Loi n° 1.435 du 8 novembre 2016 relative à la lutte contre la criminalité technologique.

journaldemonaco.gouv.mc/Journaux/2016/Journal-8304/Loi-n-1.435-du-8-novembre-2016-relative-a-la-lutte-contre-la-criminalite-technologique

ALBERT II
PAR LA GRACE DE DIEU
PRINCE SOUVERAIN DE MONACO

Avons sanctionné et sanctionnons la loi dont la teneur suit, que le Conseil National a adoptée dans sa séance du 27 octobre 2016.

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 : Est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée, 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\.
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 dont le maximum peut être porté jusqu'au montant du profit éventuellement réalisé.
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 389-11 : 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. ».

Art. 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 : 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 pour les besoins :
1°) de la mise en œuvre des dispositions de la loi n° 1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale ;
2°) de la recherche, de la constatation et de la poursuite des infractions pénales, dans le seul but de permettre, en tant que de besoin, la mise à disposition du pouvoir judiciaire d'informations ;
3°) de la mise en œuvre des missions de l'Agence Monégasque de Sécurité Numérique.
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 réserve 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 bénéficiaires ou 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 389-12 : 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. ».

Art. 3.

En cas de vol ou de perte, les opérateurs exploitant un réseau radioélectrique de communication ouvert au public ou fournissant des services de radio-communication 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 perdus ou volés.
Sur simple appel auprès de l'opérateur concerné, celui-ci doit bloquer immédiatement la ligne téléphonique dudit terminal et, à compter de la réception de la déclaration officielle de vol de l'un de ces terminaux, transmise par la direction de la sûreté publique, ledit opérateur doit bloquer le terminal dans un délai de quatre jours ouvrés.
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 bloquer le terminal.

Art. 4.

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 :
1°) volé ou obtenu illégalement un instrument de paiement ;
2°) contrefait ou falsifié un instrument de paiement en vue d'une utilisation frauduleuse ;
3°) frauduleusement 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°) frauduleusement utilisé un instrument de paiement volé ou obtenu illégalement, faux ou falsifié.
Article 389-15 : Est puni de cinq ans d'emprisonnement et du 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 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. ».

Art. 5.

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 ».

Art. 6.

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. ».

Art. 7.

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. ».

Art. 8.

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. ».

Art. 9.

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 ».

Art. 10.

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. ».

Art. 11.

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
Art. 12.

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 du secret professionnel et des droits de la défense, le juge d'instruction ou l'Officier de police judiciaire régulièrement commis 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 ne peut être procédé à l'ouverture des scellés et au dépouillement des documents qu'en présence de l'inculpé et de son défenseur, ceux-ci dûment convoqués par lettre recommandée avec demande d'avis de réception postal.
Le juge d'instruction 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. ».

Art. 13.

Les deux premiers alinéas de l'article 101 du Code de procédure pénale sont abrogés.

Art. 14.

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. ».

Art. 15.

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. ».

Art. 16.

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. ».

Art. 17.

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. ».

Art. 18.

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. ».

Art. 19.

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. ».

Art. 20.

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. ».

Art. 21.

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. ».

Art. 22.

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, ou que ces données sont protégées par un mécanisme d'authentification, 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 l'accès à ces informations, leur version en clair 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 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 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.
Le fait, pour l'une des personnes visées à l'alinéa précédent, 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 organismes ou personnes visés au présent article mettent à disposition les informations demandées ou requises par voie informatique dans les meilleurs délais.
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 demandées ou requises. ».

TITRE III
DISPOSITIONS RELATIVES A LA SECURITE
DES SYSTEMES D'INFORMATION
Art. 23.

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.

Art. 24.

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.

Art. 25.

Aux fins de répondre à une attaque visant les systèmes d'information de la Principauté et de nature à nuire substantiellement à ses intérêts fondamentaux, 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.

Art. 26.

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 24, 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.

Art. 27.

Le Ministre d'Etat, conformément à l'article 23, 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 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 24.

Art. 28.

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 24, 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 24 préserve la confidentialité des informations recueillies à l'occasion des contrôles.
Les conditions de mise en œuvre du présent article sont précisées par arrêté ministériel.

Art. 29.

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 28.
Est puni d'une amende de 150.000 euros le fait, pour les mêmes personnes, d'omettre d'informer le Ministre d'Etat des incidents affectant le fonctionnement ou la sécurité des systèmes d'information mentionnés à l'article 27.
Les personnes morales déclarées responsables des infractions prévues au présent article encourent une amende dont le montant est égal au quintuple de l'amende prévue pour les dirigeants des opérateurs d'importance vitale.
La présente loi est promulguée et sera exécutée comme loi de l'Etat.
Fait en Notre Palais à Monaco, le huit novembre deux mille seize.

ALBERT.

Par le Prince,
Le Secrétaire d'Etat :
J. BOISSON.