des bombes logiques ou toute autre forme de sabotage informatique.

Il peut également s'agir de procédés techniques comme la saturation des capacités d'accès ou l'utilisation d'une carte d'interruption.

Concernant l'élément moral d'une telle infraction, il est prévu que son auteur agisse intentionnellement et sans droit c'est-à-dire qu'il ait conscience de l'entrave ou de l'altération du système qu'il engendre.

Les dispositions projetées de l'article 389-3 du Code pénal ont pour objet de sanctionner pénalement l'action frauduleuse sur les données contenues dans un système d'information.

Les pratiques incriminées sont nombreuses et visent toutes les formes d'introduction de modifications ou de suppression de données, 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.

Ainsi, sont réprimés le fait d'incorporer de nouveaux caractères informatiques sur un support du système et le fait de supprimer des données par effacement, écrasement, ou bien encore par déplacement hors du système ou dans une zone non autorisée.

Cet article vise également les modifications de données qui, en général, se traduisent également par une introduction ou une suppression de celles-ci.

Par ailleurs, le texte incrimine l'action qui consiste à agir de manière à modifier ou à supprimer le mode de traitement ou de transmission des données informatiques. Cette disposition vise tout spécialement l'introduction d'un virus qui 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.

Le délit d'atteinte frauduleuse aux données requiert un élément moral comme l'indique le terme « *intentionnellement* » qui consiste pour l'auteur d'une telle infraction à avoir conscience qu'il agit frauduleusement sur les données.

L'article 389-4 du Code pénal, tel qu'inséré par l'article premier du projet de loi, vise celui qui se sera rendu coupable d'utiliser en connaissance de cause, savoir en sachant qu'elles ont fait l'objet d'atteintes irrégulières, les données altérées, falsifiées ou contrefaites.

Cette incrimination se justifie par le fait que celui qui use de données informatiques endommagées n'est pas forcément le même que celui qui se rend coupable de l'infraction d'atteinte aux données, décrite à l'article précédent.

Les dispositions projetées de l'article 389-5 du Code pénal ont pour objectif de protéger le droit au respect des données transmises en particulier par courriers électroniques ou fichiers informatiques. Toutes les formes de transfert électronique des données sont concernées.

L'interception réalisée par des « *moyens techniques* » recouvre à la fois l'écoute, le contrôle, la surveillance du contenu et l'obtention du contenu directement, c'est-à-dire par accès au système d'information, ou indirectement, par l'emploi de dispositifs d'écoute.

L'enregistrement des données peut également être sanctionné par l'application de ce texte.

Les « *moyens techniques* » correspondent soit à des dispositifs techniques connectés aux lignes de transmission, soit à des dispositifs de collecte et d'enregistrement de communications sans fil. Il peut s'agir par exemple de logiciels ou de codes d'accès.

L'infraction s'applique aux transmissions non publiques de données informatiques, ce terme qualifiant la nature du moyen de transmission et non la nature des données transmises.

Sont donc visées les données qui sont considérées par les personnes concernées comme devant être tenues secrètes. Le terme « *non publiques* » peut donc s'appliquer aux communications effectuées par le biais des réseaux publics ou bien encore aux communications de salariés à des fins professionnelles ou non pourvu que les participants souhaitent communiquer de manière confidentielle.

L'élément moral requiert d'agir intentionnellement et sans droit, savoir en ayant conscience de transgresser un interdit.

Ainsi, par exemple, l'utilisation des « *cookies* » ne devrait pas tomber sous le coup de la loi car cette pratique ne correspond pas en principe à une utilisation sans droit.

L'article 389-6 projeté du Code pénal réprime la commission intentionnelle d'actes illicites spécifiques se rapportant à certains dispositifs, tels que des programmes informatiques, ou données d'accès, utilisés abusivement dans le but de commettre des atteintes à un système d'information.

La commission de ces infractions nécessite en effet le plus souvent l'emploi d'outils de piratage ce qui peut conduire à l'existence d'un marché noir de la production et de la mise à disposition de ces outils. Une telle disposition permet donc de s'attaquer directement à la source de bons nombres d'atteintes à des traitements automatisés de données.

Concernant la terminologie employée, « *diffuser* » désigne l'action qui consiste à transmettre à autrui un dispositif, un mot de passe ou bien encore un code d'accès, tandis que « *mettre à disposition* » vise l'action qui consiste, quant à elle, à mettre en ligne un dispositif, un mot de passe, ou un code d'accès afin qu'ils soient utilisés par autrui.

Le fait que le dispositif soit « *principalement* » conçu ou adapté pour permettre la commission d'un délit relatif à un système d'information signifie que les programmes ou les données informatiques ne doivent pas avoir été spécialement ou exclusivement créés pour réaliser une telle infraction.

Une approche restrictive de la notion de dispositif « *conçu ou adapté* » rendrait pratiquement impossible l'application de ce texte.

Concernant l'élément moral, l'infraction doit être commise intentionnellement et sans droit. A cette intention s'ajoute celle spécifique qui consiste à utiliser ce dispositif ou ce mot de passe ou bien encore le code d'accès pour commettre l'une quelconque des infractions prévues aux articles précédents.

Dès lors, parce qu'ils relèvent a priori de l'exercice d'un droit, les outils créés pour l'essai autorisé ou pour la protection d'un système d'information ne tombent pas, quant à eux, dans le champ d'application de cette infraction.

Il en est ainsi par exemple des dispositifs permettant d'analyser les réseaux conçus par des professionnels pour vérifier la fiabilité des produits informatiques ou pour contrôler la sécurité des réseaux.

L'article premier du projet de loi introduit également un nouvel article 389-7 au Code pénal, qui concerne la falsification informatique, et s'applique aux données informatiques formant un document public ou privé ayant des effets juridiques.

La falsification informatique consiste dès lors en la création ou la modification sans autorisation des données enregistrées de manière à ce qu'elles acquièrent une valeur probante différente pouvant, dans le cadre de transactions juridiques, porter atteinte à l'authenticité des informations fournies par ces données et donner lieu à des tromperies.

Cette tromperie quant à l'authenticité peut porter sur l'auteur du document en cause mais aussi sur la véracité des informations qu'il contient.

Par ailleurs, sont visées par ce texte les formes les plus variées de falsification informatique : ainsi, l'introduction non autorisée de données vise la fabrication d'un faux document alors que l'altération, l'effacement ou la suppression des données informatiques sont des opérations ultérieures entreprises sur un document existant constituant de ce fait une falsification de document authentique.

Les dispositions projetées de l'article 389-8 du Code pénal mettent en exergue le fait que les nouvelles technologies multiplient les possibilités de commettre des infractions économiques comme la fraude.

Le comportement frauduleux le plus fréquent concerne ainsi l'escroquerie à la carte bancaire dont l'ampleur constitue un frein au développement du commerce électronique.

Cet article a donc pour objet de rendre passible d'une sanction pénale toute manipulation abusive effectuée au cours d'un traitement de données en vue d'effectuer un transfert illicite de propriété.

Cette manipulation informatique frauduleuse est entendue fort largement car elle recouvre toute sorte d'agissements tels que l'introduction, l'altération, la suppression de données informatiques, ainsi que toute forme d'atteinte au fonctionnement d'un système d'information.

Elle doit occasionner un préjudice patrimonial à la victime de l'infraction. Cette notion de préjudice devant s'entendre largement car elle vise, outre le numéraire, toutes les immobilisations corporelles ou incorporelles ayant une valeur économique.

L'auteur de l'infraction doit en retirer, quant à lui, sans droit, un bénéfice économique que ce soit pour lui-même ou pour autrui.

Enfin, l'infraction doit être commise intentionnellement. Autrement dit, la malhonnêteté caractérise l'élément moral de l'infraction.

L'article 389-9 du Code pénal, introduit par l'article premier du projet de loi, incrimine l'association de malfaiteurs informatiques.

Les termes « *groupement* » et « *entente* » ne sont pas définis de manière à ce que cet article puisse s'appliquer, dès lors que le groupement ou l'entente résulte d'un simple concours de volonté.

Le nombre de participants est indifférent, et il n'est pas nécessaire que le groupement ou l'entente ait été dès l'origine spécialement formé pour commettre un délit informatique.

Ainsi, les participants à un groupement ou une entente dont l'activité serait licite à sa création peuvent tomber sous le coup de la loi si ce groupement ou cette entente glisse peu à peu vers la délinquance informatique.

L'élément matériel doit, sauf en cas de recel, se traduire par un ou plusieurs faits produits en amont de la commission des infractions. Il peut s'agir par exemple de divers échanges d'informations sur la manière d'introduire un virus, de « *casser* » un code, ou bien encore d'accéder à un système d'information.

L'élément moral de cette infraction requiert une participation volontaire au groupement ou à l'entente ce qui suppose la conscience de son activité ou de son objet et la volonté de participer à la commission d'un délit informatique.

Cette disposition permet donc de réprimer les comportements informatiques délictueux autres que ceux de l'auteur principal et que la seule infraction consommée.

Pour assurer l'efficacité de la répression en matière de délinquance informatique, l'article 389-10 projeté du Code pénal dispose que la tentative est punissable et fait encourir les mêmes peines que la commission elle-même des délits informatiques.

Les dispositions projetées de l'article 389-11 du Code pénal imposent aux opérateurs de communication 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. Un droit à l'anonymat des personnes sur les réseaux est ainsi consacré compte tenu de leur extrême traçabilité.

Le manquement à cette obligation est sanctionné 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 opérateurs peuvent également réaliser un traitement de données relatives au trafic pour fournir aux abonnés qui y consentent d'autres services à valeur ajoutée pour une période qui ne peut excéder celle des relations contractuelles.

En outre, cet article traite des conditions dans lesquelles les données permettant de localiser l'équipement terminal de l'usager peuvent être utilisées, conservées et traitées. Ainsi, elles ne peuvent être utilisées pendant la communication à des fins autres que son acheminement.

Par ailleurs, elles ne peuvent être conservées et traitées après l'achèvement de la communication qu'avec le consentement de l'abonné. Il s'agit d'un consentement éclairé en ce sens que l'abonné doit être informé des catégories de données en cause, de la durée du traitement, de sa finalité et de la transmission éventuelle de ces données à des tiers. Ce consentement doit être révocable à tout moment et sans frais pour l'abonné.

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

Enfin, l'article premier du projet de loi introduit au cœur du Code pénal un nouvel article 389-12, lequel 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.

L'article 2 du projet de loi prévoit que les délits relatifs aux systèmes d'information sont considérés, du point de vue de la récidive, comme étant le même délit.

Les articles 3 et 4 incriminent tous les aspects de la production, de la possession et de la diffusion de pornographie enfantine afin de protéger les mineurs contre toute forme d'exploitation sexuelle.

L'article 3 sanctionne plusieurs comportements dont notamment le fait de fixer, enregistrer, produire de la pornographie enfantine.

Sont également visés, pour lutter contre la propagation d'un tel phénomène, toutes les formes de diffusion et de transmission de la pornographie enfantine, y compris le fait d'offrir (prélude à la fourniture effective), le fait d'importer, d'exporter, de faire importer, de faire exporter, de se procurer (ce qui concerne le téléchargement) de la pornographie enfantine.

Enfin, cet article incrimine le fait de posséder de la pornographie enfantine et vise ainsi directement les pédophiles, dernier maillon de cette chaîne de la délinquance pédopornographique.

Il prévoit une aggravation des peines encourues lorsqu'un réseau de communications a servi pour la diffusion de l'image ou de la représentation d'un mineur.

Cet article donne également une définition de la notion d'« *images à caractère pornographique* » qui correspond à :

- l'image ou la représentation d'un mineur, ou d'une personne pouvant être confondue avec un mineur,

- une image réaliste, savoir ne représentant pas en fait un mineur, comme par exemple une image fabriquée par ordinateur, se livrant à un comportement sexuellement explicite.

Quant à l'article 4, il réprime la fabrication, le transport ou la diffusion d'un message à caractère violent ou pornographique ou attentatoire à la dignité humaine susceptible d'être vu ou perçu par un mineur par quelque moyen que ce soit et quel qu'en soit le support.

Aucune différence n'est ainsi faite selon la nature de ce dernier. Il peut donc s'agir, par exemple, de magazines, de photographies, de films, de disques compact (CD-Rom), d'un site Internet, accessibles au mineurs.

Sont ainsi visés les messages violents, dégradants, reflétant des déviations, des perversions sexuelles ou avilissantes, contraires aux bonnes mœurs, voire à l'ordre public, notamment si des mineurs sont en cause, ou bien des scènes sexuelles non simulées.

En revanche, lorsque de tels supports font l'objet d'un commerce par correspondance ou d'une correspondance privée, y compris électronique, l'infraction n'est pas constituée si l'émetteur du message n'a pas l'intention d'envoyer ce message à un mineur.

L'article 5 est porteur d'une innovation significative. Avec l'apparition et le développement des nouvelles technologies de l'information et de la communication, il est devenu nécessaire de modifier l'article 15 de la loi n°1.299 du 15 juillet 2005 sur la liberté d'expression publique, lequel incrimine les provocations aux crimes et délits, les délits contre la chose publique, les délits contre les personnes comme la diffamation ou l'injure, afin d'étendre son champ d'application aux moyens de communication au public par voie électronique. En effet, nombreux sont les exemples de diffamation, d'injure, ou bien encore de propos xénophobes sur Internet.

Les articles 6 et 7 ont pour objectif de modifier les articles 230 et 234 du Code pénal afin d'inclure dans le champ de cette incrimination une nouvelle forme d'expression possible de la menace, c'est-à-dire par le biais des réseaux de communication comme l'Internet étant précisé que, à la différence de l'injure et de la diffamation, la menace ne doit pas avoir nécessairement un caractère public.

Enfin, l'article 8 sanctionne pénalement la menace comportant une motivation raciste et xénophobe et s'inscrit dans le cadre de la lutte contre le cyberterrorisme dont les ressorts peuvent reposer, pour partie, sur de telles considérations.

Ainsi, la menace doit être commise 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 réelle ou supposée. Il convient au demeurant de rappeler que la formulation ainsi 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.

Comme pour l'article précédent, la menace à caractère raciste et xénophobe ne doit pas nécessairement être proférée en public pour être sanctionnée pénalement.

Les articles 9 à 19 modifient le Code de procédure pénale en créant de nouvelles dispositions et en modifiant certaines déjà existantes afin de doter les autorités judiciaires des pouvoirs leur permettant d'enquêter et de poursuivre toute infraction commise ou facilitée par l'utilisation d'un système d'information et de collecter les preuves électroniques qu'ils contiennent.

Les articles 9 à 12 visent à renforcer les attributions du juge d'instruction en lui permettant de procéder, dans le cadre de perquisitions, à la saisie des données informatiques utiles à la manifestation de la vérité et complètent à cette fin les articles 100, 103, 105, et 106 du Code de procédure pénale.

Il s'agit ainsi d'harmoniser les attributions du juge d'instruction et celles du procureur général précitées.

Les articles 13 à 17 visent à renforcer les attributions du procureur général en lui permettant de procéder, dans le cadre de perquisitions, à la saisie des données informatiques, et complètent à cette fin les articles 255 à 258 et 264 du Code de procédure pénale.

La perquisition classique portant sur des documents, des dossiers, ou des objets est ainsi étendue aux données informatiques contenues dans un système à condition, toutefois, qu'elles soient utiles à la manifestation de la vérité c'est-à-dire qu'elles permettent d'établir qu'une infraction spécifique, objet des poursuites, a été commise.

Techniquement, il se peut, en effet, que les données recherchées ne soient pas stockées dans l'ordinateur faisant l'objet de la perquisition mais soient toutefois facilement accessibles par ce système.

La saisie des données informatiques peut être effectuée de deux manières, soit par la mise sous scellés du support physique de ces données (disque dur d'un ordinateur, CD-Rom par exemple) soit par la réalisation d'une copie de ces données sur un support papier ou un autre support (disquette, CD-Rom, ou clé USB).

Une fois la copie réalisée, le procureur général décide s'il y a lieu d'effacer définitivement sur le support physique qui n'a pas été placé sous scellés les données informatiques en cause, en fonction du critère selon lequel la détention ou l'usage de ces données s'avère dangereux pour la sécurité des personnes et des biens.

Il lui revient également de prendre connaissance, seul, des documents, données informatiques, papiers lettres ou autres objets avant de procéder à leur saisie afin de préserver le respect du secret professionnel et des droits de la défense.

L'article 18 complète l'article 266 du Code de procédure pénale autorisant les officiers de police judiciaire, auxiliaires du procureur général, à effectuer tous les actes de la compétence de ce dernier en cas d'extrême urgence, de manière à ce que tous les éléments saisis comprennent également les données informatiques recueillies.

L'article 19 prévoit l'introduction au sein du Code de procédure pénale d'un nouveau titre VIII au Livre I, intitulé « *Dispositions communes* », comportant les nouveaux articles 268-1 à 268-6.

Ces dispositions ont pour objectif de renforcer les attributions des autorités judiciaires dans le cadre de leurs investigations et de les autoriser à requérir d'une personne physique ou morale qualifiée les prestations visant à mettre au clair des données chiffrées qui s'avèrent nécessaires à la manifestation de la vérité.

Certaines données peuvent en effet être cryptées et leur déchiffrement est alors indispensable, voire déterminant des investigations entreprises.

Il importe dans ces conditions que les autorités disposent des pouvoirs nécessaires pour s'adjoindre le concours de personnes disposant du savoir et de la technologie permettant de déchiffrer ces données.

L'article 19 prévoit en outre l'introduction d'un article 268-6 au sein du Code de procédure pénale, lui-même contenu dans une nouvelle section II, insérée au titre VIII du Livre I, intitulée « *Des enquêtes* ».

Ces dispositions créent des obligations à la charge des organismes publics et des personnes morales de droit privé qui doivent déférer à toute réquisition de l'officier de police judiciaire tendant à la mise à disposition des informations utiles à la manifestation de la vérité contenues dans le ou les systèmes informatiques, y compris les traitements de données informatiques, qu'ils administrent.

Les opérateurs de télécommunications peuvent quant à eux être tenus de prendre les mesures propres à assurer la préservation du contenu des informations consultées par les personnes utilisatrices, pour une durée maximale d'un an.

Afin d'éviter tout risque de déperdition des preuves, ce qui nécessite d'intervenir rapidement, ces dispositions prévoient que l'officier de police judiciaire peut former ses réquisitions par voie télématique et informatique.

Agir vite permet en effet de lutter plus efficacement contre la volatilité des preuves qui caractérise l'usage des nouvelles technologies.

Le non-respect de ces obligations, savoir le fait de refuser de répondre sans motif légitime à ces réquisitions, engage la responsabilité pénale de son auteur qui peut être une personne morale.

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, ainsi rédigée :

« *SECTION IV*
DES DELITS RELATIFS AUX SYSTEMES D'INFORMATION

Article 389-1 : Quiconque aura accédé ou se sera maintenu, intentionnellement et sans droit, 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, 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, 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, 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.

Article 389-2 : Quiconque aura, intentionnellement et sans droit, 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.

Est qualifiée d'entrave au fonctionnement d'un système d'information, toute action ayant pour effet, objet ou finalité de paralyser un système d'information par l'introduction, la transmission, l'endommagement, l'effacement, la modification, l'altération ou la suppression de données informatiques.

Est qualifiée d'altération du fonctionnement d'un système d'information, 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 389-3 : Quiconque aura, intentionnellement et sans droit, introduit, endommagé, effacé, détérioré, modifié, altéré ou supprimé des données informatiques ou agit 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.

Article 389-4 : Quiconque aura, intentionnellement et sans droit, fait usage de données informatiques volontairement endommagées, effacées, détériorées, modifiées, ou altérées sera puni d'un emprisonnement de cinq ans et de l'amende prévue au chiffre 4 de l'article 26.

Article 389-5 : Quiconque aura, intentionnellement et sans droit, intercepté par des moyens techniques, des données informatiques, lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système d'information, y compris les émissions électromagnétiques provenant d'un système d'information transportant de telles données informatiques, sera puni d'un emprisonnement de trois ans et de l'amende prévue au chiffre 4 de l'article 26.

Article 389-6 : Le fait, intentionnellement et sans droit, de produire, importer, détenir, offrir, céder, diffuser ou mettre à disposition :

1°) un dispositif, y compris un programme informatique, ou toute donnée informatique, principalement conçus ou adaptés pour commettre l'une des infractions prévues aux articles 389-1 à 389-5,

2°) un mot de passe, un code d'accès ou des données informatiques similaires permettant d'accéder à tout ou partie d'un système d'information pour commettre l'une des infractions prévues aux articles 389-1 à 389-5, est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

Le présent article est sans application lorsque la production, l'importation, la détention, l'offre, la cession la diffusion ou la mise à disposition n'a pas pour but de commettre l'une des infractions visées aux articles 389-1 à 389-5, comme dans le cas d'essai autorisé ou de protection d'un système d' information.

Article 389-7 : Quiconque aura, intentionnellement et sans droit, introduit, altéré, effacé ou supprimé des données informatiques, engendrant des données non authentiques, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient authentiques, qu'elles soient ou non directement lisibles et intelligibles, sera puni d'un emprisonnement de cinq ans et de l'amende prévue au chiffre 4 de l'article 26.

Article 389-8 : Quiconque aura, intentionnellement et sans droit, 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.

Article 389-9 : Quiconque participe à un groupement formé ou à une entente établie en vue de préparer, commettre, faciliter la commission ou le recel d'une des infractions prévues par les articles 389-1 à 389-8 est puni des peines prévues pour l'infraction elle-même.

Article 389-10 : Quiconque tente de commettre une des infractions prévues aux articles 389-1 à 389-8 est puni des peines prévues pour l'infraction elle-même.

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 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.

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 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 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.

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 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.

Les opérateurs et les prestataires de services peuvent, en outre, réaliser un traitement des données relatives au trafic en vue de commercialiser leurs propres services de communications électroniques ou de fournir des services à valeur ajoutée, si les abonnés 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.

Sans préjudice des dispositions 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.

Les données conservées et traitées dans les conditions définies aux 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.

Les opérateurs et les prestataires de services prennent toutes mesures pour empêcher une utilisation de ces données à des fins autres que celles prévues au présent article.

Le fait, pour les opérateurs ou les prestataires de services chargés de l'exploitation de réseaux et de services de télécommunications et de communications électroniques, ou un de leurs agents de ne pas procéder aux opérations tendant à effacer ou à rendre anonymes les données relatives au trafic, dans les cas où ces opérations sont prescrites par la loi est puni d'un emprisonnement d'un an et de l'amende prévue au chiffre 4 de l'article 26.

Le fait, pour les opérateurs et les prestataires de services chargés de l'exploitation des réseaux et des services de télécommunications et de communications électroniques, ou un de leurs agents de ne pas conserver les données techniques dans les conditions où cette conservation est exigées par la loi, est puni d'un emprisonnement d'un an et de l'amende prévue au chiffre 4 de l'article 26.

<u>Article 389-12</u> : 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,

2°) 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 ».

ARTICLE 2

L'article 40 du chapitre V, intitulé « *Des peines de la récidive pour crimes et délits* », du titre unique du Livre I du Code pénal, est modifié 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, sera 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 389-12 inclus.

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

ARTICLE 3

Il est inséré dans la section VII du chapitre I du titre II du Livre III du Code pénal un nouvel article numéroté 294-3, ainsi rédigé :

« *Article 294-3 : Le fait, en vue de sa diffusion, de fixer, d'enregistrer, de produire, de se procurer ou de transmettre l'image ou la représentation d'un mineur lorsque cette image ou cette représentation présente un caractère pornographique est puni d'un emprisonnement de six mois à trois ans et de l'amende prévue au chiffre 3 de l'article 26. La tentative est punie des mêmes peines.*

Le fait d'offrir ou de diffuser une telle image ou représentation, par quelque moyen que ce soit, de l'importer ou de l'exporter, de la faire importer ou de la faire exporter, est puni des mêmes peines.

Le fait de détenir une telle image ou représentation est puni de six mois à deux ans d'emprisonnement et de l'amende prévue au chiffre 2 de l'article 26.

Les peines sont portées de un à cinq ans d'emprisonnement et à l'amende prévue au chiffre 4 de l'article 26 lorsqu'il a été utilisé, pour la diffusion de l'image ou de la représentation d'un mineur à destination d'un public non déterminé, un réseau de communications électroniques.

Les dispositions du présent article sont également applicables aux images pornographiques d'une personne dont l'aspect physique est celui d'un mineur, sauf s'il est établi que cette personne était âgée de dix-huit ans au jour de la fixation ou de l'enregistrement de son image.

Sont considérées comme des images à caractère pornographique

1°) l'image ou la représentation d'un mineur se livrant à un comportement sexuellement explicite ;

2°) l'image ou la représentation d'une personne qui apparaît comme un mineur se livrant à un comportement sexuellement explicite,

3°) l'image réaliste représentant un mineur se livrant à un comportement sexuellement explicite.

L'expression « image réaliste » désigne notamment l'image altérée d'une personne physique, en tout ou partie créée par des méthodes numériques ».

ARTICLE 4

Il est inséré dans la section VII du chapitre I du titre II du Livre III du Code pénal un nouvel article numéroté 294-4, ainsi rédigé :

« Article 294-4 : Le fait soit de fabriquer, de produire, de transporter, de diffuser par quelque moyen que ce soit et quel qu'en soit le support un message à caractère violent ou pornographique ou de nature à porter gravement atteinte à la dignité humaine, soit de faire commerce d'un tel message, est puni d'un emprisonnement de six mois à trois ans et de l'amende prévue au chiffre 3 de l'article 26 lorsque ce message est susceptible d'être vu ou perçu par un mineur.

ARTICLE 5

Sont insérés au premier alinéa de l'article 15 de la loi n° 1.299 du 15 juillet 2005 sur la liberté d'expression publique, après les mots « *soit par des placards ou affiches exposés au regard du public* » les mots «, *soit par tout moyen de communication au public par voie électronique* ».

ARTICLE 6

L'article 230 du Code pénal est modifié comme suit :

« *Article 230 : Quiconque, par écrit anonyme ou signé ou par symbole, signe matériel ou par quelque autre moyen que ce soit, y compris par le biais d'un système d'information aura menacé autrui d'assassinat, d'empoisonnement ou de meurtre ainsi que de tout attentat emportant une peine criminelle, sera puni d'un emprisonnement de un à cinq ans et de l'amende prévue au chiffre 4 de l'article 26, dans le cas où la menace aurait été faite avec ordre de déposer une somme d'argent dans un lieu indiqué ou sous condition.* »

ARTICLE 7

L'article 234 du Code pénal est modifié comme suit :

« *Article 234 : Quiconque aura menacé verbalement, par écrit ou par quelque autre moyen que ce soit, y compris par le biais d'un système d'information de voies de fait ou de violences autres que celles visées à l'article 230, si la menace a été faite avec ordre ou sous condition, sera puni d'un emprisonnement de un à six mois et de l'amende prévue au chiffre 2 de l'article 26 ou de l'une de ces deux peines seulement* ».

ARTICLE 8

Il est inséré après l'article 234 du Code pénal un nouvel article numéroté 234-1, ainsi rédigé :

« *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, 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 ».

ARTICLE 9

L'article 100 du Code de procédure pénale est modifié comme suit:

« *Article 100 : Le juge d'instruction peut saisir ou faire saisir tous les documents, données informatiques, papiers ou autres objets utiles à la manifestation de la vérité, lesquels sont placés sous scellés, après inventaire. Cependant, si leur inventaire sur place présente des difficultés, ils font l'objet de scellés fermés provisoires jusqu'au moment de leur inventaire et de leur mise sous scellés définitifs et ce, en présence des personnes qui ont assisté à la perquisition suivant les modalités prévues aux articles 93, 95, 96 ou 97.*

Il est procédé à la saisie des données informatiques nécessaires à la manifestation de la vérité en plaçant sous scellés soit le support physique de ces données, soit une copie réalisée en présence des personnes qui assistent à la perquisition.

Si une copie est réalisée, il peut être procédé, sur ordre du juge d'instruction, à l'effacement définitif, sur le support physique qui n'a pas été placé sous scellés, des données informatiques dont la détention ou l'usage est illégal ou dangereux pour la sécurité des personnes ou des biens.

Il ne peut procéder à l'ouverture des scellés qu'en présence de l'inculpé ou de son défenseur, ceux-ci dûment convoqués par lettre recommandée avec demande d'avis de réception.

Il en dresse inventaire dans un rapport qui doit mentionner toute ouverture ou réouverture des scellés. Lorsque les opérations sont terminées, le rapport et les scellés sont déposés au greffe général. Ce dépôt est constaté par procès-verbal ».

ARTICLE 10

L'article 103, alinéa 1, du Code de procédure pénale est modifié comme suit:

« *Le juge d'instruction prend seul connaissance des documents, données informatiques, papiers, lettres, télégrammes ou autres objets saisis, dès que le scellé lui est remis* ».

ARTICLE 11

Le premier alinéa de l'article 105 du Code de procédure pénale est modifié comme suit :

« *Si les nécessités de l'instruction ne s'y opposent pas, l'inculpé, la partie civile ou toute autre personne qui prétend avoir droit sur des documents, données informatiques, papiers, lettres, télégrammes ou autres objets placés sous la main de la justice, peut, jusqu'à la clôture de l'information, en réclamer la restitution au juge d'instruction, ou demander, à leur frais, la délivrance d'une copie ou une photocopie* ».

ARTICLE 12

L'article 106 du Code de procédure pénale est modifié comme suit :

« *Article 106 : Toute communication de documents, données informatiques, papiers, lettres, télégrammes ou autres objets saisis, sans l'autorisation de l'inculpé ou des personnes ayant des droits sur ces documents, données informatiques, papiers, lettres, télégrammes ou autres objets, à une personne non qualifiée pour en prendre connaissance, ainsi que tout usage de cette communication sera puni de l'amende prévue au chiffre 3 de l'article 26* ».

ARTICLE 13

L'article 255 du Code de procédure pénale est modifié comme suit:

« *Article 255 : Il procède, en opérant les perquisitions nécessaires, à la saisie des documents, données informatiques, papiers, lettres ou autres objets en la possession des personnes qui paraissent avoir participé aux faits incriminés ou qui sont susceptibles de détenir les pièces, informations ou objets s'y rapportant.*

Ces opérations ont lieu en présence des personnes chez lesquelles les perquisitions sont effectuées et, en cas d'empêchement, en présence d'un fondé de pouvoir désigné par elles ou, à défaut, de deux témoins. Il en est dressé procès-verbal.

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

Les documents, données informatiques, papiers, lettres ou autres objets saisis sont placés sous scellés après inventaire. Cependant, si leur inventaire sur place présente des difficultés, ils font l'objet de scellés fermés provisoires jusqu'au moment de leur inventaire et de leur mise sous scellés définitifs et ce, en présence des personnes qui ont assisté à la perquisition suivant les modalités prévues au deuxième alinéa.

Le procureur général peut procéder à l'ouverture des scellés. Il en dresse inventaire dans un rapport qui doit mentionner toute ouverture ou réouverture des scellés. Lorsque les opérations sont terminées, le rapport et les scellés sont déposés au greffe général. Ce dépôt est constaté par procès-verbal.

Lorsque la saisie porte sur des pièces de monnaie ou des billets de banque, ayant cours légal dans la Principauté ou à l'étranger, contrefaits, il doit transmettre pour analyse et identification au moins un exemplaire de chaque type de pièces ou billets suspectés de faux à l'autorité qui sera désignée par ordonnance souveraine.

Les dispositions de l'alinéa précédent ne sont pas applicables lorsqu'il n'existe qu'un seul exemplaire de type de pièces ou billets nécessaire à la manifestation de la vérité.

Il est procédé à la saisie des données informatiques nécessaires à la manifestation de la vérité en plaçant sous scellés soit le support physique de ces données, soit une copie réalisée en présence des personnes qui assistent à la perquisition.

Si une copie est réalisée, il peut être procédé, sur instruction du procureur général, à l'effacement définitif, sur le support physique qui n'a pas été placé sous scellés, des données informatiques dont la détention ou l'usage est illégal ou dangereux pour la sécurité des personnes ou des biens.

Le procureur général ne maintient que la saisie des documents, données informatiques, papiers, lettres ou autres objets utiles à la manifestation de la vérité ».

ARTICLE 14

L'article 256 du Code de procédure pénale est modifié comme suit:

« *Article 256 : Le procureur général a toutefois l'obligation de provoquer préalablement toutes mesures utiles pour assurer le respect du secret professionnel et des droits de la défense.*

Il a, seul, avec les personnes désignées à l'article précédent, le droit de prendre connaissance des documents, données informatiques, papiers, lettres ou autres objets avant de procéder à leur saisie ».

ARTICLE 15

L'article 257 du Code de procédure pénale est modifié comme suit :

« *Article 257 : Toute communication de documents, données informatiques, papiers, lettres ou autres objets saisis, sans l'autorisation de l'inculpé ou des personnes ayant des droits sur ces documents, données informatiques, papiers, lettres ou autres objets, à une personne non qualifiée pour en prendre connaissance, ainsi que tout usage de cette communication sera puni de l'amende prévue à l'article 106* ».

ARTICLE 16

L'article 258 du Code de procédure pénale est modifié comme suit:

« *Article 258 : Le procureur général appelle toutes les personnes qui peuvent avoir des renseignements à donner et reçoit leurs déclarations qu'elles signent.*

Si elles sont susceptibles de fournir des renseignements sur les documents, données informatiques, papiers, lettres ou autres objets saisis, les personnes présentes lors de la perquisition peuvent être retenues sur place par le procureur général le temps strictement nécessaire à l'accomplissement de ces opérations ».

ARTICLE 17

L'article 264 du Code de procédure pénale est modifié comme suit:

« *Article 264 : Le procureur général transmet, sans délai, au juge d'instruction, pour être procédé ainsi qu'il est dit au titre VI du présent livre, les procès-verbaux et autres actes dressés conformément aux prescriptions des articles précédents, ainsi que les documents, données informatiques, papiers, lettres ou autres objets saisis. L'inculpé reste en état de mandat d'amener* ».

ARTICLE 18

L'article 266, alinéa 3, du Code de procédure pénale est modifié comme suit :

« *Ils peuvent même, en cas d'extrême urgence, faire tous les actes de la compétence du procureur général, dans les formes et suivant les règles ci-dessus établies. Ils transmettent alors, sans délai, au procureur général les procès-verbaux, les documents, données informatiques, papiers, lettres ou autres objets saisis et tous les renseignements recueillis, pour être procédé, sur ses réquisitions, comme il est dit au titre VI du présent code* ».

ARTICLE 19

Il est ajouté un titre VIII au Livre I du Code de procédure pénale, ainsi rédigé :

« *TITRE VIII – DISPOSITIONS COMMUNES*

SECTION I
DE LA MISE AU CLAIR DES DONNEES CHIFFREES NECESSAIRES A LA MANIFESTATION DE LA VERITE

Article 268-1 : Sans préjudice des dispositions des articles 107, 260 et 266, lorsqu'il apparaît que des données saisies ou obtenues au cours de l'enquête ou de l'instruction ont fait l'objet d'opérations de transformation empêchant d'accéder aux informations en clair qu'elles contiennent, ou de les comprendre, le procureur général, la juridiction d'instruction ou la juridiction de jugement saisie de l'affaire peut désigner toute personne physique ou morale qualifiée, en vue d'effectuer les opérations techniques permettant d'obtenir la version en clair de ces informations ainsi que, dans le cas où un moyen de cryptologie a été utilisé, la convention secrète de déchiffrement, si cela apparaît nécessaire.

Si la personne ainsi désignée est une personne morale, son représentant légal soumet à l'agrément du procureur général, de la juridiction d'instruction ou de la juridiction saisie de l'affaire le nom de la ou les personnes physiques qui, au sein de celle-ci et en son nom, effectueront les opérations techniques mentionnées au premier alinéa. Les personnes ainsi désignées prêtent serment dans les conditions prévues à l'article 116.

Article 268-2 : Le procureur général, la juridiction d'instruction ou la juridiction de jugement saisie de l'affaire adresse une réquisition écrite à la personne désignée dans les conditions prévues à l'article 268-1 qui fixe le délai dans lequel les opérations de mise au clair doivent être réalisées. Le délai peut être prorogé dans les mêmes conditions de forme. A tout moment, l'autorité judiciaire requérante peut ordonner l'interruption des opérations prescrites.

Article 268-3 : Dès l'achèvement des opérations ou dès qu'il apparaît que ces opérations sont techniquement impossibles ou à l'expiration du délit 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.

Ces pièces sont immédiatement remises à l'autorité judiciaire requérante.

Les éléments ainsi obtenus font l'objet d'un procès-verbal de réception et sont versés au dossier de la procédure.

Article 268-4 : Les décisions judiciaires prises en application du présent chapitre n'ont pas de caractère juridictionnel et ne sont susceptibles d'aucun recours.

Article 268-5 : Les personnes requises en application des dispositions de la présente section sont tenues d'apporter leur concours à la justice.

SECTION II
DES ENQUETES

Article 268-6 : Sur demande de l'officier de police judiciaire, qui peut intervenir par voie télématique ou informatique, les organismes publics ou les personnes morales de droit privé mettent à sa disposition les informations utiles à la manifestation de la vérité, à l'exception de celles protégées par un secret prévu par la loi, contenues dans le ou les systèmes informatiques ou traitements de données nominatives qu'ils administrent.

L'officier de police judiciaire, intervenant sur réquisition du procureur général ou sur autorisation expresse du juge d'instruction, peut requérir des opérateurs de télécommunications de prendre, sans délai, toutes mesures propres à assurer la préservation, pour une durée ne pouvant excéder un an, du contenu des informations consultées par les personnes utilisatrices des services fournis par les opérateurs.

Les organismes ou personnes visés au présent article mettent à disposition les informations requises par voie télématique ou informatique dans les meilleurs délais.

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 et de l'amende prévue au chiffre 4 de l'article 26 ».
