N° 934 Le 24 octobre 2016

___

RAPPORT SUR LE PROJET DE LOI, N° 934, RELATIVE A LA LUTTE CONTRE LA CRIMINALITE TECHNOLOGIQUE

(Rapporteur au nom de la Commission de Législation : Monsieur Thierry POYET)

Le projet de loi relative à la criminalité technologique a été transmis au Secrétariat Général du Conseil National le 27 février 2015 et enregistré par celui-ci sous le numéro 934. Il a été déposé lors de la Séance Publique du 26 mai 2015 au cours de laquelle il a été renvoyé devant la Commission de Législation.

Ce projet de loi a pour objet d'apporter, conformément aux engagements internationaux de la Principauté, une réponse juridique à la problématique de la criminalité technologique en intégrant en droit monégasque les outils nécessaires à l'appréhension des diverses dimensions de cette forme particulière de criminalité.

En premier lieu, ce texte tient compte du fait que la criminalité technologique, ou cybercriminalité, forme un ensemble très hétérogène. Elle comprend ainsi les infractions commises par l'entremise des technologies de l'information et des communications, que celles-ci facilitent la commission d'infractions d'ores et déjà connues du droit pénal ou permettent la commission de nouvelles infractions restant à définir.

Il introduit en effet, dans le Code pénal monégasque, un ensemble de délits relatifs aux systèmes d'information. Certains, comme le délit d'intrusion ou de blocage d'un système d'information, correspondent à de nouvelles infractions. D'autres en revanche, à l'instar du délit de transmission ou de détention frauduleuse de données informatiques ou de menaces, sont la déclinaison d'infractions existantes. De plus, il y insère diverses obligations à la charge des opérateurs et prestataires de services chargés de l'exploitation des réseaux et des services de télécommunication et de communications électroniques, en particulier celle de rendre anonyme

les données ayant trait aux communications acheminées par les systèmes d'information dont ils assurent la gestion.

Ce projet de loi intègre ainsi en droit interne les dispositions de la Convention sur la cybercriminalité du Conseil de l'Europe, dont la ratification a été autorisée par la loi n° 1.402 du 5 décembre 2013.

Il s'avère cependant que cette intégration n'est pas complète puisque les infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes, prévues par l'article 10 de la Convention restent à introduire en droit monégasque. Votre Rapporteur prend toutefois acte du fait que le Gouvernement reviendra ultérieurement vers le Conseil National afin de lui soumettre un projet de loi relatif à ces questions.

En revanche, bien que le Gouvernement n'ait pas signé le Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais d'un système d'information, le projet de loi réprime les menaces commises par le biais d'un système d'information envers une personne ou un groupe de personnes à raison, notamment, de leur origine. Votre Rapporteur souhaite néanmoins indiquer que, dans l'hypothèse où Monaco ratifierait ce Protocole additionnel, la transformation de la proposition de loi n° 221, relative au renforcement de la protection des personnes contre la diffamation et l'injure, votée par l'Assemblée le 29 juin 2016, devrait permettre l'intégration des dispositions de son article 3 en droit monégasque. En effet, cette proposition de loi vise « *tout support par voie de communication électronique* ». Or, le matériel raciste et xénophobe dont il est question dans ce Protocole additionnel comprend « *tout matériel écrit, toute image ou toute autre représentation d'idées ou de théories qui préconise ou encourage* » le racisme ou la xénophobie.

Par ailleurs, en réponse à la décision-cadre du Conseil de l'Union européenne du 28 mai 2001, et en application de l'Accord monétaire entre l'Union européenne et la Principauté de Monaco, le projet de loi introduit plusieurs infractions relatives aux instruments de paiement, parmi lesquelles la contrefaçon ou la falsification d'un tel instrument en vue d'une utilisation frauduleuse.

En deuxième lieu, ce texte tend à limiter les difficultés auxquelles doivent faire face les Etats lorsqu'ils tentent de poursuivre les auteurs d'infractions liées à la criminalité technologique, lesquelles résultent du fait que ces derniers agissent dans un environnement immatériel et transnational, dans lequel il leur est possible de demeurer anonymes.

Ainsi, le projet de loi modifie les règles de procédure pénale, afin que la nature immatérielle des données informatiques ne fasse pas obstacle à leur saisie par les services compétents. En outre, le cadre le plus souvent transnational dans lequel s'insère la commission de ce type d'infractions impose, quant à lui, un renforcement de la coopération judiciaire internationale. C'est la raison pour laquelle la Convention sur la cybercriminalité met en place une telle coopération, par l'intermédiaire de la Convention européenne d'entraide judiciaire en matière pénale à laquelle Monaco est partie.

En dernier lieu, en réponse au caractère occulte de la criminalité technologique, ainsi qu'à l'impact économique considérable des infractions qui s'y rattachent, lequel est estimé à l'échelle mondiale à près de 500 milliards de dollars, le projet de loi met en place des mesures de nature préventive.

Il étend pour cela les pouvoirs de police administrative du Ministre d'Etat au domaine de la sécurité des systèmes d'information et prévoit la création d'une autorité administrative spécialisée aux fins de préparer et d'exécuter les mesures qui en résultent. Cette autorité administrative spécialisée a ainsi vu le jour avec la promulgation de l'ordonnance souveraine n° 5.664 du 23 décembre 2015 créant l'Agence Monégasque de Sécurité Numérique (AMSN).

Compte tenu de la proximité des notions de système d'information et de traitement d'informations nominatives, la Commission s'est interrogée sur les rôles respectifs de l'AMSN et de la CCIN. La première est, en effet, chargée de veiller à la sécurité des systèmes d'information de l'Etat, des secteurs d'activité d'importance vitale et des opérateurs d'importance vitale, tandis que la seconde a pour mission de s'assurer que le responsable du traitement a effectivement prévu des mesures techniques et d'organisation appropriées pour protéger les informations nominatives.

A cet égard, votre Rapporteur remercie les membres de la CCIN, du Haut-Commissariat à la protection des droits, des libertés et à la médiation, du Gouvernement, de l'AMSN et de Monaco Télécom d'avoir pris part aux consultations réalisées par la Commission. Les échanges auxquels elles ont donné lieu ont permis d'éclairer les travaux de la Commission, en ce qu'ils ont mis en lumière les différences existant, à la fois entre les notions précédemment évoquées et les compétences respectives de l'AMSN et de la CCIN.

Ainsi, il s'avère que les traitements d'informations nominatives constituent une catégorie particulière de système d'information relevant de la législation sur la protection des informations nominatives. Dès lors, les domaines d'intervention de l'AMSN et de la CCIN ne sont pas les mêmes. La nouvelle agence est compétente pour connaître des questions de sécurité à un niveau « macroscopique », celui des systèmes d'information utilisés par l'Etat, au sein des secteurs d'activités et par les opérateurs d'importance vitale. En revanche, la CCIN ne connaît des questions de sécurité qu'à un niveau « microscopique », celui des traitements d'informations nominatives.

De même, les missions de l'AMSN et de la CCIN n'ont pas exactement le même objet, puisque cette dernière se concentre sur la définition des informations devant être protégées, tandis que l'AMSN s'attache seulement à déterminer les moyens devant être mobilisés afin d'assurer efficacement cette protection.

Ainsi, les compétences de la CCIN et celles de l'AMSN étant, en définitive, différentes, tant par leur nature que par leur objet, leur articulation apparaît envisageable, même s'il est vrai que les membres de chacune de ces entités sont astreints au secret professionnel. En effet, en pratique l'AMSN ne devrait pas avoir besoin de connaître le contenu des éléments que la CCIN désigne comme devant être protégés en vertu de la législation sur les informations nominatives pour définir, le cas échéant, les moyens devant être mis en œuvre pour assurer leur protection.

Votre Rapporteur est donc certain qu'à l'avenir un dialogue constructif pourra s'établir sur cette base entre ces deux organismes, afin que la sécurité des systèmes d'information en général et celle des traitements d'informations nominatives en particulier soit la plus élevée possible en Principauté.

La Commission est cependant bien consciente que la sécurisation des systèmes d'informations des secteurs d'activités et des opérateurs d'importance vitale représente un investissement conséquent. Elle estime donc que la montée en puissance de la sécurisation des systèmes d'information prévue par le projet de loi doit s'accompagner d'une concertation et d'un dialogue régulier entre la nouvelle agence et ces opérateurs.

Sous le bénéfice de ces observations d'ordre général, votre rapporteur en vient désormais à l'exposé technique des remarques et amendements de la Commission.

♦ ♦ ♦

L'article premier du projet de loi insère une section IV au sein du chapitre II du titre II du Livre III du Code pénal dans lequel sont définis les délits relatifs aux systèmes d'information.

Ainsi, ***l'article 389-8*** projeté réprime d'une peine de cinq ans d'emprisonnement et de l'amende prévue au chiffre 4 de l'article 26 du Code pénal, la personne qui, dans l'intention d'obtenir un bénéfice économique pour elle-même ou pour autrui, cause un préjudice patrimonial à un tiers à la suite, notamment, de l'effacement ou de la suppression de données informatiques.

Soucieuse, d'une part, de tenir compte de l'esprit de lucre ayant animé l'auteur de l'infraction et, d'autre part, de s'assurer que la sanction encourue soit véritablement dissuasive, la Commission a décidé d'indiquer que l'amende prononcée par le juge, qui est celle indiquée au chiffre 4 de l'article 26 du Code pénal, pouvait être portée jusqu'au montant du profit éventuellement réalisé par l'auteur de l'infraction.

L'article 389-8 du Code pénal est donc modifié de la manière suivante :

> *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****.*

En outre, ***l'article 389-6*** punit des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée, le fait de fournir de manière frauduleuse des équipements, des dispositifs ou des données informatiques en vue de permettre ou faciliter la commission de l'un des délits relatifs aux systèmes d'information.

Pour davantage de clarté, la Commission a toutefois estimé que la rédaction de cet article devait être modifiée afin d'y indiquer le *quantum* des peines encourues au début de celui-ci et non à la fin.

Ainsi, l'article 389-6 du Code pénal est modifié de la manière suivante :

Est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée, ~~***L***~~***l****e 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~~****.***

Par ailleurs, lors de l'étude du projet de loi il est apparu que, contrairement notamment à son article 2, son article premier ne précisait pas les types de peines susceptibles d'être encourues par les personnes morales déclarées responsables d'une ou plusieurs des infractions relatives aux systèmes d'information.

La Commission a donc inséré un ***article 389-11***, afin d'y indiquer les peines pouvant être prononcées à l'encontre des personnes morales, étant précisé que celles-ci sont les mêmes que celles qui figurent à l'article 389-12 introduit dans le Code pénal par l'article 2 du projet de loi.

Il est inséré un article 389-11 à la section IV au sein du chapitre II du titre II du Livre III du Code pénal, rédigé comme suit :

> ***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.***

A l'occasion de cet ajout, il a été relevé que ***l'article 389-12***, de même que ***l'article 389-18*** et l'article 29 nouveau du projet de loi, indiquent que « *les personnes morales peuvent être déclarées responsables pénalement, dans les conditions prévues par l'article 4-4* [du Code pénal] *des délits prévus* », soit par l'article lui-même, soit dans la section du Code pénal dans laquelle celui-ci se trouve.

Or, la Commission a estimé qu'une telle rédaction s'articulait mal, d'une part, avec la lettre de l'article 4-4 du Code pénal, qui dispose que la personne morale peut être déclarée pénalement responsable de « *tout crime, délit ou contravention lorsqu'ils ont été commis pour son compte, par l'un de ses organes ou représentants* », et, d'autre part, avec l'objectif de la loi n° 1.349 du 25 juin 2008, modifiant le Livre premier du Code pénal, dont l'exposé des motifs indique qu'« *il a été décidé* [de] *poser le principe général de la responsabilité pénale de la personne morale et* [de] *renvoyer, pour son application, à la sagesse du juge* ».

Les membres de la Commission ont, par conséquent, décidé de supprimer le morceau de phrase précédemment mentionné au sein des articles suivants : article 389-12 (article 2 du projet de loi), article 389-18 (article 4 nouveau) et article 29 nouveau du projet de loi.

Ainsi, les articles 389-12 et 389-18, issus respectivement de l'article 2 et de l'article 4 nouveau du projet de loi, et l'article 29 nouveau ont été modifiés de la manière suivante :

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 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 27 ancien (article 29 nouveau) du projet de loi : […] 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 **dont le montant est égal au quintuple de l'amende prévue pour les dirigeants des opérateurs d'importance vitale** ~~suivant les modalités prévues à l'article 29-6 du même code~~.

♦♦♦

L'article 2 du projet de loi définit, dans une section particulière du Code pénal, les obligations incombant aux opérateurs et prestataires de services chargés de l'exploitation des réseaux et des services de télécommunications et de communications électroniques, en particulier en ce qui concerne l'anonymisation des données relatives au trafic et, le cas échéant, les conditions et le temps durant lequel ils devront les conserver.

A cet égard, votre Rapporteur souhaite que le Gouvernement, dans l'édiction des dispositions réglementaires, prête une attention particulière à l'harmonisation des durées de conservation.

Les membres de la Commission ont entendu élargir, au sein de ***l'article 389-11-2*** projeté, les exceptions au principe d'anonymisation des données relatives au trafic consacré à l'article 389-11-1. Ils ont donc prévu qu'il peut être dérogé à ce principe, outre pour les besoins de la police judiciaire, d'une part, pour ceux 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 et, d'autre part, pour ceux de l'exécution des missions dévolues à l'AMSN.

Ainsi, l'article 389-11-2 a été modifié de la manière suivante :

> ~~*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, i*~~***I****l 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.*

La Commission a souhaité indiquer à ***l'article 389-11-5*** qui définit le contenu des données relatives au trafic devant être exceptionnellement conservées, que celles-ci portent exclusivement sur l'identification des personnes bénéficiaires ou utilisatrices des services fournis par les opérateurs, et pas seulement sur les seules personnes utilisatrices. Elle a, en effet, observé que le bénéficiaire d'une ligne de téléphonie, bien qu'il ait conclu un contrat avec un

opérateur, n'est pas nécessairement l'utilisateur de cette dernière ou, à tout le moins, son seul utilisateur.

Ainsi, l'article 389-11-5 a été modifié de la manière suivante :

> *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.*

Enfin, les membres de la Commission ont constaté que, bien qu'il soit inséré dans le Code pénal, ***l'article 389-11-6*** n'assortit d'aucune sanction pénale l'obligation qu'il fait peser sur les opérateurs exploitant un réseau radioélectrique de communication ouvert au public ou fournissant des services de radiocommunication au public. Ils ont donc souhaité que, par souci de cohérence, ce texte dépourvu de sanction pénale figure au sein d'un article spécifique du projet de loi, et non dans le Code pénal lui-même.

L'article 389-11-6 a donc fait l'objet d'un amendement de suppression.

♦♦♦

La Commission a introduit un article 3 nouveau au sein du projet de loi reprenant les dispositions de l'article 389-11-6, qui obligent les opérateurs de téléphonie mobile à bloquer le terminal qui leur aura été signalé volé, dans les quatre jours ouvrés suivant la réception de la déclaration officielle de vol transmise par la Direction de la Sûreté Publique.

En outre, à la suite des échanges avec le Gouvernement, les membres de la Commission ont toutefois souhaité qu'une distinction soit établie entre, d'une part, le blocage de la ligne téléphonique et, d'autre part, celui du terminal, dans la mesure où le premier pouvait être immédiat, tandis que le second, parce qu'il devait être répercuté à travers le monde, nécessitait davantage de temps, ce qui justifiait qu'un délai de quatre jours ouvrés soit laissé à l'opérateur.

La Commission ayant déplacé ce texte hors du Code pénal, elle a estimé que son champ d'application devait être étendu à l'hypothèse de la perte du terminal, dans la mesure où celle-ci peut, en particulier lorsqu'elle donne lieu à une utilisation malveillante, s'avérer tout aussi préjudiciable qu'un vol. Toutefois, pour des questions d'ordre probatoire, si le blocage de la ligne téléphonique peut résulter d'un simple appel auprès de l'opérateur concerné, aussi bien en cas de vol qu'en cas de perte, en revanche, le blocage du terminal proprement dit survient uniquement à compter de la réception officielle de la déclaration de vol.

Il est inséré un article 3 au projet de loi relative à la lutte contre la criminalité technologique, rédigé comme suit :

> **En cas de vol ou de perte, 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 ou perdus.**

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.

♦♦♦

L'article 4 nouveau du projet de loi insère une section IV au chapitre II du titre II du Livre III du Code pénal, regroupant les infractions aux instruments de paiement.

Ainsi, ***l'article 389-14*** punit, notamment, le vol et l'obtention illégale d'un instrument de paiement, ainsi que la contrefaçon et la falsification d'un tel instrument en vue d'une utilisation frauduleuse.

Le premier alinéa de cet article indique que l'auteur des infractions visées doit avoir agi avec une intention frauduleuse. La Commission a considéré que la mention de l'intention frauduleuse est redondante en ce qui concerne les comportements précités. En revanche, elle admet la pertinence d'une telle précision, s'agissant d'agissements qui, à l'instar de ceux mentionnés aux chiffres 3 et 4, peuvent être réalisés de bonne foi.

La Commission a donc supprimé la mention de l'adverbe « *frauduleusement* » au premier alinéa de l'article 389-14 et l'a fait figurer au début de ses chiffres 3 et 4.

Ainsi, l'article 389-14 a été modifié de la manière suivante :

*~~e~~**E**st 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°) **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.*

♦♦♦

A l'occasion de l'étude de l'article 10 nouveau du projet de loi, qui punit « *le fait, pour quiconque ayant connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé* » dans le cadre de la commission d'une infraction « *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* », l'attention de la Commission a été attirée sur le fait que l'application combinée de ces dispositions et de celles du treizième alinéa de l'article 255 du Code de procédure pénale, tel qu'il est modifié par l'article 16 nouveau du projet de loi, était susceptible de porter atteinte au droit de la personne de ne pas participer à sa propre incrimination.

Ce second texte prévoit, en effet, qu'« *il pourra être ordonné 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* ». Dès lors, il a été indiqué à la Commission qu'une personne pourrait être contrainte de fournir au pouvoir judiciaire, notamment le mot de passe protégeant l'accès d'un système d'information, au risque de participer ainsi à sa propre incrimination.

Cependant, il s'avère que le domaine d'application de l'article 10 nouveau du projet de loi est limité puisqu'il vise seulement les conventions secrètes de déchiffrement d'un moyen de cryptologie, ce qui exclut la communication d'un simple mot de passe en vue d'accéder à un système d'information qui n'est pas pourvu d'un système de cryptage. En outre, ces deux textes ne peuvent être appliqués de façon cumulative, dans la mesure où le premier indique que le pouvoir judiciaire doit avoir agi en application des titres III et VI du livre Ier du code de procédure pénale. Or, l'article 255 du Code de procédure pénale figure dans le titre VII du livre premier dudit Code, relatif aux crimes et délits flagrants.

La Commission a donc décidé de ne pas amender l'article 10 nouveau du projet de loi.

♦♦♦

L'article 12 nouveau du projet de loi modifie les dispositions de l'article 100 du Code de procédure pénale, afin de permettre la perquisition et la saisie de données informatiques sous le contrôle du juge d'instruction.

La Commission a apporté plusieurs modifications au ***premier alinéa*** de cet article qui prévoit que, « *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* ».

Elle a tout d'abord entendu y supprimer l'expression « *le cas échéant* ». Elle a, en effet, estimé que cette suppression était préférable, dans la mesure où, contrairement à ce que pourrait laisser penser la rédaction initiale de ce texte, le respect des droits de la défense doit nécessairement être pris en considération lors de la mise en œuvre de ces dispositions. De plus, elle considère qu'il n'est pas utile de préciser que le secret professionnel ne doit être respecté que pour autant qu'il existe.

La Commission a ensuite complété cet alinéa afin d'y indiquer, à l'instar de ce qui est prévu par le premier alinéa de l'article 101 du Code de procédure pénale, que seul l'officier de police judiciaire régulièrement requis peut prendre connaissance des éléments avant de procéder à leur saisie.

De surcroît, soucieuse de s'assurer qu'il soit procédé à l'ouverture des scellés dans des conditions garantissant le respect des droits de la défense, la Commission a décidé d'insérer un ***cinquième alinéa*** précisant que l'ouverture des scellés ne peut avoir lieu qu'en présence de l'inculpé et de son défenseur, lesquels devront être dûment convoqués par lettre recommandée avec demande d'avis de réception postal.

Ainsi, l'article article 12 nouveau du projet de loi a été modifié de la manière suivante :

Article ~~11~~**12**
(Texte amendé)

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* ***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.

~~*Il*~~ ***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.* »

♦♦♦

La Commission s'est inspirée des dispositions des deux premiers alinéas de l'article 101 du Code de procédure pénale, d'une part, pour modifier le premier alinéa de l'article 100 du Code de procédure, afin d'y désigner les personnes autorisées à prendre

connaissance des éléments avant de procéder à leur saisie, et, d'autre part, pour introduire au sein dudit article un quatrième alinéa précisant les conditions d'ouverture des scellés.

A la suite de l'insertion de ces deux amendements, il est apparu que les dispositions ainsi ajoutées à l'article 100 du Code de procédure pénale étaient les mêmes que celles qui figurent aux deux premiers alinéas de l'article 101 dudit Code de procédure pénale. Dès lors, la Commission a décidé d'insérer un nouvel article 13 au sein du projet de loi prévoyant l'abrogation des deux premiers alinéas de l'article 101 du Code de procédure pénale.

Il est inséré un nouvel article 13 au sein du projet de loi, rédigé comme suit :

Article 13

(Amendement d'ajout)

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

♦♦♦

L'article 22 nouveau du projet de loi crée un titre IX au sein du Livre I du Code de procédure pénale comprenant des dispositions communes relatives, notamment, à la mise au clair des données chiffrées nécessaires à la manifestation de la vérité.

Durant l'étude de ***l'article 268-5***, qui indique que la mise au clair des données concerne les données ayant « *fait l'objet d'opérations de transformation empêchant d'accéder aux informations en clair qu'elles contiennent, ou de les comprendre* », la Commission a observé que l'accès à des données informatiques pouvait également être entravé du fait de l'existence d'un mécanisme d'authentification pouvant, par exemple, consister en un mot de passe ou en un procédé de contrôle biométrique.

Aussi, pour permettre aux enquêteurs et, le cas échéant, au juge d'instruction d'avoir accès à des données protégées de cette manière, la Commission a souhaité viser expressément les données protégées par un mécanisme d'authentification.

Ainsi, l'article 268-5 a été modifié de la manière suivante :

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,*** ~~*la*~~ ***leur*** *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.

L'article 268-10 prévoit la possibilité pour un officier de police judiciaire de demander, par voie télématique ou informatique, à des organismes publics ou à des personnes morales de droit privé de mettre « *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* ».

De plus, il permet également à un officier de police judiciaire, lorsqu'il intervient sur réquisition du procureur général ou sur autorisation expresse du juge d'instruction, de requérir des opérateurs et des prestataires de services de télécommunication et de communications électroniques de prendre des mesures conservatoires d'une durée maximale d'une année.

À la suite de l'étude de ce texte, la Commission a interrogé le Gouvernement sur la nécessité d'envisager expressément la notion de « *voie télématique* », dans la mesure où ce mode de transmission pouvait être considéré comme ayant été remplacé par la transmission par voie informatique. En réponse, le Gouvernement a indiqué, dans sa lettre du 4 octobre dernier, qu'il partageait la position de la Commission. Les membres de la Commission ont donc décidé de supprimer le terme « *télématique* » de ses ***premier et troisième alinéas***.

En outre, la Commission a entendu modifier le ***troisième alinéa*** de cet article afin d'y indiquer, d'une part, que l'obligation de transmission dans les meilleurs délais porte indistinctement sur les informations qui sont demandées en vertu du premier alinéa et sur celles qui sont requises par application du deuxième alinéa et, d'autre part, que cette obligation pèse seulement sur les opérateurs et les prestataires de services chargés de l'exploitation des réseaux et des services de télécommunications et de communications électroniques.

Par ailleurs, la Commission a prévu que l'obligation de transmission visée au troisième alinéa concerne à la fois les informations demandées et celles qui sont requises et a donc mentionné que l'ordonnance souveraine visée au ***dernier alinéa*** détermine les modalités de traitement des informations demandées ou requises.

Enfin, la Commission a déplacé le ***quatrième alinéa*** de ce texte en troisième position, dans le but de préciser que des poursuites pénales sont encourues uniquement par les personnes mentionnées au deuxième alinéa qui auraient refusé de répondre, sans motif légitime, aux réquisitions qui leur auraient été adressées.

Ainsi, l'article 268-10 a été modifié de la manière suivante :

> *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.*
> ***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* ~~*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 ***demandées ou*** *requises.*

♦♦♦

L'article 25 nouveau du projet de loi définit les cas dans lesquels l'AMSN peut intervenir à la suite d'une attaque visant les systèmes d'information de la Principauté.

Afin de mieux délimiter le domaine d'intervention de l'AMSN, la Commission a précisé que celle-ci n'aurait lieu que lorsque l'attaque nuit substantiellement non pas aux intérêts « *vitaux* » de la Principauté, mais à ses intérêts « *fondamentaux* ». Elle a, en effet, estimé que ce changement de terminologie était préférable pour éviter toute confusion, dans la mesure où les intérêts vitaux dont il est question à cet article ne font pas l'objet d'une définition juridique, contrairement aux intérêts fondamentaux visés dans la loi n° 1.430 portant diverses mesures relatives à la préservation de la sécurité nationale, votée par l'Assemblée le 6 juillet 2016.

Ainsi, l'article 25 nouveau du projet de loi a été modifié de la manière suivante :

Article ~~23~~25
(Texte amendé)

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** ~~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.

♦♦♦

L'article 29 nouveau du projet de loi fixe les peines encourues par les dirigeants des opérateurs d'importance vitale (OIV), ainsi que par les personnes morales, en cas de non-respect des obligations prévues dans le titre III du projet de loi.

La Commission a constaté qu'aucune sanction pénale ne pouvait être prononcée à l'encontre des OIV qui omettent d'informer le Ministre d'Etat des incidents affectant le fonctionnement ou la sécurité des systèmes d'information, conformément aux dispositions du premier alinéa de l'article 28 nouveau du projet de loi. Elle a donc décidé d'insérer un quatrième alinéa aux termes duquel une telle omission est punie d'une amende de 150 000 euros.

De plus, la Commission a estimé que l'amende prévue à l'article 29-6 du Code pénal n'était pas suffisamment dissuasive. Elle propose, par conséquent, que le montant de l'amende pouvant être prononcée par le juge soit égal au quintuple de l'amende prévue pour les dirigeants des OIV.

Enfin, la Commission a modifié le renvoi figurant à la fin du troisième alinéa de cet article afin de viser l'article 28, tenant compte ainsi de la renumérotation imposée par l'insertion de deux amendements d'ajout aux articles 3 et 13 du projet de loi, et corrigeant par la même une erreur typographique présente dans le texte transmis au Conseil National.

Ainsi, l'article 29 nouveau du projet de loi a été modifié de la manière suivante :

Article ~~27~~**29**
(Texte amendé)

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~~**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~~, dans les conditions prévues à l'article 4-4 du Code pénal,~~ 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** ~~suivant les modalités prévues à l'article 29-6 du même code~~.

♦ ♦ ♦

Sous le bénéfice de ces observations, votre Rapporteur vous invite désormais à adopter sans réserve le projet de loi tel qu'amendé par la Commission de Législation.