C-2-15
24 février 2015

PROJET DE LOI RELATIVE A LA LUTTE CONTRE LA CRIMINALITE TECHNOLOGIQUE

EXPOSE DES MOTIFS

Le développement des technologies de l'information et de la communication a conduit, en ce début du XXIème siècle, à une véritable révolution numérique. Grâce aux nouveaux moyens de communication électronique, on assiste en effet, depuis plusieurs années, déjà à l'essor de la société de l'information, dans laquelle les progrès de la technologie constituent une source sans cesse renouvellée d'expansion.

Force est de constater que les activités criminelles ont su également s'adapter aux évolutions technologiques et, de nouveaux types d'agissements répréhensibles sont apparus, dont la réalisation a été rendue possible ou facilitée par le recours aux technologies et aux réseaux numériques.

Ces nouveaux actes criminels, qu'ils soient spécifiques au monde informatique ou qu'ils renvoient à des infractions connues du monde réel pour lesquelles les technologies de l'information et de la communication offrent de nouvelles possibilités de réalisation, ont en commun d'être marqués par leur caractère transnational, leur immatérialité, et leur volatilité, ainsi que par l'utilisation de techniques d'anonymisation par leurs auteurs. La criminalité en cause est ainsi, à de nombreux égards, spécifique tant par la puissance de son développement que par l'extrême diversité des formes sous lesquelles elle peut se présenter.

L'ensemble de ces caractéristiques n'est pas sans conséquence sur le système pénal des Etats dont les réponses traditionnelles, conçues et élaborées pour un environnement physique et national, se sont rapidemment avérées inadaptées pour saisir cette nouvelle réalité de l'ère numérique, faisant, par la même, de la sécurité numérique un nouvel enjeu stratégique pour toutes les entités qu'elles soient publiques ou privées.

Dans ce contexte, le Conseil de l'Europe a adopté, le 23 novembre 2001 à Budapest, la Convention STCE n° 185 sur la Cybercriminalité. Signée le 2 mai 2013 par la Principauté, cette convention multilaterale a donné lieu, le 27 novembre 2013, au vote à l'unanimité, par le Conseil National de la loi n° 1.402 du 5 décembre 2013 portant approbation de ratification de la Convention sur la cybercriminalité du Conseil de l'Europe.

Les objectifs de la Convention sont les suivants :

- l'harmonisation des éléments des infractions ayant trait au droit pénal matériel national et les dispositions connexes en matière de criminalité technologique ;

- la modification des procédures pénales en vigueur dans les Etats, afin de leur donner les pouvoirs nécessaires à l'instruction et à la poursuite d'infractions de ce type, ainsi que d'autres infractions commises au moyen d'un système d'information ou pour lesquelles les preuves existent sous forme électronique ;

- la mise en place d'un régime rapide et efficace de coopération internationale.

Ainsi, la Convention invite les Etats parties à prendre les mesures nécessaires pour conférer une qualification pénale aux différentes infractions ressortant de la criminalité informatique en donnant des définitions juridiques aux infractions suivantes : accès illégal, interception illégale, atteinte à l'intégrité des données, atteinte à l'intégrité du système, abus de dispositifs, falsification informatique, fraude informatique, infractions se rapportant à la pornographie enfantine et infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes.

En matière de procédure, la Convention énonce également les mesures que les Etats sont tenus de prendre, qu'il s'agisse de la conservation rapide de données stockées dans un système informatique, de la conservation et de la divulgation rapide de données relatives au trafic, de la perquisition et saisie de données informatiques stockées ou encore de la collecte en temps réel des données relatives au trafic et de l'interception de données relatives au contenu.

Quant au protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe, il constitue aussi un outil de lutte indispensable, compte tenu des possibilités qu'offre l'Internet pour mener des actions de propagande raciste et négationniste.

Si la signature, par les autorités monégasques de la Convention sur la cybercriminalité, est intervenue en 2013, force est cependant de constater que le législateur monégasque n'a pas attendu cette date pour adopter d'importantes réformes législatives lesquelles ont eu pour effet de placer des domaines substantiels du droit interne dans le sillage des objectifs conventionnels.

Tel a été le cas des réformes issues du vote des lois n° 1.344 du 26 décembre 2007 relatives au renforcement des crimes et délits contre l'enfant et n° 1.343 du 26 décembre 2007 dite « justice et liberté » ou plus récemment de la loi n° 1.394 du 9 octobre 2012 portant réforme des Codes pénal et de procédure pénale en matière de corruption et de techniques spéciales d'enquête.

Par ailleurs, l'adoption de la loi n° 1.383 du 2 août 2011 sur l'Economie Numérique, a permis à la Principauté de se doter, dans le domaine du numérique, de dispositions juridiques encadrant les activités du commerce électronique, la signature et les certificats électroniques, la responsabilité des prestataires techniques et la cryptologie.

Malgré ces nombreux développements législatifs, le droit monégasque se devait d'être encore spécialement adapté dans le domaine pénal, et ce, aux fins de donner une réponse à la mesure de la spécificité et de la gravité de ces nouvelles formes de criminalité.

En déposant sur le bureau de l'Assemblée le présent projet de loi, le Gouvernement Princier entend ainsi achever son processus de ratification de la Convention sur la cybercriminalité, en procédant aux modifications de la législation nationale nécessaires pour en renforcer la compatibilité avec les engagements souscrits en cette matière auprès du Conseil de l'Europe.

Au délà de ces considérations, le présent projet de loi constitue également aux yeux du Gouvernement Princier la manifestation d'une véritable stratégie de lutte contre la cybercriminalité, articulée autour de trois axes principaux :

- la modernisation des infractions de droit pénal classique ;

- l'aménagement des instruments procéduraux traditionnels par rapport aux technologies de l'information et de la communication ;

- la création d'une autorité administrative spécialisée dans la lutte contre les cyber-menaces et cyber-attaques, chargée de veiller à la protection des systèmes d'information de la Principauté ainsi que de réagir aux cyber-attaques dont elle pourrait faire l'objet.

Face au défi majeur que constitue la lutte contre la criminalité technologique ou cybercriminalité, entendue comme l'ensemble des infractions pénales commises sur les réseaux numériques dont l'Internet, la réforme législative telle que proposée par le Gouvernement Princier poursuit l'objectif d'y apporter une réponse pertinente à travers la mise en place d'un cadre juridique approprié permettant de traiter efficacement ces types d'infractions.

Sous le bénéfice de ces observations à caractère général, le présent projet de loi appelle les commentaires particuliers ci-après.

Du point de vue formel, le présent projet de loi est divisé en trois titres :

1. Titre premier : dispositions de droit pénal

2. Titre II : dispositions de procédure pénale

3. Titre III : dispositions relatives à la sécurité des systèmes d'information

Le Titre premier concerne l'insertion de nouvelles dispositions au sein du Code pénal (article premier à 10) savoir, les délits relatifs aux systèmes d'information, les dispositions relatives aux opérateurs et prestataires de services chargés de l'exploitation des réseaux et des services de télécommunications et de communications électroniques qui obtiennent, conservent et exploitent les données de connexion des utilisateurs desdits services, les infractions relatives aux instruments de paiement, différents types de menaces par voie de communications électroniques, le refus de communication de clés de déchiffrement, ainsi que le délit d'usurpation d'identité.

Le Titre II apporte des modifications au sein du Code de procédure pénale (article 11 à 20), en ce qui concerne notamment les perquisitions et saisies de données informatiques, les enquêtes et la mise au clair des données chiffrées.

Enfin, devant la montée des menaces et des cyber-attaques, le Titre III institue une autorité administrative spécialisée, chargée de veiller à la sécurité des systèmes d'information de la Principauté (article 21 à 27).

Le Gouvernement a donc souhaité, au sein des trois premiers articles du Titre I du présent projet de loi, prévoir l'insertion, dans le Code pénal, de trois nouvelles sections - IV, V et VI - dans le chapitre II du titre II de son livre III, portant sur les crimes et délits et sur leur répression.

In concreto, l'article premier du Titre premier prévoit la création, dans le Code pénal, d'une nouvelle section IV au chapitre II du titre II de son livre III intitulée « *Des délits relatifs aux systèmes d'information* », composée des nouveaux articles 389-1 à 389-10.

L'article 389-1 projeté incrimine l'accès et le maintien frauduleux dans un système d'information, ainsi que la modification des données informatiques qui les accompagne.

A cet égard, il apporte une définition légale du système d'information, de l'accès frauduleux, du maintien frauduleux, ainsi que des données informatiques, et ce, en tenant compte des éléments de définitions retenus dans la Convention du Conseil de l'Europe sur la cybercriminalité.

S'agissant de l'accès frauduleux lui-même, le libellé du futur article est suffisamment général pour permettre de sanctionner des types de comportements tels que le décryptage du mot de passe, l'insertion d'un mot de passe préalablement obtenu de manière illicite, l'utilisation des faiblesses du système de contrôle d'accès, ou encore l'introduction d'un virus tel que le cheval de Troie. Il résulte de ces nouveaux éléments qu'en pratique, l'accès devra être considéré sans droit lorsqu'il se fera par une personne n'y étant pas habilitée, l'accès inopiné ou le maintien involontaire ne devant dès lors pas être poursuivi.

Une aggravation des peines est prévue losrque le fait d'accéder ou de se maintenir de façon frauduleuse dans le système d'information s'accompagnera de l'ingérence dans les données qui y sont présentes (incluant l'endommagement, l'effacement, la détérioration, la modification, l'altération et la suppression).

Quant à l'incrimination de l'entrave au fonctionnement d'un système d'information, celle-ci est déclinée à l'article 389-2 projeté, qui prévoit l'entrave et l'altération du fonctionnement du système d'information.

Par ailleurs, les dispositions prévues par le futur article 389-3 du Code pénal ont pour objet de sanctionner pénalement l'action frauduleuse sur les données informatiques contenues dans un système d'information. Ainsi, seront sanctionnées l'atteinte à l'intégrité des données informatiques comme les fuites d'information. A l'image de l'article 323-3 du Code pénal français, l'article projeté offre un large champ d'application puisque seront concernées les actions tant d'extraction et de détention que de reproduction et de transmission des données informatiques. Dès lors, ce texte permettra notamment, d'incriminer des actes de soustraction frauduleuse de données à proprement parler, sans avoir à caractériser la qualification juridique du vol qui nécessite la soustraction alors qu'il n'y aura eu que reproduction, extraction, détention ou transmission des données.

Dans le même sens, le nouvel article 389-4 prévoit les sanctions pour l'utilisation frauduleuse des données informatiques provenant d'un acte volontaire d'endommagement, d'effacement, de détérioration, de modification ou d'altération de celles-ci. Cette disposition s'est en effet révélée nécessaire pour lutter concrètement contre les atteintes aux données, sachant que ces dernières peuvent avoir été soustraites pour le compte d'une personne différente de celle ayant commis l'infraction principale.

En ce qui concerne plus spécifiquement l'interception frauduleuse des données informatiques, elle est prévue par l'article 389-5 projeté qui permet de protéger le droit à respect des données transmises par et dans le système d'information, notamment *via* la messagerie électronique. Sur le fondement de ces dispositions, les écoutes illitcites, ainsi que d'autres moyens techniques illicites de surveillance de contenus véhiculés par les systèmes pourront ainsi être sanctionnés.

Toutes ces différentes infractions peuvent être commises de manière cumulative ou alternative, il est en effet possible, par exemple, de se rendre coupable de maintien frauduleux dans tout ou partie d'un système d'information, alors que l'accès à celui-ci s'est effectué en toute légalité. Les dispositions nouvellement envisagées permettront ainsi d'apréhender l'ensemble de ces situations.

Sur un plan plus général, le nouvel article 389-6 du Code pénal sanctionne, de son coté, la production, l'importation, la détention, l'offre, la cession ou l'obtention, en vue d'utiliser ou de mettre à disposition un équipement, un dispositif ou un programme informatique, y compris un logiciel qui aura été conçu ou adapté pour permettre la commission de toutes les infractions précedemment définies. Par ailleurs, seront également visés les mots de passe et codes d'accès dès lors qu'ils rendraient possible l'accès dans un système d'information pour commettre les infractions concernées. En revanche, serait exclue du champ d'application des futures dispositions répréssives l'utilisation des éléments ci-dessus lorsqu'ils le seraient dans le cadre d'essai autorisé, de la recherche ou de la protection d'un système d'information.

Le Gouvernement Princier a également souhaité incriminer spécifiquement l'infraction de falsification informatique à l'article 389-7 projeté. Ledit article permettra d'incriminer différents actes de tromperie, en sanctionnant le fait de créer ou de modifier, sans autorisation, les données de manière à ce qu'elles acquièrent une valeur probante différente de celle initialement prévue, de tels agissements pouvant, dans le cadre de transactions juridiques, porter atteinte à l'authenticité des informations fournies par le biais de ces données.

Dans ce sillon, le fait de causer un préjudice patrimonial à un tiers à travers la commission d'une des infractions visées, et ceci dans l'intention d'obtenir un bénéfice économique sera, quant à lui, sanctionné à le futur article 389-8 projeté.

Pour être complet, le Gouvernement a entendu incriminer, avec la création du nouvel article 389-9, non seulement la commission des infractions ci-dessus visées en bande organisée mais également le fait de les préparer ou d'en faciliter la commission, ainsi que le recel de celles-ci.

Enfin, l'article 389-10 projeté sanctionne la tentative des actes d'atteinte au système d'information ou aux données informatiques.

L'article 2 du présent projet de loi insère, avec la création des articles 389-11-1 à 389-12 projetés, dans le Code pénal, une nouvelle section V au chapitre II du titre II de son livre III, laquelle prévoit des obligations incombant aux opérateurs et prestataires de services de télécommunications et de communications électroniques. *De facto*, la lutte contre la criminalité technologique concerne l'ensemble des acteurs, qu'ils soient publics ou privés. L'objectif de ces nouveaux articles est de lutter contre des atteintes à la vie privée des personnes au moyen des nouvelles technologies. Les mesures envisagées érigent, tout d'abord, en principe l'obligation pour les opérateurs et les prestataires de procéder à l'effacement ou à l'anonymisation des données de communication dès leur achèvement, consacrant, par là même l'anonymat des internautes (article 389-11-1).

Néanmoins, ce droit n'est pas absolu et les nouveaux articles 389-11-2 et 389-11-3 prévoient des exceptions à l'obligation d'effacement de certaines catégories de données techniques en instaurant la possibilité de leur conservation pour les besoins de la recherche et dans le cadre des poursuites pénales (article 389-11-2), ainsi que pour les besoins de facturation et du paiement des prestations, de la commercialisation des services et de la sécurité des réseaux (article 389-11-3).

La conservation ainsi admise sera cependant limitée dans le temps et exigera, dans le cas de données utilisées à des fins de commercialisation des services, le consentement exprès des abonnés. Il est également prévu que les opérateurs puissent conserver certaines données à des fins de sécurité de leurs réseaux.

L'article 389-11-4 projeté apporte des précisions concernant la localisation des équipements terminaux des personnes. Ainsi, les données obtenues par les opérateurs permettant de localiser l'équipement ne pourront être utilisées à des fins autres que l'acheminement de la communication et toute conservation et traitement ultérieurs seront assujettis au consentement de celle-ci, étant précisé que ce consentement sera révocable à tout moment et gratuitement. Un devoir d'information sur le type de données concernées, la durée de traitement, ses fins et les éventuelles transmissions à des tiers, incombera aux opérateurs.

Le nouvel article 389-11-5 précise que les données concernées par la présente section sont uniquement des données techniques et d'identification qui ne peuvent porter, en aucun cas, sur le contenu des communications effectuées ou des informations consultées. L'article rappelle également que leur traitement est soumis au respect de la loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives.

Il établit au surplus, une obligation de moyen pesant sur les opérateurs et prestataires qui devront ainsi prendre toutes mesures pour empêcher une utilisation des données autre que celle admise par le présent texte.

Par ailleurs, des sanctions sont prévues à l'encontre des opérateurs et prestataires qui manqueraient à leurs obligations d'effacement, d'anonymisation ou de conservation des données.

L'article 389-11-6 projeté concerne quant à lui, le cas particulier de vol d'un téléphone mobile. A cet égard, le mécanisme envisagé consiste à imposer aux opérateurs, informés du vol d'un téléphone portable par le biais d'une déclaration officielle de vol prenant la forme d'un dépôt de plainte, de bloquer, dans un délai de 4 jours ouvrés, l'accès au réseau de radiocommunication et aux services qu'ils proposent, de manière à ce que l'appareil soit rendu inutilisable (sauf les appels aux numéros d'urgence). La présente disposition a pour but d'apporter une solution efficace au problème de la vente de téléphones portables ayant été dérobés, notamment à l'étranger. On relèvera cependant qu'en cas d'absence de dépôt de plainte, l'opérateur ne pourra procéder qu'au blocage de la carte SIM, celui-ci exonérant alors uniquement le propriétaire du téléphone du paiement de l'usage frauduleux qui pourrait être fait de sa ligne.

Enfin, pour être complet, le nouvel article 389-12 instaure le régime de responsabilité des personnes morales pour des infractions concernées par la présente section, conformément à l'article 4-4 du Code pénal.

Le Gouvernement Princier a, en outre, souhaité répondre le plus précisément possible à la transposition, en droit monégasque, de la décision-cadre du Conseil de l'Union européenne du 28 mai 2001 concernant la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces (2001/413/JAI) et ce, en application de l'Accord monétaire entre l'Union européenne et la Principauté de Monaco du 29 novembre 2011 rendu exécutoire par l'Ordonnance Souveraine n° 3.559 du 5 décembre 2011.

A cette fin, l'article 3 du présent projet de loi prévoit l'insertion, au chapitre II du titre II du livre III du Code pénal, d'une nouvelle section VI portant sur les infractions relatives aux instruments de paiement et introduisant les nouveaux articles 389-13 à 389-19.

En premier lieu, l'article 389-13 projeté définit les instruments de paiement concernés, savoir notamment, les cartes de crédit, les autres cartes émises par des établissements financiers, les chèques de voyage, les autres chèques et les lettres de change.

Le nouvel article 389-14 établit, quant à lui, les sanctions en cas de vol, contrefaçon ou falsification d'un instrument de paiement. Sont également punis les faits de réceptionner, d'obtenir, de transporter, de vendre, de céder, de détenir ou d'utiliser des instruments de paiement volé, faux, falsifié ou obtenus illégalement.

Le fait d'effectuer un transfert d'argent ou de valeur monétaire frauduleux est, pour sa part, sanctionné à l'article 389-15 projeté. La formulation large englobant « la valeur monétaire » permet d'inclure dans le champ d'application de cet article les paiements électroniques qui s'effectuent en monnaie virtuelle, du type bitcoins qui correspondent à des unités de compte utilisés par un système de paiement reposant sur l'internet.

Le transfert doit, par ailleurs, être réalisé dans le but de procurer un avantage économique à soi-même ou à un tiers. Deux hypothèses de réalisation de la présente infraction sont envisagées : par l'introduction, l'altération, l'effacement ou la suppression des données et par la perturbation du fonctionnement d'un logiciel ou d'un système d'information.

Pour le reste, le nouvel article 389-16 prévoit les sanctions dans le cas de la fabrication, réception, obtention vente ou cession illégales d'un dispositif permettant la commission de deux infractions visées ci-dessus – à savoir la contrefaçon et la falsification des instruments de paiement, ainsi que le transfert d'argent frauduleux. L'article précise qu'il s'agit, concernant la contrefaçon et la falsification des instruments de paiement, des « *instruments, articles, logiciels ou tout autre moyen spécialement adapté* » et de « *logiciels* » concernant les transferts frauduleux.

Enfin, l'article 389-17 projeté incrimine la commission (incluant aussi la préparation, la facilitation ou le recel) des infractions ci-dessus visées en bande organisée. Les peines sont les mêmes que celles prévues pour les infractions elles-mêmes, le montant de l'amende étant amené au décuple des montants initiaux.

Pour être complet sur cette problématique, la responsabilité des personnes morales pour les infractions visées par la présente section est encadrée par le nouvel article 389-18.

Au final, la tentative de ces infractions est sanctionnée à l'article 389-19 projeté.

S'agissant des peines applicables en matière de récidive, pour les infractions visées dans les trois sections ci-dessus – celles relatives aux systèmes d'information, celles relatives à l'exploitation des données de communication et celles relatives aux instruments de paiement – l'article 4 du présent projet de loi les introduit dans le Code pénal au moyen d'un avant-dernier alinéa spécifiquement réservé aux délits punis par les articles 389-1 à 389-16, inséré au sein de l'article 40 du chapitre V du titre unique du livre I du Code pénal.

Pour ce qui concerne l'article 5 du projet de loi, le Gouvernement Princier a entendu incriminer également les menaces d'assassinat, d'empoisonnement et de meurtre, ainsi que tout attentat emportant une peine criminelle qui seraient effectués par le biais d'un système d'information. L'article 230 actuel du Code pénal est donc modifié en ce sens.

De même, l'article 6 du présent projet propose-t-il une adaptation de l'article 234 du Code pénal actuellement en vigueur relatif aux menaces de violences par le biais d'un système d'information.

Par ailleurs, et pour tenir compte de la gravité des infractions commises *via* un système d'information, l'article 7 du présent projet, prévoit, de manière générale, au titre du nouvel article 234-2 du Code pénal, une aggravation des peines s'agissant des menaces ayant pour origine une discrimination de personnes à raison de leur origine ou appartenance à une ethnie, une nation, une race ou une religion, ou encore à raison de leur orientation sexuelle.

L'article 8 du projet est destiné à créer, à la suite de l'article 208 du Code pénal un nouveau paragraphe intitulé « *Entrave à la justice* » lequel a vocation à accueillir l'article 208-1 nouvellement introduit par l'article 9 du présent projet. Cette nouvelle disposition sanctionne le fait de refuser au pouvoir judiciaire la communication de clé de déchiffrement - dénommée « *la convention secrète de déchiffrement* » -.

La présente disposition est un complément logique au contenu de l'article 392-3 du Code pénal créé par la loi n° 1.383 du 2 août 2011 sur l'économie numérique qui a introduit l'aggravation des peines lorsqu'un moyen de cryptologie est utilisé pour préparer ou commettre un crime ou un délit, ou pour en faciliter la préparation ou la commission.

L'article 10 du présent projet prévoit l'insertion d'un nouvel article 308-6 à la fin de la section XI du chapitre premier du titre II du Code pénal, relative aux atteintes à la vie privée et familiale. L'introduction de cette nouvelle disposition permet d'incriminer non seulement l'infraction classique d'usurpation d'identité, mais également lorsqu'elle est réalisée par le biais d'un réseau de communication par voie électronique.

Le Titre II du présent texte, comportant les articles 11 à 20, procède à l'adaptation des dispositions déjà applicables en matière de procédure pénale, pour inclure les documents et les données informatiques dans le régime relatif aux saisies et perquisitions lors d'une instruction ainsi qu'aux procédures particulières d'instruction des crimes et délits flagrants. Les dispositions concernées constituent donc une adaptation de la législation existante aux fins de permettre la mise sous-main de justice des supports et des données informatiques.

Dans ce sens, l'article 11 du projet de loi modifie l'actuel article 100 du Code de procédure pénale en prévoyant, dans le cadre des perquisitions ou saisies au cours de l'instruction, la recherche et la saisie des documents et des données informatiques. Dans le cas des données informatiques, la saisie se manifeste par la mise sous scellés soit du support physique (clé USB, disque dur externe, etc.), soit de la copie de celles-ci.

Les articles 12 et 13 modifient, quant à eux, les articles 103 et 106 actuels du Code de procédure pénale en intégrant, dans leur champ d'application respectif, les documents et données informatiques faisant l'objet de saisies et de perquisitions lors de la phase de l'instruction.

Les articles 14 à 19 du présent projet de loi, modifient les articles 255, 256, 257, 258, 264 et 266 du Code de procédure pénale relatifs à l'instruction en cas de crime ou de flagrant délit, en y intégrant dans leur champ d'application respectif les documents et données informatiques.

De ce point de vue une attention particulière doit être apportée aux modifications affectant l'actuel article 255 du Code de procédure pénale lesquelles complètent, de manière significative, les règles actuelles de la perquisition en ce qui concerne notamment les conditions auxquelles les autorités compétentes pourront accéder aux systèmes d'information et en recueillir les données.

Ainsi, le procureur général ou les officiers de police judiciaire habilités se voient autorisés à accéder « *par un système d'information implanté sur les lieux où se déroule la perquisition, à des données intéressant l'instruction en cours et stockées dans ledit système ou dans un autre système d'information dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial* ».

Par ailleurs, et dans les limites imposées par les engagements internationaux souscrits par la Principauté, les données stockées dans les systèmes d'information situés à l'étranger pourront également être recueillies.

Enfin, en énonçant que le procureur général « peut ordonner à toute personne connaissant le fonctionnement du système d'information ou les mesures appliquées pour protéger les données informatiques qu'il contient, de fournir toutes les informations raisonnablement nécessaires pour l'application du présent article », l'article 255 tel que modifié par le projet de loi consacre une obligation de communication de mots de passe et autres identifiants sans lesquels le procureur général ne pourrait avoir accès au système d'information.

L'article 20 insère un nouveau titre IX au sein du Livre I du Code de procédure pénale, relatif aux dispositions communes à la police judiciaire et l'instruction. *De* facto, ledit titre prévoit des dispositions communes pour la mise au clair des données chiffrées par des moyens cryptographiques (articles 268-5 à 268-9 projetés), ainsi que pour la mise à disposition des données par les organismes publics ou les personnes morales de droit privé (article 268-10 projetés).

Le Titre III du présent projet de loi a pour objet de créer une autorité administrative spécialisée aux fins de lutter contre les cyber-menaces et cyber-attaques. *De facto,* l'environnement lié aux technologies de l'information et de la communication est la cible de nombreuses menaces. L'ouverture des réseaux et leur complexité croissante associant des acteurs aux multiples profils, ont renforcé la vulnérabilité des systèmes d'information. Les attaques peuvent prendre différentes formes et avoir diverses finalités : détruire, altérer ou encore accéder à des données sensibles dans le but de les modifier ou de nuire au bon fonctionnement des réseaux et des personnes publiques et privées.

Pour mémoire, le nombre de fraudes se traduit chaque année dans le monde par des coûts s'élevant à des milliards d'euros, en particulier pour les banques et les entreprises. Par ailleurs, il convient de relever que les systèmes d'information peuvent offrir des services vitaux ou essentiels sur lesquels reposent la sûreté et l'économie nationales des États. Dès lors, la sécurité numérique apparaît aujourd'hui comme un véritable enjeu de souveraineté, nécessitant que l'activité de protection des systèmes d'information soit placée au plus près de l'autorité centrale gouvernementale.

Afin de doter la Principauté d'instruments juridiques propres à assurer la maîtrise des moyens informatiques nécessaires à la mise en oeuvre d'une sécurité des systèmes d'information (S.S.I.) efficace, le Gouvernement Princier a donc décidé de créer une autorité administrative spécialisée qui, placée sous l'autorité du Ministre d'État disposerait de services dirigés par un directeur et comprenant des fonctionnaires et agents spécialisés en matière de sécurité numérique (article 21 et 22 du projet de loi).

Cette autorité, ainsi que cela est détaillé à l'article 23, pourra, aux fins de répondre à des attaques visant les systèmes d'information de la Principauté, procéder à des opérations de neutralisation desdites attaques en détenant au besoin, des équipements permettant de réaliser les nouvelles infractions créées par le présent projet qui figureront aux articles 389-1 à 389-10 du Code pénal.

Au surplus, le présent projet de texte, tout en fixant les prérogatives de l'autorité, donne pour la première fois une définition légale tant des secteurs d'activité d'importance vitale que des opérateurs d'importance vitale (O.I.V.). Tel est l'objet des articles 24 et 25 du projet de loi. Ces opérateurs, considérés par la Commission européenne comme « *des installations physiques et des technologies de l'information, les réseaux, les services et les actifs qui, en cas d'arrêt ou de destruction, peuvent avoir de graves incidences sur la santé, la sécurité ou le bien-être économique des citoyens ou encore le travail des gouvernements des Etats membres* » sont effectivement indispensables au bon fonctionnement du pays et représentent aujourd'hui des cibles particulièrement exposées aux attaques informatiques. Il s'avère donc nécessaire de les protéger mais également de les encourager à renforcer les mesures de protection de leurs systèmes d'information.

Aussi, le présent projet de loi introduit-il au moyen des articles 26 et 27 projetés, une obligation, pour les O.I.V., d'appliquer les règles de sécurité qui seront prescrites par voie règlementaire et de soumettre leur système d'information à des contrôles qui seront effectués par la future autorité administrative de sécurité numérique. A défaut, ces opérateurs s'exposeront alors à des sanctions pénales.

Tel est l'objet du présent projet de loi.

* * * * *

PROJET DE LOI

TITRE PREMIER
DISPOSITIONS DE DROIT PENAL

Article premier

Est inséré une section IV au chapitre II du titre II du Livre III du Code pénal, rédigée comme suit :

« *Section IV – Des délits relatifs aux systèmes d'information*

Article 389-1 : Quiconque aura accédé ou se sera maintenu, 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 qui pourra être portée au double en fonction des circonstances.

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 informatiques ainsi que les données informatiques stockées, traitées, récupérées ou transmises par ce dispositif ou cet ensemble de dispositifs en vue du fonctionnement, de l'utilisation, de la protection et de la maintenance de celui-ci.

Est qualifié d'accès frauduleux, toute action de pénétration ou d'intrusion irrégulière, par quelque moyen que ce soit, dans tout ou partie d'un système d'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 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 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 4 de l'article 26.

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

Article 389-2 : Quiconque aura, frauduleusement, entravé ou altéré le fonctionnement de tout ou partie d'un système d'information, 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, frauduleusement, introduit, endommagé, effacé, détérioré, modifié, altéré, supprimé, extrait, détenu, reproduit, transmis ou rendu inaccessible 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.

Article 389-4 : Quiconque aura, frauduleusement, 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, frauduleusement, 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, frauduleusement, de produire, importer, détenir, offrir, céder, diffuser, obtenir en vue d'utiliser ou mettre à disposition :

> *1°) un équipement, un dispositif, y compris un programme informatique, ou toute donnée principalement conçus ou adaptés pour permettre la commission d' une ou plusieurs 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, de la recherche ou de protection d'un système d'information.

Article 389-7 : Quiconque aura, frauduleusement, 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, 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, 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 une bande organisée ou à une entente établie en vue de préparer, commettre, faciliter la commission ou le recel, caractérisées par un ou plusieurs faits matériels, d'une ou plusieurs des infractions prévues par les articles 389-1 à 389-8, est puni des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

Article 389-10 : Quiconque tente de commettre une des infractions prévues aux articles 389-1 à 389-9 est puni des peines prévues pour l'infraction elle-même. »

Article 2

Est inséré une section V au chapitre II du titre II du livre III du Code pénal, rédigé comme suit :

« *Section V – Des opérateurs et prestataires de services chargés de l'exploitation des réseaux et des services de télécommunications et de communications électroniques*

Article 389-11-1 : 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 articles 389-11-2 à 389-11-5.

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.*

Article 389-11-2 : 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 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 détermine, dans les limites fixées par l'article 389-11-5, 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.

Article 389-11-3 : 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 déterminées, dans les limites fixées par l'article 389-11-5, selon l'activité des opérateurs et des prestataires de services et la nature de la communication, par ordonnance souveraine.

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.

Les opérateurs ou prestataires de service peuvent également conserver certaines données en vue d'assurer la sécurité de leurs réseaux.

Article 389-11-4 : Sans préjudice des dispositions des articles 389-11-2 et 389-11-3 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.

Article 389-11-5 : Les données conservées et traitées dans les conditions définies aux articles 389-11-2 à 389-11-4 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° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives, modifiée.

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 3 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 exigée par la loi, est puni d'un emprisonnement d'un an et de l'amende prévue au chiffre 3 de l'article 26.

Article 389-11-6 : Les opérateurs exploitant un réseau radioélectrique de communication ouvert au public ou fournissant des services de radiocommunication au public sont tenus de mettre en œuvre les dispositifs techniques destinés à interdire, à l'exception des numéros d'urgence, l'accès à leurs réseaux ou à leurs services des communications émises au moyen de terminaux mobiles, identifiés et qui leur ont été déclarés volés. Ces terminaux doivent être bloqués dans un délai de quatre jours ouvrés à compter de la réception par l'opérateur concerné de la déclaration officielle de vol, transmise par la direction de la sûreté publique.

Toutefois, l'officier de police judiciaire peut requérir des opérateurs, après accord donné par le procureur général ou le juge d'instruction, de ne pas appliquer les dispositions du premier alinéa.

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 :

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.

En matière correctionnelle, lorsqu'aucune peine d'amende n'est prévue à l'encontre des personnes physiques, l'amende encourue par les personnes morales est de 1 000 000 euros. »

Article 3

Est inséré une section VI au chapitre II du titre II du Livre III du Code pénal, rédigée comme suit :

« *Section VI – Des infractions relatives aux instruments de paiement*

Article 389-13 : au sens de la présente loi, on entend par instrument de paiement tout instrument corporel autre que la monnaie légale protégé contre les imitations ou les utilisations frauduleuses, notamment de par sa conception, son codage ou une signature, et qui permet, de par sa nature particulière, à lui seul ou en association avec un autre instrument de paiement, à son titulaire ou utilisateur d'effectuer un transfert d'argent ou de valeur monétaire.

Sont ainsi concernés notamment, les cartes de crédit, les autres cartes émises par les établissements financiers, les chèques de voyage, les autres chèques et les lettres de change.

Article 389-14 : est puni de cinq ans d'emprisonnement et de l'octuple de l'amende prévue au chiffre 4 de l'article 26, le fait, pour quiconque, d'avoir frauduleusement :

1°) volé ou obtenu illégalement un instrument de paiement ;

2°) contrefait ou falsifié un instrument de paiement en vue d'une utilisation frauduleuse ;

3°) réceptionné, obtenu, transporté, vendu ou cédé à un tiers ou encore détenu un instrument de paiement volé ou obtenu illégalement, faux ou falsifié, en vue d'une utilisation frauduleuse ;

4°) utilisé un instrument de paiement volé ou obtenu illégalement, faux ou falsifié.

Article 389-15 : est puni de cinq ans d'emprisonnement et quintuple de l'amende prévue au chiffre 4 de l'article 26, le fait, pour quiconque, d'effectuer ou faire effectuer frauduleusement, un transfert d'argent ou de valeur monétaire, causant ainsi de manière illicite une perte de propriété à un tiers dans le but de procurer un avantage économique illégal à la personne qui commet l'infraction ou à une tierce partie, en :

1°) introduisant, altérant, effaçant ou supprimant des données informatiques, en particulier des données permettant l'identification, ou

2°) perturbant le fonctionnement d'un logiciel ou d'un système informatique.

Article 389-16 : est puni de cinq ans d'emprisonnement et de l'octuple de l'amende prévue au chiffre 4 de l'article 26 du Code pénal, le fait pour quiconque, d'avoir frauduleusement, fabriqué, reçu, obtenu, vendu ou cédé à un tiers ou détenu illégalement :

1°) des instruments, articles, logiciels ou tout autre moyen spécialement adapté pour commettre les infractions visées au 2°) de l'article 389-14 ;

2°) des logiciels ayant pour objet la commission des infractions visées à l'article 389-15.

Article 389-17 : Quiconque participe à une bande organisée ou à une entente établie en vue de préparer, commettre, faciliter la commission ou le recel, caractérisées par un ou plusieurs faits matériels, d'une ou plusieurs des infractions prévues par les articles 389-14 à 389-16, est puni des peines prévues pour l'infraction elle-même et du décuple de l'amende prévue au chiffre 4 de l'article 26.

Article 389-18 : 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 :

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. »

Article 389-19 : La tentative des délits prévus à la présente section est punie des mêmes peines que les délits eux-mêmes. »

Article 4

Est inséré un avant dernier alinéa à 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, rédigé comme suit :

« *Il en sera également ainsi pour les délits punis par les articles 389-1 à 389-16 inclus* ».

Article 5

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

« *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 6

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

« *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 7

Il est inséré après l'article 234-1 du Code pénal un nouvel article numéroté 234-2, rédigé comme suit :

« *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 aux articles 233 et 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 8

Est inséré, à la Section IV du Chapitre III du Livre III du Code pénal, après l'article 208, un § 12 intitulé « *Entrave à la justice* ».

Article 9

Est inséré à la suite du § 12 un article 208-1 rédigé comme suit :

« *Est puni d'un à quatre ans d'emprisonnement et de l'amende prévue au chiffre 4 de l'article 26 le fait, pour quiconque ayant connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, de refuser de remettre ladite convention au pouvoir judiciaire ou de la mettre en œuvre, sur ses réquisitions délivrées en application des titres III et VI du livre Ier du code de procédure pénale.*

Si le refus est opposé alors que la remise ou la mise en œuvre de la convention aurait permis d'éviter la commission d'un crime ou d'un délit ou d'en limiter les effets, la peine est portée au double de la peine initialement prévue et au double de l'amende prévue au chiffre 4 de l'article 26. »

Article 10

Est inséré un article 308-6 au Code pénal rédigé comme suit :

« *Quiconque aura sciemment usurpé l'identité d'un tiers ou une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa réputation ou de l'utiliser pour en tirer un profit quelconque, sera puni d'un emprisonnement de six mois à trois ans et de l'amende prévue au chiffre 4° de l'article 26 dont le maximum pourra être porté au double.*

Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication par voie électronique »

TITRE II
DISPOSITIONS DE PROCEDURE PENALE

Article 11

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

« *Lorsqu'il y a lieu, au cours de l'instruction, de rechercher des documents ou des données informatiques et sous réserve des nécessités de l'information et du respect, le cas échéant, du secret professionnel et des droits de la défense, le juge d'instruction ou l'Officier de police judiciaire ont seuls le droit d'en prendre connaissance avant de procéder à la saisie.*

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 immédiatement 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.

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 12

L'article 103 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.*

Il maintient la saisie de ceux qui sont utiles à la manifestation de la vérité et il fait remettre les autres à l'inculpé ou aux destinataires.

Dans le cas prévu par le second alinéa de l'article précédent, les lettres et télégrammes ne pourront être ouverts par le juge d'instruction qu'en présence du tiers destinataire, s'il réside dans la Principauté, ou lui dûment appelé.

Les télégrammes et les lettres, dont la saisie est maintenue, sont communiqués, dans le plus bref délai, en original ou en copie, à l'inculpé ou au destinataire, à moins que cette communication ne soit de nature à nuire à l'instruction.

Si les nécessités de l'instruction ne s'y opposent pas, l'inculpé, la partie civile ou toute autre personne peuvent demander à leur frais et dans le plus bref délai copies ou photocopies des données informatiques, papiers, lettres, télégrammes ou autres objets placés sous scellés, jusqu'à la clôture de l'information. »

Article 13

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

« *Toute communication de documents, données informatiques, papiers, lettres, télégrammes ou autres objets saisis, faite 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 par la loi 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 14

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

« *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 lui interdire 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 du précédent alinéa 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.

Le procureur général ou, sous sa responsabilité, les officiers de police judiciaire peuvent, au cours d'une perquisition effectuée dans les conditions prévues par le présent code, accéder par un système d'information implanté sur les lieux où se déroule la perquisition, à des données intéressant l'instruction en cours et stockées dans ledit système ou dans un autre système d'information dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial.

S'il est préalablement avéré que ces données, accessibles à partir du système initial ou disponibles pour le système initial, sont stockées dans un autre système d'informations situé en dehors du territoire national, elles sont recueillies par le procureur général, sous réserve des conditions d'accès prévues par les engagements internationaux en vigueur.

Ainsi, 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 conserve que la saisie des documents, données informatiques, papiers, lettres ou autres objets utiles à la manifestation de la vérité.

En outre, il pourra ordonner à toute personne connaissant le fonctionnement du système d'information ou les mesures appliquées pour protéger les données informatiques qu'il contient, de fournir toutes les informations raisonnablement nécessaires pour l'application du présent article.

Dans les lieux où un crime a été commis, il est interdit, sous peine de l'amende prévue au chiffre 1 de l'article 26, à toute personne non habilitée, de modifier avant les premières opérations de l'enquête judiciaire l'état des lieux et d'y effectuer des prélèvements quelconques.

Toutefois, exception est faite lorsque ces modifications ou ces prélèvements sont commandés par les exigences de la sécurité ou de la salubrité publique, ou par les soins à donner aux victimes. »

Article 15

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

« *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 16

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

« *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 par la loi pour en prendre connaissance, ainsi que tout usage de cette communication sera puni de l'amende prévue à l'article 106.* »

Article 17

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

« *Le procureur général appelle et entend toutes les personnes qui peuvent avoir des renseignements à donner sur les documents, données informatiques, papiers, lettres ou autres objets saisis.*

Il est dressé un procès-verbal de 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 18

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

« *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 19

Le troisième alinéa de l'article 266 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 20

Est inséré un titre IX au Livre I du Code de procédure pénale, rédigé comme suit :

« *TITRE IX – DISPOSITIONS COMMUNES*

Section I – De la mise au clair des données chiffrées nécessaires à la manifestation de la vérité.

« *Article 268-5 : 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 268-6 : 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 268-5 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 268-7 : 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.

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 268-8 : Les décisions judiciaires prises en application du présent chapitre n'ont pas de caractère juridictionnel et ne sont susceptibles d'aucun recours.

Article 268-9 : Les personnes requises en application des dispositions de la présente section sont tenues d'apporter leur concours à la justice.

Section II – Des enquêtes

Article 268-10 : 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 d'informations 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 et des prestataires de services chargés de l'exploitation des réseaux et des services de télécommunications et de communications électroniques 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 et prestataires.

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'un an d'emprisonnement et de l'amende prévue au chiffre 4 de l'article 26 du Code pénal.

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 détermine les catégories d'organismes visés au premier alinéa ainsi que les modalités d'interrogation, de transmission et de traitement des informations requises. »

TITRE III
DISPOSITIONS RELATIVES A LA SECURITE DES SYSTEMES D'INFORMATION

Article 21

Le Ministre d'Etat veille à ce que toutes mesures soient prises aux fins d'assurer, dans la Principauté, la sécurité des systèmes d'information.

Article 22

Aux fins de préparer et d'exécuter les mesures mentionnées à l'article précédent, une autorité administrative spécialisée est créée par ordonnance souveraine.

Cette autorité dispose de services dirigés par un Directeur et comprenant des fonctionnaires et des agents spécialisés en matière de sécurité numérique, spécialement commissionnés et assermentés pour l'exercice de leurs missions.

Ils ne peuvent utiliser ou divulguer les renseignements recueillis dans le cadre de leur mission à d'autres fins que celles prescrites par la présente loi, sous peine des sanctions prévues à l'article 308 du Code pénal.

Article 23

Aux fins de répondre à une attaque visant les systèmes d'information de la Principauté et de nature à nuire substantiellement à ses intérêts vitaux, qu'ils soient de nature publique ou privée, l'autorité administrative spécialisée peut, dans les conditions fixées par ordonnance souveraine, procéder aux opérations techniques nécessaires à la caractérisation de ladite attaque et à la neutralisation de ses effets en accédant aux systèmes d'information qui en sont à l'origine.

L'autorité administrative spécialisée peut, aux mêmes fins, détenir des équipements, des instruments, des programmes informatiques et toutes données susceptibles de permettre la réalisation d'une ou plusieurs des infractions prévues aux articles 389-1 à 389-10 du Code pénal, en vue d'analyser leur conception et d'observer leur fonctionnement.

Article 24

Pour les besoins de la sécurité des systèmes d'information de l'Etat et des secteurs d'activité d'importance vitale, les agents mentionnés à l'article 22, peuvent obtenir des opérateurs de communications électroniques, exploitant des réseaux ou fournisseurs de services de télécommunications ou d'accès à Internet, l'identité, l'adresse postale et l'adresse électronique d'utilisateurs ou de détenteurs de systèmes d'information vulnérables, menacés ou attaqués, afin de les alerter sur la vulnérabilité ou la compromission de leur système.

Au sens du premier alinéa, un secteur d'activité d'importance vitale est constitué d'activités concourant à un même objectif ayant trait à la production et la distribution de biens ou de services indispensables à la satisfaction des besoins essentiels pour la vie de la population monégasque, à l'exercice de l'autorité de l'Etat, au fonctionnement de l'économie ainsi qu'à la sécurité de l'Etat.

Lesdits secteurs d'activité sont désignés par arrêté ministériel.

Article 25

Le Ministre d'Etat, conformément à l'article 21, fixe par arrêté ministériel les règles de sécurité nécessaires à la protection des systèmes d'information des opérateurs d'importance vitale.

Aux fins d'application de la présente loi, on entend par opérateurs d'importance vitale, des opérateurs publics ou privés :

- exerçant dans des secteurs essentiels pour le fonctionnement des institutions et des services publics, pour l'activité économique ou plus généralement pour la vie en Principauté ;

- exploitant des établissements ou utilisant des installations ou des ouvrages dont l'indisponibilité risquerait de d'affecter de façon importante les intérêts précités.

Les règles de sécurité mentionnées au premier alinéa peuvent imposer aux opérateurs d'importance vitale de mettre en œuvre des systèmes qualifiés de détection.

Ces systèmes sont exploités par des prestataires de services qualifiés en matière de sécurité de système d'information agréés par l'autorité administrative mentionnée à l'article 22.

Article 26

Les opérateurs d'importance vitale sont tenus d'appliquer les règles de sécurité à leurs frais et d'informer sans délai le Ministre d'Etat des incidents affectant le fonctionnement ou la sécurité des systèmes d'information mentionnés à l'article précédent.

A la demande du Ministre d'Etat, lesdits opérateurs soumettent leurs systèmes d'information à des contrôles, effectués par l'autorité administrative mentionnée à l'article 22, destinés à vérifier le niveau et le respect des règles de sécurité.

Le coût desdits contrôles est à la charge de l'opérateur concerné.

L'autorité administrative mentionnée à l'article 22 préserve la confidentialité des informations recueillies à l'occasion des contrôles.

Les conditions en œuvre du présent article sont précisées par arrêté ministériel.

Article 27

Est puni d'une amende de 150 000 euros le fait, pour les dirigeants des opérateurs d'importance vitale, d'omettre d'établir un plan de protection ou de réaliser les travaux prévus à l'expiration du délai défini par une mise en demeure.

Est puni d'une amende de 150 000 euros le fait, pour les mêmes personnes, d'omettre, après une mise en demeure, d'entretenir en bon état les dispositifs de protection antérieurement établis.

Est puni d'une amende de 150 000 euros le fait, pour les mêmes personnes, de ne pas satisfaire aux obligations de contrôle prévues à l'article 29.

Les personnes morales déclarées responsables, dans les conditions prévues à l'article 4-4 du Code pénal, des infractions prévues au présent article, encourent une amende suivant les modalités prévues à l'article 29-6 du même code.

*****