DOCTRINE JURIDIQUE :

L'EXTENSION DE LA CIRCONSTANCE DE BANDE ORGANISÉE

PAR LA LOI DU 13 NOVEMBRE 2014 RENFORÇANT LA LUTTE CONTRE LE TERRORISME : L'EXEMPLE DES ATTEINTES AUX STAD

EMMANUEL DAOUD

AVOCAT AU BARREAU DE PARIS,
CABINET VIGO

CÉLINE GODEBERGE

AVOCAT AU BARREAU DE PARIS,
CABINET VIGO

Le 8 avril 2015, TV5 Monde était victime d'une puissante cyberattaque. La chaîne a d'abord perdu le contrôle de ses sites Internet et de ses comptes sur les réseaux sociaux, puis l'ensemble de ses onze chaînes ont viré à l'écran noir. Sa page Facebook arborait une photo de profil d'un homme portant un keffieh et le drapeau noir de Daech. En photo de couverture, on pouvait lire les mots " CYBERCALIPHATE - Je suIS IS "[1] . Le piratage a été attribué à l'État islamique[2]. Si le contrôle des réseaux sociaux de la chaîne a été repris rapidement, l'antenne est restée perturbée jusqu'au lendemain soir. Plusieurs jours ont été nécessaires pour sécuriser le système d'information, et davantage pour identifier la faille de sécurité.

La réponse judiciaire a quant à elle été immédiate. Dès le lendemain, le parquet de Paris a ouvert une enquête pour accès, maintien frauduleux et entrave au fonctionnement d'un système de traitement automatisé de données, infractions prévues aux articles 323-1 et 323-2 du Code pénal, ainsi que pour association de malfaiteurs en lien avec une entreprise terroriste[3].

La notion de traitement automatisé de données a été introduite en droit français par la loi du 6 janvier 1978, dite Informatique et Libertés[4]. Dix ans plus tard, la loi du 5 janvier 1988 a envisagé les atteintes proprement dites aux systèmes de traitement automatisé de données (STAD)[5]. Aujourd'hui, le dispositif sanctionnant les pénétrations non autorisées dans un STAD est défini aux articles 323-1 à 323-8 du Code pénal.

Quatre infractions sont envisagées : l'accès ou le maintien frauduleux dans un STAD (art. 323-1CP), c'est-à-dire l'intrusion dans le coeur du réseau de l'opérateur avec des finalités telles que le sabotage ou l'espionnage ; l'entrave au fonctionnement d'un STAD (art. 323-2CP), c'est-à-dire la perturbation du service, l'arrêt provoqué du service informatique attaqué ; l'introduction frauduleuse de données dans un STAD ou la suppression ou modification des données qu'il contient (art. 323-3CP) ; le fait de mettre à disposition un programme spécialement adapté pour commettre les infractions précitées (art. 323-3-1CP), infraction visant à réprimer de façon autonome un comportement relevant de la complicité.

Les peines sont comprises entre deux et sept ans d'emprisonnement, et 60 000 euros et 300 000 euros d'amende, le quantum des peines étant plus élevé lorsque les atteintes sont commises contre un STAD mis en oeuvre par l'Etat.

Le quantum des peines a été récemment augmenté par la loi du 24 juillet 2015 relative au renseignement[6], alors que la loi du 13 novembre 2014 renforçant les dispositions de lutte contre le terrorisme[7] ne l'avait pas modifié. Néanmoins, les modifications majeures du dispositif répressif en matière d'atteintes à un STAD tiennent surtout à la loi de 2014.

La loi du 13 novembre 2014 a tout d'abord étendu le champ d'application de l'article 323-3 du Code pénal afin que soit réprimé non seulement le fait

d'introduire frauduleusement des données dans un STAD, de supprimer ou de modifier des données, mais également le fait d'extraire, de détenir, de reproduire ou de transmettre frauduleusement ces données.

Ensuite, par la création d'un nouvel article 323-4-1, la loi a introduit dans le Code pénal la circonstance de bande organisée pour les infractions d'atteinte aux systèmes de traitement automatisé de données à caractère personnel mis en oeuvre par l'État.

Enfin, la loi a modifié l'article 706-72 du Code de procédure pénale, afin de rendre applicable aux délits d'atteintes à un STAD commis en bande organisée et prévus par le nouvel article 323-4-1 du Code pénal, la procédure d'enquête et de poursuite dérogatoire, applicable en matière de criminalité organisée.

Cette procédure, prévue aux articles 706-73 et suivants du Code de procédure pénale, permet d'appliquer aux crimes et délits relevant de la criminalité organisée des techniques spéciales d'enquête, telles que la surveillance, l'infiltration, la garde à vue prolongée jusqu'à 96 heures et avec une intervention différée de l'avocat, les perquisitions en dehors des heures légales, l'interception de correspondances émises par la voie des télécommunications (écoutes téléphoniques), la sonorisation et la fixation d'images dans certains lieux ou véhicules, ou encore la captation de données informatiques.

Si ce sont la nouvelle circonstance de bande organisée et les modifications procédurales consécutives qui vont nous intéresser ici, il n'est pas inutile de faire quelques observations sur l'extension du champ de l'article 323-3. Cet article réprime désormais " *Le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient* ".

Jusqu'à la loi du 13 novembre 2014, le vol de données n'était pas envisagé par les dispositions relatives aux atteintes à un STAD, qui se limitaient à sanctionner la pénétration dans le STAD, sans prendre en compte la captation des données ou leur détention frauduleuse. Le vol de données était donc poursuivi sur le fondement du vol ou de l'abus de confiance[8]. Or, ces infractions paraissaient inadaptées à la spécificité du vol de données.

En effet, s'agissant du vol, défini à l'article 311-1 du Code pénal comme la soustraction frauduleuse de la chose d'autrui, la question de savoir si une donnée était une " chose " pouvait être discutée. Pour beaucoup, une donnée n'est pas une chose à proprement parler, mais " *un élément immatériel distinct de tout support de stockage* "[9]. En outre, la captation d'une donnée n'implique pas nécessairement qu'elle soit soustraite au STAD, c'est-à-dire qu'elle en disparaisse. La donnée " volée " peut être seulement extraite pour pouvoir être ensuite reproduite, mais demeurer toujours dans le STAD.

S'agissant de l'abus de confiance, l'infraction trouvait notamment à s'appliquer dans le cadre du contrat de travail, par exemple lorsque le salarié conservait des données confidentielles après la rupture de son contrat de travail.

L'abus de confiance est défini à l'article 314-1 du Code pénal comme " *Le fait par une personne de détourner, au préjudice d'autrui, des fonds, des valeurs ou un bien quelconque qui lui ont été remis et qu'elle a acceptés à charge de les rendre, de les représenter ou d'en faire un usage déterminé.* " L'infraction implique donc de constater une remise à titre précaire, un détournement, un préjudice pour autrui et un élément intentionnel.

Si l'abus de confiance vise tant les biens matériels qu'immatériels, telles les données contenues dans un STAD, il nécessite également un détournement, c'est-à-dire une utilisation contraire ou étrangère aux finalités de la remise[10]. Or, en dehors du cas où les données sont remises pour un usage professionnel, les données extraites, détenues, reproduites ou transmises, n'ont bien souvent pas fait l'objet d'une remise préalable. L'infraction d'abus de confiance ne pouvait donc viser qu'une partie limitée des hypothèses de vol de données.

Il y a donc lieu de penser que le vol de données, qu'il soit commis dans le cadre professionnel ou non, sera désormais poursuivi sur le fondement de l'article 323-3 du Code pénal, et non plus sur le fondement des infractions de droit commun de vol et d'abus de confiance.

Si on regrette souvent la création de nouvelles infractions, symptôme d'une infatigable inflation législative, force est de constater que la loi du 13 novembre 2014 ne procède ici qu'à

l'extension d'une infraction déjà existante. En outre, l'extension du champ d'application de l'article 323-3 a le mérite de mettre fin à l'ambiguïté concernant le fondement pertinent pour poursuivre le vol de données.

La question qui reste néanmoins en suspens est celle de savoir si la loi du 13 novembre 2014 avait vocation à introduire une telle extension dans la mesure où, on le rappelle, son objet était le renforcement de la lutte contre le terrorisme. On ne perçoit qu'avec difficulté le lien entre ces nouvelles dispositions et la lutte contre le terrorisme.

Le même reproche peut être adressé à l'article 17 de la loi qui, par l'introduction d'un nouvel article 323-4-1 dans le Code pénal, a étendu la circonstance de bande organisée aux quatre atteintes à un STAD précitées, lorsqu'elles sont commises à l'encontre d'un système de traitement de données à caractère personnel et mis en oeuvre par l'État.

Lors des débats parlementaires, un député avait lui-même relevé que cette nouvelle disposition n'avait " *pas de lien avec la lutte contre le terrorisme, qui [était] pourtant l'objet du projet de loi* "[11].

Officiellement, les nouvelles dispositions de l'article 323-4-1 visent à renforcer le caractère dissuasif des différentes incriminations relatives aux atteintes aux STAD, en prévoyant pour ces infractions une circonstance aggravante de bande organisée (I). En réalité, l'extension de la circonstance de bande organisée vise surtout à étendre le régime de la criminalité organisée aux atteintes aux STAD mis en oeuvre par l'État, qui pourront désormais faire l'objet de techniques spéciales d'enquête (II).

I. L'introduction de la circonstance aggravante de bande organisée

Aux termes de l'article 323-4-1 du Code pénal, créé par la loi du 13 novembre 2014 et modifié par la loi du 24 juillet 2015, " *Lorsque les infractions prévues aux articles 323-1 à 323-3-1 ont été commises en bande organisée et à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en oeuvre par l'État, la peine est portée à dix ans d'emprisonnement et à 300 000 € d'amende.*".

À la lecture de ce texte et des travaux parlementaires, on comprend que seules les atteintes à un STAD à caractère personnel mis en oeuvre par l'État sont ainsi concernées par la nouvelle circonstance de bande organisée. Il faudrait toutefois que cette notion soit clairement définie, ce qui n'est pour l'heure pas le cas. La raison de cette imprécision réside certainement dans le fait que la circonstance de bande organisée n'a été introduite que pour appliquer les techniques spéciales d'enquête aux délits d'atteinte à un STAD, et se voit ainsi détournée de son objet.

A. Le système de traitement automatisé de données à caractère personnel mis en oeuvre par l'État : une notion à définir

Dans le projet de loi initial, la circonstance aggravante de bande organisée était applicable à toutes les atteintes à un STAD prévues par les articles 323-1 à 323-3 du Code pénal. Toutefois, à la suite d'un amendement parlementaire, le choix a été fait de circonscrire le dispositif aux atteintes contre les STAD à caractère personnel mis en oeuvre par l'État[13].

La raison avancée était que le projet de loi étendait le régime procédural de la criminalité organisée aux seules atteintes commises en bande organisée à un STAD mis en oeuvre par l'État. En somme, l'objectif était d'aligner les régimes entre les infractions pouvant être aggravées par la circonstance de bande organisée, et celles relevant de la criminalité organisée.

On peut naturellement se féliciter d'un tel choix, qui conduit à limiter l'application de règles dérogatoires. Cependant, d'innombrables questions émergent, et notamment : qu'est-ce qu'un système de traitement automatisé de donnés mis en oeuvre par l'État ?

Cette question est essentielle car si le STAD n'est pas mis en oeuvre par l'État, alors la circonstance aggravante de bande organisée n'a pas vocation à s'appliquer. Pourtant, aucun des travaux parlementaires publiés n'a répondu à cette question. Il semble même que la difficulté n'ait pas été évoquée.

Les commentateurs de la loi ont donc avancé des hypothèses et, comme souvent, ne pouvant sonder le coeur du législateur, ils sont en désaccord. À titre d'exemple, certains affirment que les STAD des opérateurs d'importance vitale (OIV) sont visés par le nouveau texte[14], d'autres le réfutent explicitement[15].

On précise qu'aux termes de l'article R1332-2 du Code de la

défense, un secteur d'activités d'importance vitale est constitué d'activités concourant à la production et la distribution de biens ou de services indispensables à la satisfaction des besoins essentiels pour la vie des populations, à l'exercice de l'autorité de l'État, au fonctionnement de l'économie, au maintien du potentiel de défense, ou à la sécurité de la Nation, dès lors que ces activités sont difficilement substituables ou remplaçables.

L'Agence nationale de sécurité des systèmes d'information (ANSSI) a ainsi défini douze secteurs d'importance vitale, et identifié 218 opérateurs français d'importance vitale publics et privés à " cyber protéger " en priorité. La qualité d'OIV impose notamment à ces opérateurs de mettre en place des systèmes de détection des intrusions dont ils font l'objet et de procéder à des audits.

Parmi ces 218 opérateurs, il y a 33 services de l'État (activités civiles, militaires et judiciaires)[16]. Il est possible que ceux-ci soient visés par l'article 323-4-1 du Code pénal. Pour le savoir, il conviendrait de répondre à une seconde question, sur laquelle le législateur ne s'est pas attardé non plus : qui est l'État au sens de l'article 323-4-1 du Code pénal ?

La notion de traitement de données à caractère personnel mis en oeuvre par l'État apparaît dans la loi de 1978 dite Informatique et Libertés, aux articles 26 et 27, qui prévoient les cas dans lesquels les traitements doivent être autorisés par un acte réglementaire, pris après avis motivé et publié de la CNIL. Or, ces articles visent " *les traitements de données à caractère personnel mis en oeuvre pour le compte de l'État, d'une personne morale de droit public ou d'une personne morale de droit privé gérant un service public* ".

On peut donc raisonnablement se demander si seuls les STAD mis en oeuvre par l'État au sens strict sont concernés, ou bien si ceux mis en oeuvre par une personne morale de droit public, voire une personne morale de droit privé gérant un service public, sont également visés par l'article 323-4-1. En outre, le système de traitement doit-il nécessairement avoir été mis en oeuvre par l'État directement, ou bien peut-il avoir été mis en oeuvre pour son compte ?

Seul le juge nous dira si l'on doit lire le nouvel article 323-4-1 du Code pénal en lien avec les dispositions de la loi dite Informatique et Libertés, ou bien si, dans le respect du principe d'interprétation stricte de la loi pénale, seules les atteintes à un STAD à caractère personnel mis en oeuvre par l'État, autorité étatique, peuvent être commises en bande organisée.

Enfin, d'un point de vue purement critique, on peut se demander si le critère de mise en oeuvre par l'État est cohérent. Le législateur justifie son choix en expliquant que l'atteinte portée à la sécurité publique est plus grave lorsqu'il s'agit d'un système de traitement mis en oeuvre par l'État.

De notre point de vue, la gravité d'une attaque informatique ne se mesure pas qu'en fonction de la personne qui met en oeuvre le système de traitement, mais surtout en fonction des données qui sont traitées.

Si l'État a vocation à traiter des données intéressant la sûreté, la défense ou la sécurité publique, tel est également le cas de nombreuses entreprises privées dans les secteurs stratégiques. Il ne paraît pas cohérent que la circonstance de bande organisée ne puisse pas s'appliquer à de telles atteintes, pour la seule raison qu'elles concernent des STAD qui n'ont pas été mis en oeuvre par l'État.

Les imprécisions du nouveau texte, et les questions d'interprétation qui en résultent, posent nécessairement la question de sa conformité au principe de légalité, qui requiert que la loi pénale soit claire et précise, afin d'en permettre une interprétation stricte. Nul doute que le Conseil constitutionnel, qui n'a pas été saisi *a priori*, sera appelé à se prononcer sur le respect de ce principe, par la voie d'une question prioritaire de constitutionnalité (QPC).

A notre sens, ces imprécisions s'expliquent par le fait que la circonstance de bande organisée n'a été introduite que pour appliquer les techniques spéciales d'enquête aux délits d'atteinte à un STAD.

B. La circonstance de bande organisée détournée de son objet répressif pour des besoins procéduraux

L'article 323-4 du Code pénal réprime l'hypothèse dans laquelle les atteintes à un STAD sont commises en participant à un groupement formé ou une entente établie. Cet article prévoit ainsi que " *La participation à un groupement formé ou à une entente établie en vue de la*

préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3-1 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée ".

Cette incrimination est similaire à celle de l'association de malfaiteurs, définie à l'article 450-1 du Code pénal comme " *tout groupement formé ou entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'un ou plusieurs crimes ou d'un ou plusieurs délits punis d'au moins cinq ans d'emprisonnement* ".

L'association de malfaiteurs ne trouve donc à s'appliquer que pour les délits punis d'au moins cinq ans d'emprisonnement. Or, ainsi qu'il a été précisé, les délits d'atteintes à un STAD sont punis de peines comprises entre deux et sept ans d'emprisonnement, et 60 000 et 300 000 euros d'amende. Ainsi, pour les délits dont la peine est inférieure à cinq ans d'emprisonnement, l'association de malfaiteurs ne trouve pas à s'appliquer.

Afin de prendre en compte le groupement formé ou l'entente préétablie, c'est-à-dire la matérialité de l'association de malfaiteurs, pour tous les délits d'atteinte à un STAD, y compris ceux punis d'une peine inférieure à cinq ans d'emprisonnement, le législateur avait donc fait le choix d'incriminer de manière autonome ce comportement délictuel. L'entente préétablie était ainsi déjà sanctionnée par le biais de l'article 323-4.

La circonstance de bande organisée, étendue aux atteintes à un STAD par la loi du 13 novembre 2014, est définie à l'article 132-71 du Code pénal, aux termes duquel : " *Constitue une bande organisée au sens de la loi tout groupement formé ou toute entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs infractions* ".

En pratique, chacun sait que le cumul des poursuites et des condamnations du chef d'association de malfaiteurs et d'une infraction commise en bande organisée n'est pas rare, chacune de ces infractions réprimant un comportement chronologiquement distinct : avant la commission de l'infraction, voire à défaut, pour l'association de malfaiteurs, et durant la commission de l'infraction s'agissant de la circonstance de bande organisée.

En réalité, ce n'est pas pour prendre en compte et réprimer un comportement délictuel particulièrement dangereux que le législateur a introduit la circonstance de bande organisée, mais bien pour soumettre la poursuite de ces infractions aux techniques spéciales d'enquête.

La commission des lois du Sénat ne s'en cache pas : " *La justification première de cette modification est d'ailleurs moins de créer une nouvelle circonstance aggravante que de permettre l'application des procédures applicables en matière de criminalité organisée* " [17].

La technique consistant à étendre, par le biais de la circonstance de bande organisée, le régime procédural applicable à la criminalité organisée à des crimes et délits qui n'en relèvent pas, n'est d'ailleurs pas nouvelle[18].

À titre d'exemple, en matière de contrefaçon, depuis 2007[19], l'article 706-1 du Code de procédure pénale prévoit que, lorsque les infractions visées sont commises en bande organisée, les articles 706-80 à 706-87 relatifs à la surveillance et l'infiltration sont applicables. De même, depuis 2013 en matière de fraude fiscale[20], l'article 706-1-1, 2° du Code de procédure pénale prévoit que, lorsque les infractions visées sont commises en bande organisée, les techniques spéciales d'enquête sont applicables, à l'exception de la garde à vue prolongée de 96 heures et des perquisitions de nuit.

Comme il l'avait déjà fait auparavant, le législateur a donc, par le biais de la circonstance de bande organisée ainsi détournée de son objet répressif, étendu le régime procédural de la criminalité organisé aux atteintes à un STAD à caractère personnel mis en oeuvre par l'État, délits qui pourront désormais être soumis aux techniques spéciales d'enquête.

II. L'extension du régime de la criminalité organisée

A. Les techniques spéciales d'enquête : les gardes fous imposés par le Conseil constitutionnel

En modifiant l'article 706-72 du Code de procédure pénale, la loi du 13 novembre 2014 a étendu le régime procédural de la criminalité organisée aux atteintes à un STAD commises en bande

organisée. Ces infractions relèvent désormais de la compétence des juridictions interrégionales spécialisées et peuvent faire l'objet de techniques spéciales d'enquête, à l'exception de la garde à vue prolongée de 96 heures et des perquisitions de nuit.

Le législateur n'a en effet pas inclus ces nouvelles infractions dans la liste générale de l'article 706-73 du Code de procédure pénale, mais prévu un article spécifique, visant expressément les techniques spéciales d'enquête applicables aux atteintes à un STAD commises en bande organisée.

Ainsi, aux termes de l'article 706-72, al. 1er du Code de procédure pénale, en matière d'atteintes à un STAD à caractère personnel mis en oeuvre par l'État et commises en bande organisée, la compétence des officiers de police judiciaire et des agents de police judiciaire est étendue à l'ensemble du territoire national pour la surveillance des suspects (art. 706-80 CPP).

En outre, sont désormais applicables à l'enquête, à la poursuite, à l'instruction et au jugement de ces délits, les techniques spéciales d'investigation suivantes : la surveillance (art. 706-80 CPP), l'infiltration (art. 706-81 à 706-87 CPP), l'enquête sous pseudonyme (art. 706-87-1 CPP), les écoutes téléphoniques (art. 706-95 CPP), le recours aux sonorisations et aux fixations d'images de certains lieux et véhicules (art. 706-96 à 706-102 CPP), la captation de données informatiques (art. 706-102-1 à 706-102-9 CPP), et la faculté d'ordonner des mesures conservatoires sur les biens de la personne mise en examen (art. 706-103 CPP).

Ces techniques d'investigation sont également applicables à l'enquête, à la poursuite, à l'instruction et au jugement du blanchiment des atteintes à un STAD commises en bande organisée, ainsi qu'à l'association de malfaiteurs lorsqu'elle a pour objet la préparation de l'un de ces délits (art. 706-92, al. 2 CPP)

Si le législateur a exclu la garde à vue prolongée, assortie de la possibilité de différer l'intervention de l'avocat, ainsi que les perquisitions en dehors des heures légales, ce n'est pas sans raison.

En effet, le Conseil constitutionnel a déjà sanctionné par deux fois le législateur qui avait tenté d'appliquer tout le régime de la criminalité organisée à des infractions économiques, telles que la fraude fiscale ou l'escroquerie, même aggravées par la circonstance de bande organisée.

Ainsi, dans une décision du 4 décembre 2013, le Conseil constitutionnel a considéré que les infractions " *de corruption et de trafic d'influence ainsi que de fraude fiscale et douanière, constituent des délits qui ne sont pas susceptibles de porter atteinte en eux-mêmes à la sécurité, à la dignité ou à la vie de personnes* ". Partant, les dispositions permettant de recourir, pour ces infractions, à la garde à vue selon les modalités fixées par l'article 706-88 du Code de procédure pénale (garde à vue prolongée de 96 heures), ont été déclarées inconstitutionnelles[21]. Par cette décision, le Conseil constitutionnel refusait l'application de la garde à vue dérogatoire aux faits relevant de la délinquance économique.

De la même façon, dans une décision du 9 octobre 2014, le Conseil constitutionnel a considéré que " même lorsqu'il est commis en bande organisée, le délit d'escroquerie n'est pas susceptible de porter atteinte en lui-même à la sécurité, à la dignité ou à la vie des personnes ", et qu'ainsi, en permettant de recourir à la garde à vue dérogatoire de 96 heures, " le législateur a permis qu'il soit porté à la liberté individuelle et aux droits de la défense une atteinte qui ne peut être regardée comme proportionnée au but poursuivi "[22].

Si on ne peut reprocher au législateur de s'être conformé aux décisions du Conseil constitutionnel, force est néanmoins de constater qu'il n'en a pas forcément compris l'esprit.

Le Conseil constitutionnel n'a pas donné, comme le soutiennent certains, un blanc-seing pour " *appliquer certaines procédures applicables aux crimes et délits relevant de la criminalité organisée à des délits n'en relevant pas* "[23].

Au contraire, les décisions du Conseil constitutionnel invitent le législateur à équilibrer la balance entre la nécessité de préserver la sécurité de l'État et la vie des personnes d'une part, et les libertés fondamentales et principes constitutionnels d'autre part. Parmi ces principes, celui d'accessibilité et d'intelligibilité de la loi.

B. Un système de renvoi complexe, contraire au principe d'intelligibilité et d'accessibilité de la loi

En modifiant l'article 706-72 du Code de procédure pénale, le législateur a créé une nouvelle

procédure dérogatoire pour les infractions d'atteinte à un STAD mis en oeuvre par l'État et commises en bande organisée. Si cette nouvelle disposition respecte les deux décisions d'inconstitutionnalité précitées, force est de constater qu'elle crée une confusion sur la procédure applicable.

En effet, à l'intérieur même du régime dérogatoire applicable à la criminalité organisée, on trouve désormais des " sous-régimes " dérogatoires, qui appartiennent à la criminalité organisée sans que les infractions visées n'en relèvent.

Tel est le cas de la fraude fiscale commise en bande organisée, de la corruption active ou passive, du trafic d'influence, de certains délits douaniers et de l'abus de biens sociaux, infractions pour lesquelles les articles 706-1-1 et 706-1-2 du Code de procédure pénale prévoient qu'elles sont soumises à certaines mesures spéciales d'investigation relevant de la criminalité organisée. On a pu penser un temps que ce " sous-régime " dérogatoire était fondé sur un critère commun entre ces infractions. En effet, elles relèvent toutes du droit pénal économique, et sont généralement considérées par le législateur comme les infractions les plus graves de cette catégorie.

Il n'en est rien puisque, depuis la loi du 13 novembre 2014, sont également sujettes à l'application de ce " sous-régime " dérogatoire, les infractions de provocation et d'apologie du terrorisme, et les atteintes à un STAD à caractère personnel mis en oeuvre par l'État commises en bande organisée.

En effet, en matière de provocation aux actes de terrorisme et d'apologie de ces actes, la loi du 13 novembre 2014 a introduit un nouvel article 706-24-1 dans le Code de procédure pénale, qui prévoit que les dispositions dérogatoires relatives à la garde à vue et aux perquisitions ne sont pas applicables aux délits de provocation et d'apologie du terrorisme. Le reste de la procédure applicable en matière de criminalité organisée s'applique néanmoins à ces délits[24].

On a ainsi un régime général, déjà dérogatoire de la procédure de droit commun, applicable en matière de criminalité organisée et prévu aux articles 706-73 et suivants du Code de procédure pénale, et une multitude de " sous-régimes " applicables à diverses infractions, que le législateur a inclus artificiellement dans le champ de la criminalité organisée alors qu'elles n'en relèvent pas. En somme, à chaque infraction son régime.

Ce régime d'exception est non seulement particulièrement obscur, dans la mesure où la technique des renvois est illisible, et, partant, il est manifestement contraire au principe d'accessibilité et d'intelligibilité de la loi.

Le Conseil constitutionnel a vu depuis longtemps dans ce principe un objectif à valeur constitutionnelle. Ainsi, dans une décision du 16 décembre 1999, il affirme et rattache explicitement l'accessibilité et l'intelligibilité de la loi aux articles 4, 5, 6 et 16 de la Déclaration des droits de l'homme et du citoyen de 1789[25].

Le principe d'accessibilité et d'intelligibilité de la loi impose au législateur d'adopter des dispositions suffisamment précises et des formules non équivoques[26], afin de prémunir les sujets de droit contre une interprétation contraire à la Constitution ou contre le risque d'arbitraire, sans reporter sur des autorités administratives ou juridictionnelles le soin de fixer les règles dont la détermination n'a été confiée qu'à la loi[27].

On peut légitimement avancer que la mise en place du mécanisme des renvois, ainsi que l'enchevêtrement de plusieurs systèmes dérogatoires au sein même du régime applicable à la criminalité organisée, portent atteinte, par leur complexité, à l'objectif de valeur constitutionnelle d'accessibilité et d'intelligibilité de la loi.

Conclusion

Pour le législateur, " *Les attaques informatiques réalisées contre les systèmes de traitement automatisé de données mis en oeuvre par l'État sont des armes que peuvent utiliser les terroristes* "[28], ce qui justifiait donc l'extension de la circonstance de bande organisée.

Pourtant, on l'a lu et constaté, l'extension de la circonstance de bande organisée n'avait d'autres finalités que d'appliquer à certaines atteintes à un STAD les techniques spéciales d'enquête applicable en matière de criminalité organisée, alors même que les atteintes aux STAD ne relèvent pas par nature de la criminalité organisée.

Certes, le champ d'application de l'article 706-72 modifié du Code de procédure pénale est limité, puisqu'il ne s'applique qu'aux seules atteintes à un STAD commises en bande organisée. Or ces atteintes commises en bande organisée ne peuvent être, selon les dispositions du nouvel article 323-4-1 du Code pénal, que des atteintes à un STAD " mis en oeuvre par l'État ". Toutefois, rien n'interdit aux autorités de poursuite de choisir en début de procédure de qualifier les faits avec la circonstance de bande organisée.

Or, la qualification retenue en début de procédure fixe le cadre de l'enquête. Elle détermine les pouvoirs coercitifs des enquêteurs et l'étendue des atteintes autorisées à la vie privée, par le biais des écoutes téléphoniques et sonorisations notamment. Il existe donc un véritable risque d'instrumentalisation de la circonstance de bande organisée.

Si, pour le législateur, l'extension de la circonstance de bande organisée était justifiée par la nécessité de lutter contre le terrorisme et de protéger des cyberattaques les STAD mis en oeuvre par l'État, il a créé une nouvelle procédure d'exception, qui prend place dans un ensemble dérogatoire déjà obscur et inintelligible.

Au nom d'un impératif de cyberdéfense et dans une logique sécuritaire, le législateur, en adoptant de façon accélérée la loi du 13 novembre 2014, a oublié les mots de Mireille Delmas-Marty : " *L'État qui prétend éradiquer toute insécurité, même potentielle, est pris dans une spirale de l'exception, de la suspicion et de l'oppression qui peut aller jusqu'à la disparition plus ou moins complète des libertés* " [29]

Notes :

1. Le Figaro, « La chaine TV5 Monde piratée par des militants de l'Etat islamique », 9 avril 2015, URL : http://tvmag.lefigaro.fr/programme-tv/article/television/86345/la-chaine-tv5-monde-piratee-par-des-militants-de-l-etat-islamique.html
2. France TV Info, « Piratage de TV5 Monde : ce que l'on sait et ce que l'on ne sait pas », 10 avril 2015, URL : http://www.francetvinfo.fr/faits-divers/terrorisme/piratage-de-tv5-monde/piratage-de-tv5-monde-ce-que-l-on-sait-et-ce-que-l-on-ne-sait-pas_873143.html
3. Le Figaro, « Cyberattaque : TV5 Monde reprend sa diffusion, la faille de sécurité n'a pas été trouvée », 9 avril 2015, URL : http://www.lefigaro.fr/actualite-france/2015/04/09/01016-20150409ARTFIG00159-attaque-de-tv5-la-dgsi-et-la-sous-direction-antiterroriste-saisies.php
4. Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JORF du 7 janvier 1978 p. 227
5. Loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique, JORF du 6 janvier 1988 p. 231
6. Loi n° 2015-912 du 24 juillet 2015 relative au renseignement
7. Loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme, JORF n°0263 du 14 novembre 2014 p. 19162
8. TGI Versailles, 18 déc. 2007, n° 0511965021, L. c/ Valéo (abus de confiance) ; TGI Clermont-Ferrand, ch. corr., 26 sept. 2011, Sctés X et Y c/ Mme Rose, Commentaire E. A. CAPRIOLI, Communication Commerce électronique n° 3, Mars 2012, comm. 36 (vol et abus de confiance)
9. Circulaire du 5 décembre 2014 de présentation de la loi n°2014-1353 renforçant les dispositions relatives à la lutte contre le terrorisme - Renforcement de la coordination de la lutte antiterroriste, BO Justice et Libertés du 31 décembre 2014, N°2014-12, Section 4
10. Voir l'analyse de E. A. CAPRIOLI, « Condamnation pour abus de confiance d'un salarié ayant détourné des données professionnelles à des fins personnelles », Communication Commerce électronique, n°2, février 2015, comm. 17
11. Observations de D. AUROI, Compte-rendu de la première séance du 18 septembre 2014, Article 12
12. Projet de loi, Loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme, Article 12
13. Assemblée nationale, Première lecture, Compte-rendu de la première séance du 18 septembre 2014, Article 12
14. E. DUPIC, « Une nouvelle loi pour renforcer les dispositions relatives à la lutte contre le terrorisme », Gaz. Pal. 2014, n° 330
15. M. QUÉMÉNER, « Les dispositions relatives au numérique de la loi n°2014-1353 du 13 novembre 2014 renforçant la lutte contre le terrorisme », Revue Lamy Droit de l'Immatériel, n°111, Janvier 2015, p. 21
16. Rapport n° 343 (2010-2011) de M. J. de ROHAN, fait au nom de la commission des affaires étrangères et de la défense, déposé le 9 mars 2011, URL : http://www.senat.fr/rap/l10-343/l10-3438.html
17. Rapport n°9 (2014-2015) de MM Jean-Jacques HYEST et Alain RICHARD, au nom de la commission des lois
18. H. ROUIDI, « La loi n°2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme : quelles évolutions ? », publié dans le dossier « Les nouvelles dispositions de lutte contre le terrorisme », AJ Pénal 2014, p. 555
19. Loi n° 2007-1544 du 29 octobre 2007 de lutte contre la contrefaçon, JORF n°252 du 30 octobre 2007 p. 17775
20. Loi n° 2013-1117 du 6 décembre 2013 relative à la lutte contre la fraude fiscale et la grande délinquance économique et financière, JORF n°0284 du 7 décembre 2013 p. 19941
21. Conseil constitutionnel, Décision n°2013-679 DC du 4 décembre 2013, cons. 77
22. Conseil constitutionnel, Décision n°2014-420/421 QPC du 9 octobre 2014, cons. 13
23. Rapport n°9 (2014-2015) de MM Jean-Jacques HYEST et Alain RICHARD, au nom de la commission des lois, Article 12 bis
24. Voir notre article : E. DAOUD et C. GODEBERGE, « La loi du 13 novembre 2014 constitue-t-elle une atteinte à la liberté d'expression ? De la nouvelle définition de la provocation aux actes de terrorisme et de l'apologie de ces actes », publié dans le dossier « Les nouvelles dispositions de lutte contre le terrorisme », AJ Pénal 2014, p. 563
25. Conseil constitutionnel, Décision n°99-421 DC du 16 décembre 1999, cons. 13
26. Conseil constitutionnel, Décision n°2011-644 DC du 28 décembre 2011, cons. 16
27. Conseil constitutionnel, Décision n°2014-694 DC du 28 mai 2014, cons. 7 ; Conseil constitutionnel, Décision n°2013-685 du 29 décembre 2013, cons. 88
28. Projet de loi renforçant les dispositions relatives à la lutte contre le terrorisme, Etude d'impact, 8 juillet 2014, § 2.7.3.3
29. M. DELMAS-MARTY, « Libertés et sureté dans un monde dangereux », Seuil, 2010