LA REVUE DU
GRASCO

www.grasco.eu
www.larevuedugrasco.eu

N°16— Juillet 2016

Parution trimestrielle
Gratuite
ISSN 2272-981X

EDITORIAL

L'attentat perpétré le 14 juillet 2016 à Nice qui a fait 84 morts dont 13 mineurs et 308 blessés dont 70 sont toujours hospitalisés et dont 19 ont un pronostic vital encore engagé, a plongé le pays tout entier dans l'effroi y compris plusieurs hommes politiques dont les déclarations, de toute évidence, révèlent qu'ils ont cédé à la peur et au désarroi.

Dans une démocratie, l'exercice du pouvoir exige de celles et ceux à qui il a été confié par le suffrage universel, d'être capables, lorsque l'épreuve frappe, de faire face, ensemble, en refusant les clivages partisans pour garantir la pérennité de l'Etat de droit.

Comme l'a parfaitement analysé Patrick Lagadec, spécialiste de la gestion du risque et de la gestion de crise, ancien directeur de recherche à l'Ecole Polytechnique, la résilience collective commande « d'opposer aux dynamiques de mort des dynamiques de vie ». Il est impératif de refuser de sombrer dans « un repli archaïque sur la peur et la haine » et cultiver au contraire, « une dynamique de vie » qui « signifie courage psychologique et intellectuel pour inventer, tisser des liens nouveaux » (La Croix, 17 juillet 2016).

Le mode opératoire utilisé, le recours à un véhicule-bélier était imprévu bien que connu et préconisé de longue date par la propagande djihadiste. D'autres modes opératoires, d'autres profils d'acteurs imprévus surgiront, à l'évidence. C'est pourquoi, Patrick Lagadec invite les dirigeants à « s'impliquer de façon décisive » de manière à « se mettre en capacité de naviguer dans l'imprévu », « sans quoi les informations ne circuleront pas, les crises ne seront ni anticipées ni gérées ».

A Nice, le profil du terroriste interpelle. Totalement inconnu des services de renseignement, il ne faisait l'objet d'aucun signalement pour une quelconque radicalisation. Il ne pouvait pas être décelé par le dispositif mis en place dès avril 2014 comportant notamment la création d'un numéro vert pour les familles et dont l'utilité, au demeurant, ne saurait être remise en cause puisqu'il a déjà permis de signaler plus de 5 000 individus et d'empêcher de nombreux départs.

En revanche, selon le Procureur de Paris, François Molins, le terroriste était connu des services de police et de justice pour des

SOMMAIRE

EDITO 1

INTERVIEW :

DANIÈLE JOURDAIN-MENNINGER, PRÉSIDENTE DE LA MISSION INTERMINISTÉRIELLE DE LUTTE CONTRE LES DROGUES ET LES CONDUITES ADDICTIVES (MILDECA) 4

PHÉNOMÉNOLOGIE DE LA CRIMINALITÉ ORGANISÉE :

LES ENTREPRISES FACE À LA CYBERCRIMINALITÉ, PAR ADELINE CHAMPAGNAT 12

DOCTRINE :

LES PROCÉDURES DE LA CRIMINALITÉ ORGANISÉE ET LA LOI DU 3 JUIN 2016 : QUELS DÉFIS POUR LA DÉFENSE PÉNALE ? PAR MAXIME TESSIER 19

LE NOUVEAU DÉLIT DE TRAFIC DE BIENS CULTURELS PROVENANT D'UN THÉÂTRE D'OPÉRATIONS DE GROUPEMENTS TERRORISTES : QUELLE EFFICACITÉ ?, PAR DOROTHÉE GOETZ 27

COMMENTAIRE JURISPRUDENTIEL :

LE CUMUL DES POURSUITES FISCALES ET PÉNALES À L'ÉPREUVE DE LA CONSTITUTION, PAR CHANTAL CUTAJAR 38

DU CÔTÉ DES PRATICIENS :

ÉVOLUTION DES SERVICES DE PAIEMENT : ENJEUX ET RISQUES, PAR DAN BENISTY 41

DU CÔTÉ DES VICTIMES :

REGARD SUR LES DISPOSITIFS D'AIDE ET D'INDEMNISATION DES VICTIMES D'ATTENTATS, PAR CLAUDE LIENHARD 45

REGARDONS AILLEURS :

L'OFFICE ANTI-FRAUDE DE CATALOGNE, UNE APPROCHE DIFFÉRENTE DE LA LUTTE CONTRE LA CORRUPTION, PAR BRUNO GONZÁLEZ VALDELIÈVRE 49

COOPÉRATION JUDICIAIRE ET POLICIÈRE :

LE RÔLE COMPLÉMENTAIRE DU RÉSEAU JUDICIAIRE EUROPÉEN ET D'EUROJUST DANS LA LUTTE CONTRE LA CRIMINALITÉ TRANSFRONTALIÈRE, PAR FLORIN-RĂZVAN RADU 59

RAPPORT:

SYNTHÈSE DU RAPPORT INTÉRIMAIRE SOCTA 2015, PAR ELENA PELLISER 68

COMPTES-RENDUS DE COLLOQUES, SÉMINAIRES :

COMPTE RENDU DE LA RÉUNION « IDENTITÉ SÉCURISÉE : UN ENJEU ÉCONOMIQUE ET SÉCURITAIRE MAJEUR, LA FRANCE EN RETARD » 76

COMPTE RENDU DE LA TABLE RONDE SUR LA LUTTE CONTRE LE FINANCEMENT DU TERRORISME EN FRANCE 78

faits de menaces, violences, vols et dégradations commis entre 2010 et 2016. Le 24 mars 2016 il est condamné à six mois de prison avec sursis pour avoir agressé un automobiliste et provoqué une fracture du crâne avec une palette de bois qu'il lui a envoyé au visage parce que ce dernier lui demandait de déplacer son véhicule qui encombrait la route.

Ce nouveau profil de terroriste doit nous amener à nous interroger sur la manière de prendre en compte dans le cadre d'une stratégie de prévention, les condamnations judiciaires et la mine d'informations contenues dans le dossier du condamné. L'analyse criminelle de ces informations devrait être systématisée au moyen de programmes informatiques capables de faire apparaître des atypismes à l'image des dispositifs mis en oeuvre pour déceler les flux financiers illicites.

En outre, la perméabilité de certains profils psychologiques fragiles aux thèses de l'Etat islamique favorisant le passage à l'acte doit également être l'objet d'attentions particulières. En l'état du droit il n'est pas possible de confier à un expert psychiatre le soin d'évaluer la dangerosité d'un individu alors même que plusieurs signes inquiétants se sont manifestés.

Les Etats de droit doivent trouver les moyens de se protéger tout en respectant les principes qui les caractérisent en tant qu'Etats de droit. L'analyse systématique des données relatives aux personnes condamnées et leur suivi, source d'ingérence dans la vie privée est aujour'hui nécessaire. Mais elle ne sera acceptable que si la garantie des droits est préservée. Les avocats doivent réfléchir à la place qui doit être la leur dans ces nouveaux dispositifs qui restent à inventer.

Il est clair que le développement d'un dispositif reposant sur l'analyse et le traitement des informations sur les personnes condamnées sous le prisme du risque terroriste nécessitera de doter la chaîne judiciaire de moyens supplémentaires.

Il est impératif, pour qu'une politique criminelle de lutte contre le terrorisme soit en même temps efficace et respectueuse de l'Etat de droit, qu'elle prenne en compte la nature protéiforme de la menace terroriste. La prévention du passage à l'acte d'individus agissant de manière apparemment autonome l'impose.

La lutte contre le terrorisme a un prix. Les proches des victimes décédées le savent mieux que quiconque.

Notes :

1 Auteur de « Le continent des imprévus. Journal de bord des temps chaotiques, Manitoba/ Les Belles Lettres.

LA REVUE DU GRASCO

Numéro ISSN : 2272-981X

Université de Strasbourg, UMR-DRES 7354

11, rue du Maréchal Juin - BP 68 - 67046 STRASBOURG CEDEX

Site internet : http://www.GRASCO.eu

Adresse mail : information@grasco.eu

Directrice de la revue du GRASCO : Chantal CUTAJAR

Directrice adjointe de la revue du GRASCO : Jocelyne KAN

Rédacteur en chef -Conception : Sébastien DUPENT

Relecture - Correction : Claudia-Vanita DUPENT

Isabelle FISHER

COMITÉ SCIENTIFIQUE DU GRASCO

Jean Pradel : Jean PRADEL né en 1933 fut successivement magistrat (de 1959 à 1969), puis professeur agrégé en 1969. D'abord affecté à la Faculté de droit de Tunis, il gagne Poitiers en 1972. Il a écrit divers ouvrages, notamment - Droit pénal général, Procédure pénale, Droit pénal comparé, Droit pénal spécial (en collaboration avec M. Danti-Juan) et Droit pénal européen (avec G. Corstens, président de la Cour suprême des Pays-Bas et G. Vermeulen). Il a présidé l'Association française de droit pénal et participé à de nombreux congrès internationaux

Yves Strickler : Docteur de l'Université de Strasbourg, Maître de conférences à Toulouse, Professeur agrégé à Nancy, puis à Strasbourg où il a dirigé l'Institut d'études judiciaires, exercé les fonctions de Vice-président du Conseil scientifique et créé la Fédération de recherche CNRS *L'Europe en mutation*, il est depuis 2010 **Professeur à l'Université Nice Sophia Antipolis**, où il dirige le *Centre d'études et de recherches en droit des procédures* (CERDP). Il y enseigne le droit civil et le droit processuel.

François Fourment : professeur de droit privé et sciences criminelles à l'Université de Lorraine. Il y dirige l'Institut François Geny (EA n° 1138). Il est spécialiste de droit pénal, plus particulièrement de procédure pénale, de droit pénal européen des droits de l'Homme et de droit pénal de la presse. Il est notamment l'auteur d'un manuel de procédure pénale (éditions Paradigme) et responsable des chroniques de jurisprudence de procédure pénale (trimestrielles) et de droit de la presse (quadrimestrielles) à la *Gazette du Palais*, dont il codirige l'édition trimestrielle spécialisée de "Droit pénal et procédure pénale".

Michel Storck : professeur à l'Université de Strasbourg. Il dirige le Centre du droit de l'entreprise. Il est responsable du Master droit des affaires. Il est Président de la Fondation des Presses Universitaires de Strasbourg. Il assure des enseignements en droit des affaires, notamment en droit des marchés financiers.

Juliette Lelieur : maître de conférences à l'Université de Strasbourg, membre de l'Unité mixte de recherche DRES et habilitée à diriger des recherches, membre de la Commission nationale des sanctions (lutte contre le blanchiment de capitaux). Spécialisée en droit pénal des affaires et droit pénal international, européen et comparé, elle a été chercheuse à l'Institut Max Planck de droit pénal étranger et international ainsi qu'à l'Université de Bâle et a participé aux travaux du Groupe de travail sur la corruption de l'OCDE en tant que collaboratrice du Président. Elle a codirigé la publication de deux ouvrages : L'espace judiciaire européen civil et pénal : Regards croisés, Dalloz, 2009 et Combattre la corruption sans juge d'instruction, Secure-Finance, 2011.

Jean-Paul Laborde : conseiller à la Cour de cassation, chambre commerciale. Il a dirigé pendant de longues années la branche prévention du terrorisme de l'Office des Nations Unies contre la Drogue et le Crime (ONUDC) basé à Vienne. Il a été Directeur de l'Equipe spéciale de la lutte contre le terrorisme des Nations Unies et Conseiller spécial du Secrétaire général. Il est l'auteur notamment de "État de droit et crime organisé – Les apports de la Convention des Nations Unies contre la criminalité transnationale organisée", Paris, Dalloz, 2005.

Claude Mathon : avocat général à la Cour de cassation (chambre criminelle). Auparavant, après avoir développé une carrière essentiellement comme procureur de la République, il a dirigé le Service Central de Prévention de la Corruption. A cette occasion, outre les matières satellites de la corruption comme les fraudes, le blanchiment..., il a eu l'opportunité de se spécialiser en intelligence économique et a présidé à la rédaction de trois rapports : «Entreprises et intelligence économique, quelle place pour la puissance publique ? - 2003 », « Intelligence économique et corruption - 2004 », « La protection du secret des affaires : enjeux et propositions - 2009 ».

Jocelyne Leblois-Happe : Professeur à l'Université de Strasbourg, chargée de cours à l'Université Albert-Ludwig de Fribourg-en-Brisgau, membre du groupe European Criminal Policy Initiative et du groupe d'experts sur la politique pénale de l'UE auprès de la commission européenne

INTERVIEW

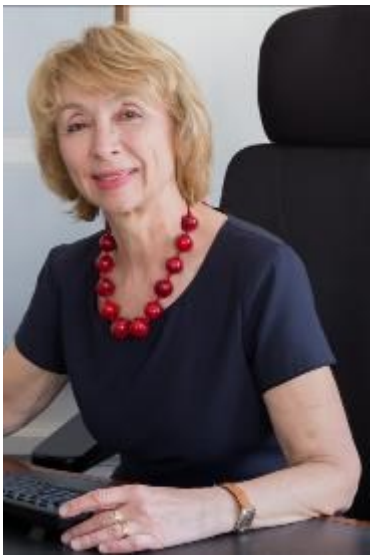
DANIÈLE JOURDAIN-MENNINGER, PRÉSIDENTE DE LA MISSION INTERMINISTÉRIELLE DE LUTTE CONTRE LES DROGUES ET LES CONDUITES ADDICTIVES (MILDECA)

PROPOS RECUEILLIS PAR JOCELYNE KAN

L.R.D.G. : Quelles sont les raisons pour lesquelles la MILDECA a remplacé la MILDT (Mission interministérielle de lutte contre la drogue et la toxicomanie) par décret du 11 mars 2014 ?

Lorsque j'ai été nommée présidente de la MILDT en septembre 2012, ma première tâche a été d'impulser le travail d'élaboration du nouveau plan gouvernemental de lutte contre les drogues et les conduites addictives, pour les années 2013-2017. Dans ce cadre, il m'est apparu important de redéfinir le champ de compétence de cette mission car son rôle d'impulsion et de coordination de l'action publique souffrait d'un certain nombre d'imprécisions d'ordre juridique.

En effet, le décret de 1999 instituant sous leur forme actuelle le Comité interministériel de lutte contre la drogue et la toxicomanie et de prévention des dépendances et la Mission interministérielle de lutte contre la drogue et la toxicomanie, codifié en 2005 dans les articles R 3411-11 à R 3411-16 du Code de la santé publique, n'indiquait pas explicitement que la compétence de la Mission interministérielle concernait la globalité des substances psychoactives et des conduites addictives et cela sur l'ensemble des volets de la réduction de l'offre et de la demande.



Le plan gouvernemental 2013/2017 validé par le Premier ministre lors de la réunion du comité interministériel du 19 septembre 2013 a donc proposé de renforcer la gouvernance au niveau central et territorial.

Par conséquent l'article R 3411-13 du Code de la santé publique a été modifié en conséquences et le terme « toxicomanies » a été remplacé par « conduites addictives » permettant ainsi de préciser la compétence de la Mission interministérielle sur l'ensemble des substances psychoactives et des addictions sans produit. Cette modification était également nécessaire afin de mettre en cohérence la politique publique avec l'état des connaissances scientifiques en la matière.

Il s'agissait également d'inscrire dans ce même article réglementaire la lutte contre le trafic parmi les domaines où sa coordination s'exerce, afin de couvrir l'ensemble de la politique publique en la matière. La référence à la réduction de l'offre, en écho avec la réduction de la demande, s'inscrit par ailleurs pleinement dans la perspective d'approche intégrée de la lutte contre la drogue et les conduites addictives.

L.R.D.G. : Quel est l'état des lieux des drogues, de leur usage, des conduites addictives en France

et quelles sont les tendances récentes ?

Tout d'abord, je précise que s'agissant de l'état des lieux des drogues, de leur usage et des conduites addictives, il existe un opérateur sous la tutelle de la MILDECA, qui a été créé en 1993, l'Observatoire français des drogues et des toxicomanies (OFDT). C'est un groupement d'intérêt public qui a pour objet d'éclairer les pouvoirs publics, les professionnels du champ et le grand public sur le phénomène des drogues et des addictions. Il rassemble, via son dispositif permanent d'observation et d'enquêtes, des informations provenant de sources différentes et scientifiquement validées sur les substances licites comme illicites. Il fait également l'analyse et la synthèse des données dispersées relatives aux drogues issues de différentes sources. Il est en mesure d'apporter un concours méthodologique à la préparation et au suivi des travaux d'évaluation du plan gouvernemental. Il renseigne et documente de multiples questions dans le domaine des substances psychoactives et des dépendances : qui consomme et comment les produits ? quels sont les dommages sanitaires et sociaux occasionnés par ces usages ? quelles sont les opinions et les perceptions sur les drogues ? quelles réponses publiques sont apportées au phénomène ? comment évoluent les marchés ? L'OFDT travaille également sur les jeux de hasard et d'argent et la question de l'abus d'écrans.

L'OFDT est aussi l'un des relais nationaux en tant que point focal de l'Observatoire européen des drogues et des toxicomanies (EMCDDA), agence de l'Union européenne basée à Lisbonne, qui a pour mission de fournir des informations objectives fiables et comparables au niveau européen sur le phénomène des drogues illicites et des toxicomanies et leurs conséquences.

Au vu des études menées par cet organisme, l'alcool et le tabac sont les substances psychoactives les plus consommées en France. Le cannabis est de loin la substance illicite la plus consommée, 10 fois plus que la cocaïne ou l'ecstasy et 55 fois plus que l'héroïne pour les consommations annuelles.

Nous disposons aussi d'enquêtes menées auprès d'un échantillon représentatif de la population française, comme le Baromètre santé et les enquêtes en population jeune (Enquête sur la Santé et les Consommations lors de l'Appel de Préparation À la Défense (ESCAPAD), European School Project on Alcohol and other Drugs (ESPAD), Health Behaviour in School-Aged Children (HBSC)). Elles permettent de donner des estimations du nombre de consommateurs de substances psychoactives dans l'ensemble de la population.

Ces chiffres donnent un ordre de grandeur du nombre des usagers et doivent de ce fait être lus comme des données de cadrage.

Les données dont nous disposons, sur les expérimentations et les usages réguliers selon le sexe et l'âge, font apparaître le poids de la consommation d'alcool et de tabac à tous les âges, même si parmi les plus jeunes la part des usagers de cannabis est relativement importante. Les hommes apparaissent toujours plus consommateurs que les femmes, à l'exception des médicaments psychotropes, et on assiste à une consommation croissante du tabac chez les jeunes femmes. Concernant les différences entre générations, les produits illicites s'avèrent quasi-exclusivement consommés par les plus jeunes. Le tabagisme est de moins en moins fréquent avec l'âge alors que l'usage d'alcool a tendance au contraire à augmenter.

En France, environ 78 000 décès prématurés par an peuvent être attribués au tabagisme. Un fumeur a une espérance de vie diminuée de 20 à 25 ans par rapport à un non fumeur.

S'agissant de l'alcool, le nombre de décès annuels est évalué à 49 000, dont un tiers par cancer et un quart par maladie cardiovasculaire. La consommation excessive et chronique d'alcool est directement à l'origine de certaines pathologies telles que la cirrhose du foie, la psychose alcoolique ou le syndrome d'alcoolisation foetale. Une alcoolisation ponctuelle excessive peut aussi entraîner des accidents (de la route, professionnels ou de la vie courante), des rixes et des suicides. On estime que la conduite sous l'influence de l'alcool est responsable d'environ 1 400 décès par an.

Le cannabis occupe sur le plan sanitaire une place spécifique par rapport aux autres drogues illicites. Si sa toxicité suscite beaucoup de discussions et recherches son caractère néfaste a été clairement établi chez le jeune en pleine maturation cérébrale. Si l'on ne dispose pas de données sur les décès par cancers ou maladies cardio-vasculaires

imputables au cannabis, sa consommation serait responsable de 170 à 190 décès annuels par accidents de la circulation.

Concernant les drogues injectables, l'usage de drogues peut entraîner des maladies infectieuses (sida, hépatites, infections bactériennes) en lien avec les voies d'administration des substances, principalement l'injection, et des troubles induits par la substance elle-même (troubles du comportement ou surdoses). En 2011, 340 décès par surdose ont été dénombrés. Avec 60 décès par sida en 2012 parmi les usagers de drogues par voie injectable, la baisse initiée au milieu des années 1990 se poursuit lentement. La prévalence de la séropositivité au VIH décroît chez les usagers de drogues, tout comme les nouveaux cas de sida (88 en 2012, contre 1 319 en 1995). La prévalence de la séropositivité au virus de l'hépatite C (VHC) diminue lentement depuis 1999, mais reste beaucoup plus élevée que celle du VIH.

L.R.D.G. : Que prévoit le plan gouvernemental de lutte contre les drogues et les conduites addictives ?

Le plan 2013-2017 repose sur trois grandes priorités :

- Fonder l'action publique sur l'observation, la recherche et l'évaluation : en progressant dans la compréhension des conduites addictives ; en soutenant la recherche sur les nouveaux traitements médicamenteux et les stratégies thérapeutiques innovantes ainsi que les recherches en sciences sociales ; en faisant de la recherche un outil d'aide à la décision.

- Prendre en compte les populations les plus exposées pour réduire les risques et les dommages sanitaires et sociaux : en empêchant, retardant et limitant les consommations des jeunes ; en améliorant le soin et l'accompagnement des femmes usagères de drogue ; en rapprochant les dispositifs des populations les plus éloignées (que ce soit pour des raisons géographiques ou sociales) ; par la prévention des addictions dans le monde du travail.

- Renforcer la sécurité, la tranquillité et la santé publiques au niveau national et international : en luttant contre les trafics et contre toutes les formes de délinquance liées aux consommations de substances psychoactives ; en favorisant l'acceptabilité sociale des usagers et des dispositifs de soins et de réduction des risques notamment par les actions de médiation sociale ; en améliorant l'articulation entre les champs judiciaire et sanitaire ; en luttant contre le trafic au niveau local et international ; en prenant en compte les phénomènes émergents en matière de trafic.

L.R.D.G. : Comment s'exerce la coopération de la Mission interministérielle avec l' Agence de recouvrement des avoirs saisis et confisqués (AGRASC) dans la lutte contre les trafics ?

La MILDECA entretient des liens étroits avec l'AGRASC depuis le début de son fonctionnement en 2011. Ce sont deux partenaires naturels qui promeuvent conjointement la saisie et la confiscation en étant convaincus de l'efficacité des réponses pénales qui impactent le patrimoine, singulièrement dans les affaires de criminalité organisée.

L'AGRASC gère les sommes saisies dans les procédures judiciaires ainsi qu'un grand nombre de biens saisis (les immeubles, les biens saisis avant jugement…), et verse à la MILDECA le produit des biens confisqués dans les affaires de trafic de stupéfiants afin d'alimenter le fonds de concours drogues. Ce fonds de concours, géré par la MILDECA, est intégralement affecté à la lutte contre l'usage et le trafic de stupéfiants. Les sommes versées sur le compte du fonds sont réparties chaque année entre les ministères régaliens, qui ont été à l'origine des saisies et confiscations des biens des trafiquants de drogue, pour financer des actions qui s'inscrivent dans la stratégie du plan gouvernemental préparé par la MILDECA. Une partie de ces sommes est en outre spécifiquement affectée à des actions de prévention de la consommation de drogues.

De ce fait, le fonds de concours a la triple vocation de priver les trafiquants des bénéfices de leur trafic et de leur patrimoine, de renforcer l'action des services engagés dans la lutte contre l'usage et les trafics de drogue et de contribuer à la prévention des consommations de drogues.

Un véritable mouvement de fonds en ce sens existe dans les services d'enquête et les juridictions, qui s'est accéléré avec la loi du 9 juillet 2010 créant l'AGRASC, posant un véritable régime de saisie à des fins conservatoires des biens susceptibles d'être confisqués, et prévoyant des procédures particulières pour la saisie des biens spécifiques. Dans ce contexte, le nombre et la complexité des

biens saisis s'accroissent.

Le régime juridique né de la loi du 9 juillet 2010 devrait permettre davantage de confiscations, notamment en matière de trafic de stupéfiants, car la confiscation est évidemment plus aisée au moment de la condamnation si le bien est déjà saisi : d'une part, parce que les investigations auront permis de mettre à jour le patrimoine des trafiquants qui se sont adaptés aux saisies en procédant au blanchiment des sommes provenant du trafic ; ensuite, parce que certaines formalités auront été faites en amont (par exemple vérification de l'absence d'hypothèque avant la saisie conservatoire d'un immeuble...) et enfin, parce que la saisie aura évité la dilapidation des biens et l'organisation de l'insolvabilité pendant la durée de la procédure.

Pour ce faire, nous devons encore travailler afin que ces dispositions récentes trouvent leur pleine application. Au moment du jugement de l'affaire, s'il n'est pas statué sur le sort des biens saisis, ceux-ci pourront alors être réclamés par leurs propriétaires, et, s'ils ne le sont pas, seront reversés au budget général sans abonder le fonds de concours drogues. Dans plusieurs cours d'appel, les magistrats du parquet et de l'instruction ont instauré des pratiques afin de permettre l'identification rapide des biens saisis, par exemple une cote patrimoine recelant l'ensemble des éléments de la procédure concernant les saisies effectuées, afin que la juridiction de jugement ait l'ensemble de ces éléments à sa disposition sans recherche complexe dans la procédure.

La formulation utilisée par le tribunal pour prononcer la saisie a aussi son importance. La pratique la plus rigoureuse consiste à énumérer les biens (avec les numéros de scellés correspondants lorsqu'il y en a) confisqués. Si le tribunal souhaite confisquer l'ensemble des biens saisis, il convient d'utiliser la formule générale « le tribunal prononce la confiscation des biens saisis » et non « la confiscation des scellés ». En effet, certains biens saisis ne sont pas des scellés et ne peuvent alors pas être confisqués (immeubles, comptes bancaires...). Il faut savoir en revanche qu'il n'est pas nécessaire de préciser dans la décision que les biens saisis, en matière de stupéfiants, abonderont le FDC drogues. Il suffit simplement que toute décision de confiscation définitive, de quelque nature qu'elle soit, soit adressée à l'AGRASC, et c'est l'AGRASC qui aiguillera les fonds entre le budget général de l'État et le FDC drogues.

La MILDECA a rédigé récemment une note, en lien notamment avec l'AGRASC, à destination des directeurs de greffe, afin de répondre aux questions techniques que pose l'abondement du fonds de concours drogues. Cette note a été diffusée par une dépêche conjointe de la DSJ et de la DACG du 22 mars dernier.

L'AGRASC et la MILDECA interviennent aussi en formation continue des enquêteurs et professionnels de justice sur ces questions. Les juridictions doivent être en mesure de décider en opportunité des biens qui doivent être confisqués ou non. Nous nous attachons à donner toute leur portée aux dispositions de la loi du 9 juillet 2010. Un travail important est réalisé par les services d'enquête et les magistrats pour identifier le patrimoine des trafiquants et dresser la cartographie des flux financiers. Chacun est mobilisé pour que ce travail porte ses fruits.

L.R.D.G. : D'après-vous, le « tout répressif » est-il un moyen efficace pour prévenir la récidive ? Y-a-t-il une nouvelle approche de la prévention dans le champ de la délinquance liée aux addictions ?

Dans le plan gouvernemental de lutte contre les drogues et les conduites addictives 2013/2017, l'enjeu de la lutte contre toutes les formes de délinquance liées aux consommations de substances psychoactives est un des trois axes prioritaires du plan.

Les actions actuellement pilotées par la MILDECA dans le cadre du plan gouvernemental participent à la fois d'une démarche de réflexion sur les réponses pénales mises en oeuvre, et d'une démarche d'expérimentation dans le cadre d'un projet pilote engagé avec le tribunal de grande instance de Bobigny pour lutter contre la récidive, à destination des publics ayant des conduites addictives. Par ailleurs, la MILDECA soutient et accompagne les projets mis en oeuvre par le ministère de la Justice concernant la prévention, la prise en charge, la réduction des risques pour les personnes placées sous main de justice.

La MILDECA a ainsi participé en novembre 2013 à une visite d'études sur la prise en charge judiciaire et sanitaire de la toxicomanie au Canada initiée et organisée par le magistrat de liaison français à Ottawa. Les programmes de traitement de la toxicomanie, qui ont été observés

à Montréal et Vancouver, sont articulés autour de l'idée d'une approche globale de la personne et d'une concertation renforcée entre les différents acteurs du programme, notamment ceux de la santé et de la justice.

C'est la raison pour laquelle la MILDECA et le ministère de la Justice ont, au retour de cette mission, proposé un projet d'expérimentation pilote de prise en charge socio-judiciaire des auteurs d'infractions souffrant d'addiction à l'alcool ou aux drogues. La juridiction de Bobigny, qui a déjà été le site de nombreuses expérimentations, a accepté le principe de ce projet, ainsi que le Service Pénitentiaire d'Insertion et de Probation (SPIP) de Seine Saint Denis. Le ministère de la Santé et l'Agence Régionale de Santé (ARS) d'Ile-de-France se sont associés à sa construction avec l'ensemble des acteurs nationaux et locaux, institutionnels et associatifs des champs judiciaires et sanitaires, concernés par le projet, notamment la Fédération Addiction et la Fédération Citoyens et Justice.

Le projet pilote a été construit en commun avec l'ensemble des services concernés en 2014 et a débuté le 30 mars 2015 par les premières orientations prononcées en audience pour une entrée des probationnaires dans le programme spécifique, qui comporte un suivi comportant au moins 5 heures par jour dans un local dédié avec une équipe médico-sociale spécifique au dispositif rattachée à un CSAPA, une équipe du SPIP de Seine-Saint-Denis et des personnels d'associations proposant des activités culturelles, corporelles et/ou sportives.

L'élément fondamental de ce projet est son évaluation scientifique : il ne s'agit pas d'affirmer par conviction que certaines pratiques professionnelles et programmes fonctionnent mieux que d'autres, mais bien de développer en France, et notamment en cette matière, la pratique de l'évaluation des politiques publiques mises en place. Concernant le projet de Bobigny, il est construit, avec l'appui d'un comité scientifique, en utilisant les connaissances issues de programmes similaires dans d'autres pays et déjà évalués. Ce projet fait d'ores et déjà l'objet d'une évaluation concernant sa mise en oeuvre et l'évolution des pratiques professionnelles qu'il induit. Il fera l'objet d'une évaluation d'impact au regard de la prévention de la récidive. D'autres pays comme les États-Unis et le Québec, ou plus près de nous la Belgique, l'Irlande, ont déjà mis en oeuvre ce type de dispositifs spécialisés en matière d'addictions et de drogues, et les ont évalués, y compris en ce qui concerne leur coût-avantage pour la collectivité relativement à celui de la prison. C'est ainsi dans une perspective très pragmatique que ces pays ont choisi de s'engager de manière massive dans ce type de réponses pénales.

Par ailleurs, la MILDECA a soutenu, depuis le début de la mise en oeuvre du plan, un grand nombre de projets présentés par le ministère de la Justice et/ou travaillés en commun avec la MILDECA et les autres ministères concernés, qui ont pour objet de renforcer les liens entre les champs sanitaire et judiciaire, de mieux les articuler, et d'apporter des réponses aux addictions présentées par les publics placés sous main de justice en milieu ouvert et en milieu carcéral.

La MILDECA apporte ainsi un soutien financier aux actions innovantes permettant notamment d'expérimenter de nouvelles pratiques professionnelles impliquant à la fois la santé et la justice dans le champ de la délinquance liée aux addictions.

Concernant les évaluations et réflexions pilotées par la MILDECA, nous avons confié à une équipe de chercheurs une étude concernant le lien entre la consommation d'alcool et de stupéfiants et les atteintes aux personnes, et l'appréhension de cette problématique par les professionnels de justice. Il n'existait pas encore d'étude réalisé sur ce lien à partir de procédures judiciaires, alors qu'il est empiriquement évalué par les professionnels comme important.

Dans le cadre fixé par la lettre de mission qui m'a été adressée par le Premier ministre en 2012,invitant la MILDECA à être force de proposition quant aux évolutions juridiques nécessaires à l'efficacité de la lutte contre la drogue, la toxicomanie et les conduites addictives, la MILDECA a réuni un groupe de travail qui s'est attaché à réfléchir, dans une approche juridique et technique, à l'efficacité de la réponse pénale appliquée aux usagers de stupéfiants, et aux pistes de réforme légale opportunes concernant notamment la norme et ses modalités de mise en oeuvre. Le contexte actuel de très forte consommation de cannabis par les adolescents, l'examen des systèmes juridiques de nos voisins européens, l'importance des moyens déployés par les services d'enquête et la justice pour répondre à ces faits, nous poussent en

effet à interroger la lisibilité et l'efficacité de la norme en matière d'usage de stupéfiants en posant notamment la question de la peine d'emprisonnement encourue pour simple usage.

Concernant l'usage de stupéfiants, le Code de la santé publique pose deux principes : « une personne usant de façon illicite de substances ou plantes classées comme stupéfiants bénéficie d'une prise en charge sanitaire organisée par l'agence régionale de santé » (art L. 3411-1 du CSP) » ; « L'usage illicite de l'une des substances ou plantes classées comme stupéfiants est puni d'un an d'emprisonnement et de 3750 euros d'amende » (art L.3421-1 du CSP) ».

L.R.D.G. : Comment situez-vous la politique de réduction des risques ?

Un troisième pilier juridique concernant la réponse publique à l'usage de stupéfiants a récemment évolué : il s'agit de la politique de réduction des risques.

La France a inscrit la politique de réduction des risques, d'abord expérimentée par voie de circulaires du ministre de la Santé, dans son droit positif par la loi n° 2004-806 du 9 août 2004 relative à la politique de santé publique qui posait simplement l'objectif de prévenir la transmission des infections, la mortalité par surdose par injection de drogue intraveineuse et les dommages sociaux et psychologiques liés à la toxicomanie par des substances classées comme stupéfiants. L'ensemble des interventions étaient détaillées dans un décret.

La politique de réduction des risques a connu une évolution récente importante avec la loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé.

L'article 41 de cette loi définit dans le Code de la santé publique (art L. 3411-7 et suivants) de manière claire et précise la politique de réduction des risques et des dommages en listant les types d'interventions autorisées par la loi et en rappelant expressément que les intervenants en réduction des risques agissant conformément aux principes posés par la loi ne peuvent voir leur responsabilité pénale engagée. L'article 41 prévoit par ailleurs que cette politique de réduction des risques est mise en oeuvre en milieu carcéral : cela ouvre la voie aux programmes d'échanges de seringues en prison.

La politique de réduction des risques, d'abord mise en place pour répondre à l'urgence d'une situation catastrophique sur le plan des contaminations VIH et hépatites, correspond en réalité à une évolution bien plus générale dans la prise en charge sanitaire des addictions.

En effet, l'évolution de la compréhension des mécanismes de l'addiction a permis le passage d'une logique en termes de produits (chaque produit à un effet addictif, il convient de le supprimer afin de faire cesser l'addiction) à une logique en termes de mécanismes neurobiologiques de l'addiction communs à l'ensemble des substances. Il s'agit de la rencontre entre un produit, avec ses caractéristiques propres concernant les effets sur le fonctionnement du cerveau, ses effets sur la santé, ses effets psychotropes, avec un individu, son environnement, son histoire, sa personnalité, son patrimoine génétique. Des constantes sont observées par les chercheurs et les addictologues dans ces mécanismes de l'addiction, à savoir un parcours obligatoirement composé de moments de réduction, de maîtrise de la consommation, et de rechutes. En fonction de ces observations, la prise en charge des addictions a évolué d'une situation dans laquelle le sevrage était considéré comme la seule voie (dans une logique de produit, on supprime le produit, donc on supprime l'addiction), à une situation dans laquelle chaque cas individuel est évalué et pris en compte, ce qui implique des modalités de prises en charge diversifiées afin de s'adapter à chaque situation. C'est ainsi que pour certains, une abstinence avec des groupes de parole ou une communauté thérapeutique (en résidentiel) sera efficace ; pour d'autres, cela sera la réduction progressive de la consommation avec un accompagnement, avec ou sans traitement médicamenteux ou traitement de substitution ; pour d'autres enfin, une prise en charge en psychothérapie ou en psychiatrie devra accompagner la démarche (comorbidités psychiatriques). Certains ne parviendront à stabiliser leur consommation qu'avec un traitement de substitution poursuivi sur le très long terme, si ce n'est à vie.

Ce qui ressort de cette évolution, c'est que le sevrage et l'arrêt immédiat et total de la consommation n'est pas la voie unique de la prise en charge des addictions, voire n'est pas adaptée dans de nombreux cas. Il existe par ailleurs d'autres situations intermédiaires dans la consommation de produits que l'addiction, à savoir

l'expérimentation, la consommation festive, l'usage récréatif sporadique, et certaines consommations peuvent ne pas causer, de fait, de dommages graves pour l'individu et la société.

La politique de réduction des risques est donc un paradigme qui s'inscrit dans un continuum, et non en opposition, avec le soin ; dans certaines situations, il sera impossible de faire cesser totalement la consommation d'un individu, et la politique publique visera ainsi à réduire le plus possible les dommages pour lui et les dommages sociaux causés par ces consommations, ce qui va dans le bon sens pour la collectivité. Il est important, et nous y travaillons à la MILDECA, que les professionnels de justice aient connaissance de ces évolutions afin d'en tenir compte dans les réponses pénales et le suivi des condamnés.

L.R.D.G. : Quelle est l'action internationale de la MILDECA ? Que pensez-vous de la Résolution résultant de la session extraordinaire de l'Assemblée générale des Nations Unies du mois d'avril 2016 sur le problème mondial de la drogue ?

La mondialisation représente un défi en matière d'addictions et de trafics, mais elle constitue également l'occasion de mieux connaître les expériences positives et les bonnes pratiques, de mutualiser les moyens de lutte contre le trafic, de partager les valeurs et les acquis. Au plan international, la MILDECA incarne l'approche globale de la France en matière de lutte contre la drogue et la toxicomanie, visant une politique équilibrée entre les mesures de prévention, de soins et de lutte contre le trafic. Elle promeut cette approche multidisciplinaire, ayant comme clé de voûte le respect des droits humains dans toutes les instances internationales et dans ses relations bilatérales.

La politique française s'inscrit dans le respect des conventions internationales et dans un cadre européen qui évolue au fil du temps.

Notre action internationale repose sur cinq piliers repris dans le Plan gouvernemental de lutte contre les drogues et les conduites addictives (2013-2017) :

- Partager les acquis tout en soutenant les axes prioritaires de la France au sein des organisations européennes et internationales (Union européenne, Groupe Pompidou du Conseil de l'Europe, ONUDC, etc.) ;

- Cibler l'action en soutenant la mise en oeuvre et le financement de programmes dans nos zones d'action prioritaires (Afrique de l'Ouest, Afghanistan, Amérique latine et Caraïbes) ;

- Renforcer la sécurité intérieure en favorisant l'échange d'informations opérationnelles et la mutualisation du renseignement avec nos partenaires de confiance ;

- Promouvoir une approche économique de prévention et de lutte contre le trafic de drogue, c'est-à-dire encourager l'identification, la saisie et la confiscation des avoirs liés aux trafics ;

- Offrir une alternative économique viable aux cultivateurs de drogues illicites.

Du 19 au 21 avril 2016, la communauté internationale s'est réunie à New-York pour la session extraordinaire de l'Assemblée générale des Nations Unies (SEAGNU) sur les drogues. Cette rencontre avait pour objectif de définir une nouvelle stratégie mondiale en matière de lutte contre les usages et les trafics de drogues. Dès le premier jour de la SEAGNU, la communauté internationale a adopté par consensus une déclaration finale en sept parties. Ces 24 pages réaffirment l'importance des trois Conventions des Nations Unies sur les drogues tout en proposant une politique plus équilibrée associant lutte contre l'offre et contre la demande, qui reprend très largement la position européenne.

Je me félicite particulièrement que ce texte comporte des recommandations opérationnelles concrètes en vue de répondre au problème mondial de la drogue. Il met l'accent sur la santé publique, la prévention et les aspects sanitaires et sociaux ainsi que sur le respect des droits de l'homme, ce qui constitue une avancée fondamentale. Je me réjouis également de la place importante accordée à la promotion des programmes de soin et de prévention fondés sur des faits scientifiques (evidence-based policies), ce que nous défendons à la MILDECA afin de renouveler les politiques de prévention et de promouvoir des actions de réduction des risques qui ont fait leur preuve.

S'il y a pourtant une chose que je regrette, c'est l'absence de référence à l'abolition de la peine de mort dans cette déclaration finale. Malgré les efforts de plusieurs délégations, tant pour la France que pour l'Union européenne et d'autres pays, nos demandes sont restées lettre morte. L'attente était pourtant forte tant de la part de

certains États que des représentants de la société civile. Je reste profondément convaincue qu'un moratoire sur la peine de mort pour tous les crimes, y compris ceux liés à la consommation et/ou au trafic de drogues, est une nécessité absolue pour l'ensemble de la communauté internationale. C'est pourquoi je me félicite que l'Union européenne se soit exprimée de manière forte à l'issue de l'adoption de la déclaration finale pour réaffirmer sa position.

Même si toutes nos demandes n'ont pas été retenues, je considère cette SEAGNU comme une réussite pour la France, l'Union européenne, mais surtout pour l'ensemble de la communauté internationale. Le compromis auquel nous sommes parvenus avec l'ensemble de nos partenaires réaffirme le caractère central des trois Conventions de contrôle des drogues tout en insistant sur la nécessité de mener des politiques globales et équilibrées aux niveaux national, régional et international. Surtout, elle marque une évolution en s'écartant de politiques prioritairement centrées sur la réduction de l'offre, et en mettant les droits de l'homme, la santé et le bien-être des populations au centre des débats.

OUVRAGES RÉCENTS

LE CONTINENT DES IMPRÉVUS :

JOURNAL DE BORD DES TEMPS CHAOTIQUES

AUTEUR : PATRICK LAGADEC

EDITEUR : MANITOBA - LES BELLES LETTRES

Présentation de l'éditeur

Depuis le tournant du siècle, citoyens et responsables sont confrontés à la multiplication des défis majeurs sur toutes les lignes de front : des dislocations géopolitiques ont bouleversé nos cartes de référence, un état de dérèglement économique et de mutation culturelle s'est durablement installé, des épidémies au potentiel gravissime ont déferlé à l'échelle intercontinentale, le désordre climatique commence à présenter la note...

Le risque est de voir l'émotion anxiogène bloquer toute réflexion, conduire au découragement et à l'abandon, exacerber la nostalgie d'un ordre ancien qui n'est plus.

L'auteur du présent ouvrage ne fuit pas la réalité de ces formidables mégachocs et il sait que l'on ne résout pas des problèmes inédits avec d'anciens remèdes. En un mot, une prise de distance sereine, rationnelle mais nourrie d'expérience personnelle et cosmopolite, est nécessaire.

C'est ce que propose ce journal de bord qui, au fil des pages, appelle à ce que l'auteur nomme un dépassement : un dépassement de nos craintes pour forger, en profondeur, de nouvelles visions, aptitudes et grammaires d'action.

Patrick Lagadec a été directeur de recherche à l'École polytechnique (1977-2013) et s'est consacré à l'étude des risques majeurs, des situations de crise et des grandes ruptures. Pour consolider son travail de recherche, il a opéré en France et à l'étranger en tant que consultant auprès d'états-majors industriels, d'administrations publiques et d'ONG. Son site Internet (www.patricklagadec.net) propose de nombreux textes et des entretiens vidéo avec de grands témoins à travers le monde, ainsi que ses interventions à la radio et à la télévision lors de situations de crise grave.

LES ENTREPRISES FACE À LA CYBERCRIMINALITÉ

ADELINE CHAMPAGNAT

COMMISSAIRE DE POLICE, CONSEILLER DU PRÉFET CHARGÉ DE LA LUTTE CONTRE LES CYBERMENACES
À LA MISSION DE LA LUTTE CONTRE LES CYBERMENACES AU MINISTÈRE DE L'INTÉRIEUR

La diffusion et l'utilisation des technologies de l'information et de la communication (TIC) s'intensifient et s'accélèrent dans le monde. « *Forte d'une population très largement connectée et portée par une économie numérique en croissance soutenue, la France [quant à elle] dispose de talents et d'atouts à la pointe de l'innovation européenne et mondiale. Le numérique est également un espace de compétition et de confrontation. Concurrence déloyale et espionnage, désinformation et propagande, terrorisme et criminalité, trouvent dans le cyberespace un nouveau champ d'expression. (...) Oeuvrer pour la sécurité du numérique, c'est favoriser le développement d'un cyberespace gisement de croissance pérenne et lieu d'opportunités pour les entreprises françaises, c'est affirmer nos valeurs démocratiques, c'est enfin préserver la vie numérique et les données personnelles des Français*[1]. »

C'est par ces mots que Monsieur Manuel Valls, Premier ministre, a fixé les enjeux de la cybersécurité pour la France, pour ses acteurs économiques et pour nous tous qui sommes utilisateurs des outils et réseaux informatiques.

Afin de remplir cette exigence de sécurité, l' État[2], et en premier lieu le ministère chargé de la sécurité intérieure, doit **lutter contre la cybercriminalité** et **protéger** les institutions et les intérêts nationaux, conformément aux recommandations du Livre blanc de la défense et de la sécurité nationale, dans un contexte durablement marqué par la menace terroriste (c'est l'objet de la cyberdéfense), ainsi que les systèmes d'information des particuliers, acteurs économiques et collectivités publiques (c'est l'objet de la *sécurité des systèmes d'information*).

Il est classiquement admis que le terme de cybercriminalité recouvre trois catégories d'infractions :

- les infractions spécifiques aux technologies de l'information et de la communication : l'espionnage industriel, l'intrusion dans la vie privée, les infections virales, les mises hors services des systèmes informatiques, etc.

- les infractions dites de "diffusion" par les systèmes d'information de contenus illicites : la pédopornographie, les délits d'apologie et d'incitation au terrorisme, à la haine raciale sur Internet, etc.

- les infractions facilitées par l'usage des systèmes d'information : les escroqueries en ligne, les contrefaçons, les usages frauduleux de moyens de paiement électronique, etc.

On voit que certains cybercrimes vont spécifiquement viser les entreprises et plus particulièrement leur patrimoine informationnel qui fait leur richesse. Dans ces conditions, on comprend que les réseaux de criminalité organisée investissent de plus en plus dans les cyberattaques qui présentent l'avantage d'être menées à distance, de manière anonyme et souvent en toute impunité.

Face à ce constat (I), l'État s'organise et encourage ses services à mener un dialogue effectif et constructif avec le secteur privé (II).

I. L'exposition croissante des entreprises à la cybercriminalité

Avec la numérisation continue de la société et corrélativement l'augmentation de la surface d'attaque, les entreprises apparaissent de plus en plus exposées à la cybercriminalité[3].

Les attaques ciblent majoritairement les données de l'entreprise[4] et la motivation des commanditaires est dans la majorité des cas, mais pas exclusivement, financière.

Elles peuvent être réalisées :

- à des fins crapuleuses, pour récupérer des données pour les exploiter ou les revendre (données bancaires, fichiers clients...) ;

- à des fins d'espionnage industriel des informations confidentielles des entreprises (vol de propriété intellectuelle);

- à des fins de déstabilisation (vol d'informations puis leur publication). Ces attaques ont pour objet et pour effet de porter atteinte à l'image de l'entreprise touchée. Elles révèlent ses vulnérabilités en matière de sécurisation des données et entament la confiance de ses clients ou de ses partenaires. Par exemple, le piratage très médiatisé des données d'utilisateurs du site de rencontres d'Ashley Madison à l'été 2015 par le groupe de hackers se nommant « *The Impact Team* » avait précisément pour objectif de porter atteinte à l'économie du site en détruisant sa réputation et sa notoriété numériques ;

- à des fins de sabotage en ayant pour effet d'interrompre voire de stopper définitivement l'activité de l'entreprise victime. L'attaque subie les 8 et 9 avril 2015 par la chaîne *TV5 Monde* est une illustration. La société pétrolière Saudi Aramco basée en Arabie Saoudite, victime d'une cyber-attaque en août 2012, avait mis, quant à elle, plus d'une semaine à restaurer l'ensemble de ses systèmes bureautiques.

Au risque financier, auquel sont classiquement confrontées les entreprises, s'ajoute une importante menace d'atteinte à leur image et à leur réputation, plus difficilement évaluables.

La médiatisation de certaines cyberattaques planifiées et organisées depuis l'extérieur de l'entreprise[5] (B) ne doit pas conduire à négliger les dangers venant de l'intérieur[6] (A).

A. Ne pas négliger le rôle joué par les collaborateurs dans la réalisation des cyberattaques

Les cyberattaques peuvent être le fait d'individus internes à l'entreprise, ou travaillant directement à son profit (sous-traitants), bénéficiant d'un accès privilégié à des données sensibles, qu'ils soient malveillants (i.) ou simplement imprudents (ii.).

i. Les "insiders" malveillants

Les "insiders[7]" malveillants[8] passent généralement à l'acte à la suite d'un évènement déclencheur telle qu'une sanction disciplinaire, un refus de promotion ou un récent licenciement. Ils sont dans une situation de conflit avec l'entreprise et agissent dès lors avant tout pour porter un coup, sinon interrompre définitivement, son activité[9]. Dans ces cas, la responsabilité du chef d'entreprise peut être engagée sur le plan civil en raison des fautes qui viendraient à être commises par un salarié[10].

Il peut s'agir d'un collaborateur interne à l'entreprise qui, confronté à des problèmes financiers, n'envisage d'autres recours que le détournement informatique d'actifs (fraude comptable).

L'appât du gain peut aussi pousser "l'insider" à accepter de se mettre au service d'un réseau de criminalité organisée qui bénéficiera alors de sa connaissance des données les plus précieuses pour les détourner avec sa complicité et les revendre.

ii. Les "insiders" imprudents ou simplement négligents

Les comportements à risques du salarié représentent des menaces permanentes pour les entreprises. La faille humaine[11] est en effet certainement celle qui reste la plus exploitée des cyberdélinquants.

Il se trouvera toujours un employé, un stagiaire pour ouvrir un mail frauduleux ou un SMS (un spam), véhiculant des escroqueries (type "*Phishing*" ("*hameçonage*") pour les plus connues), voire contenant des virus ou chevaux de Troie permettant aux cybercriminels de récupérer des données confidentielles.

Le "phishing" vise aussi bien les particuliers que les entreprises ; "hameçonnés", ils sont conduits à remettre aux attaquants qui se font passer pour des interlocuteurs de confiance (notamment des banques, des assurances, des opérateurs de téléphonie mobile, les impôts, la sécurité sociale,...), des informations confidentielles telles que des mots de passe, des numéros de compte bancaire...

Le "phishing" relève de la criminalité organisée[12] et peut être qualifié d'escroquerie en bande organisée[13]. Il peut aussi être constitutif de collecte frauduleuse de données nominatives[14],

d'usurpation d'identité en ligne[15], de contrefaçon de droits intellectuels (pages web, marques, logo, charte graphique...)[16], et d'atteinte à un système de traitement automatisé de données[17].

Conçus pour opérer en toute discrétion, les programmes malveillants (type *Blackshade RAT*) implémentés par l'ouverture d'un courriel reçu par un collaborateur de l'entreprise autorisent aussi les auteurs à accéder au serveur de l'entreprise attaquée et à récupérer tous les documents partagés.

Si ces informations ne peuvent pas être directement monétisées, elles permettent a *minima* aux attaquants de se renseigner sur l'entreprise (organigrammes, emplois du temps, signatures et documents comptables) et de les utiliser pour obtenir indûment le versement de fonds. Apparues en 2010, ces escroqueries aux faux ordres de virement internationaux restent très prisées de certains groupes criminels qui se sont spécialisés dans ce type de délinquance astucieuse.

Ces attaques sont basées sur les techniques dites "d'ingénierie sociale" visant à amener les victimes à communiquer sans retenue des informations pourtant personnelles et confidentielles.

De même, l'ouverture d'une pièce jointe à un courriel, peut provoquer l'installation d'un *ransomware* ou *cryptoloker*. Une fois sur la machine cible, il en chiffre le contenu pour priver l'utilisateur de ses données. Il lui est demandé de payer une rançon sous peine de ne jamais récupérer ses documents et contenus. Les utilisateurs de ces *rançongiciels* communiquent généralement la clé de déchiffrement une fois le paiement effectué, mais ce n'est jamais une garantie.

Enfin, par simple négligence, un salarié peut oublier de renouveler le nom de domaine de son entreprise dans les délais impartis et permettre ainsi à un concurrent d'usurper son nom ou celui de ses marques. Ce "cybersquatteur" pourra être poursuivi entre autres, pour contefaçon[18].

B. Des cyberattaques techniques plus agressives et caractéristiques du crime organisé

Planifiées et organisées depuis l'extérieur, les cyberattaques techniques exploitent des failles ou vulnérabilités des réseaux informatiques ou téléphoniques des entreprises (i.) ; les auteurs ont aussi recours à des outils particulièrement efficaces pour conduire une cyberattaque: les "botnets" (ii.).

i. L'exploitation de failles ou de vulnérabilités

Il s'agit pour les plus connues des attaques en "défacement" ou "défiguration de site Internet" qui consistent à modifier voire détruire les pages web, le plus souvent la page d'accueil.

Alors même que le piratage téléphonique (ou *phreaking*) et les exploits du premier *phreaker* surnommé "Captain Crunch"[19] apparaissaient, à l'instar du piratage informatique, dès les années 1960, la sécurité téléphonique est restée le parent pauvre de la lutte contre la cybercriminalité. Certes, c'est de moins en moins vrai pour les Smartphones mais cela reste trop souvent le cas de la téléphonie fixe des entreprises.

Les autocommutateurs téléphoniques privés (standards téléphoniques) ou "PABX"[20] assurent le cheminement des communications téléphoniques entre le réseau des opérateurs de téléphonie et le réseau privé de l'entreprise.

Certains paramétrages par défaut autorisent les cyberattaquants à utiliser le PABX d'une entreprise pour appeler en masse des numéros surtaxés que les cyber-attaquants auront préalablement loués. On comprend dès lors que le montant du préjudice peut devenir très élevé pour l'entreprise légitime utilisatrice du PABX et largement bénéfique pour les escrocs.

ii. Le recours aux "botnets"[21]

Il s'agit d'un réseau d'ordinateurs infectés et détournés à l'insu de leurs légitimes propriétaires par un "botmaster" à des fins criminelles. D'avis d'expert, "*les botnets sont de plus en plus puissants et sont désormais l'oeuvre des groupes mafieux qui cherchent sans cesse à accroître la puissance de frappe en contaminant un nombre toujours croissant de machines afin d'augmenter la capacité de leur réseau*[22]."

Les "botnets" peuvent servir aux "attaques en déni de service distribué" (ou DDoS) qui consistent à adresser au serveur de l'entreprise visée un nombre de requêtes tel qu'il n'est plus dans la capacité de les traiter. Cette attaque a pour effet de rendre indisponible un service ou l'accès à un service d'une entreprise (tel que le site de vente en ligne).

Ils peuvent aussi permettre la diffusion massive de spams frauduleux (le *Spamming*) mais également le vol et le détournement de données (notamment bancaires) à grande échelle.

Les cibles principales restent les

établissements financiers et les sites de e-commerce qui ont pignon sur Internet. La finalité des pirates est généralement d'obtenir une rançon en échange du retour à la normal du trafic de requêtes.

II. Vers une mobilisation générale contre la cybercriminalité

On comprend que les entreprises détiennent une partie du remède à la cybercriminalité (B). Cette dimension est prise en compte dans la construction d'une stratégie nationale de lutte contre la cybercriminalité (A).

A. Un nouveau cadre stratégique

"*La stratégie nationale*[23] *pour la sécurité du numérique doit s'appuyer en particulier sur la formation et sur la coopération internationale et doit être portée par l'ensemble de la communauté nationale : le gouvernement, les administrations, les collectivités territoriales, les entreprises et plus largement, tous nos compatriotes. Elle est l'affaire de tous*".

C'est par ces mots que le Premier ministre jette les bases d'une nouvelle Stratégie pour la sécurité du numérique présentée le 16 octobre 2015.

L'action du ministère de l'Intérieur, chargé au premier plan de la lutte contre la cybercriminalité, s'inscrit dans ce cadre. Elle comporte deux volets opérationnels : un volet préventif (i.) et un volet réactif (ii).

i. Le volet opérationnel préventif

Les mesures préventives ont pour objectif d'anticiper les menaces et de protéger les acteurs économiques a priori contre les risques et dangers numériques auxquels ils sont exposés.

Pour être en capacité d'adapter la réponse à apporter aux atteintes à leur sécurité, le ministère de l'intérieur s'organise pour disposer d'un état actualisé chiffré et qualitatif des cybermenaces[24].

Les directions concernées concourent à l'élaboration d'une synthèse recensant l'état des cybermenaces contre la France et ses intérêts gouvernementaux, ses intérêts fondamentaux, ses acteurs économiques et sa population.

La sensibilisation de tous les acteurs sur les risques encourus et les moyens de protection existants constitue aussi un élément essentiel de la stratégie puisqu'il contribue à réduire les risques encourus et à les motiver à participer activement au renforcement de leur propre cybersécurité.

Chaque année, la direction générale de la sécurité intérieure (DGSI) organise près de 1400 conférences sur la protection de l'information et la sécurité numérique notamment à l'endroit des entreprises. La sous-direction de lutte contre la cybercriminalité (SDLC) de la direction centrale de la police judiciaire (DCPJ) participe activement à cet effort de sensibilisation[25], tout comme le centre de lutte contre les criminalités numériques de la gendarmerie nationale (C3N).

L'État renforce les compétences des référents sûreté de la préfecture de police, de la gendarmerie et de la police nationales afin qu'ils permettent aux entreprises qu'ils conseillent de mieux se prémunir contre ce type de criminalité.

La sensibilisation des acteurs économiques passe aussi par la voie partenariale avec le secteur associatif : elle peut prendre la forme de "guide[s] des bonnes pratiques de l'informatique" qui présentent les règles essentielles pour sécuriser les équipements numériques[26] diffusés sous format papier ou sur des sites Internet dédiés[27]. Elle permet aux internautes de signaler des contenus illicites (Spam[28] et sites de Phishing[29] par exemple).

Toutefois, l'expérience opérationnelle montre qu'aucun système d'information et de communication, quel que soit son niveau de protection, n'est parfaitement sécurisé. Dès lors, les entreprises doivent être en mesure de disposer des capacités suffisantes pour détecter qu'elles ont été la cible de cyber-attaques, mais aussi pour réagir une fois l'incident détecté, traiter cet incident puis rétablir les systèmes affectés[30].

ii. Le volet opérationnel réactif

Le ministère de l'Intérieur travaille aux côtés de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) à l'amélioration du traitement des victimes d'actes de cyber-malveillances, en particulier les petites et moyennes entreprises. Il s'agit d'identifier les partenaires locaux (réparateurs informatiques, sociétés spécialisées dans la réponse aux incidents ou encore les associations d'entraide) et étatiques (policiers et gendarmes) susceptibles d'accompagner les victimes.

Quant aux entreprises dont "*l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation*", la loi de programmation militaire du 18 décembre 2013 leur impose de

respecter un certain nombre de règles de sécurité. Ces "opérateurs d'importance vitale" doivent mettre en place des dispositifs de détection d'attaques adaptés, déclarer les incidents significatifs, permettre à l' État ou à des prestataires qualifiés de vérifier par des audits le niveau de sécurité de ces systèmes et, en cas de crise grave, d'imposer les mesures nécessaires, "*sans négociation possible*". La France a été le premier pays européen à se doter de ce type de législation contraignante pour les entreprises ; elle devra toutefois subir quelques aménagements après l'entrée en vigueur en 2018 de la directive européenne NIS (Network and Information Security) qui traite des mesures à mettre en place afin de sécuriser les systèmes d'informations de certaines entreprises délivrant des services dits "essentiels" des 28 États membres de l'Union européenne pour prévenir tout risque de cyberattaques.

Afin d'éviter le renouvellement des cyberattaques, le ministère de l'Intérieur mobilise tous les acteurs concernés pour lever les obstacles à l'identification, la recherche et l'interpellation des auteurs.

Il est vrai que si les services opérationnels[31] parviennent généralement à identifier les auteurs des cyberattaques qui visent des victimes particulières (pornographie enfantine[32], diffamation, cyberharcèlement), les obstacles s'accumulent et sont parfois fatals lorsqu'il s'agit d'attaques contre les STAD (attaques en déni de service distribué, piratages informatique) lancées depuis l'étranger[33].

L'installation de "cyberparadis", l'inadaptation des outils juridiques traditionnels parce que trop longs à mettre en oeuvre (les demandes d'entraide pénale internationales) alors que la preuve numérique est éphémère, la dépendance des officiers de police judiciaire aux acteurs de l'Internet étrangers qui détiennent les données nécessaires à la poursuite des investigations, obligent à repenser la manière de développer les enquêtes[34].

Une interaction effective et constructive avec le secteur privé est tout d'abord encouragée. Le dialogue initié par le ministre de l'intérieur après les actes terroristes perpétrés en janvier 2015 avec les grands opérateurs américains de l'Internet[35] permet d'améliorer sensiblement l'efficacité des enquêtes judiciaires.

Dans le même ordre d'idée, l'association récente du parquet de Paris[36] aux côtés des services d'enquête spécialisés[37] à la Global Cyber Alliance (CGA)[38] d'origine américaine qui regroupe des partenaires institutionnels, privés et académiques, devrait permettre à terme aux enquêteurs d'accéder à des informations permettant un développement plus efficace des enquêtes.

Ensuite, la veille juridique mise en place sous la coordination du préfet chargé de la lutte contre les cybermenaces permet de vérifier régulièrement si les textes législatifs et réglementaires sont toujours adaptés en ce qu'ils permettent de poursuivre et de sanctionner les nouvelles formes de cybercriminalité. Son objectif est aussi d'éclairer les enquêteurs de terrain sur telle ou telle difficulté juridique rencontrée.

Enfin, il ne suffit pas que la France soit bien préparée à l'intérieur de ses frontières car l'expérience opérationnelle montre que les cyberattaques sont généralement planifiées et organisées depuis l'extérieur de notre territoire. Il est donc nécessaire de disposer d'une collaboration européenne et internationale renforcée.

Cette coopération prend la forme de contacts bilatéraux notamment avec les pays sources de cybercriminalité. Elle passe aussi par des échanges entre les services compétents des différents États au sein des instances européennes (Le centre européen de lutte contre la cybercriminalité (EC3) d'Europol- Eurojust) ou internationales (le "*Global Complex for Innovation* (IGCI)" d'Interpol). Outre le partage d'informations sur les cyberattaques menées par des organisations criminelles visant les entreprises, son objectif est aussi la définition d'approches et de solutions partagées, sinon communes[39].

B. Les entreprises détiennent aussi une partie du remède à la cybercriminalité

On voit que les entreprises concentrent l'essentiel des cyberrisques ; mieux les connaître et les anticiper permet sans conteste à leurs dirigeants de réduire les dangers numériques encourus (i). Cette prise de conscience contribue aussi au développement des entreprises du secteur de la cybersécurité (ii).

i. La nécessaire maîtrise et anticipation des cyber-risques pour mieux s'en prémunir

Le degré de prise en compte du risque numérique reste très différent d'une entreprise à une autre. Si les opérateurs d'importance vitale (OIV) sont légalement tenus de respecter un certain nombre de règles de cybersécurité, les autres entreprises attendront trop souvent d'être victimes d'une cyberattaque avant de prendre les mesures qui s'imposent.

Pourtant, compte tenu des menaces que représentent les cyberattaques pour l'activité des entreprises, les cyberrisques doivent être pris en compte en les intégrant *ab initio* pleinement dans la politique globale de sécurité des organisations : recensement et classification des informations en fonction de leur degré de sensibilité, politique de gestion des accès aux systèmes d'information, signature par le salarié d'une charte de bonne utilisation de la boîte mail et de l'Internet, plans de sensibilisation aux règles d'hygiène informatique ou de formation initiale et continue des salariés, plans de gestion de crise, plans de continuité et de reprise d'activité de l'entreprise en cas d'attaques cyber,...

Au final et "*désormais, la valeur d'une société se juge aussi par sa capacité à résister à des cyberattaques*[40]." Les cybermenaces font effectivement aujourd'hui partie des risques qui entrent en ligne de compte lorsqu'une société entend en acquérir une autre. Les cyberrisques sont notamment audités dans le cadre des *due diligence*[41].

ii. L'offre croissante de cybersécurité

L'offre de cybersécurité s'est accrue sensiblement et les entreprises du secteur sont désormais en mesure de proposer des solutions adaptées à chaque entreprise.

Selon l'étude du pôle interministériel de prospective et d'anticipation des mutations économiques (PIPAME)[42] présentée à l'occasion du FIC 2016, la cybersécurité représenterait en effet 10% du CA marchand de la filière nationale de la sécurité et 6% des emplois du secteur marchand. Le nombre d'entreprises françaises concerné serait estimé à 600 dans la filière cybersécurité.

Toujours selon cette étude, ce secteur bénéficie d'opportunités réelles de développement avec la prise de conscience des enjeux de sécurité, des réglementations nouvelles, l'émergence de thèmes nouveaux (objets connectés, villes intelligentes, automobiles connectées, transformation numérique, « *privacy by design* », diversification de la cybercriminalité, etc).

Dans le même temps, le développement du marché de la cyberassurance dédié à la couverture des risques liés à la cybercriminalité permet aux entreprises de mieux se prémunir des coûts liés à une cyberattaque (attaque), et de bénéficier rapidement le cas échéant, de l'assistance d'experts mobilisés et financés par l'assureur.

Conclusion

On l'a vu, une entreprise, quelle que soit sa taille, est confrontée à tout moment à la cybercriminalité. Qu'il s'agisse par exemple, d'actes de malveillances visant à interrompre son activité ou à détourner ses données, les conséquences pour l'entreprise sont souvent désastreuses, parfois irrémédiables.

Par ailleurs, quand on sait que la valeur économique d'une entreprise se mesure désormais à son degré d'exposition aux cyberrisques, il est impératif qu'elle se dote d'une politique de sécurisation des systèmes d'information et de communication adaptée.

Ainsi, l'implication des entreprises aux côtés des services de l'État est aujourd'hui une nécessité pour rendre l'environnement numérique plus sûr. Rappelons enfin que si les contraintes budgétaires et financières sont réelles pour les petites structures, il existe des bonnes pratiques d'hygiène informatique peu coûteuses et faciles à mettre en oeuvre. Gageons que ce cyberpari puisse être gagné.

Notes :

1 Préface de la Stratégie nationale pour la sécurité du numérique présentée le 16 octobre 2015.

2 Article L111-1alinéa 2 du Code de la sécurité intérieure : « l'État a le devoir d'assurer la sécurité en veillant, sur l'ensemble du territoire de la République, à la défense des institutions et des intérêts nationaux, au respect des lois, au maintien de la paix et de l'ordre publics, à la protection des personnes et des biens. »

3 La récente étude de Price Water House Coopers (PwC) réalisée auprès de 6337 entreprises localisées dans 115 pays entre juillet et septembre 2015 fait état de ce que la cybercriminalité représente 53% des fraudes rapportées, contre 28% il y a deux ans. Les cyberattaques auraient coûté 3,7 milliards de dollars aux entreprises françaises en 2015 (www.pwc.fr/enquêtefraude2016). Les données de l'International Business Report, tirées d'un sondage réalisé auprès de 2500 dirigeants d'entreprise à travers 35 pays, révèlent qu'une entreprise sur six a été victime de cybercriminalité au cours de l'année 2015 et que le montant des dommages causés s'est élevé à 315 milliards de dollars.

4 Le rapport iOCTA (internet Organised Crime Threat) produit par Europol fait état d'une augmentation en 2015 du détournement des données (www.europol.europa.eu/content/internet-organised-crimes-threat-assessment-iocta-2015).

5 C'est le cas par exemple de la cyberattaque du site web TF1.fr en janvier 2016, les pirates se présentant sous le nom de « Linker Squad » affirmaient avoir dérobé adresses e de courriels, mots de passe et données bancaires de « 1,9 million de clients » en passant par ce site. C'est encore le cas de la cyberattaque de Sony à la fin de l'année 2014 ou de l'attaque informatique en novembre 2015 contre le groupe de jouets éducatifs VTech avec le vol des profils de milliers d'enfants.

6 A la lecture de l'édition 2016 de l'étude de

Price Water House Coopers (PwC), il apparaît que la fraude d'origine interne aux entreprises semble avoir reculé : seuls 30% des fraudeurs seraient des collaborateurs de l'entreprise contre 39% en 2014.

7 « Insider » : « initié » : qui est dans la place.

8 Pour illustration, début janvier 2015, la banque américaine, Morgan Stanley annonçait qu'un de ses employés, Glen Marsh 31ans, avait volé des données concernant jusqu'à 10% des clients de son activité de gestion de fortune, les noms des titulaires et les numéros de comptes. Les données d'environ 900 clients de Morgan Stanley avaient été brièvement affichées sur Internet.

9 Ces faits de sabotage d'une base de données sont constitutifs des infractions visées aux articles 323-1 et 323-3 du Code pénal.

10 Voir l'article 1384 du Code civil.

11 Par opposition à la vulnérabilité « technique ».

12 Voir « Cybermenaces, entreprises et internautes » de Myriam Quéméner 2008.

13 Article 313-2 du Code pénal.

14 Article 226-18 du Code pénal.

15 Article 226-4-1 du Code pénal.

16 Article L 335-3 du Code de la propriété intellectuelle.

17 Article 323-3 du Code pénal.

18 Voir note n°16.

19 Captain Crunch, de son vrai nom John Draper est un phreaker (pirate téléphonique) américain. Son surnom provenait des boîtes de céréales Cap'n Crunch de la société Quaker Oats.Vers la fin des années 60, le céréalier offrait avec ses produits un sifflet pour les enfants. Ce jouet permettait de reproduire la tonalité utilisée par une compagnie téléphonique pour passer des appels longue distance. La découverte de cette propriété a été exploitée par les phreakers pour passer des appels gratuitement.

20 PABX : Private Automatic Branch eXchange.

21 BOTNET : Abrévation de roBOTs of Network, traduire par « roBOTs en réseaux (NET). »

22 Cf. Le « guide pratique du chef d'entreprise face au risque numérique », page 34.

23 La stratégie nationale pour la sécurité du numérique a été élaborée avec l'ensemble des ministères. Elle a été soumise par le secrétaire général de la défense et de la sécurité nationale à l'approbation du Premier ministre en application du 7ème de l'article R 1132-3 du Code de la défense.

24 Axe 1 du plan d'action « lutte contre les cybermenaces en matière de sécurité intérieure » du 28 mai 2015 : Disposer en permaneNce d'une vision claire et actualisée de l'état des cybermenances.

25 Créée par arrêté du 29 avril 2014, la SDLC comporte une division de l'anticipation et de l'analyse a vocation à construire une réponse publique aux particuliers et aux entreprises non identifiées comme des « opérateurs d'importance vitale » et cibles privilégiées des cyberattaques. Cette division comporte également une cellule d'information du public, axée sur l'identification des nouveaux modes opératoire (diffusion d'alertes en ligne, campagnes de sensibilisation aux dangers de l'Internet) et els bonnes pratiques permettant de minimiser les risques d'attaque.

La DCPJ est aussi responsable de la plateforme de signalement des contenus illicites de l'Internet du ministère de l'Intérieur (plateforme PHAROS).

26 Par exemple : www.ssi.gouv.fr/uploads/2015/03/guide_cgpme_bonnes_pratiques.pdf

27 Voir par exemple les travaux CECyF, association loi 1901 regroupant des partenaires institutionnels, académiques, industriels et associatifs, avec l'objectif de promouvoir des actions pour la prévention, la formation et la recherche et le développement contre la cybercriminalité (www.cecyf.fr).

28 Pour signaler un spam : www.signal-sapam.fr

29 Pour signaler et bloquer un site de phishing : https://phishing-initiative.eu

30 La direction centrale de la police judiciaire a publié un guide « Réagir à une attaque informatique : 10 préconisations. »

31 Les services opérationnels spécialisés dans la lutte contre la cybercriminalité sont : la sous-direction de lutte contre la cybercriminalité (SDLC) de la direction centrale de la police judiciaire (DCPJ) en charge de la criminalité organisée) dimension internationale ou utilisant un modus operendi novateur, le centre de lutte contre la criminalité numérique (C3N) de la gendarmerie nationale, la Brigade d'enquête sur les aux technologies de l'information (BEFTI) de la préfecture de police de Paris, la Direction Générale de la Sécurité Intérieure (DGSI) qui lutte contre les ingérences étrangères et qui est en charge des enquêtes judiciaires sur les cyberattaques ciblant l'État, les OIV et certaines entreprises sensibles.

32 Les services d'enquêtes spécialisés dans la lutte contre la pédopornographie sont l'Office central pour la répression des violences aux personnes (OCRVP) et l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) de la DCPJ, la Brigade de protection des mineurs (BPM) de la préfecture de police de Paris et le C3N de la gendarmerie nationale.

33 Propos tenus par le préfet chargé de la lutte contre les cybermenaces Jean-Yves LATOURNERIE à l'occasion du FIC 2016.

34 Propos tenus par le préfet chargé de la lutte contre les cybermenaces Jean-Yves LATOURNERIE à l'occasion du FIC 2016.

35 Google, Microsoft, Appel, Twitter et Facebook.

36 La section de lutte contre la cybercriminalité du parquet de Paris a adhéré à la GCA le 22 février 2016.

37 La SLDC de la DCPJ.

38 La GCA est une association à but non lucratif d'origine américaine (parquet de New York) ; son objet est de lutter contre les cyber-risques (notamment le phising, les attaques en DDoS, les sites Internet compromis) par la mise en place d'une plate forme d'échanges.

39 Par exemple sur la durée de conservation des données numériques.

40 M. Van den Berghe, Protéger le patrimoine informationnel de l'entreprise, Revue Préventique n°145, mars 2016, p. 20.

41 Ou « audits d'acquisition ».

42 Étude PIPAME pilotée par le ministère de l'Intérieur (DMIS), avec le concours du SGDSN, de l'ANSSI et de la DGE en partenariat avec HexaTrust, Systemic, EDEN, pôle SCS, Cluster CNCS by Euratechnologies, la MEITO, PRISSM, couvrant une large partie du territoire national.

Inscription à la newsletter et à la revue du GRASCO

Par mail : abonnement@larevuedugrasco.eu

Diffusion gratuite de vos offres d'emploi, événements, manifestations et parutions ouvrages[1]

Par mail : information@grasco.eu

1 après validation de la rédaction

LES PROCÉDURES DE LA CRIMINALITÉ ORGANISÉE ET LA LOI DU 3 JUIN 2016 : QUELS DÉFIS POUR LA DÉFENSE PÉNALE ?

MAXIME TESSIER

AVOCAT AU BARREAU DE RENNES,
CHARGÉ D'ENSEIGNEMENT À L'UNIVERSITÉ DE RENNES 1

Le 5 juin 2016, entraient en vigueur les premières dispositions de la loi n° 2016-731 du 3 juin 2016 « renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale[1]», laquelle avait été présentée en ces termes par le gouvernement de M. Manuel VALLS, dans l'exposé des motifs du projet de loi : « *Les attentats qui ont douloureusement touché notre pays cette année ont renforcé la conviction du Gouvernement de la nécessité d'adapter notre dispositif législatif de lutte contre le crime organisé et le terrorisme afin de renforcer de façon pérenne les outils et moyens mis à la disposition des autorités administratives et judiciaires, en dehors du cadre juridique temporaire de l'état d'urgence*[2]. »

La Commission nationale consultative des droits de l'homme (CNCDH), dans son avis adopté sur le projet, avait très justement souligné que cette réforme s'inscrivait « dans un contexte postérieur aux attentats de 2015[3] », c'est-à-dire ceux de *Charlie Hebdo*, de *l'Hypercasher* et du 13 novembre[4], et a fortiori dans le contexte de l'état d'urgence.

À l'instar des précédentes lois ayant instauré ou réformé des procédures d'exception en matière pénale, les motivations ayant présidé à l'adoption de la loi du 3 juin 2016 trouvent ainsi leur source dans l'importance croissante prise par la notion de sécurité dans le débat public, laquelle est devenue en quelques années un « *enjeu politico-médiatique formidable*[5] », résonnant en écho des attaques terroristes perpétrées en France ou à l'étranger.

En 2010, dans son ouvrage intitulé *Liberté et sûreté dans un monde dangereux*, le professeur Mireille DELMAS-MARTY expliquait que la série d'attentats du 11 septembre 2001 avait modifié tant la perception que les réactions individuelles et collectives face aux dangers et à l'insécurité d'une part, et « *libéré les responsables politiques, symboliquement et juridiquement de l'obligation de respecter les limites propres à l'État de droit d'autre part*[6]. »

Déjà en 2003, Maître Jean DANET, avocat honoraire et enseignant-chercheur à l'Université de Nantes, soulignait qu'en France le « *paradigme de l'insécurité* » était devenu « *la carte et la boussole* » de la réponse pénale, de sorte que les attentats avaient surtout contribué à légitimer et à banaliser une pensée sécuritaire qui existait depuis bien plus longtemps, jusqu'au sein de formations politiques qui y étaient auparavant hostiles[7].

Le fait qu'un gouvernement socialiste, entre 2014 et 2016[8], s'attache à consolider et à renforcer des dispositifs exceptionnels dont il avait combattu l'entrée en vigueur initiale, du temps où ses membres siégeaient dans l'opposition, en est une illustration significative[9].

Le projet devenu la loi du 3 juin 2016 poursuivait un « *triple objectif*[10] » : « renforcer *l'efficacité de la lutte contre la criminalité organisée, et notamment le terrorisme* » (titre Ier de la loi, articles 1er à 53), « renforcer *les garanties au cours de la procédure pénale [...] afin de rendre*

notre procédure totalement conforme aux exigences constitutionnelles et européennes » (titre II de la loi, articles 54 à 68), et « *procéder à des simplifications qui faciliteront le travail des enquêteurs et des magistrats* » (titre II de la loi, articles 69 à 101).

Ce triple objectif voulait lui-même « *assurer une meilleure accessibilité, une plus grande équité et* » surtout garantir « *l'efficacité de notre procédure pénale* », la notion d'efficacité ne pouvant être comprise ici que sous le prisme de la lutte contre la criminalité (et non sous celui de la défense des droits fondamentaux, malgré l'adoption de dispositions pour les renforcer), confirmant la place fondamentale occupée désormais par les critères de « rendement » ou d'« efficience » dans l'économie d'une justice pénale qui se métamorphose sous la pression du « management » néolibéral[11].

Les réflexions qui vont suivre porteront essentiellement sur le premier de ces objectifs, et notamment sur le volet consistant à « *donner aux services enquêteurs et aux magistrats de nouveaux moyens d'investigation et de poursuite des infractions délictuelles et criminelles, lesquelles tendent à devenir de plus en plus sophistiquées et astucieuses, notamment en matière de criminalité et de délinquance organisées*[12] ».

La loi du 3 juin 2016 constitue en réalité l'une des ramifications de la loi n° 2004-204 du 9 mars 2004 « portant adaptation de la justice aux évolutions de la criminalité », dite « loi Perben II », laquelle avait instauré le titre XXV du livre IV du Code de procédure pénale intitulé « *De la procédure applicable à la criminalité et à la délinquance organisées* », dont les dispositions ont leur siège aux articles 706-73 à 706-106.

La loi du 3 juin 2016 complète en effet ce « code dans le code[13] » et confirme le changement de paradigme amorcé en 2004 au sein de la procédure pénale.

La loi Perben II, comme la loi du 3 juin 2016, ne visait pas tant à créer de nouvelles incriminations qu'à procéder à une énumération à droit constant en recourant – pour l'essentiel, mais pas toujours ensuite – au concept de « bande organisée » défini par l'article 132-71 du Code pénal[14].

En l'état actuel du droit, les infractions retenues sont ventilées sur trois listes codifiées aux articles 706-73 (infractions auxquelles les procédures d'exception sont applicables de droit), 706-73-1 (infractions auxquelles les procédures d'exception sont applicables de droit, à l'exclusion de la garde à vue spéciale de l'article 706-88) et 706-74 du Code de procédure pénale (autres infractions commises en bande organisée et formes classiques du délit d'association de malfaiteurs, auxquelles les procédures d'exception sont applicables si la loi le prévoit).

La loi du 3 juin 2016 a complété deux de ces listes en ajoutant à celle de l'article 706-73 les délits en matière d'armes et de produits explosifs qu'elle a elle-même créés dans le Code pénal. L'article 706-73-1, quant à lui, mentionne désormais le délit d'atteinte aux systèmes de traitement automatisé de données à caractère personnel mis en oeuvre par l'État commis en bande organisée prévu à l'article 323-4-1 du Code pénal[15], le délit d'évasion commis en bande organisée prévu au second alinéa de l'article 434-30 du même Code, les délits d'importation, d'exportation, de transit, de transport, de détention, de vente, d'acquisition ou d'échange d'un bien culturel provenant d'un théâtre d'opérations de groupements terroristes qu'elle a créés via le nouvel article 322-3-2 du Code pénal, ainsi que les délits de blanchiment autres que ceux mentionnés à l'article 706-73.

L'article 706-74 n'a toutefois pas été modifié et conserve sa rédaction issue de la loi n° 2015 -993 du 17 août 2015 « portant adaptation de la procédure pénale au droit de l'Union européenne ».

L'intérêt du mécanisme réside en ce que tout fait qui recevrait une qualification prévue par l'un de ces trois articles pourrait déclencher le régime d'exception prévu par le titre XXV, lequel prévoit à la fois la compétence des huit juridictions interrégionales spécialisées[16] (ou JIRS, art. 706-75 à 706-79-1 Code de procédure pénale), ainsi que la possibilité de recourir aux moyens d'investigations dérogatoires du droit commun prévus par les articles 706-80 à 706-106 du Code de procédure pénale[17].

Ces procédures sont la surveillance (art. 706-8), l'infiltration (art. 706-81 à 706-87), l'enquête sous pseudonyme (art. 706-87-1), la garde à vue spéciale (art. 706-88 à 706-88-1), les perquisitions spéciales (art. 706-89 à 706-94), les interceptions de correspondances émises par la voie des communications électroniques (art. 706-95), auxquelles s'ajoute désormais le

« recueil des données techniques de connexion » ou « *IMSI catching* » (art. 706-95 à 706-95-10), les sonorisations et fixations d'images de certains lieux ou véhicules (art. 706-96 à 706-102), la captation des données informatiques (art. 706-102-1 à 706-102-9), les mesures conservatoires (art. 706-103), outre des dispositions complémentaires, communes (art. 706-105) ou spécifiques à certaines infractions (art. 706-106).

La loi du 3 juin 2016 autorise désormais des perquisitions de nuit dans des locaux d'habitation, dans le cadre des enquêtes de police judiciaire et des instructions ouvertes concernant les infractions de terrorisme, lorsqu'il y a urgence et qu'une telle mesure est « *nécessaire afin de prévenir un risque d'atteinte à la vie ou à l'intégrité physique* » (cf. art. 706-90 et 706-91).

Encore et surtout, cette loi permet à présent « *le recours, dans le cadre de l'enquête préliminaire ou de flagrance, à des actes jusqu'ici réservés à l'instruction*[18] », c'est-à-dire le recours aux sonorisations et fixations, ainsi qu'aux captations des données informatiques, ces dernières étant au surplus élargies aux données stockées sur un ordinateur, outre celles qui s'affichent sur l'écran, à l'image de ce qui était déjà permis pour le renseignement[19].

De façon inédite, ces dernières procédures peuvent être mises en oeuvre par les officiers de police judiciaire, sur autorisation du juge des libertés et de la détention saisi sur requête du procureur de la République, sans qu'il soit nécessaire d'ouvrir une information judiciaire concernant l'une des infractions visées par les listes des articles 706-73 à 706-74 du Code de procédure pénale.

Aussi, la loi du 3 juin 2016 confirme-t-elle le tournant pris par la procédure pénale depuis 2004 en ce qu'elle permet l'extension du champ des « *pouvoirs autorisés de police judiciaire*[20] », et confirme la position renforcée des officiers de police judiciaire et du ministère public par rapport au juge d'instruction, et a fortiori par rapport à la défense et à ses moyens.

La CNCDH notait en effet que ces modifications consacraient « *un déséquilibre de la procédure pénale au profit de l'enquête* » et elle déplorait à l'unanimité « *cette prolifération de textes législatifs, relevant davantage d'une approche politique et émotionnelle que d'un travail législatif réfléchi [...]* ».

La CNCDH soulignait également l'« *absence de réflexion d'ensemble* », regrettait à l'instar du Conseil d'État la « *pauvreté de l'étude d'impact*[21] » et craignait en définitive « *la diffusion, au sein des nouvelles dispositions de procédure pénale, d'une logique prédictive propre au droit pénal de la dangerosité*[22]. »

Pour autant, les rapporteurs du texte à l'Assemblée nationale justifiaient la création de ces nouvelles dispositions aux motifs qu'elles étaient « *fortement attendues* » par le monde judiciaire – on supposera ici que les auteurs désignaient plus particulièrement les magistrats du parquet, les juges d'instruction voire les officiers de police judiciaire qui exercent leurs fonctions au sein ou auprès des JIRS – lequel appellerait depuis « *plusieurs années* » à une « *modernisation et à une adaptation des moyens* » mis à sa disposition pour remplir ses missions[23], ou tout du moins à un renforcement des moyens existants.

Il est curieux de constater que l'argument selon lequel ce sont les praticiens du monde judiciaire qui réclameraient la création de moyens d'investigation dérogatoires du droit commun avait déjà été utilisé en 2003 par la Chancellerie afin de légitimer, par la « base » en quelque sorte, l'adoption de tels mécanismes.

M. François MOLINS, à l'époque directeur-adjoint des affaires criminelles et des grâces et actuel procureur de la République près le tribunal de grande instance de Paris, expliquait en effet que « *l'instauration d'un nouveau dispositif [s'ajoutant au droit commun] était une nécessité incontournable* », fondée non seulement sur la politique pénale du gouvernement, mais également sur le constat que la quasi-unanimité des parquetiers se seraient accordés sur « *l'inefficacité de l'action judiciaire* » et « *l'insuffisance des moyens spécialisés*[24] ».

La réutilisation d'arguments identiques afin de motiver l'accroissement du champ des procédures d'exception – au détriment du droit commun et surtout des droits fondamentaux – ne manque pas d'inquiéter les plus pessimistes qui voient depuis longtemps dans l'adoption de ces différents textes « *l'instauration d'un État d'exception permanent*[25] », ou a minima un enchaînement de dispositions dont on ne peut plus se dégager, c'est-à-dire un engrenage.

Face à un tel constat, la citation de M. Guy BRAIBANT choisie par

la CNCDH dans son avis prend ici tout son sens lorsqu'elle souligne que « "*les crises laissent derrière elles, comme une marée d'épais sédiments de pollution juridique*[26]*.*", *dès lors que les lois prévoyant des mesures extraordinaires survivent aux circonstances qui les ont fait naître*". »

Il est tout aussi singulier de relever, dans le texte de la loi comme dans les travaux parlementaires, un véritable « mélange » au sens chimique du terme (certains parleront d'« amalgame ») entre les notions de « terrorisme » et de « crime organisé ».

L'intitulé de la loi semble en effet les placer sur un même plan en ce qu'il vise « *la lutte contre le crime organisé, le terrorisme et leur financement* ».

D'aucuns penseront, certes, que l'intitulé procède bien à une distinction en prenant le soin de citer les deux phénomènes.

Cela étant, le rapport de Mme CAPDEVIELLE et de M. POPELIN réactive l'impression d'un amalgame en ce qu'il justifie «*l'élargissement des mesures spéciales d'investigation* » sous le titre : « *Combattre le terrorisme en luttant contre la criminalité organisée, le trafic d'armes et la cybercriminalité* »[27].

Il ne s'agit pas d'affirmer que terrorisme et criminalité organisée constitueraient deux phénomènes complètement imperméables au plan criminologique, ni qu'il n'existerait aucune porosité entre ces deux formes de criminalité.

Au plan théorique, on pourrait effectivement admettre[28] la conception selon laquelle le terrorisme constitue une forme ou une branche particulière de la criminalité organisée.

Néanmoins, des controverses apparaissent inéluctablement lorsque de telles notions se confrontent à l'épreuve d'une traduction sous la forme juridique, par leur intégration au sein du Code de procédure pénale, dès lors que cet exercice suppose l'élaboration d'une définition et la détermination de critères plus ou moins rigides du fait de leur caractère normatif.

Or, le « crime organisé » (comme la notion de « terrorisme ») recouvre diverses acceptions, formes et représentations de la délinquance[29], de tels *dissensus* s'expliquant – comme l'écrivait le professeur Raymond GASSIN – parce que l'idée de « criminalité organisée » se rapporte d'abord à un modus operandi et aurait par conséquent des « *visages multiples* ».

C'est pourquoi les différentes définitions proposées ne permettent pas de distinguer clairement les formes multiples de ce phénomène criminologique[30], lequel recouvre des réalités et des enjeux très différents selon qu'il s'agisse du trafic de stupéfiants (et selon la nature exacte des produits trafiqués, la délinquance n'est pas non plus la même), du trafic d'armes, de la traite des êtres humains, des proxénétismes (les caractéristiques de cette délinquance variant aussi selon qu'il s'agisse par exemple de la prostitution forcée de femmes originaires du Nigéria ou de celles issues d'Europe de l'Est), du travail dissimulé, d'escroquerie, de vols ou encore de recels pour ne citer que ces exemples.

Aussi, le fait que soit apportée à ces différents phénomènes une réponse pénale unique car identique – sur le plan purement processuel – suscite immanquablement une controverse quant à la proportionnalité des procédures d'exception ainsi qu'à leur légitimité au regard des restrictions portées aux droits fondamentaux, et *in fine* aux droits de la défense comme à ses moyens concrets d'action.

Autrement dit, cette controverse n'est pas suscitée par le souci du législateur de prévoir des moyens adaptés à la recherche, la poursuite et au jugement des auteurs d'infractions agissant dans un cadre organisé : elle existe à partir du moment où la notion de « terrorisme » est assimilée à celle de « crime organisé » afin de justifier l'extension des moyens de la coercition et la restriction du champ des libertés fondamentales.

Enfin, le fait que ces « nouveaux moyens » aient pour but, tel que l'écrit la loi, de permettre au monde judiciaire de « *lutter* » contre le crime organisé appelle également discussion et réflexion, cette terminologie, loin d'être inédite, n'étant pas neutre et questionnant de façon explicite ce que devrait être l'office du juge en matière pénale au XXIe siècle[31].

Le juge et notamment celui d'une JIRS, jusqu'à celui de la Chambre criminelle, a-t-il pour mission de « lutter » contre le crime organisé, au sens de se battre contre lui ou de l'affronter ?

Une première réponse pourrait être que le juge a bien pour mission de lutter contre le crime, car il constitue la seule autorité compétente pour mettre hors d'état de nuire les criminels et les délinquants, en prononçant par exemple des placements en

détention provisoire ou des peines privatives de liberté. L'équité d'une telle Justice serait toutefois sujette à caution puisqu'elle reviendrait à placer dans le même camp les officiers de police judicaire, le ministère public et les magistrats du siège (sans oublier l'administration des douanes, l'administration fiscale, les URSSAF, l'administration pénitentiaire, les parties civiles, etc.), face à une défense qui resterait *de facto* le seul gardien effectif des libertés et ne serait pas (toujours) appréhendée comme force de proposition critique[32], mais en réalité comme un adversaire.

Une deuxième conception pourrait être de soutenir que le juge n'a absolument pas pour mission de lutter contre le crime, mais que sa mission consiste à appliquer la loi de manière indépendante par rapport à la défense d'une part, et aux officiers de police judiciaire et au ministère public d'autre part, ces derniers étant les seuls à avoir pour fonction de lutter contre la criminalité et la délinquance (organisées).

Formulée ainsi, cette proposition occulterait toutefois de manière excessive « l'office sanctionnateur[33] » du juge, c'est pourquoi il convient non pas de l'abandonner totalement – car elle correspond selon nous au « *modèle du procès équitable*[34] » – mais de la compléter.

En effet, si le juge n'a pas pour mission de « lutter » contre le crime, il constitue l'autorité de contrôle, à chaque stade de la procédure, des charges ou preuves résultant du dossier contre le mis en cause, ainsi que de leur suffisance pour renverser la présomption d'innocence et entrer en voie de condamnation au-delà de tout doute raisonnable. C'est ainsi le juge qui prononce les peines pouvant aller jusqu'à la réclusion criminelle à perpétuité devant la cour d'assises spéciale, sans oublier les peines complémentaires et plus particulièrement les confiscations qui aujourd'hui constituent un objectif explicite de la politique pénale[35].

La différence entre ces deux conceptions de l'office du juge (d'une JIRS) réside ainsi dans la place plus ou moins excessive qui est accordée à « l'office sanctionnateur » et à « l'office de vérité[36] » par rapport aux autres facettes de l'office du juge, et notamment « l'office libéral », qui vise à « *garantir les libertés individuelles à toute personne notamment suspectée, détenue, retenue ou hospitalisée contre son gré* » et qui trouve son siège à l'article 66 de la Constitution.

Si nous sommes favorables à la seconde conception, il demeure que ce débat – loin d'être illégitime, y compris pour les partisans de la première – est l'expression de la tension inhérente à la procédure pénale, « *trait d'union entre deux intérêts également puissants, également sacrés, qui veulent à la fois être protégés, l'intérêt général de la société qui veut la justice et prompte répression des délits, l'intérêt des accusés qui lui est aussi un intérêt social et qui exige une complète garantie des droits de la collectivité et de la défense*[37] ».

La recherche d'un équilibre entre ces deux intérêts – et donc entre l'office sanctionnateur et l'office libéral – constitue « *l'âme de la procédure pénale*[38] » pour reprendre l'expression des professeurs Serge GUINCHARD et Jacques BUISSON, et ces deux intérêts et offices influencent nécessairement « l'office jurisprudentiel[39] », lequel, « *pour paraphraser Aristote* », a été défini par l'IHEJ comme « *l'art de rechercher ce qui est bon pour le cas soumis au juge et ce qui est bon pour le système juridique en général, et notamment la sécurité juridique*[40] ».

« *Coeur même de la fonction de juger*[41] », la jurisprudence a aujourd'hui vocation à compléter une Loi se résultant à « *un produit semi-fini*[42] », et cela à partir des nombreuses controverses alimentées par la doctrine comme par les praticiens, et particulièrement les juges, les procureurs, les enquêteurs et les avocats, notamment en défense.

Une réflexion individuelle ou collective[43] sur les défis jurisprudentiels (et démocratiques) posés par un nouveau texte tel que la loi du 3 juin 2016 est donc incontournable, dans les Barreaux mais pas seulement, afin que chacun soit en mesure d'accomplir pleinement sa mission dans le procès pénal, y compris la défense.

« *En matière de criminalité organisée, la responsabilité de la défense est infinie*[44] », c'est pourquoi il lui appartient, dans ce domaine plus encore que dans les autres, chaque fois que c'est possible, de soulever de nouveaux problèmes de droit, d'imaginer des solutions juridiques innovantes, d'exercer des recours (y compris en déposant des mémoires personnels devant la Cour de cassation[45]), c'est-à-dire de jouer pleinement

son rôle dans la production prétorienne.

Outre le fait que la conventionalité de certaines des nouvelles dispositions peut susciter des débats dans l'enceinte judiciaire, il convient de souligner que la loi du 3 juin 2016 n'a pas fait l'objet d'un contrôle de constitutionnalité *a priori*, laissant toutes possibilités et perspectives pour d'éventuelles questions prioritaires de constitutionnalité.

Face aux procédures d'exception, c'est en définitive l'exercice par la défense de toutes ses prérogatives qui seul pourra constituer le rempart et la garantie ultimes du respect du procès équitable et des droits de fondamentaux, lesquels, à l'instar de la liberté de la presse, ne « *s'usent que quand on ne s'en sert pas* ».

Si la défense doit exercer pleinement son rôle, il lui arrive toutefois d'être confrontée à des difficultés d'ordre matériel ou organisationnel qui ne doivent pas être ignorés car elles impactent directement sa capacité à remplir sa mission.

Il peut s'agir de questions telles que la difficulté pour étudier voire pour imprimer des procédures constituées de dizaines de tomes et de milliers de cotes, de l'impossibilité de rencontrer fréquemment des clients mis en examen lorsqu'ils sont incarcérés à longue distance des cabinets, des difficultés pour organiser une défense collective, ou encore du fait que certains clients disposent de ressources insuffisantes pour exercer des voies de recours ou se sentent découragés et ne souhaitent pas allonger les délais de la procédure en interjetant appel ou en formant des pourvois.

Dès qu'elle en a l'occasion, la défense doit cependant tenter le maximum – dans le respect de la déontologie de la profession d'avocat – pour exercer sa fonction critique[46], en particulier à une époque où « *l'exception s'adapte à de nouveaux contextes et à de nouvelles cibles* », pour reprendre les mots de l'universitaire Mme Vanessa CODACCIONI[47].

Car procéder à la critique des pratiques policières et judiciaires, du dossier de la procédure, de la norme pénale (de fond et forme) comme de la politique pénale (en soulignant ses contradictions) est non seulement une possibilité pour assurer la défense de l'usager, mais c'est également une nécessité pour défendre l'État de droit contre tout glissement vers une compression toujours plus importante des libertés fondamentales.

La fonction critique de la défense ne saurait néanmoins être confondue avec une « *volonté de déstabiliser les magistrats* », de « *perturber le cours normal de la justice* », de se montrer « *agressive avec l'institution judiciaire* », ou encore avec une « *stratégie de tension* » tel qu'on peut le lire dans le « Rapport du groupe de travail relatif à la protection des magistrats » en date du 28 juin 2016[48].

Il est regrettable qu'un rapport signé à la fois par le Directeur des Affaires criminelles et des Grâces, la Directrice des Affaires Civiles et du Sceau et par la Directrice des Services Judiciaires tire, à partir de pratiques éventuellement discutables de certains avocats, des généralités visant l'ensemble d'une profession et plus spécifiquement sa « nouvelle génération », plutôt que d'ouvrir un débat ou de créer des espaces de discussion pour que chacun s'interroge et discute sur la place, le rôle, et les défis de chacun des acteurs de la « Justice JIRS ».

La défense n'a pas non plus vocation à « *participer à l'émergence de la vérité* » aux côtés ou à la place du juge. Le fait qu'elle s'y refuse ne se signifie pas qu'elle s'inscrit dans une « *opposition systématique à l'action de l'autorité judiciaire*[49] », ou alors il faut considérer que le droit de se taire, le droit de ne pas s'auto-incriminer ou encore le droit à l'assistance d'un avocat constituent des entraves à l'exercice de la Justice.

En réalité, la critique est essentielle à la défense pour rester libre, indépendante et au service des intérêts de son client, à plus forte raison dans les dossiers de criminalité organisée où l'accroissement des pouvoirs d'investigation implique des garanties maximales.

Demeurer une force de proposition critique et libre constituera sans aucun doute le défi le plus difficile à relever pour la défense surtout dans un contexte sécuritaire et sous le régime des procédures d'exception. Le relever est toutefois indispensable pour que soit préservé l'équilibre du procès pénal, et *in fine* Justice et Démocratie.

Notes :

1 Loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale, JORF n° 0129 du 4 juin 2016, texte n° 1. NOR : JUSD1532276L.

2 Projet de loi n° 3473 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la

procédure pénale, enregistré à la Présidence de l'Assemblée Nationale le 3 février 2016, p. 3.

3 CNCDH, Assemblée plénière, Avis sur le projet de loi renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale, 17 mars 2016, n° 1.

4 C. CAPDEVIELLE, P. POPELIN, députés, Rapport n° 3515 fait au nom de la commission des lois constitutionnelles, de la législation et de l'administration générale de la République, sur le projet de loi (n° 3473) renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale, p. 12 : « Alors que le projet de loi était en cours de préparation par le Gouvernement, notre pays a été douloureusement frappé, au mois de novembre 2015, par de nouveaux attentats terroristes, quelques mois après les attaques perpétrées contre le journal Charlie Hebdo à Paris et le magasin Hypercasher de Vincennes. »

5 F. GROS, Le Principe Sécurité, coll. NRF Essais, Gallimard, 2012, p.9, cité in M. TESSIER, Les procédures de la criminalité organisée devant la Cour de cassation, préface de Jean DANET, coll. Bibliothèques de droits, L'Harmattan, 2014, p. 15. Cf. également la position prise par le Président du Syndicat des Avocats de France, Maître Florian BORG, dans la Lettre du SAF du mois de mai 2016, p. 5 : « L'état d'urgence et la réforme pénales'inscrivent dans une tendance lourde sécuritaire avec pour risque réel de basculer dans un régime arbitraire au détriment des droits de la défense. »

6 M. DELMAS-MARTY, Libertés et sûreté dans un monde dangereux, coll. La couleur des idées, Seuil, 2010, p.12, cité in M. TESSIER, op. cit., p. 15.

7 J. DANET, « Le droit pénal et la procédure pénale sous le paradigme de l'insécurité », Archives de politique criminelle, 2003/1 n° 25, pp. 37-38, cité in M. TESSIER, op. cit., pp. 15-16.

8 Cf. Outre la loi du 3 juin 2016 : loi n° 2012-1432 du 21 décembre 2012 sur la sécurité intérieure et la lutte contre le terrorisme ; loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme ; loi n° 2015-912 du 24 juillet 2015 relative au renseignement ; loi n° 2015-1501 du 20 novembre 2015 prorogeant l'application de la loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence et renforçant l'efficacité de ses dispositions.

9 A l'Assemblée nationale, le 11 février 2004, lors du scrutin (n° 437) sur l'adoption de la future loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité (loi « Perben II »), les députés suivants, actuels Président de la République, Premier ministre et ministres, s'étaient prononcés contre le texte : M. François HOLLANDE, M. Manuel VALLS, M. Jean-Marc AYRAULT, M. Jean -Yves LE DRIAN, Mme Ségolène ROYAL, M. Alain VIDALIES, M. André VALLINI. Le groupe socialiste, à l'unanimité, s'était opposé à son adoption.

10 Projet de loi n° 3473 renforçant la lutte contre le crime organisé…, loc. cit., p. 4 et s..

11 Cf. J. DANET, La justice pénale entre rituel et management, coll. L'Univers des normes, Presses universitaires de Rennes, 2010.

12 C. CAPDEVIELLE, P. POPELIN, députés, Rapport n° 3515…, p. 12.

13 Expression employée par certains auteurs pour qualifier ce nouveau titre lors de l'adoption de la loi « Perben II ». Cf. notamment : J. DANET, Défendre, Pour une défense pénale critique, coll. Etats de droits, Dalloz, 2e édition, 2004, p. 84 ; J. PRADEL, « Vers un "aggiornamento" des réponses de la procédure pénale à la criminalité, apports de la loi n° 2004-204 du 9 mars 2004 dite Perben II », JCP G, n° 19, I 132 et 134, cités in M. TESSIER, op. cit., p. 19.

14 La définition du concept de « bande organisée » a été complétée par la jurisprudence de la Cour de cassation, notamment pour la distinguer de l'infraction d'association de malfaiteurs. Il a ainsi été jugé par la Haute juridiction qu'il résulte de la décision du Conseil constitutionnel n° 2004-492 DC du 2 mars 2004 « que la bande organisée suppose la préméditation des infractions et, à la différence de l'association de malfaiteurs, une organisation structurée entre ses membres » (Cass. Crim. 8 juillet 2015, n° 14-88.329, Publié au Bulletin).

15 Cf. Les nouveaux articles 222-52 à 222-54,222-56 à 222-59,322-6-1 et 322-11-1 du Code pénal.

16 Paris, Lyon, Marseille, Lille, Rennes, Bordeaux, Nancy et Fort-de-France. Cf. la page de présentation des JIRS au grand public sur le site internet du Ministère de la Justice : http://www.justice.gouv.fr/organisation-de-la-justice-10031/lordre-judiciaire-10033/les-juridictions-interregionales-specialisees-13836.html (consulté pour la dernière fois le 25 juin 2016) : « Les JIRS bénéficient de dispositifs novateurs en matière d'enquête (infiltrations, sonorisations, équipes communes d'enquête entre plusieurs pays). Les JIRS sont la démonstration de la capacité d'adaptation de la justice à la criminalité et à la délinquance modernes. L'autorité judiciaire se voit ainsi dotée d'outils l'autorisant à se montrer volontariste et offensive face aux organisations criminelles souvent transnationales dont le démantèlement est de plus en plus complexe. »

17 Cf. M. TESSIER, op. cit., pp. 19-20.

18 Cf. notamment : Conseil d'État, Assemblée Générale, Section de l'intérieur, Section des finances, 28 janvier 2016, avis (n° 391004) sur un projet de loi renforçant la lutte contre le crime organisé et son financement, l'efficacité et les garanties de la procédure pénale, n° 9 (« Sur la conception de la procédure pénale »).

19 Ibid., n°11 et 12.

20 Cf. S. GUINCHARD, J. BUISSON, Procédure pénale, 8e édition, LexisNexis, 2012, n° 1058, cité in M. TESSIER, op. cit., p. 20. Lors du colloque de défense pénale du Syndicat des Avocats de France organisé à Marseille les 14 et 15 mai 2016, Madame Vanessa CODACCIONI soulignait quant à elle que « la répression s'est déplacée du procès à l'avant-procès. »

21 CE, 28 janvier 2016, loc. cit., n°5 : « L'étude d'impact du projet de loi est apparue, sur certains points, insuffisantes : soit que les données permettant d'apprécier l'utilité de la mesure introduite n'aient pas été suffisamment exposées ; soit en raison d'une présentation lacunaire de l'état du droit ; soit encore du fait de l'absence d'éléments de droit comparé. »

22 CNCDH, Assemblée plénière, Avis, loc. cit., n° 3 à 8.

23 C. CAPDEVIELLE, P. POPELIN, députés, Rapport n° 3515…, p. 11.

24 F. MOLINS, « De la nécessité de lutter plus activement contre les nouvelles formes de criminalité », AJ Pénal 2004, p. 177, cité in M. TESSIER, op. cit., p. 15.

25 C. LAZERGES, A. VALLINI, « Le cauchemar Perben II », Libération, 19 janvier 2004, cf. site internet du journal : http://www.liberation.fr/tribune/2004/01/19/le-cauchemar-perben-ii_465725. Ce constat est également partagé en 2016 par des membres de la droite parlementaire. Ainsi, le député Patrick DEVEDJIAN (LR), co-rapporteur sur la mise en application de la loi a-t-il écrit : « Le terrorisme et son obsession nous ont rattrapés et dépassés et la simplification recherchée a laissé place à la normalisation de l'exception, comme la loi sur le renseignement avait commencé à le faire. Plusieurs mesures de l'état d'urgence font leur entrée dans le droit commun avec un risque important pour les libertés individuelles. » (cf. C. CAPDEVIELLE, P. POPELIN, députés, Rapport n° 3515…, p. 55).

26 G.BRAIBANT, « l'État face aux dangers », Pouvoirs, 1979, p. 8, cité in CNCDH, Assemblée plénière, Avis sur …, loc. cit., p. 3.

27 C. CAPDEVIELLE, P. POPELIN, députés, Rapport n° 3515…, p. 3.

28 Et cela sans que l'auteur de ces lignes prétende disposer d'une quelconque légitimité pour se prononcer sur la question, autrement que sa qualité de citoyen.

29 M.-L. CESONI (dir.), Criminalité organisée : des représentations sociales aux définitions juridiques, LGDJ, Paris, 2004, p. 6, cité in M. TESSIER, op. cit., p. 16.

30 R. GASSIN, Criminologie, coll. Précis, Dalloz, 1988, § 282, cité in Y. BISIOU, « Le concept de criminalité organisée en France », in M.-L. CESONI (dir.), op. cit., p. 625, cité in M. TESSIER, op. cit., p. 17.

31 Cf. A. GARAPON, S. PERDRIOLLE, B. BERNABE, La Prudence et l'Autorité, Juges et Procureurs du XXIe siècle, Odile Jacob, 2014. Cet ouvrage, issu d'un rapport de l'Institut des Hautes Etudes sur la Justice (IHEJ) a décomposé l'office du juge en six critères : l'office jurisprudentiel, l'office processuel, l'office de vérité, l'office tutélaire, l'office sanctionnateur et l'office libéral.

32 Sur la défense pénale, cf. l'ouvrage de référence de J. DANET, Défendre. Pour une défense pénale critique, op. cit.,et notamment p. 260 : « Ni Don Quichotte de ruptures imaginaires, ni valet de connivence, la défense est une critique. Ni bateleur, ni complice de l'accusé ou de ses juges, la défense doit faire respecter la légitimité de sa fonction sociale. Ni technicien, nipotiche, l'avocat est partenaire de justice. Les discours de ladéfense ressortent de la pédagogie et de la politique s'ils veulent alimenter les débats nécessaires à toute démocratie. »

33 Cf. A. GARAPON, S. PERDRIOLLE, B. BERNABE, op. cit. : L'« office sanctionnateur » du juge consiste à « sanctionner les infractions poursuivies et établies en veillant à ce que le condamné soit réintégré dans la société à l'issue de sa peine et qu'il ne présente plus de danger excessif pour elle. »

34 Cf. J. DANET, Défendre, p. 37 : « le procès équitable paraît s'imposer comme un nouveau modèle, transcendant les modèles accusatoires et inquisitoires, pour fournir un nouvel idéal de procès, plus soucieux des droits de la défense. » Cf. également D. SALAS, Du procès pénal, PUF, 1992.

35 Cf. Circulaire (n° CRIM-2016-06/E1/02.06.2016) de politique pénale de M. Jean-Jacques URVOAS, Garde des Sceaux, ministre de la Justice, 2 juin 2016, p. 6 : « les dossiers complexes devront donner lieu, de manière systématique, à des investigations sur le patrimoine et les ressources des mis en cause, afin de procéder, le cas échéant, à des saisies, puis à des confiscations […] Au-delà, il convient surtout de s'assurer de l'effectivité des saisies effectuées, par des réquisitions systématiques sur la destination de ces biens, les peines de confiscation s'avérant encore trop peu prononcées. »

36 36 Cf. A. GARAPON, S. PERDRIOLLE, B. BERNABE, op. cit. : L'« office de vérité » du juge consiste à « établir la « vérité des faits de manière indépendante, procédurale et argumentée »

37 F. HELIE, Traité de l'instruction criminelle ou théorie du Code d'instruction criminelle, t. 1, Paris, Plon, 2e édition, 1866, p. 4, cité in C. CAPDEVIELLE, P. POPELIN, députés, Rapport n° 3515…, p. 11.

38 S. GUINCHARD, J. BUISSON, op. cit., n° 2368, cité in M. TESSIER, op. cit., p. 128.

39 Cf. A. GARAPON, S. PERDRIOLLE, B. BERNABE, op. cit., p. 58, cité in M. TESSIER, op. cit., p. 128. Ibid.

40 Ibid.

41 Ibid., cité in M. TESSIER, op. cit., p. 26.

42 A. GARAPON, Le gardien des promesses, Le juge et la démocratie, Odile Jacob, 1996, p. 37, cité in M. TESSIER, op. cit., p. 25.

43 Cf. À titre d'exemple le colloque défense pénale organisé par le Syndicat des Avocats de France à Marseille les 14 et 15 mai 2016 : « Défendre sous les lois d'exception ». De telles réflexions sont également proposées par certains Barreaux sur ces sujets dans le cadre des commissions pénales.

44 Ces mots ont été prononcés en plaidoirie le 29 janvier 2016 par Maître Catherine GLON, Avocat au Barreau de Rennes, devant le tribunal correctionnel (JIRS) de Rennes.

45 C'est notamment ce que conseillait Maître François SAINT-PIERRE lors d'un colloque organisé le 25 mars 2016 par l'Institut de défense Pénale (dir. Ph. VOULAND, F. SAINT-PIERRE)à Rennes.

46 Cf. J. DANET, Défendre. Pour une défense pénale critique, op. cit., p. 257 et suivantes : « La défense n'est pas condamnée à la connivence lorsque la rupture n'est pas de mise. La défense pénale n'existe au contraire que dans un processus critique ».

47 Cf. Paroles prononcées dans le cadre du colloque de défense pénale organisé par le Syndicat des Avocats de France à Marseille les 14 et 15 mai 2016 : « Défendre sous les lois d'exception ».

48 Rapport du groupe de travail relatif à la protection des magistrats, remise à M. Jean-Jacques URVOAS, Garde des Sceaux, ministre de la Justice, le mardi 28 juin 2016.

49 Ibid.

OUVRAGES RÉCENTS

RAPPORT MORAL SUR L'ARGENT DANS LE MONDE 2015-2016

AUTEUR / EDITEUR : ASSOCIATION D'ECONOMIE FINANCIÈRE

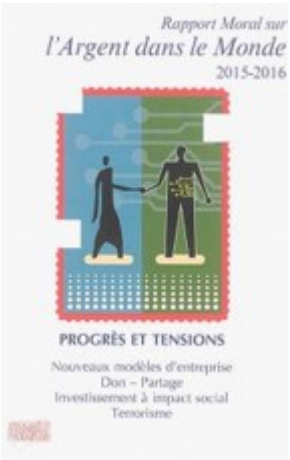
Présentation de l'éditeur

Devenu au fil de ses vingt années de parution une grande référence, le Rapport Moral sur l'Argent dans le Monde 2015-2016, de l'Association d'Economie Financière, réunie sous l'égide de la Caisse des Dépôts et de son directeur général, Pierre-René LEMAS, la contribution d'une quarantaine d'auteurs, praticiens ou experts de ce domaine.

Le rapport traite de l'émergence de nouveaux modèles et de nouveaux comportements :

Progrès et tension ont marqué le monde au cours de l'année écoulée. En effet ubérisation et économie du partage modifient le cadre de nombreuses activités, les modèles d'Entreprise se transforment, la responsabilité écologique est omniprésente.

Les critères de l'investissement responsable et la prise en compte de son impact social se généralisent, impulsés par le Fin Tech et l'économie sociale et solidaire.



En outre ces évolutions porteuses de progrès doivent intégrer celles d'un nouveau contexte lié à l'émergence du terrorisme qui constitue en réalité une autre donnée économique sous ses différents aspects (financement, impact, prévention).

Comme le remarque avec pertinence, François CHAMPARNAUD, qui introduit cet ouvrage, délégué général de l'Association d'Economie Financière, « …nous sommes entrés dans le temps des paradoxes ou générosité, solidarité et progrès avancent sur un fond de drames et de tensions et nos systèmes économiques et financiers ont tendance à amplifier ces contradictions….. ».

Ce rapport moral reste l'instrument privilégié de réflexion et de travail pour éclairer les enjeux fondamentaux de notre système financier en fournissant une large synthèse des grands débats du monde de la finance.

LE NOUVEAU DÉLIT DE TRAFIC DE BIENS CULTURELS PROVENANT D'UN THÉÂTRE D'OPÉRATIONS DE GROUPEMENTS TERRORISTES : QUELLE EFFICACITÉ ?

DOROTHÉE GOETZ

DOCTEUR EN DROIT PÉNAL ET SCIENCES CRIMINELLES

Si la loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement et améliorant l'efficacité et les garanties de la procédure pénale concerne majoritairement l'enquête au sens très large[1], le chapitre V du Titre I, intitulé « dispositions améliorant la lutte contre le blanchiment et le financement du terrorisme » recèle néanmoins d'importantes mesures. Il en est ainsi du plafonnement des cartes prépayées, du renforcement des pouvoirs de Tracfin qui comporte la possibilité de signaler aux organismes assujettis des situations à risque afin d'instaurer une vigilance renforcée, de l'extension du droit de communication aux organismes gérant les systèmes de paiement et de la création de l'infraction de trafic de biens culturels provenant d'un théâtre d'opérations de groupements terroristes. L'article 29 de la loi insère ce nouveau délit à l'article 322-3-2 du Code pénal qui précise désormais : *« est puni de sept ans d'emprisonnement et de 100 000 € d'amende le fait d'importer, d'exporter, de faire transiter, de transporter, de détenir, de vendre, d'acquérir ou d'échanger un bien culturel présentant un intérêt archéologique, artistique, historique ou scientifique en sachant que ce bien a été soustrait d'un territoire qui constituait, au moment de la soustraction, un théâtre d'opérations de groupements terroristes et sans pouvoir justifier la licéité de l'origine de ce bien. »*

L'intérêt de cette disposition est évident. En effet, les groupements terroristes ne détruisent plus aveuglement les biens culturels pour anéantir « *l'identité de l'adversaire, son histoire, sa culture, sa foi* (...) »[2] mais agissent aussi souvent à des fins mercantiles. Ainsi, en plus de porter atteinte à la mémoire d'une civilisation, le pillage des sites archéologiques peut constituer une source de financement du terrorisme. L'exemple de Daesh est éloquent. En effet, cette organisation terroriste a conquis, au fil du temps, de vastes territoires dotés d'un riche patrimoine préislamique, telle l'ancienne Mésopotamie, berceau des civilisations antiques[3]. Le site de Palmyre, pillé par Daesh, a donné lieu à un trafic d'objets archéologiques qui a généré de substantiels revenus[4]. C'est ainsi que des « antiquités de sang[5] » peuvent se retrouver, après un jeu de reventes successives, sur le marché de l'art et alimenter les caisses du terrorisme. Même si « aucun des chiffres circulant à ce sujet n'est officiel »[6], il s'agirait, au plan mondial, du troisième commerce illégal le plus important après celui de la drogue et des armes[7] La difficulté d'évaluer ce trafic s'explique par deux raisons. Primo, ces ventes confidentielles s'effectuent entre initiés et, de ce fait, leur recensement est extrêmement difficile. Secundo, elles se réalisent souvent plusieurs années après le vol afin d'en effacer toute traçabilité. Les objets volés se voient alors attribuer une nouvelle histoire de vie[8] afin de tromper la vigilance des autorités du pays destinataire des biens écoulés frauduleusement[9].

Cette pratique n'est pas nouvelle. Les conflits armés sont

souvent le théâtre de pillages dont les organisateurs espèrent tirer profit[10]. Par exemple, lors de la dislocation de la Yougoslavie dans les années 1990, des agissements similaires ont ponctué le déroulement du conflit alors que les belligérants ne se réclamaient pas du terrorisme[11]. S'agissant du terrorisme, en dehors des scènes de pillage et de destruction de l'emblématique cité de Palmyre, d'autres sites ont connu le même sort : - destruction des Bouddhas du VIe siècle à Bamiyan, en Afghanistan, en 2001, - pillage des musées de Bagdad et de Mossoul durant la guerre d'Irak en 2003, - destruction du patrimoine Malien en 2013 et 2014....

Cette réalité bouleverse depuis plusieurs années la communauté internationale[12]. Dès 1970[13], sous l'impulsion de l'Unesco, un cadre juridique dédié a été mis en place au plan international. Depuis, des progrès significatifs ont été réalisés et l'Onu porte régulièrement un intérêt à cette question[14]. Deux règlements européens ont ainsi été adoptés pour faire suite à deux résolutions des Nations Unies[15]. Ces textes d'application directe posent, sous certaines conditions, un principe d'interdiction du commerce de biens culturels en provenance de l'Irak[16] et de la Syrie[17]. L'Office des Nations Unies contre la Drogue et le Crime (ONUDC) manifeste, dans la Convention dite de Palerme[18], la même préoccupation par rapport au trafic des biens culturels. L'Union européenne s'est aussi emparée de la question[19] dont l'illustration ressort des conclusions du Conseil de l'Union européenne des 13 et 14 décembre 2011 relatives à la prévention de la criminalité visant les biens culturels et à la lutte contre ce phénomène[20].

En France, après les attentats de novembre 2015, un appel à la vigilance a été lancé à la profession des antiquaires. Depuis la loi n° 2001-420 du 15 mai 2001, les marchands de biens dit de grandes valeurs sont soumis au dispositif anti- blanchiment et doivent, à ce titre, se conformer aux dispositions prévues aux articles L 561-2 à L. 561-36 du Code monétaire et financier. Dans un courrier[21] adressé aux deux syndicats d'antiquaires le 13 novembre 2015, le ministre des Finances et des Comptes publics, Michel Sapin, a jugé « *indispensable d'appeler l'attention de l'ensemble des professionnels du secteur du commerce de biens culturels aux risques de financement du terrorisme, de Daesh en particulier.* » Le rapport du groupe d'action financière internationale (Gafi) relatif au financement de Daesh précise que « *bien qu'il soit quasiment impossible de prouver l'existence d'un lien direct entre Daesh et la vente d'un bien culturel donné, Daesh se finance grâce aux antiquités de deux façons différentes, à la fois en vendant les biens pillés et en taxant les trafiquants qui procèdent au transport des objets d'art à travers les territoires sous son contrôle.* » [22]

Bien que ce mode de financement du terrorisme ne soit pas nouveau, il connaît aujourd'hui un essor sans précédent[23]. En effet, d'après Monsieur Jean-Luc Martinez, président-directeur du musée du Louvre et archéologue, « *Daesh a organisé le vol des antiquités comme une industrie* ». Ceci explique que la France a sensiblement renforcé la lutte à partir du deuxième semestre de l'année 2015. Ainsi, trois jalons ont déjà été posés antérieurement à la loi du 3 juin 2016.

Premièrement, le projet de loi relatif à la liberté de création, à l'architecture et au patrimoine (projet LCAP) requiert des évolutions du cadre juridique en matière de trafic de biens culturels[24]. Son article 18 B, voté en première lecture par l'Assemblée nationale et le Sénat puis supprimé par la commission mixte paritaire, proposait déjà de modifier le Code du patrimoine en y insérant quatre nouvelles mesures. Il s'agissait de la possibilité d'annuler l'entrée dans les collections publiques de biens, acquis de bonne foi, dont il s'avérerait qu'ils ont été à l'origine volés ou exportés illicitement[25] ; la possibilité de recevoir en dépôt des biens culturels étrangers menacés par un conflit armé ou une catastrophe naturelle[26] ; l'interdiction d'importer des biens culturels en l'absence d'un certificat d'origine[27] et l'interdiction d'importer, d'exporter, de faire transiter et de faire commerce de biens culturels ayant quitté illicitement un État lorsqu'une résolution du Conseil de l'ONU a été prise en ce sens (situation qui, aujourd'hui, concerne uniquement les biens en provenance de la Syrie après le 15 mars 2011 et de l'Irak après le 6 août 1990).

Deuxièmement, le rapport Martinez[28]. Le président de la République, en visite au Louvre le 18 mars 2015, date qui - hasard malheureux du calendrier - correspondait au jour de l'attentat du musée du Bardo à Tunis, a confié à Monsieur Jean-Luc Martinez le soin de réaliser un rapport sur les menaces pesant sur le patrimoine. Ce travail a été le

fruit de cinquante propositions qui ont fournis une solide contribution à la loi du 3 juin 2016.

Troisièmement, la France a soutenu une proposition informelle lancée par l'Allemagne[29] au printemps 2015 et qui consistait à demander à la Commission européenne la mise en place d'un instrument pour empêcher les importations illicites de biens culturels dans l'espace communautaire. Suite à cette initiative, la ministre de la Culture française a proposé à ses homologues allemand et italien de cosigner une lettre adressée le 7 décembre 2015 aux deux commissaires européens concernés afin d'obtenir rapidement un règlement interdisant l'importation illicite liée au financement du terrorisme de biens culturels au sein de l'Union européenne[30]. Parallèlement, et dès le 31 mars 2015, Michel Sapin, ministre de l'Économie et des Finances, et son homologue allemand, Wolfgang Schäuble, se sont également ouverts à la Commission européenne pour réclamer, au plan européen, de nouvelles actions[31].

L'article 29 de la loi du 3 juin 2016 vient donc compléter le dispositif déjà lancé. La création d'une incrimination, spécialement en matière terroriste, n'est pas exceptionnelle. Monsieur le Professeur Mayaud relève qu'en ce domaine « *les incriminations se sont multipliées régulièrement au risque de perdre une vision d'ensemble de la matière voire même une certaine cohérence* »[32]. En effet, depuis 1986, de nombreuses lois visant à lutter contre le terrorisme ont abondé le Code pénal, le Code de procédure pénale et le Code de la sécurité intérieure[33]. En 1991, dans son rapport intitulé « de la sécurité juridique[34] » le Conseil d'État dénonçait déjà cet activisme pénal en le qualifiant de « marée normative », de « logorrhée législative et réglementaire ». Madame Julie Alix remarque même qu'« *on n'ose plus dire législateur, tant sa part contributive est faible lorsque les lois sont votées en urgence, et surtout lorsqu'elles concernent des sujets aussi fédérateurs dans la classe politique que la lutte contre le terrorisme* »[35].

C'est ainsi que se pose la question de l'efficacité du nouveau délit crée par l'article 29 de la loi. La création de nouvelles infractions devant strictement répondre au principe de nécessité des incriminations[36], nous ne pouvons faire l'impasse sur une question essentielle : cette nouvelle infraction était-elle nécessaire ? Si la pratique judiciaire apportera un éclairage sur l'utilité répressive de la nouvelle disposition, l'analyse juridique peut d'ores et déjà susciter certaines réserves, tant à propos de la nécessité (I) que de l'efficacité (II) du texte.

I La nécessité de l'incrimination

Sauf à interpréter largement les dispositions existantes, aucune d'entre elles ne saisissait juridiquement, avant l'adoption de la loi du 3 juin 2016, les agissements visés par l'article 29 de la loi. Ainsi, l'espace d'incrimination semblait « disponible » (A) au sens où l'entendait le Doyen Carbonnier pour qui « *(…) la disponibilité est [l'] utilité essentielle [de la norme]*[37] ». Pour autant, une importante question, relative à la nature de l'incrimination nouvelle (B), reste à trancher : doit-il s'agir d'une incrimination terroriste ?

A La disponibilité de l'espace d'incrimination

Parmi les textes figurant dans le Code pénal, il nous semble qu'il n'en existe aucun qui réprime précisément les mêmes agissements que ceux visés par l'article 29 de la loi. Deux articles peuvent tout de même nourrir le débat : il s'agit des articles 322-3-1(i) et 421-2-2 (ii) du Code pénal.

i. Une incrimination différente de l'article 322-3-1 du Code pénal

L'article 322-3-1 du Code pénal, crée par la loi du 15 juillet 2008[38] dispose que « *la destruction, la dégradation ou la détérioration est punie de sept ans d'emprisonnement et de 100 000 € d'amende lorsqu'elle porte sur : 1° Un immeuble ou objet mobilier classé ou inscrit en application des dispositions du code du patrimoine ou un document d'archives privées classé en application des dispositions du même code ; 2° Une découverte archéologique faite au cours de fouilles ou fortuitement, un terrain sur lequel se déroulent des opérations archéologiques ou un édifice affecté au culte (…)* ». En application de ce texte, la jurisprudence a par exemple considéré que délit est constitué par le fait de ramasser des minéraux dans les déblais d'une mine, malgré un panneau portant interdiction de faire des fouilles sur ce site archéologique[39].

L'amendement numéro 13 présenté devant le Sénat envisageait la suppression de l'article 29 de la loi au motif qu'il réprime des agissements déjà prévus par l'article 322-3-1 du Code pénal. Or, si le premier réprime

le trafic qui découle du pillage de biens culturels opéré dans un territoire aux prises avec le terrorisme, le second sanctionne le fait, non pas de financer le terrorisme en se livrant au trafic tout en connaissant la provenance illicite du bien, mais de détruire, dégrader ou détériorer un tel bien. Selon l'article 111-4 du Code pénal, la loi pénale est d'interprétation stricte. Bien que parfois l'interprétation des incriminations entraîne des distorsions finalistes justifiées par les besoins de la répression[40], le juge ne peut pas créer des incriminations. C'est pourquoi l'article 322-3-1 du Code pénal ne saurait être utilisé pour réprimer, non pas la dégradation d'un bien mais l'importation, l'exportation, le transit, le transport, la détention, la vente, l'acquisition ou l'échange, en toute connaissance de cause de sa provenance d'un théâtre d'opérations de groupements terroristes.

Le même constat s'impose à propos de l'article 421-2-2 du Code pénal.

ii. Une incrimination différente de l'article 421-2-2 du Code pénal

L'article 421-2-2 du Code pénal dispose que « *constitue également un acte de terrorisme le fait de financer une entreprise terroriste en fournissant, en réunissant ou en gérant des fonds, des valeurs ou des biens quelconques ou en donnant des conseils à cette fin, dans l'intention de voir ces fonds, valeurs ou biens utilisés ou en sachant qu'ils sont destinés à être utilisés, en tout ou partie, en vue de commettre l'un quelconque des actes de terrorisme prévus au présent chapitre, indépendamment de la survenance éventuelle d'un tel acte.* » Cet article, inséré par la loi du 15 novembre 2001[41] dans la partie du Code pénal relative au terrorisme, vise précisément le fait de financer le terrorisme au moyen de la fourniture, de la gestion ou de la réunion d'un « bien quelconque ». Le financement du terrorisme par le trafic de biens culturels pourrait rentrer dans le champ d'application de l'article 421-1-2 du Code pénal en ce sens que le bien culturel est un bien quelconque. Toutefois, le champ d'application de la disposition précitée est plus restreint que celui de l'article 29 de la loi du 3 juin 2016 tant du point de vue de l'élément matériel que de l'élément moral. En effet, relatif à la seule fourniture, gestion ou réunion des biens quelconques[42], ce texte ne vise pas l'importation, l'exportation, le transit, la détention, la vente, le transport, l'acquisition ou l'échange du bien. De plus, cette incrimination nécessite de prouver l'intention que les fonds soient utilisés ou soient destinés à être utilisés à la commission d'un acte de terrorisme. Sur ce point, l'article 29 de la loi exige seulement de savoir que le bien a été soustrait d'un territoire qui constituait, au moment de la soustraction, un théâtre d'opérations de groupements terroristes et de ne pas pouvoir justifier la licéité de l'origine de ce bien.

Si l'espace d'incrimination était bien disponible, reste ensuite à déterminer la nature de l'incrimination. Sur ce point, les propositions du Sénat et de l'Assemblée nationale n'étaient pas à l'unisson. Le Sénat souhaitait insérer le nouveau délit dans le Titre II du livre III, intitulé « des crimes et des délits contre les biens » alors que l'Assemblée Nationale, de son côté, voulait l'intégrer dans les dispositions relatives au terrorisme, après l'article 421-2-6 du Code pénal. La commission mixte paritaire s'est ralliée à la position du Sénat. La nouvelle incrimination figure donc désormais à l'article 322-3-2 du Code pénal.

B La nature de l'incrimination

Selon Monsieur le Professeur Mayaud « *la réaction au terrorisme est d'abord une affaire d'incrimination.* » En cette matière « l*e travail du législateur suit une voie qui n'a jamais été démentie, celle de l'élargissement, de l'extension, manifestée par des infractions de plus en plus nombreuses* ». La commission mixte paritaire, malgré l'attractivité de créer une incrimination terroriste (i) a fait le choix opportun de ne pas faire du nouveau délit un délit terroriste ii).

i. L'attractivité d'une incrimination terroriste

Intégrer la nouvelle incrimination dans les dispositions relatives au terrorisme présenterait plusieurs avantages. D'abord, la création d'un délit terroriste entraîne inévitablement, dans son sillage, des répercussions sur la procédure applicable. En effet, les liens tissés, en matière de terrorisme, entre le droit de fond et la procédure sont très forts puisque la coloration terroriste d'une infraction permet de recourir à des règles de procédures dérogatoires au droit commun. Cette particularité s'explique par le fait qu'il est

nécessaire, en cette matière, de se doter de moyens juridiques adaptés à la menace terroriste. Ces moyens, pour être efficaces, supposent d'être plus contraignants que ceux mis en oeuvre dans la procédure de droit commun. Ensuite, faire du nouveau délit une incrimination terroriste aurait permis d'identifier clairement le lien qui unit le trafic de biens culturels avec le financement du terrorisme et de responsabiliser les divers acteurs de la chaîne du trafic, y compris les acheteurs. Enfin, l'origine géographique du bien, qui est un des éléments constitutifs de l'infraction, fait référence aux « théâtres d'opérations de groupements terroristes ». De fait, en faire un délit de droit commun, obligerait les juges à se tourner vers les dispositions propres au terrorisme pour définir le champ d'application de l'infraction. Il est vrai que la technique du renvoi vers les dispositions terroristes est parfois judicieusement utilisée par le législateur lui-même. L'exemple des contrôles d'identités prévus à l'article 78-2-2 du Code de procédure pénale en est une bonne illustration[43]. Introduit dans le Code de procédure pénale peu après les attentats du 11 septembre 2001 par la loi n° 2001-1062 du 15 novembre 2001[44], puis pérennisé par la loi n° 2003-239 du 18 mars 2003[45], cet article permet, sur réquisitions écrites du procureur de la République et pour une liste d'infractions limitativement énumérées [actes de terrorisme visés par les articles 421-1 à 421 -6 du Code pénal notamment], de « *procéder non seulement aux contrôles d'identité prévus au sixième alinéa de l'article 78-2 mais aussi à la visite des véhicules circulant, arrêtés ou stationnant sur la voie publique ou dans des lieux accessibles au public».* Dans ce cas, il est logique que ces contrôles d'identités spécifiques ne figurent pas dans les dispositions relatives au terrorisme puisque le terrorisme n'est que « *l'une des formes graves ou insidieuses de criminalités*[46] » contre lesquelles le législateur souhaite lutter avec l'article 78-2-2 du Code de procédure pénale. La situation n'est pas identique dans l'article 29 de la loi du 3 juin 2016 qui vise, à travers l'expression de « théâtre de groupements d'opérations terroristes », une seule forme de criminalité.

En outre, le projet de règlement européen pour lutter contre l'importation illicite de biens culturels au sein de l'Union européenne établit lui aussi le lien entre le trafic de biens culturels et le terrorisme. Les ministres réclament en effet à la Commission européenne « un cadre juridique parfaitement adapté à la lutte contre le trafic illicite des biens culturels, ce qui contribuera à assécher le financement du terrorisme ». Pourtant, et contre toute attente, la commission mixte paritaire n'a pas érigé le nouveau délit en une incrimination terroriste.

ii. Le choix d'une incrimination non terroriste

En positionnant la nouvelle infraction à l'article 322-3-2 du Code pénal, la commission mixte paritaire a fait le bon choix. En effet, même si l'auteur de l'infraction n'ignore pas que le bien a été soustrait d'un territoire qui constituait, au moment de la soustraction, un théâtre d'opérations de groupements terroristes et qu'il n'est pas en mesure de justifier la licéité de l'origine de ce bien, il n'est pas pour autant coupable d'un acte de terrorisme au sens des articles 421-1 et suivants du Code pénal. C'est donc uniquement en raison du potentiel « contexte terroriste » dans lequel le trafic s'inscrit que le rattachement de l'article 29 de la loi aux dispositions du Code pénal relatives au terrorisme aurait pu se justifier. Bien qu'en matière de terrorisme[47] la dimension préventive offre un intérêt indéniable, ériger l'article 29 de la loi en une incrimination terroriste aurait alimenté une ambigüité entre cette forme de soutien et les véritables acteurs du terrorisme. Cette ambiguïté, déjà entretenue par les lois précédentes, comporte deux risques majeurs. Premièrement, elle peut servir de prétexte pour déroger à des libertés fondamentales. Deuxièmement, la multiplication des incriminations contenues dans la partie du Code pénal relative au terrorisme affaiblit la force et la portée des dispositions applicables en la matière. En ce sens, Monsieur le Professeur Mayaud considère que la législation en matière de terrorisme « *donne l'impression d'un immense désordre, d'hésitation, voire d'un manque de recul par rapport à ce qui mériterait une sérieuse réflexion d'ensemble*[48]*.* » Ainsi, en insérant la nouvelle incrimination après l'article 322-3-1 du Code pénal, le législateur affirme sa volonté de ne pas poursuivre l'intégration dans le Titre II du livre III du Code pénal intitulé « du terrorisme » d'infractions qualifiées de terroristes uniquement par rapport à l'environnement dans lequel elles ont été commises.

Ce choix s'inspire sans doute de l'article 18 B du projet de loi LCAP,

dans sa rédaction antérieure à la réunion de la commission mixte paritaire. Cet article proposait d'enrichir le Code du patrimoine et énonçait qu'« *il est interdit d'importer, d'exporter, de faire transiter, de transporter, de détenir, de vendre, d'acquérir et d'échanger des biens culturels présentant un intérêt archéologique, artistique, historique ou scientifique lorsqu'ils ont quitté illicitement le territoire d'un État dans les conditions fixées par une résolution du Conseil de sécurité de l'Organisation des Nations Unies adoptée en ce sens* ». Ainsi, tant dans l'article 18 B du projet de loi LCAP que dans l'article 29 de la loi du 3 juin 2016, bien qu'il ne s'agisse pas d'une incrimination terroriste, le lien avec le financement du terrorisme est expressément visé. Lors des débats relatifs au titre II du projet de loi LCAP dans lequel figurait l'article 18 B, il avait été relevé qu'« *en se livrant à la contrebande directe ou indirecte des biens culturels provenant de sites archéologiques, des musées et des bibliothèques, ils [les groupements terroristes] financent leurs crimes abjects (...).*» La principale distinction entre le champ d'application de l'article 29 de la loi de 2016 et celui de l'article 18 B est l'existence, ou non, d'une résolution de l'ONU. En présence d'une telle résolution, le second avait prévu d'exposer l'auteur de l'infraction à une peine de deux années d'emprisonnement et à une amende de 450 000 euros. Le premier, en l'absence de résolution onusienne, entraîne une peine de 7 ans d'emprisonnement et 100 000 euros d'amende. En conséquence, en cas de cohabitation entre ces deux textes, pour des faits identiques, la peine privative de liberté aurait été plus forte en l'absence d'une convention de l'ONU. Or, l'article 8 de la Déclaration des droits de l'homme et du citoyen de 1789 indique que « *les lois ne doivent établir que des peines strictement et évidemment nécessaires.* » Bien que le Conseil constitutionnel estime « *qu'il ne lui appartient pas de substituer sa propre appréciation à celle du législateur en ce qui concerne la nécessité des peines attachées aux infractions définies par celui-ci*[49] », il ne se refuse pas à contrôler la proportionnalité des peines. En effet, peuvent être censurées « *les dispositions législatives prévoyant des peines manifestement disproportionnées par rapport aux faits reprochés* »[50]. Dans le même esprit, le Conseil de l'Europe insiste régulièrement, depuis une recommandation de 1992 relative à la cohérence dans le prononcé des peines, sur la nécessité d'assurer la proportionnalité entre la gravité de l'infraction et la peine[51]. En l'espèce, en cas de coexistence entre les deux articles, on aurait pu raisonnablement douter de la conformité du dispositif avec le principe de proportionnalité des peines. Cela explique que la Commission mixte paritaire réunie à l'occasion du projet de loi LCAP a supprimé l'article 18 B. L'article 29 de la loi du 3 juin 2016 s'en inspire toutefois dans son choix de ne pas conférer à l'incrimination nouvelle une nature terroriste.

La nécessité de créer cette nouvelle incrimination étant établie, reste à déterminer l'efficacité du texte retenu.

II. L'efficacité de l'incrimination

Au sujet de la rédaction des textes d'incrimination, Monsieur le Professeur Mayaud relève qu'en matière de terrorisme, et malgré une couverture substantielle par le droit, les textes s'accompagnent souvent de « faiblesses rédactionnelles »[52]. Tel nous semble être le cas de certains aspects de l'article 29 de la loi du 3 juin 2016 (A). De fait, le caractère hybride de l'article suscite certaines réserves par rapport à l'efficacité future du texte (B).

A. Les faiblesses rédactionnelles du texte

L'article 29 comporte deux paragraphes. Dans son I, le texte prévoit les éléments constitutifs de l'infraction ainsi que les peines applicables (i). Dans le II, le texte précise la procédure applicable (ii).

i. Le I de l'article 29

Le I de l'article 29 incrimine le fait d'importer, d'exporter, de faire transiter, de détenir, de vendre, d'acquérir, de transporter ou d'échanger un bien culturel présentant un intérêt archéologique, artistique, historique ou scientifique, dès lors que trois conditions cumulatives sont réunies. D'abord, le bien doit avoir été soustrait d'un territoire qui constituait, au moment de la soustraction, un théâtre d'opérations de groupements terroristes. Ensuite, la personne incriminée doit avoir connaissance de ce fait et, enfin, elle doit ne pas pouvoir justifier la licéité de l'origine de ce bien.

L'expression connue[53] de « *théâtre d'opérations de groupements terroristes*[54] » figure déjà dans deux dispositions créées par la loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme : l'article L224-1 du Code de sécurité intérieure et l'article 421-2-6 du Code pénal. Le Conseil

constitutionnel a été saisi le 15 juillet 2015 par le Conseil d'État d'une question prioritaire de constitutionnalité (QPC) relative à la conformité aux droits et libertés que la Constitution garantit des dispositions de l'article L224-1 du Code de la sécurité intérieure[57]. Les Sages ont déclaré les dispositions de l'article L224-1 du Code de la sécurité intérieure conformes à la Constitution. Le Conseil d'État a récemment utilisé cette notion[58], au sujet de la fermeture d'une salle de prière en rappelant « *que plusieurs des prédicateurs ayant officié à la mosquée ainsi que des fidèles ont fait l'objet de mesures d'interdiction de sortie du territoire français sur le fondement de l'article L224-1 du Code de la sécurité intérieure, qui concerne les Français dont il existe de sérieuses raisons de penser qu'ils projettent des déplacements à l'étranger ayant pour objet la participation à des activités terroristes ou sur un théâtre d'opérations de groupements terroristes (...).* »

Pourtant, l'expression de « théâtre d'opérations de groupements terroristes » n'est à aucun moment définie par le législateur. En outre, elle ne fait pas l'objet d'une liste fixée par décret. En effet, en raison d'une possible extension rapide de ces territoires, il est difficile de les délimiter de manière exhaustive. Madame Alix évoque cette souplesse nécessaire au sujet de l'autoradicalisation de certains individus qui prennent le départ vers des théâtres de guerre dont les destinations sont « Syrie, Irak aujourd'hui, Afghanistan, Pakistan hier et peut-être demain »[59]. C'est pourquoi la délimitation des théâtres d'opérations de groupements terroristes est laissée à la jurisprudence. Si cette souplesse est nécessaire, elle pose tout de même question compte tenu des difficultés du législateur à définir de l'acte de terrorisme et risque d'entraîner, à propos de l'article 29 de la loi, des difficultés probatoires. Le Sénat proposait de substituer à l'expression de « théâtres d'opérations de groupements terroristes » celle de « théâtres d'opérations de groupes armés », s'épargnant ainsi les difficultés évoquées. *Primo* l'utilisation de cette expression aurait permis de gommer la référence au terrorisme en évitant de faire ressurgir les difficultés de définition de l'acte de terrorisme lui-même. *Secundo*, compte tenu du caractère protéiforme du terrorisme (terrorisme écologique, terrorisme par recrutement, terrorisme par provocation ou apologie, terrorisme par entreprise individuelle), elle aurait facilité la preuve de l'infraction visée par l'article 29.

Sur l'élément intentionnel, le Conseil d'État s'était prononcé en ces termes. Il a « *estimé que la connaissance de la seule provenance de biens culturels d'une aire géographique au sein de laquelle opèrent des groupements terroristes, si elle peut laisser présumer une origine illicite de ces biens, ne peut suffire à caractériser une incrimination pénale du fait de leur possession ou de leur vente. De surcroît, une incrimination aussi largement définie pourrait être contraire aux principes de la libre circulation des marchandises consacrée par les articles 36 et suivants du Traité sur le fonctionnement de l'Union européenne* ». C'est pourquoi, il a jugé « *indispensable de préciser que cette incrimination ne vise que les biens soustraits de leur territoire d'origine et dont la licéité de la provenance ne peut être justifiée*[61] ». Ainsi, l'article 29 de la loi du 3 juin 2016, qui s'inspire de l'article 35[62] de la même loi, exige que la personne incriminée ait eu connaissance de la soustraction du bien en provenance d'un théâtre d'opérations de groupements terroristes et ne puisse pas justifier la licéité de l'origine de ce bien. En renversant la charge de la preuve, le texte fait peser une présomption d'origine illicite tendant à faciliter l'établissement de l'infraction pour des situations où, en pratique, l'origine du bien est difficile à établir. L'intérêt de ce renversement partiel de la charge de la preuve est de responsabiliser les acheteurs qui constituent un maillon de la chaîne du trafic de biens culturels provenant de théâtres de guerre. Un collectionneur de bonne foi qui ne connaît pas la provenance du bien et qui est en mesure de justifier la licéité de son origine ne sera pas inquiété, de même que celui qui conserve des oeuvres à des fins de protection, en accord avec les autorités publiques françaises. La CNCDH relève à juste titre que si ces dispositions ne sont pas de nature à violer la présomption d'innocence au regard des exigences découlant des articles 9 de la DDHC[63] et 6-2 de la CEDH[64], elles en « atténuent néanmoins considérablement la portée »[65].

Le II de l'article 29, qui concerne la procédure applicable au nouveau délit, suscite, lui aussi, certaines réserves.

ii. Le II de l'article 29

L'article 29 II de la loi complète l'article 706-73-1 du Code de

procédure pénale en y ajoutant, dans son 6°, une référence « *aux délits d'importation, d'exportation, de transit, de transport, de détention, de vente, d'acquisition ou d'échange d'un bien culturel prévus à l'article 322-3-2 du code pénal.* » L'infraction est donc soumise au régime procédural dérogatoire de la criminalité organisée, à l'exception des dispositions de l'article 706-88 relatives à la garde à vue[66].

Lors de la première lecture du texte à l'Assemblée nationale, il avait été retenu d'intégrer le délit prévu à l'article 29 dans la partie du Code pénal relative au terrorisme. Toutefois, le texte excluait, pour l'application de cette infraction, trois des règles procédurales dérogatoires prévues en matière terroriste. Les deux premières exclusions étaient mises en oeuvre par l'introduction d'une référence au délit de trafic de biens culturels provenant d'un théâtre d'opérations de groupements terroristes à l'article 706-24-1 du Code de procédure pénale, qui écarte déjà l'application, pour les délits de provocation au terrorisme et d'apologie du terrorisme prévus à l'article 421 -2-5 du Code pénal : – de l'article 706-88 du Code de procédure pénale, qui permet de prolonger la garde à vue jusqu'à quatre jours et de différer l'intervention de l'avocat jusqu'à la soixante-douzième heure en matière de criminalité organisée et, par conséquent, en matière de terrorisme ; – des articles 706-89 à 706-94 du même code, qui autorisent les perquisitions de nuit. La troisième règle dont l'application était écartée était celle prévue à l'article 706-25-1 du Code de procédure pénale, qui allonge les délais de prescription de l'action publique et des peines en matière de terrorisme. Cette triple exclusion se justifiait. En effet, l'application des règles procédurales précitées à un délit qui, bien qu'il devienne de nature terroriste, se fonde sur un élément matériel constitué par un trafic qui n'est pas susceptible de porter atteinte en lui-même à la sécurité, à la dignité ou à la vie des personnes, aurait indéniablement soulevé des difficultés par rapport à la proportionnalité entre la gravité de l'infraction et les mesures d'enquêtes mises en oeuvre. En effet, dans sa décision n° 2004–492 DC du 2 mars 2004 sur la loi portant adaptation de la justice aux évolutions de la criminalité, le Conseil constitutionnel a énoncé que « *le législateur tient de l'article 34 de la Constitution, ainsi que du principe de légalité des délits et des peines, l'obligation de fixer lui-même le champ d'application de la loi pénale et de définir les crimes et délits en termes suffisamment clairs et précis ; que cette exigence s'impose non seulement pour exclure l'arbitraire dans le prononcé des peines, mais encore pour éviter une rigueur non nécessaire lors de la recherche des auteurs d'infractions.* » En conséquence, il a considéré que « *si le législateur peut prévoir des mesures d'investigation spéciales en vue de constater des crimes et délits d'une gravité et d'une complexité particulières, d'en rassembler les preuves et d'en rechercher les auteurs, c'est sous réserve que (...) les restrictions qu'elles apportent aux droits constitutionnellement garantis soient nécessaires à la manifestation de la vérité, proportionnées à la gravité et à la complexité des infractions commises et n'introduisent pas de discriminations injustifiées* ».

Le texte retenu par la commission mixte paritaire opte pour la même approche. Il fait le choix d'une procédure dérogatoire – celle de la criminalité organisée – tout en reconnaissant que cette procédure est applicable à la nouvelle infraction à l'exception de l'article 706-88 du Code de procédure pénale. Ce choix accentue le caractère hybride de la nouvelle incrimination.

B Le caractère hybride de la nouvelle incrimination

Bien que non intégré dans la partie du Code relative au terrorisme, l'article 29 met expressément en avant le lien entre les agissements réprimés et le terrorisme. Pourtant, malgré cette référence explicite au terrorisme, l'article 29 se retranche, à l'exception des dispositions de l'article 706-88 du Code de procédure pénale relatives à la garde à vue, vers la procédure dérogatoire de la criminalité organisée. Ce basculement se justifie par le contexte terroriste dans lequel l'infraction a pu être commise. La particularité de l'article 29 est, en effet, qu'il n'incrimine pas un acte de terrorisme mais un acte de soutien au terrorisme[67], prenant la forme d'un financement. Madame Alix relève qu' « *à partir de la loi du 22 juillet 1996 faisant suite aux attentats commis à Paris en 1995, l'immense majorité des dispositions introduites dans le Code pénal a pris la forme d'incrimination d'actes de soutien au terrorisme : soutien logistique et financier (infractions à la législation sur les armes, recels, délits d'initié, blanchiment, financement du terrorisme) mais*

également soutien humain (recel de malfaiteurs, participation aux groupes de combats et mouvements dissous, et surtout participation à une association de terroristes) »[68]. En cela, l'article 29 est un outil d'anticipation qui permet une répression en amont et en dehors de la réalisation d'un acte de terrorisme. Or, cette législation d'anticipation du terrorisme peine à trouver sa place au sein du Code pénal. Le II de l'article 29 montre bien le dilemme du législateur. D'un côté, il veut réprimer le soutien apporté à une action terroriste et le montre en utilisant l'expression de « théâtres d'opérations de groupements terroristes ». De l'autre, côté, il est conscient des difficultés juridiques entraînées par une telle avancée.

Au fur et à mesure qu'apparaissent de nouvelles incriminations terroristes d'anticipation, le législateur est contraint de multiplier les exceptions procédurales. Celles-ci viennent se greffer à la procédure dérogatoire applicable en matière de terrorisme qui est elle-même déjà complexe et peu lisible. En effet, au sein du Code de procédure pénale, la procédure applicable au terrorisme est prévue dans plusieurs titres différents du Code, ce qui montre la transversalité de la matière. À la division relative à la poursuite, à l'instruction et au jugement des actes de terrorisme, prévue par les articles 706-16 et suivants du Code de procédure pénale, s'ajoute celle relative à la procédure applicable à la criminalité et à la délinquance organisées, visée aux articles 706-73 et suivants du même code dans laquelle le législateur vient réfugier l'article 29. En outre, certains actes terroristes transitent par des infractions financières ou de type économique, tels les crimes et délits définis aux 5° à 7° de l'article 421-1 du Code pénal (recel, blanchiment, délits d'initié). Enfin, en raison de leur caractère transversal, les règles relatives à la procédure applicable en matière de terrorisme sont dispersées au sein de plusieurs codes. Si l'essentiel des règles de poursuites, d'instruction et de jugement est contenu dans le Code de procédure pénale, les dernières réformes –la loi du 3 juin 2016 ne fait pas exception à la règle- ont largement enrichi d'autres codes (Code de sécurité intérieure, Code des douanes, Code des assurances pour l'indemnisation des victimes). L'article 29 poursuit ce mouvement qui ne contribue pas à donner la cohérence tant recherchée à la législation applicable en matière de terrorisme.

À cela s'ajoute que la pleine efficacité de la lutte contre le financement du terrorisme par le trafic de biens culturels ne peut être assurée sans une mobilisation coordonnée au niveau européen, voire international. En effet, c'est « *dans le cadre du droit, du droit international comme du droit constitutionnel, que la nécessaire lutte contre le terrorisme doit être menée. Faute de quoi les démocraties ruineraient les principes qui font leur force* »[69]. Cela explique les fortes attentes en faveur d'un règlement européen relatif au trafic de biens culturels en lien avec des groupements terroristes. Annoncé par la Commission européenne pour l'année 2017[70], ce futur règlement européen risque de faire de l'article 29 un texte transitoire. En outre, pour réprimer ce trafic, le législateur a choisi de ne pas s'inspirer des préconisations de plusieurs organisations internationales, comme l'UNESCO[71], qui recommandent de l'appréhender sous un angle plus large[72]. En effet, le trafic d'oeuvres d'art ne constitue que l'une des sources de financement du terrorisme parallèlement aux revenus des matières premières (pétrole, gaz, mines de phosphate, usines de ciment, soupçons d'appropriation du marché du coton syrien par l'État islamique)[73]. De même, le trafic d'espèces sauvages représente aussi un mode de financement du terrorisme auquel la Commission européenne a consacré de récents travaux[74]. Le chapitre V du titre I de la loi du 3 juin 2016, relatif aux « dispositions améliorant la lutte contre le blanchiment et le financement du terrorisme », est pourtant muet sur ces questions.

Le 22 juin 2004, le président de l'Assemblée nationale, Jean-Louis Debré rappelait que « *la loi n'est pas faite pour seulement affirmer des évidences, mais pour fixer des normes afin de rendre possibles ces déclarations de principes » (...) Affirmer que l'air doit être pur et l'eau limpide, c'est bien. Mais cela ne suffit pas à rendre l'air pur et limpide* ». Aussi, l'article 29 de la loi du 3 juin 2016, pourra –t-il être à la hauteur de ses ambitions ?

Notes :

1 M. Léna, Présentation de la réforme pénale, AJ Pénal 2016.52.

2 F. Bugnion, La genèse de la protection juridique des biens culturels en cas de conflit armé, RICR, juin 2004, vol. 86, n°854, p. 313.

3 H. Olivier et T. Flichy De La Neuville, L'État islamique : anatomie du nouveau Califat, Bernard

Giovangeli éditeur, 2015 ; B. Manenti, L'implacable progression de l'État islamique en Irak et en Syrie, Le nouvel observateur, 19 mai 2015.

4 E. Treppoz, Palmyre : au-delà de l'indignation, l'action ! JAC 2015, n° 27.3.

5 C. Chastanier, Lutte contre le trafic des « antiquités de sang » par Daesh, JAC 2016, n°32, p.23 ; http://info.arte.tv/fr/du-moyen-orient-leurope-un-vaste-trafic-doeuvres-dart, article du 11 mars 2015.

6 Observatoire international du trafic illicite de biens culturels, « Contrer le trafic illicite des biens culturels : un défi pour la protection du patrimoine mondial », décembre 2015, p. vii.

7 Rapport de J-L Martinez au président de la République sur la protection du patrimoine en situation de conflit armé, novembre 2015, p. 36 ; Art Media Agency, « L'art : le troisième trafic mondial de biens », AMA Newsletter n° 112, 25 juill. 2013 ; C. Chastanier, Contrôle à l'exportation des biens culturels, JAC 2015, n° 23.23.

8 M. Angelloz-Pessey, Port franc : paradis des oeuvres en transit ? JAC 2015, n° 23.33.

9 http://www.senat.fr/rap/a15-474/a15-4745.html#fn13

10 X. Perrot, Jalons pour une histoire de la protection du patrimoine culturel en cas de guerre, in J.-P. Marguénaud et H. Pauliat, Les droits de l'Homme face à la guerre : D'Oradour à Srebrenica (soixantième anniversaire de la Déclaration Universelle des Droits de l'Homme), 2009, Dalloz, p. 141 à 173.

11 R. Teijgeler, Le rôle des institutions nationales et internationales pour contrer le trafic illicite des biens culturels, Ceroart, 2012.8, trad. E. Marel.

12 C. Armbruster, La revendication de biens culturels du point de vue du droit international privé, Rev. Crit DIP 2004.723

13 Convention concernant les mesures à prendre pour interdire et empêcher l'importation, l'exportation et le transfert de propriété illicites des biens culturels, 14 nov. 1970, Paris, entrée en vigueur le 24 avr. 1972.

14 ONU, résol. de l'Assemblée générale 58/17 du 3 déc. 2003 et 61/52 du 4 déc. 2006 et résol. du Conseil économique et social 2003/29 du 22 juill. 2003, 2004/34 du 21 juill. 2004 et 2008/23 du 24 juill. 2008, intitulées « Protection contre le trafic de biens culturels ».

15 Concernant l'Irak, Résolution 1483 (2003) adoptée par le Conseil de sécurité de l'Organisation des Nations Unies à sa 4761e séance, le 22 mai 2003 ; Concernant la Syrie : Résolution 2199 (2015), adoptée par le Conseil de sécurité de l'Organisation des Nations Unies à sa 7379e séance, le 12 février 2015.

16 Règl. (CE) n° 1210/2003 du Conseil du 7 juill. 2003, JOUE du 8, mod. par règl. (UE) n° 791/2014 du Conseil du 22 juill. 2014, JO du 23.

17 Règl. (UE) n° 36/2012 du Conseil du 18 janv. 2012, JOUE du 19, mod. par règl. (UE) n° 1332/2013 du Conseil du 13 déc. 2013, JOUE du 14.

18 Convention des Nations unies contre la criminalité transnationale organisée (CTO), 15 nov. 2000, Palerme, entrée en vigueur le 29 sept. 2003.

19 Présentation des principaux dispositifs existants dans l'étude sur la prévention et la lutte contre le trafic illicite des biens culturels dans l'Union européenne, réalisée pour la Commission européenne par le Centre d'étude sur la coopération juridique internationale, octobre 2011, pp. 29-57 ; Dir. 2014/60/UE du Parlement européen et du Conseil du 15 mai 2014, JOUE du 28.

20 Conseil de l'UE, 3135ème Conseil Justice et affaires intérieures, 13 et 14 décembre 2011, Conclusions du Conseil relatives à la prévention de la criminalité visant les biens culturels et la lutte contre ce phénomène.

21 Courrier rendu public sur le site commun aux ministères des finances et de l'économie, à l'adresse : http://www.economie.gouv.fr/lutte-contre-financement-terrorisme-bilan-des-mesures.

22 Rapport du Groupe d'information financière (Gafi), «Financing of the terrorist organisation islamic state in Irak and the Levant (Isil), février 2015, p. 17 : «Although it might be impossible to show a direct link between the ISIL and the sale of a specific artefact, ISIL makes money in two ways from antiquities, both through selling looted artefacts and taxing traffickers moving items through ISIL-held territory».

23 C. Chastanier, Lutte contre le trafic des « antiquités de sang » par Daesh, JAC 2016, n°32, p.23 ; CE, Avis sur un projet de loi renforçant la lutte contre le crime organisé et son financement, l'efficacité et les garanties de la procédure pénale, n° 301004.

24 Texte n° 495 (2015-2016) transmis au Sénat le 23 mars 2016.

25 C. Chastanier, op. cit.

26 Ibid.

27 Ibid.

28 J.-L. Martinez, Cinquante propositions françaises pour protéger le patrimoine de l'humanité, nov. 2015.

29 R. Peters, M. Hilgert, Recherche, législation et coopération internationale au coeur du plan d'action allemand, JAC 2016, n°32, p.32.

30 C. Chastanier, op. cit.

31 Ibid.

32 Y. Mayaud, La politique d'incrimination du terrorisme à la lumière de la législation récente, AJ Pénal 2013.442.

33 M. Léna, 1986-2016 : trente ans de lois antiterroristes, AJ Pénal 2016.105 ; C. Lazerges, De la fonction déclarative de la loi pénale, RSC 2004.194 ; H. Rouidi, La loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme : quelles évolutions ? AJ Pénal 2014.555.

34 CE, « De la sécurité juridique », rapport public annuel, La Documentation française, 1991.

35 J. Alix, Réprimer la participation au terrorisme, RSC 2014.849.

36 V. articles 5 et 8 de la DDHC.

37 J. Carbonnier, Effectivité et ineffectivité de la règle de droit, Flexible droit. Pour une sociologie du droit sans rigueur, Paris, LGDJ, 10e éd., 2001, p. 138.

38 Loi n° 2008-695 du 15 juillet 2008.

39 Crim. 28 nov. 1989, n° 89-80440, Bull. crim. N° 444.

40 Crim. 26 avril 1988, Bull. n° 178, D. 1990, note Feneaux, R.S.C. 1989, p. 111, obs. G. Levasseur.

41 Loi n°2001-1062 du 15 novembre 2001.

42 CNCDH, Assemblée plénière, 17 mars 2016, Avis sur le projet de loi renforçant la lutte contre le crime organisé, le terrorisme et leur financement et améliorant l'efficacité et les garanties de la procédure pénale, p. 18, n° 37.

43 Cass.avis, 12 janvier 2016, n° 9003, Dalloz actualité, 6 avril 2016, obs. D. Goetz.

44 RSC 2002. 674, obs. V. Bück ; Procédures 2002. Chron. 3, note J. Buisson

45 D. 2003. Chron. 1106, obs. C. Cutajar

46 Crim. 28 sept. 2010, n° 10-82.699, Dalloz actualité, 26 oct. 2010, obs. C. Girault.

47 Y. Bordenave, L. Borredon, « Un an après Merah, le nouvel âge de l'antiterrorisme », Lemonde.fr, 16 mars 2013.

48 Y. Mayaud, op. cit.

49 Décision n° 86-215 DC du 3 septembre 1986 – Loi relative à la lutte contre la criminalité et la délinquance.

50 Décision n° 80-127 DC des 19-20 janv. 1981, D. 1982. 441, note A. Dekeuwer ; Décision n° 87-237 DC du 30 déc. 1987, Rec. no 63 ; Décision no 96-377 DC du 16 juill. 1996.

51 Conseil de l'Europe, 19 octobre 1992, Recommandation n° R (92) 17 relative à la cohérence dans le prononcé des peines.

52 Y. Mayaud, La politique d'incrimination du terrorisme à la lumière de la législation récente, AJ Pénal 2013.442.

53 J. Alix, Réprimer la participation au terrorisme, RSC 2014.849.

54 Assemblée nationale, Projet de loi renforçant la lutte contre le crime organisé, le terrorisme et leur financement et améliorant l'efficacité et les garanties de la procédure pénale, n° 3473, Texte accessible sur http://www.assemblee-nationale.fr/14/projets/pl3473.asp

55 Tout Français peut faire l'objet d'une interdiction de sortie du territoire lorsqu'il existe des raisons sérieuses de penser qu'il projette : (…) 2° Ou des déplacements à l'étranger sur un théâtre d'opérations de groupements terroristes (…).

56 Constitue un acte de terrorisme le fait de préparer la commission d'une des infractions mentionnées au II, dès lors que la préparation de ladite infraction est intentionnellement en relation avec une entreprise individuelle ayant pour but de troubler gravement l'ordre public par l'intimidation ou la terreur et qu'elle est caractérisée par : (…) [le fait d'] d) Avoir séjourné à l'étranger sur un théâtre d'opérations de groupements terroristes.

57 C. Cons. Décision n° 2015-490 QPC du 14 octobre 2015.

58 CE, 25 février 2016 – n° 397153.

59 J. Alix, op. cit.

60 J-P Marguénaud, La qualification pénale des actes de terrorisme, RSC 1990.1.

61 CE, Avis sur un projet de loi renforçant la lutte contre le crime organisé et son financement, l'efficacité et les garanties de la procédure pénale, n° 301004.

62 Après l'article 415 du Code des douanes, il est inséré un article 415-1 ainsi rédigé : « Art. 415-1. – Pour l'application de l'article 415, les fonds sont présumés être le produit direct ou indirect d'un délit prévu au présent code ou d'une infraction à la législation sur les substances ou plantes vénéneuses classées comme stupéfiants lorsque les conditions matérielles, juridiques ou financières de l'opération d'exportation, d'importation, de transfert ou de compensation ne paraissent obéir à d'autre motif que de dissimuler que les fonds ont une telle origine. »

63 Cons. const. 10 juin 2009, n° 2009-580 DC, cons. 17

64 Voir notamment Cour EDH 7 octobre 1988, Salabiaku c. France, req. n° 10519/83, § 28.

65 CNCDH, Avis…., op cit., p. 19, n° 39.

66 G. Beaussonie, Loi n° 2015-993 du 17 août 2015 portant adaptation de la procédure pénale au droit de l'Union européenne, RSC 2015.940.

67 Sur cette distinction, V. J. Alix, terrorisme et droit pénal. Étude critique des incriminations terroristes, Paris, Dalloz, NBT, 2010, § 94 s. 153.

68 J. Alix, op. cit.

69 E. Decaux, Terrorisme et droit international des droits de l'homme, in : H. Laurens et M. Delmas-Marty (dir.), Terrorismes. Histoire et droit, CNRS Editions 2010, p. 304.

70 http://europa.eu/rapid/press-release_IP-16-202_fr.htm

71 http://www.unesco.org/new/fr/culture/themes/illicit-trafficking-ofcultural-property

72 CNCDH, Avis …, op.cit., p. 19, n° 37.

73 M. Rabreau, Pétrole, taxes, trafic d'humains : comment Daech se financer, Le Figaro, 26 novembre 2015 ; J-C. Brisard et D. Martinez, Islamic State : The economy-based terrorist funding, accessible sur https://risk.thomsonreuters.com/sites/default/files/GRC01815.pdf

74 http://europa.eu/rapid/press-release_IP-16-387_fr.htm

OUVRAGES RÉCENTS

L'IDENTIFICATION ELECTRONIQUE ET LES SERVICES DE CONFIANCE DEPUIS LE RÈGLEMENT EIDAS

SOUS LA DIRECTION DE : HERVÉ JACQUEMIN

EDITEUR : CRIDS—LARCIER

Présentation de l'éditeur

Quinze ans après la directive 1999/93/CE sur la signature électronique, le législateur européen a remis l'ouvrage sur le métier pour adopter, le 23 juillet 2014, un règlement sur l'identification électronique et les services de confiance pour les transactions électroniques (règlement eIDAS). La plupart de ses dispositions sont d'application à partir du 1er juillet 2016. Elles sont principalement de deux ordres.

D'une part, elles consacrent la reconnaissance mutuelle des moyens d'identification électronique délivrés par un Etat membre et qui seraient utilisés dans un autre État membre.

D'autre part, le règlement eIDAS établit un cadre juridique pour plusieurs services de con-

fiance. Outre la signature électronique, sont également visés le cachet électronique (qui doit permettre de garantir l'origine et l'intégrité d'un document électronique délivré par une personne morale), l'horodatage électronique (pour prouver l'existence des données à un moment particulier), les services d'envois recommandés et l'authentification de site internet (pour s'assurer qu'un site web est géré par celui qui s'en prétend titulaire). Le document électronique est par ailleurs traité par le règlement.

Après un éclairage technique et en sciences sociales, le présent ouvrage analyse de manière détaillée les dispositions du règlement. Plusieurs contributions sont ensuite consacrées aux perspectives internationales (en lien avec les travaux de la CNUDCI, notamment), tout en tirant des enseignements du droit comparé. Enfin, l'application du règlement est étudiée dans divers secteurs spécifiques : justice, domaine financier, e-gouvernement et e-santé.

LE CUMUL DES POURSUITES FISCALES ET PÉNALES À L'ÉPREUVE DE LA CONSTITUTION[1]

CHANTAL CUTAJAR

DIRECTEUR DU GRASCO

Par deux arrêts du 30 mars 2016, la Chambre criminelle de la Cour de cassation a saisi le conseil constitutionnel de deux QPC relatives à la conformité à la constitution des articles 1729 et 1741 C.G.I. dans le cadre de procédures engagées à l'encontre de Alec et Guy W. et Jérôme C. Dans les deux affaires, les requérants contestaient le cumul de l'application des majorations d'impôts prévues par l'article 1729 C.G.I et des sanctions pénales établies par l'article 1741 C.G.I. Dans les décisions commentées, le Conseil constitutionnel déclare la poursuite au visa de l'article 1741 C.G.I. d'une personne sanctionnée sur le fondement de l'article 1729 C.G.I, conforme à la constitution, sous trois réserves d'interprétation.

Les faits. Dans la première affaire, l'administration fiscale a notifié sur le fondement de l'article 1729 du CGI des rappels de droits de mutation à titre gratuit assortis d'intérêts de retard et de pénalités aux héritiers de Daniel W. qui avaient déposé une déclaration de succession après avoir été mis en demeure par l'administration fiscale. Ces rappels de droits étaient motivés par l'existence d'omission dans ladite déclaration. Suspectant au surplus une dissimulation frauduleuse de sommes sujettes à l'impôt, l'administration fiscale a déclenché à leur encontre des poursuites pour fraude fiscale sur le fondement de l'article 1741 du CGI. Alec et Guy W. sont renvoyés devant le tribunal correctionnel pour fraude fiscale.

Dans la seconde affaire, la révélation en décembre 2012 de l'existence d'un compte bancaire non déclaré en Suisse au nom de Jérôme C. conduit le parquet de Paris à diligenter à son encontre une enquête préliminaire. Une information judiciaire a été ouverte le 19 mars 2013 dans le cadre de laquelle les époux C. sont poursuivis au visa de l'article 1741 C.G.I. pour des déclarations minorées notamment en matière d'ISF au titre des années 2010 à 2012. L'administration fiscale avait également au visa de l'article 1729 C.G.I. prononcé une pénalité de 80 % pour manoeuvres frauduleuses.

La procédure. Alors que par le passé la Chambre criminelle avait rendu des décisions de refus de renvoi[2], elle décidait par deux arrêts n° 1736 et 2117 du 30 mars 2016 de renvoyer les deux QPC au Conseil constitutionnel. Les requérants, soutenaient que les sanctions administratives et pénales respectivement instituées par les articles 1729 et 1741 C.G.I. « s'appliquent aux mêmes faits commis par une même personne, protègent les mêmes intérêts sociaux, sont d'une nature et d'une sévérité équivalentes et, enfin, relèvent du même ordre de juridiction ». Ils en déduisent que « l'application combinée de ces deux articles serait contraire à la règle de non cumul des peines dite communément "non bis in idem", au principe de nécessité des délits et des peines ainsi qu'au principe de proportionnalité des peines, garantis par l'article 8 de la Déclaration des droits de l'homme et du citoyen de 1789 » (par. 4).

La Chambre criminelle juge que les questions présentaient « un

caractère sérieux en ce qu'elle(s) porte(nt) sur la compatibilité des dispositions critiquées avec le principe de nécessité des délits et des peines » dés lors que ces dispositions « sont susceptibles de permettre, en violation de ce principe, que des mêmes faits, définis et qualifiés de manière identique, commis par une même personne, fassent l'objet de deux poursuites, fiscale et pénale, qui visent à protéger les mêmes intérêts sociaux, peuvent aboutir au prononcé de sanctions de nature équivalente et relèvent du même ordre de juridiction ».

Notons que le Conseil constitutionnel a restreint le champ de la QPC au cas d'insuffisance volontaire de déclaration. La QPC portait dès lors « d'une part sur l'article 1729 C.G.I. et, d'autre part, sur les mots « soit qu'il ait volontairement dissimulé une part des sommes sujettes à l'impôt » figurant dans la première phrase du premier alinéa de l'article 1741 du même code » (par. 5).

Analyse. L'article 1729 C.G.I. institue, en cas de manquement délibéré du contribuable, une majoration de 40 % qui est portée à 80 % dans certains cas d'abus de droit ou si le contribuable s'est rendu coupable de manoeuvres frauduleuses.

De son côté, l'article 1741 C.G.I. punit d'une amende de 500 000 euros, qui s'élève à 1 000 000 euros en cas de fraude aggravée, et d'un emprisonnement de cinq ans, porté à sept ans en cas de fraude aggravée, quiconque a « volontairement dissimulé une part des sommes sujettes à l'impôt ». Des peines complémentaires de privation des droits civiques, civils et de famille et de publicité de la décision de condamnation peuvent également être prononcées par le juge pénal. Ces sanctions peuvent être appliquées aux contribuables qui, d'une façon frauduleuse, dissimulent volontairement des sommes soumises à l'impôt.

Il est certain que les sanctions administratives et pénales pour insuffisance de la déclaration d'impôt sont sanctionnées respectivement par les articles 1729 et 1741 C.G.I. L'article 1741 précise en effet que les sanctions qu'il prévoit s'appliquent « sans préjudice des dispositions particulières relatées dans la présente codification » et « indépendamment des sanctions fiscales applicables ».

Les requérants arguaient en conséquence que l'application combinée de ces deux articles violerait le principe *non bis in idem*, le principe de nécessité des délits et des peines ainsi que le principe de proportionnalité des peines garantis par l'article 8 de la Déclaration des droits de l'homme et du citoyen de 1789.

Au terme d'un raisonnement irréprochable selon nous, le Conseil juge que les dispositions prises isolément tout comme le principe du cumul sont conformes à la constitution (I) en apportant toutefois des réserves d'interprétation (II).

I. L'affirmation de principe de la conformité à la constitution du dispositif

A) Conformité à la constitution des dispositions prises isolément.

Le conseil constitutionnel juge que prises isolément, les dispositions de l'article 1729 C.G.I. ne sont pas contraires aux principes de nécessité des délits et des peines et de proportionnalité des peines (par. 10 et 11). Les sanctions financières visent à prévenir et à réprimer les insuffisances volontaires de déclaration de la base d'imposition ou des éléments servant à la liquidation de l'impôt et sont en lien direct avec les comportements prohibés. Le Conseil en déduit que les taux de majoration fixés par le législateur ne sont pas manifestement disproportionnés.

Il en va de même des dispositions prévues par l'article 1741 (par. 14) sous la réserve d'interprétation qui sera analysée ci-après.

B) Conformité à la constitution du principe du cumul des sanctions fiscales et pénales.

Le Conseil constitutionnel commence par affirmer l'objectif à valeur constitutionnel de la lutte contre la fraude fiscale qu'il fonde sur l'article 13 de la Déclaration de 1789 aux termes duquel, « Pour l'entretien de la force publique et pour les dépenses d'administration, une contribution commune est indispensable, elle doit être également répartie entre tous les citoyens, en raison de leurs facultés ». Les intérêts lésés sont des intérêts collectifs ainsi que les intérêts financiers de l'Etat. Il constate ensuite que l'article 1729 tout comme l'article 1741 dans ses dispositions contestées, « permettent d'assurer ensemble la protection des intérêts financiers de l'État ainsi que l'égalité devant l'impôt, en poursuivant des finalités communes, à la fois dissuasive et répressive ». Ce sont donc « le recouvrement de la nécessaire contribution publique et

l'objectif de lutte contre la fraude fiscale (qui) justifient l'engagement de procédures complémentaires dans les cas de fraudes les plus graves ». Ainsi, « aux contrôles à l'issue desquels l'administration fiscale applique des sanctions pécuniaires peuvent ainsi s'ajouter des poursuites pénales dans des conditions et selon des procédures organisées par la loi » (par. 20).

Il s'ensuit que « le principe de nécessité des délits et des peines ne saurait interdire au législateur de fixer des règles distinctes permettant l'engagement de procédures conduisant à l'application de plusieurs sanctions afin d'assurer une répression effective des infractions » (par. 21).

II. Les réserves d'interprétation

Elles concernent la mise en oeuvre de l'article 1741 C.G.I. Le respect du principe de nécessité des peines impose de considérer qu'une sanction pénale pour fraude fiscale ne peut être appliquée à un contribuable qui, pour un motif de fond, a été définitivement jugé non redevable de l'impôt (par. 13). Ensuite, l'article 1741 ne doit s'appliquer qu'aux cas les plus graves de dissimulation frauduleuse de sommes soumises à l'impôt. Cette gravité peut résulter du montant des droits fraudés, de la nature des agissements de la personne poursuivie ou des circonstances de leur intervention » (par. 21). Enfin, dans le prolongement d'une jurisprudence constante, le conseil constitutionnel décide que l'application combinée des dispositions de l'article 1729 et des dispositions contestées de l'article 1741 C.G.I. ne méconnaît pas le principe de proportionnalité des peines sous réserve que, si deux procédures sont engagées et conduisent à un cumul de sanctions, « le montant global des sanctions éventuellement prononcées ne dépasse pas le montant le plus élevé de l'une des sanctions encourues » (par. 24).

Portée.

La réserve d'interprétation énoncée au paragraphe 13 vise à neutraliser la jurisprudence constante de la Cour de cassation selon laquelle la décision du juge de l'impôt, qu'il s'agisse du juge administratif ou du juge civil, ne peut avoir, au pénal, autorité de la chose jugée[3]. Autrement dit, un contribuable peut être condamné pénalement pour soustraction frauduleuse alors même que le juge de l'impôt aurait déclaré qu'il n'était redevable d'aucune imposition. Cependant cette réserve d'interprétation ne concerne que l'hypothèse où le contribuable a été déchargé pour un motif de bien-fondé de toute imposition par un jugement définitif. Il s'ensuit tout d'abord que la seule décharge de la majoration au visa de l'article 1729 sera sans effet sur les poursuites pénales elles-mêmes. Les deux procédures pourront donc être diligentées. Ensuite, la décharge de l'impôt accordée pour un motif de procédure pourra autoriser des poursuites et une éventuelle condamnation pénale.

En d'autres termes, l'engagement de deux procédures demeure possible et le juge pénal conserve toute latitude pour apprécier les éléments constitutifs de la fraude fiscale, le juge de l'impôt étant tenu par ses constatations matérielles lorsqu'il a statué, mais n'est pas lié par sa qualification ou son interprétation des faits[4].

La réserve d'interprétation contenue dans le paragraphe 21, relative à la limitation de la mise en oeuvre de l'article 1741 C.G.I « aux cas les plus graves de dissimulation frauduleuses de sommes soumises à l'impôt », s'adresse uniquement aux autorités de poursuite et non au législateur. Pour autant, le respect du principe de nécessité des peines n'autorise la double condamnation au visa des articles 1729 et 1741 C.G.I. que pour les manquements les plus graves. Le Conseil constitutionnel prend soin de préciser que le critère de gravité doit s'apprécier en fonction « du montant des droits fraudés, de la nature des agissements, de la personne poursuivie ou des circonstances de leur intervention ». C'est donc aux juridictions pénales qu'il reviendra donc de définir la ligne de partage entre la fraude grave et celle qui ne l'est pas, dans le respect évident du principe de l'égalité des contribuables devant la loi.

Notes :

1 Décisions n° 2016-545 (M. Alec et W. et autre) et n° 2016-546 (M. Jérôme C.) QPC du 24 juin 2016. Voir dossier sur le site du conseil constitutionnel : http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2016/2016-546-qpc/decision-n-2016-546-qpc-du-24-juin-2016.147473.html

2 Notamment Cass. Crim. 25 juin 2014, n° 13-87.692.

3 Cass. crim., 13 juin 2012, n° 11-84.092

4 http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank/download/2016546QPC2016546qpc_ccc.pdf

ÉVOLUTION DES SERVICES DE PAIEMENT : ENJEUX ET RISQUES

DAN BENISTY

RESPONSABLE CONFORMITÉ AU SEIN D'UN ÉTABLISSEMENT DE PAIEMENT. EXPERT / CONFÉRENCIER EN MATIÈRE DE LUTTE CONTRE LE BLANCHIMENT D'ARGENT ET LE FINANCEMENT DU TERRORISME. PRÉSIDENT DU CHAPITRE FRANÇAIS DE L'ACAMS (ASSOCIATION OF CERTIFIED ANTI-MONEY LAUNDERING SPECIALISTS).

Les envois de fonds officiellement enregistrés vers les pays en développement se sont élevés à 431,6 milliards de dollars en 2015, soit une hausse de 0,4 % par rapport aux 430 milliards transférés en 2014. Si l'on comptabilise aussi les envois de fonds à destination des pays à revenu élevé, le montant total des transferts dans le monde a diminué de 1,7 %, passant de 592 milliards de dollars en 2014 à 581,6 milliards en 2015[1]. Cependant, on peut supposer une croissance en 2016 de ces transactions qui pourraient atteindre plus de 600 milliards d'ici 2017, portées par une conjoncture internationale plus favorable (depuis quelques années, les coûts associés aux envois de fonds sont en recul constant) mais également amplifiées par les récentes crises internationales ayant pour conséquence d'importants phénomènes de flux migratoires notamment en Europe.

L'industrie du transfert d'argent représente donc une manne colossale, mais sa conquête apparaît plus compliquée que prévue. Nombreux sont les aspirants à tenter leur chance en se lançant dans ce marché désormais dérégulé, en cassant les prix notamment sur des destinations spécifiques et/ou en se positionnant sur des services en ligne dits « plus rapides et moins chers » que le classique transfert d'argent en agence. On constate en effet que depuis la mise en place de la directive européenne des services de paiement (DSP), ces nouveaux entrants parviennent peu à peu à gagner du terrain sur les acteurs historiques et à tirer les tarifs du marché à la baisse, ce qui est profitable au client. Mais, si l'un des objectifs de la directive 2007/64/EC du 13 novembre 2007 (dite DSP1) du Parlement européen et du Conseil concernant les services de paiement dans le marché intérieur était d'ouvrir le marché des services de paiements jusqu'ici cloisonné et d'en faciliter l'accès à ces nouveaux acteurs, il apparaît in fine que ces nouveaux établissements de paiement doivent être à même de relever, d'une part, des enjeux opérationnels et commerciaux dans un environnement ultra concurrentiel, mais également, d'autre part, de satisfaire aux contraintes réglementaires de plus en plus drastiques.

Les directives sur les services de paiement ont-elles atteint leurs objectifs initiaux ? (I) Comment fonctionnent ces établissements de paiements et comment font-ils face à leur gestion du risque ? (II)

I. La directive sur les services de paiement

A. Enjeux et contraintes

La directive sur les services de paiement (DSP) a pour objectif de fixer un cadre juridique commun permettant l'instauration d'un véritable marché unique des services de paiement dans l'Espace économique européen (EEE). De ce fait, en principe, les mêmes règles sont applicables à tous les services de paiement en Europe et aux relations entre les prestataires fournissant ces services et leurs clients. En créant les « établissements de paiement », la directive aspire à ouvrir la concurrence sur le marché des paiements en brisant le monopole bancaire. Ainsi, depuis 2009, date de la transposition en droit français de cette directive, ce nouvel acteur est clairement défini au sein du Code monétaire et financier (CMF) dans les articles L522-1 à L522-5-1[2].

Les établissements de paiement représentent-ils une véritable menace pour les établissements de

crédit dans la mesure où leur création met fin au monopole des banques sur les services de paiement ?

Au même titre que les établissements de crédit, les établissements de paiement sont soumis à une surveillance des autorités de tutelle. En France, c'est l'Autorité de contrôle prudentiel et de résolution (ACPR) qui délivre un agrément, autorisant l'entreprise à fournir des services de paiement en tant qu'établissement de paiement.

Même si la loi habilite ces acteurs à fournir différents services tel que par exemple le change, en pratique c'est le transfert de fonds qui en est l'activité principale dont le modèle le plus répandu consiste à avoir recours, pour les établissements de paiement, à un réseau d'agents. Ces derniers, pour la plupart ayant une activité non bancaire, peuvent aujourd'hui offrir des services financiers (par exemple, il est possible d'effectuer un transfert d'argent chez un buraliste ou auprès de son commerce de proximité). C'est dans cette stratégie que se concentre le véritable challenge des établissements de paiement qui, d'une part, voient l'opportunité d'étendre leur maillage à un niveau européen, car lorsque l'agrément est obtenu dans un pays de l'Espace économique européen, un établissement de paiement peut étendre son activité dans un autre pays européen grâce à un passeport européen, et qui, d'autre part, doivent être en conformité avec les exigences règlementaires notamment celles en matières de lutte contre le financement de blanchiment d'argent et du financement du terrorisme.

Si la 3ème directive anti-blanchiment[3] du 26 octobre 2005 était très claire sur l'application de l'ensemble des nouvelles obligations de vigilance imposées à l'ensemble des assujettis et par conséquent aux établissements de paiement, il persistait un doute voire un manque sur la possibilité pour le pays hôte d'étendre l'application de son dispositif anti-blanchiment aux agents, sur la possibilité d'imposer l'organisation d'une structure centralisée (« central contact point ») dans le pays hôte dans le cas d'un réseau d'agents, et sur la possibilité que le superviseur d'origine puisse déléguer au superviseur hôte l'inspection des agents.

À ce titre, la 4ème directive anti-blanchiment et financement du terrorisme[4] du 20 mai 2015 a permis d'ôter tous ces doutes et notamment d'éclaircir les rôles des différentes autorités d'origine de l'agrément et d'accueil de l'activité de service de paiement. Ainsi, l'autorité compétente de l'État membre d'origine devrait être chargée de surveiller l'application, par l'entité assujettie, des politiques et procédures en vigueur au niveau du groupe en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme. Cela pourrait comprendre des inspections sur place effectuées dans des établissements installés dans un autre État membre. L'autorité compétente de l'État membre d'origine devrait coopérer étroitement avec l'autorité compétente de l'État membre d'accueil et devrait l'informer de toute question qui pourrait influencer l'évaluation qu'elles effectuent du respect par l'établissement des règles de l'État membre d'accueil en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme (Journal officiel de l'Union européenne).

Ainsi, si certains continuent à penser que les exigences prudentielles relatives à l'obtention de l'agrément d'établissement de paiement sont insuffisantes, les récents textes démontrent que les exigences règlementaires en matière de lutte contre le blanchiment de capitaux et financement de terrorisme (LCB-FT) sont les mêmes que pour un établissement de crédit et, par conséquent, qu'une insuffisance dans l'application du dispositif attendu entraînerait le même niveau de sanction.

B. Un encadrement règlementaire renforcé

L'émergence de nouvelles pratiques liées à un environnement technologique en constante évolution et la forte digitalisation des services financiers répondant à un besoin et un changement dans les habitudes des clients ont entraîné la nécessité de revoir, de nouveau, le cadre législatif des services de paiement en modifiant la première directive et en introduisant une version révisée, dite DSP2[5], le 25 novembre 2015. Cette directive confirme la volonté de faciliter l'arrivée de nouveaux acteurs sur le marché des services de paiement. Si récemment on a pu lire que de nombreuses Fintechs[6] et les GAFA[7] ont lancé des offres bancaires et souhaitent se positionner plus particulièrement sur le service de transferts de fonds internationaux, la DSP2 impose, à l'instar de tout prestataire de services de paiement, que ces nouveaux acteurs devront répondre aux obligations de régulation et de supervision en matière de services de paiement et de LCB-FT. Cette directive qui a pour but de renforcer la sécurité des services de paiement et la protection des consommateurs est l'exemple même du défi qui se joue entre l'innovation et la sécurité. Dans le contexte actuel où les gouvernements ont pour volonté de renforcer et maîtriser le risque de blanchiment d'argent et plus particulièrement celui du financement du terrorisme, nul doute sur un futur et constant renforcement règlementaire pour encadrer l'innovation digitale qui bouscule le monde bancaire et financier.

Comment fonctionnent les établissements de paiement et comment

font-ils face à leur gestion du risque ?

II. Établissements de paiement : approche par les risques et lutte contre le blanchiment de capitaux et financement du terrorisme

Les établissements de paiements, comme tout assujetti, ont l'obligation de mise en oeuvre d'une approche par les risques pour la prévention du blanchiment de capitaux et du financement du terrorisme. En comparaison avec les établissements de crédit offrant une multitude de services et produits tentaculaires et complexes, le risque lié au service de paiement pourrait paraître de prime abord simple, mais il n'en est rien. En effet, si la plupart des établissements de paiement n'offre qu'un seul type de service, le transfert de fonds, les caractéristiques de ce dernier lui confèrent une certaine typologie de risque qui nécessite une gestion assez pointue et sophistiquée.

A. Le risque produit / service

L'éventail des produits offerts par les prestataires de service de paiement (PSP) est assez réduit, consistant à offrir principalement aux clients un service de fonds. S'il est vrai que ces opérations sont majoritairement des transferts d'espèces entre personnes physiques, on voit apparaître depuis quelques années une diversification de ce service et notamment avec l'émergence de la digitalisation des services financiers. Outre, les stratégies commerciales de ces établissements à proposer à leurs clients différentes façons de faire un transfert de fonds, ces derniers ont été largement « invités » à intégrer la dématérialisation de la monnaie, politique encouragée par les différentes récentes décisions des gouvernements.

Comment alors allier l'innovation digitale et la maîtrise du risque ? Dans plusieurs pays européens et notamment en France, il existe une véritable volonté des autorités, dans le cadre de la lutte contre la fraude, le blanchiment d'argent et le financement du terrorisme, de réduire et/ou limiter les opérations en liquide permettant ainsi une meilleure traçabilité des transferts d'argent importants. Par conséquent, les établissements de paiements proposent d'autres alternatives que le paiement en cash pour les transferts de fonds et le client peut aujourd'hui effectuer : une opération directement en ligne avec un paiement en carte de crédit (avec une adaptation des seuils et des vigilances d'identification du client à distance) ; une opération à partir d'un compte bancaire (à travers les partenariats entre établissements de paiements et établissements de crédits). Ces opérations présentent un risque moins élevé qu'un transfert « de cash à cash », puisque cela implique qu'un établissement de crédit, également soumis à l'ensemble des obligations en matière de LCB-FT, a également appliqué ses règles de vigilances.

Il convient de relever aussi les opérations de transfert d'argent vers un téléphone portable / portefeuille électronique. Cette solution de paiement par mobile (ou m-paiement) revêt une effervescence particulière notamment privilégiée sur le continent africain, en Asie ou en Amérique Latine. On comprend aisément les enjeux économiques de ce marché compte tenu du nombre de porteurs de téléphones qui ne cesse de croître et l'émergence des nouveaux moyens de paiement. Ce n'est donc pas une surprise si on a récemment vu de grands acteurs télécom devenir des acteurs bancaires, ces services étant à la croisée de ces deux industries.

B. Le risque client

Dans le cadre des activités des établissements de paiement, le service de transfert d'argent est principalement utilisé par un client - personne physique - même si depuis quelques temps déjà, ce service est également proposé et utilisé par des clients - personne morale – qui sont souvent des PME ou TPE[8]. Rappelons qu'un transfert d'argent s'effectuant en moins de cinq minutes auprès d'un agent du réseau d'un établissement de paiement, est un service de paiement non adossé à un compte. On imagine alors aisément la difficulté des obligations relatives à la connaissance du client. On fait bien ici la distinction entre l'identification du client, consistant à prendre toutes les données relatives à une pièce d'identité (étape obligatoire et tout transfert de fonds) et la connaissance du client telle que définie et attendue par les autorités de tutelle. Dès 2012, l'ACPR publiait des lignes directrices relatives à la relation d'affaires et au client occasionnel en précisant que « la mauvaise compréhension de la distinction entre un client habituel ou occasionnel peut entraîner des mesures de vigilance inadaptées et donc un risque de non détection d'anomalies dans les opérations avec la clientèle. Cela affectant in fine la transmission éventuelle de déclarations à Tracfin. »[9].

Cette obligation de vigilance de la clientèle, pilier du dispositif LCB-FT, de l'approche par les risques et intrinsèquement liée aux obligations de surveillance et de déclaration, a récemment fait l'objet de précisions dans les lignes directrices conjointes de l'Autorité de contrôle prudentiel et de résolution et de Tracfin sur les obligations de déclaration et d'information à Tracfin[10].

Ainsi, afin de répondre aux obligations règlementaires mais également afin de maîtriser le risque client, les établissements de paiements se doivent de

définir les caractéristiques de leur clientèle et d'en évaluer les risques pour appliquer les différents niveaux de vigilance. Malgré les efforts des PSP dans ce domaine, en pratique cela reste un véritable challenge compte tenu des attributs du service proposé.

Même si des études ont montré qu'un très fort pourcentage de la clientèle des établissements de paiement est bancarisée (mais préférant, pour plusieurs raisons utiliser le service d'un PSP pour leur transfert d'argent), il n'en demeure pas moins une difficulté de les faire évoluer vers des questions de plus en plus intrusives sur l'origine et la finalité de leurs opérations de transfert de fonds allant parfois jusqu'à devoir demander des justificatifs afin de lever tout doute sur un potentiel comportement atypique.

C. Le risque pays

S'il existe dans la classification des risques des établissements de paiement une notion qui concentre plus particulièrement leur surveillance, c'est bien celui du risque pays. En effet, la plupart des grands acteurs de l'industrie du transfert d'argent offre un service couvrant plus de 250 pays et territoires dans le monde. Leur présence dans tous ces pays, où les partenariats leur permettent d'offrir leur service, implique une vigilance et un dispositif tout particulier devant ainsi être adaptés aux risques des différentes zones géographiques couvertes. Si les listes publiées par le Groupe d'action financière (GAFI) ou par d'autres instances nationales et internationales intervenant en matière de LCB-FT sont intégrées dans l'appréhension de ce risque, la pratique démontre qu'il est nécessaire de ne pas se limiter à cette seule source. L'expertise interne des établissements de paiements notamment en se basant sur les analyses transactionnelles et les comportements atypiques, permet de mettre en exergue des notions de risques pays complémentaires aux listes officielles. Par exemple, certains pays, qui a première vue n'apparaissent pas comme pays à risque, peuvent être utilisés comme "zone de rebond", les flux pouvant y transiter mais avec une destination finale toute autre. Ainsi, ce risque se doit être appréhendé sous de multiples angles intégrant différents scenarios potentiels de blanchiment d'argent et de financement du terrorisme. C'est la raison pour laquelle, les établissements de paiements doivent régulièrement mettre à jour leur veille géopolitique et développer une forte coopération et un partage d'information avec les Cellules de renseignement financier (CRF) et les autorités policières nationales et internationales. Ce décloisonnement nécessaire entre secteur public et secteur privé est l'une des clés de la réussite d'un risque pays mieux maîtrisé permettant de ce fait un profilage des comportements atypiques plus affiné.

Conclusion

On l'aura compris, l'ère de la digitalisation des produits financiers, et plus particulièrement des services de paiements, est en marche et son enjeu est crucial tant pour les acteurs bancaires historiques que pour les nouveaux entrants dans ce marché tant convoité. Cette nouvelle dynamique oblige tous ces acteurs à revoir leur positionnement et stratégie commerciale mais représente également un véritable défi prudentiel. Les établissements de paiement offrant un service de transfert d'argent se retrouvent face une opportunité d'étendre et de diversifier leur activité alors qu'au même moment ils doivent redoubler de vigilance avec l'accélération du risque de blanchiment de capitaux et de financement du terrorisme. Aussi, la Banque mondiale a récemment décrit le rôle important des prestataires de services de transfert international de fonds dans la lutte contre la pauvreté et la difficulté à concilier le soutien aux transferts d'argent des migrants et la lutte contre les flux financiers illicites. Cette question importante fait d'ailleurs l'objet de lignes directrices produites par le Groupe d'action financière (GAFI)[11]. Alors, comment concilier l'ouverture à la concurrence du marché des services de paiements et toutes les opportunités qui y sont rattachées avec une gestion maîtrisé des risques associés à ce produit ? Il s'agit en substance de savoir parfaitement évaluer ces risques, exercice complexe, qui demande comme précédemment évoqué une forte et étroite coopération entre les secteurs publics et privés afin de pouvoir mettre en oeuvre des mesures qui soient proportionnées aux risques que posent ces menaces grandissantes.

Notes :

1 http://www.banquemondiale.org/fr/topic/migrationremittancesdiasporaissues/overview

2 http://www.legifrance.gouvfr/affichCode.do?idArticle=LEGIARTI000020869626&idSectionTA=LEGISCTA000020869628&cidTexte=LEGITEXT000006072026&dateTexte=20110624

3 Directive 2005/60/CE du 26 octobre 2005.

4 Directive (UE) 2015/849 du Parlement européen et du Conseil du 20 mai 2015.

5 Directive 2015/2366/UE du Parlement européen et du Conseil du 25 novembre 2015.

6 FinTechs (Financial Technologies ») : start-ups dans le secteur des services financiers.

7 GAFA : Google, Apple, Facebook, Amazon.

8 PME/ TPE : Petites et Moyennes Entreprises / Très Petites Entreprises.

9 http://www.acpr.banque-france.fr/fileadmin/user_upload/acp/Controle_prudentiel/Lutte_anti-blanchiment/201204-LD-de-l-ACP-relatives-a-la-relation-d-affaires-et-au-client-occasionnel.pdf

10 http://acpr.banque-france.fr/fileadmin/user_upload/acp/publications/registre-officiel/201512-Lignes-directrices-ACPR-Tracfin-obligations-declaration.pdf

11 http://www.fatf-gafi.org/publications/fatfrecommendations/documents/rba-money-or-value-transfer.html

REGARD SUR LES DISPOSITIFS D'AIDE ET D'INDEMNISATION DES VICTIMES D'ATTENTATS

CLAUDE LIENHARD

PROFESSEUR DES UNIVERSITÉS, AVOCAT SPÉCIALISTE EN RÉPARATION DU DOMMAGE CORPOREL, PRÉSIDENT DE L'ASSOCIATION PARIS AIDE AUX VICTIMES, PRÉSIDENT FONDATEUR DE L'INAVEM.

Toutes les victimes, quelle que soit la cause de leur malheur, ont droit à la considération et à la solidarité. Le droit des victimes d'infractions pénales est aujourd'hui une réalité et les droits des victimes doivent s'inscrire et se décliner effectivement.

Dans ce qui constitue le paysage et la sociologie des victimes, les victimes d'attentats occupent une place à part comme les événements générateurs qui sont des actes de guerre contre la Nation.

La création d'un secrétariat dédié à l'aide aux victimes directement rattaché auprès du Premier ministre et dont le champ de compétence est en grande partie dédié aux victimes d'attentats vient en tant que de besoin confirmer l'approche spécifique de la situation des hommes, des femmes et des enfants dont les vies se trouvent brisées et bouleversées car emportées et impliquées dans des événements dramatiques qui visent l'État français et la communauté démocratique à laquelle nous appartenons.

La vague d'attentats qui a directement touché notre pays amène à rappeler que la France dispose d'un dispositif d'aides et d'indemnisation des victimes relativement ancien, *a priori* opérationnel bien que toujours perfectible et qui doit faire preuve de capacités d'adaptation et de souplesse en fonction de la gravité et la réitération d'actes de terrorisme.

L'ampleur des attentats successifs, ceux de janvier et novembre 2015 notamment, a amené les différents acteurs à se mobiliser totalement dans l'urgence puis nécessairement dans la durée.

Comme le rappelle l'instruction interministérielle du 12 novembre 2015 remplacée depuis par une nouvelle instruction du 13 avril 2016 relative à la prise en charge des victimes d'actes terroristes, trois impératifs s'imposent :

- l'impératif d'efficacité d'abord,
- l'impératif de cohérence ensuite,
- l'impératif d'humanité enfin.

I. Le dispositif de gestion de crise

Le dispositif de gestion de crise est désormais à vocation interministérielle et s'articule autour de la cellule interministérielle d'aide aux victimes (CIAV) qui gère la période de crise.

Ce dispositif gère l'urgence, la période post-crise étant gérée par le comité interministériel de suivi des victimes (CISV).

II. Le dispositif d'indemnisation

L'indemnisation est gérée par le Fond de Garantie des victimes des actes de Terrorisme et d'autres Infractions (FGTI).

Par application du principe de réparation intégrale qui s'impose ici comme ailleurs et encore plus comme une évidence, le FGTI doit indemniser tous les préjudices de toutes natures (physique, psychique, moral, économique...) découlant des dommages physiques et/ou psychiques consécutifs à l'acte de terrorisme, dans les conditions de droit commun. Chaque offre d'indemnisation est nécessairement individualisée. Même si une cohérence doit exister au regard du caractère collectif, pour éviter, à situation égale, des discriminations de fait.

Les principes d'indemnisation par le Fonds de Garantie sont arrêtés par son Conseil d'administration

et ont donc, *in fine* un aspect fort lié à une politique indemnitaire qui ne peut être laissée à l'appréciation des seuls techniciens du dommage corporel.

En plus des différents postes de préjudices de droit commun découlant de la nomenclature Dinthilac dont on rappellera le caractère souple et évolutif, le FGTI répare l'atteinte spécifique résultant de l'acte de terrorisme lui-même, via le PESVT (Préjudice psychologique Exceptionnel Spécifique des Victimes du Terrorisme).

Ce préjudice répare l'atteinte spécifique résultant de l'acte de terrorisme lui-même, en considération du fait qu'il atteint aveuglément, sur le sol français, des individus qui, de ce fait, se retrouvent victimes collatérales d'actes dirigés contre l'État français.

Ce préjudice exceptionnel remplace depuis 2014 le préjudice psychologique spécifique des victimes de terrorisme (PSVT) qui existait jusqu'alors pour les victimes de terrorisme.

Le PESVT s'ajoute à juste titre aux postes de préjudices auxquels la victime peut prétendre, dans le cadre de sa réparation intégrale. L'ancien PSVT était réparé par une majoration de 40 % des sommes allouées au titre du Déficit Fonctionnel Permanent (DFP), avec un minimum de 2 800 euros alloués, y compris en l'absence de DFP. Le nouveau PESVT est réparé de façon forfaitaire et bénéficie également aux victimes par ricochet.

Le PESVT a amené à effectuer un classement des victimes en 3 catégories :

- victimes du cercle 1 : victimes directes, recensées sur la liste officielle des victimes.

- victimes du cercle 2 : victimes présentes sur les lieux, mais ne subissant pas de répercussions immédiates. Elles n'ont pas conscience qu'il s'agit d'un attentat mais développent ultérieurement un traumatisme « **Post-Traumatic Stress** Disorder » (PTSD). Pour ces victimes, il existe un renversement de la charge de la preuve, c'est à elles de démontrer le lien de causalité entre leur préjudice et l'acte terroriste.

- victimes du cercle 3 : proches des victimes décédées.

En matière de terrorisme, la procédure est à vocation transactionnelle.

Le FGTI verse, en principe d'initiative, une première provision au plus tard un mois après avoir reçu la demande de la victime pour faire face aux premiers frais.

Le FGTI prend attache directement avec les victimes et/ou familles des victimes décédées figurant sur la liste unique établie par le parquet de Paris, afin de leur proposer une provision. Les victimes peuvent aussi en solliciter.

Le FGTI présente à la victime par écrit une offre d'indemnisation définitive, au plus tard trois mois après avoir reçu de la victime les justificatifs des préjudices et ceci après consolidation.

Si la victime accepte l'offre, elle dispose d'un délai de 15 jours pour se rétracter. Passé ce délai, le Fonds de Garantie verse le montant de l'indemnisation.

Si la victime n'accepte pas l'offre d'indemnisation, la voie judiciaire s'impose. A l'heure actuelle, certaines victimes ont déjà fait ce choix.

III. Le statut de victime de guerre

Les victimes ont le statut de victime civile de guerre et bénéficient ainsi du régime du Code des pensions militaires d'invalidité et des victimes de la guerre applicables aux victimes civiles de guerre (loi du 23 janvier 1990).

Elles ont droit à réparation au titre du Code des Pensions Militaires d'Invalidité et des Victimes de Guerre (CPMIVG).

Ce droit s'applique aux victimes de toute nationalité - et/ou à leurs familles - lorsque l'acte de terrorisme est commis en France, et aux victimes françaises, lorsqu'il survient à l'étranger.

Plusieurs distinctions sont à opérer *ratione personae* :

1- Les blessés graves, blessés légers et personnes impliquées (recensées sur la liste unique des victimes établie par le Parquet) peuvent prétendre à une pension militaire d'invalidité (PMI).

2- Les ascendants (père et mère) des victimes décédées peuvent déposer une demande de pension, sous réserve de remplir les conditions d'ouverture des droits à pension d'ascendant (âge et ressources notamment).

3- Les conjoints survivants, les titulaires d'un PACS, et les orphelins de moins de 21 ans ont quant à eux un droit à pension de réversion d'invalidité.

Le dispositif est cependant subsidiaire**.** Cette pension de victime civile de guerre n'est en réalité versée que si son montant est supérieur au montant des autres indemnisations ce qui est assez rare. Dans les autres cas, la pension est concédée, mais son versement est suspendu.

Il importe néanmoins que la victime fasse valoir ce droit, car il permettra la prise en compte ultérieure, et à tout moment, d'éventuelles aggravations de son état de santé. En effet, le point de départ

du droit à pension est fixé à la date de la demande et non pas à la date des faits.

C'est le ministère de la Défense, précisément la Sous-direction des pensions qui s'adresse à chaque victime blessée ou ayants cause pour les familles des victimes décédées, pour les informer sur leurs droits en matière de pension militaire d'invalidité.

IV. L'Office National des Anciens Combattants et Victimes de guerre (ONAC)

En qualité de victimes civiles de guerre, les victimes d'actes de terrorisme ont la qualité de ressortissantes de l'ONAC.

L'Office National des Anciens Combattants et Victimes de guerre (ONAC) est un établissement public administratif à caractère national sous tutelle du ministère de la Défense, doté de la personnalité civile et de l'autonomie financière.

En étroite collaboration avec les différents intervenants, l'ONAC participe à l'information des victimes et, dans l'urgence, peut mettre en oeuvre des aides financières immédiatement mobilisables, dans l'attente des premières provisions du Fonds de Garantie.

Dans la durée et cela est essentiel, l'ONAC diligente ou accompagne les procédures d'adoption par la Nation, accueille les demandes de pension civile de guerre et les relaie auprès des directions interdépartementales, organise l'aide à la réinsertion professionnelle et une assistance administrative pour seconder les démarches.

À long terme, l'ONAC peut accorder des aides individuelles (dès lors qu'il est en possession du procès verbal de transaction du FGTI) : prêts sociaux, formations de reconversion professionnelle, secours financiers...

V. Le statut de pupille de la Nation

Ce statut offre aux victimes une protection supplémentaire et particulière, en renfort de celle exercée par leurs familles.

Il faut rappeler néanmoins que les représentants légaux à savoir le plus souvent le ou les parent (s) survivant (s) restent pleinement titulaires de l'autorité parentale.

Cette mission particulière d'assistance est également confiée à l'ONAC.

Les avantages sont divers : subventions d'entretien, d'éducation, d'études et de vacances (dans le cas où les ressources familiales sont insuffisantes), aide au premier emploi, dispense des obligations du service national, exonération des droits de scolarité dans les universités...

Vont bénéficier de ce statut les victimes - directes ou enfants de victimes décédées, enfants de victimes blessées ou enfants de victimes impliquées - de moins de 21 ans, de nationalité française.

La demande doit être déposée via une requête au tribunal de grande instance (TGI) du ressort du domicile de la victim ON RETIRE ?e, effectuée par le représentant légal du mineur ou par la victime elle même lorsqu'elle est majeure (18 ans); l'adoption sera alors prononcée par le TGI.

VI. Le droit aux soins médicaux gratuits

Les victimes (proches endeuillés, victimes blessées, victimes impliquées) sont destinataire une attestation spécifique afin de leur permettre de faire valoir leurs droits auprès des professionnels et établissements de santé.

Un décret du 2 janvier 2016 relatif à la prise en charge des victimes d'actes de terrorisme par les organismes d'assurance maladie organise la gratuité des soins, en améliorant et en simplifiant les modalités de prise en charge de tels frais.

Deux catégories de victimes peuvent bénéficier de ces dispositions :

- les personnes blessées, c'est-à-dire les « personnes présentes sur les lieux de l'acte de terrorisme et ayant subi un dommage physique ou psychique immédiat directement lié à cet acte. »

- les personnes « impliquées », c'est-à-dire les « personnes présentes sur les lieux de l'acte de terrorisme qui, ultérieurement à cet acte, présentent un dommage physique ou psychique qui lui est directement lié. »

Dans ce cadre, la Caisse nationale de l'assurance maladie des travailleurs salariés (CNAMTS) est chargée de « coordonner l'action des organismes d'assurance maladie ». Elle centralise les questions des assurés, avant leur transmission, s'il y a lieu, à leur régime d'affiliation.

VII. La mention « Victime du terrorisme » sur les actes de décès

La loi n° 2012-1432 du 21 décembre 2012 relative à la sécurité et à la lutte contre le terrorisme prévoit la possibilité que soit portée une mention « Victime du terrorisme » sur les actes de décès.

Ainsi, elle dispose, au VI de son article 12, que :

« Le ministre de la Justice peut décider, avec l'accord des ayants droit, que la mention « Victime du terrorisme » est portée sur l'acte de décès de toute personne mentionnée au I.

Lorsque, pour un motif quelconque, la mention « Victime du terrorisme » n'a pas pu être inscrite

sur l'acte de décès au moment de la rédaction de celui-ci, elle est ajoutée ultérieurement dés que les éléments nécessaires de justification le permettent.

Les enfants des personnes dont l'acte de décès porte la mention « Victime du terrorisme » ont vocation à la qualité de pupille de la Nation. »

La décision est prise par arrêté du ministre de la Justice, avec l'accord des ayants droit. Cette mention peut être portée soit lors de la rédaction de l'acte de décès, soit ultérieurement si les justifications sont apportées.

VIII. L'exonération des droits de succession

Les successions des personnes décédées du fait d'un acte de terrorisme sont exonérées de l'impôt de mutation par décès (article 796 du Code général des impôts).

IX. Les acteurs associatifs au service des victimes d'attentat

- **L'association Paris Aide aux Victimes (PAV)**

www.pav75.fr

Paris Aide aux Victimes a été désigné par le ministère de la Justice pour organiser l'espace informatif dédié aux victimes des attentats du 13 Novembre 2015.

Des permanences de soutien psychologique et d'information sur les droits sont ouvertes :

Adresse : 17 boulevard Morland 75004 Paris Téléphone : 01 40 28 70 00

Contact : espaceinformatif.pav@gmail.com

- **Institut national d'aide aux victimes et de médiation (INAVEM)**

www.inavem.org

L'INAVEM est la fédération française regroupant 130 associations généralistes d'aide aux victimes. Créée en 1986, l'INAVEM a pour mission d'animer, de coordonner et de promouvoir le Réseau INAVEM, ainsi que d'engager des partenariats, des conventions pour faciliter l'accès aux personnes victimes vers les associations.

La Fédération INAVEM et ses associations adhérentes sont présentes aux côtés des victimes.

L'INAVEM a mis en contact plusieurs centaines de victimes avec leur association INAVEM de proximité. Les associations sont saisies afin que toutes les victimes bénéficient d'un interlocuteur identifié, qui les soutient dans tous les domaines du droit et du psychosocial.

Chaque victime, chaque famille de victimes, où qu'elle se trouve en France, peut connaître le nom et les coordonnées du référent unique de l'Association locale du Réseau INAVEM, conventionnée par le ministère de la Justice.

- **L'association « 13 novembre : Fraternité et Vérité »**

13onze15.org

L'association « 13 novembre : Fraternité et Vérité » a été créée le 9 janvier 2016 par des victimes et proches de victimes des attentats survenus le 13 novembre dernier à Paris et Saint-Denis. L'ensemble des sites touchés (Bataclan, terrasses, stade de France etc.) et des situations (familles endeuillées, familles de blessés, rescapés etc.) est représenté.

- **L'association Life For Paris**

www.lifeforparis.org/

La démarche de Life For Paris s'appuie sur l'idée de résilience à savoir l'aptitude d'un individu à se reconstruire et à vivre de manière satisfaisante en dépit de circonstances traumatiques.

L'association a pour ambition de favoriser l'entraide entre toutes les victimes physiques et psychiques, les membres de familles de personnes décédées, les aidants et les professionnels qui sont intervenus le soir même sur l'ensemble des lieux impliqués concernés, afin que chacun puisse trouver la force de s'en sortir et prendre un nouvel élan dans la vie.

- **La Fédération nationale des victimes d'attentats et d'accidents (FENVAC)**

www.fenvac.com

La Fédération nationale des victimes d'attentats et d'accidents collectifs (FENVAC - SOS Catastrophes & Terrorisme) a été créée en 1994 par 8 associations de victimes d'accidents survenus entre 1982 et 1993 (cf. l'historique) sous la forme d'une association type loi 1901. En 2011, son intervention est élargie au terrorisme.

X. Les avocats spécialisés au service des victimes

www.anadovi.com

La défense des victimes nécessite des compétences précises tant en droit de la responsabilité que dans la réparation du dommage corporel. L'ANADAVI regroupe des Avocats spécialisés et compétents dans ces deux domaines, qui s'engagent à ne défendre que les Victimes.

L'OFFICE ANTI-FRAUDE DE CATALOGNE, UNE APPROCHE DIFFÉRENTE DE LA LUTTE CONTRE LA CORRUPTION

BRUNO GONZÁLEZ VALDELIÈVRE

DIRECTEUR D'ANALYSE À L'OFFICE ANTI-FRAUDE DE CATALOGNE (OAC)

L'Office Anti-fraude de la Catalogne (OAC) est une institution catalane relativement nouvelle et aux caractéristiques singulières, dont la conception et l'activité offrent une approche spécifique de la lutte contre la corruption dans le secteur public.

Singulière, car il n'existe aucun autre organisme semblable en Espagne, quoique certaines institutions de lutte ou de prévention de la corruption d'autres États européens gardent quelques similitudes avec l'OAC. Différente, dans sa conception et dans son activité, car sa mission principale est la prévention et l'enquête de ce que nous pourrions désigner comme des faits de corruption non criminelle dans le secteur public catalan.

Nous allons aborder tout d'abord brièvement le contexte et le cadre juridique, constitutionnel et légal, dans lequel a été créé l'OAC par la loi du Parlement de la Catalogne 14/2008, du 5 novembre 2008. Puis, afin de bien comprendre les fonctions et les possibilités d'action de l'OAC, nous nous pencherons sur le cadre conceptuel dans lequel la situer, qui s'articule autour de cette idée de corruption non criminelle. Nous commenterons ensuite les principaux aspects organiques et opérationnels de l'OAC. Une brève référence à l'un des cas concrets dans lequel est intervenu l'OAC, largement commenté dans les médias, nous permettra d'illustrer l'interaction entre l'OAC et le Parquet et de mettre en exergue leur complémentarité dans la lutte contre la corruption, ce qui débouchera sur une réflexion finale concernant l'utilité et l'importance de l'OAC dans ce domaine.

I. Genèse et parcours de l'OAC. Cadre juridique

A. Un peu d'histoire : les gouvernements tripartites de la Catalogne et le "débat du 3%"

Nous trouvons les premières références à ce qui, bien plus tard, finira par devenir l'OAC, dans le Pacte du Tinell, l'accord politique conclu entre 3 partis politiques de gauche, le PSC (socialistes), ERC (nationalistes républicains de gauche) et ICV (éco-socialistes), à la suite des élections catalanes du 16 novembre 2003, qui donna lieu au premier gouvernement tripartite catalan, présidé par M. Pasqual Maragall. Le Pacte du Tinell prévoit déjà l'idée de créer, au sein de la Cour des Comptes catalane (Sindicatura de Comptes), un Office « destiné à préserver la transparence et le fonctionnement éthique du système public, spécialisé dans la prévention des pratiques irrégulières dans les concessions et passations de marchés publics de fournitures et de services. »

À l'origine de ce projet se trouvait la suspicion, assez généralisée dans les trois partis susmentionnés (et souvent insinuée dans les médias), de l'existence d'une corruption plus ou moins habituelle dans les gouvernements successifs du CiU (nationalistes conservateurs), le parti au pouvoir en Catalogne de façon ininterrompue depuis la transition démocratique en Espagne

de 1978.

L'expression la plus connue de cette suspicion eut lieu lors du débat au Parlement catalan du 24 février 2005 suite à de graves effondrements survenus à Barcelone lors des travaux de construction de la nouvelle ligne de métro n°9. Au cours de ce débat, le gouvernement tripartite attribua la responsabilité de ces faits au gouvernement précédent de CiU, responsable de la passation des marchés publics de ces travaux, et le Président M. Maragall adressa au chef de file de CiU, M. Mas cette interjection devenue historique : « Vous avez, messieurs, un problème, et ce problème a un nom : il s'appelle 3%...», faisant ainsi allusion au versement supposé de pots-de-vin.

Après ce célèbre débat (connu dans les médias comme le "débat du 3%"), le Parlement catalan commença les travaux législatifs pour la création de l'OAC en septembre 2005. Cependant, la fin de la législature, par la convocation d'élections anticipées en septembre 2006, mit fin à ces travaux.

Le deuxième gouvernement tripartite catalan , présidé par M. José Montilla, et le nouveau Parlement catalan, issus des élections législatives du 1er novembre 2006, reprirent à zéro les travaux législatifs interrompus, qui aboutirent finalement à l'adoption de la Loi 14/2008 du 5 novembre 2008 sur l'Office Antifraude de la Catalogne (LOAC).

Une fois la loi publiée, l'OAC commença à prendre corps avec la désignation de son premier Directeur, M. David Martínez Madero, membre du parquet anticorruption, par la résolution 471/VIII du 20/05/2009 du Parlement de la Catalogne.

L'une des toutes premières tâches menées par l'équipe originale de l'OAC fut l'élaboration de sa réglementation intérieure, les normes d'action et de régime intérieur de l'OAC (NARI), prévues par la 1ère disposition additionnelle de la LOAC. Ces normes furent approuvées par la Commission des questions institutionnelles du Parlement le 25 novembre 2009.

Au cours de l'année 2010, l'OAC recruta la majeure partie de ses effectifs, ce qui lui permit de devenir pleinement opérationnelle à partir de septembre 2010.

Malheureusement, le décès inattendu du Directeur, M. Martínez Madero, d'une crise cardiaque le 21 janvier 2011 lors d'une escale à Milan au retour d'une réunion d'experts de l'IAACA (International Association of Anti-Corruption Authorities) à Singapour, paralysa l'OAC pendant 6 mois, jusqu'en juillet 2011, quand fut désigné directeur M. Daniel de Alfonso Laso, magistrat de l'Audience de Barcelone, par la résolution 225/IX, du 29 juillet 2011.

L'ombre, sinon d'un destin funeste tout au moins d'une existence difficile, semble planer sur l'OAC. En effet, très récemment, le 29/06/2016, le Parlement a approuvé la résolution 184/XI de révocation de la nomination de M. de Alfonso pour la raison prévue à l'article 11.1 g) de la LOAC, à savoir négligence notoire et grave dans l'accomplissement des obligations et des devoirs inhérents au poste de directeur de l'OAC. À l'origine de cette révocation se trouve la diffusion dans les médias des enregistrements de deux conversations du 2014 entre le directeur de l'OAC, M. de Alfonso, et le ministre de l'Intérieur espagnol qui, apparemment, mettent en évidence un biais politique anticatalaniste dans le management du résultat d'enquêtes de l'OAC, ainsi que la planification de la communication aux médias d'informations non avérées sur certaines personnalités politiques nationalistes et indépendantistes catalanes.

Malgré ces faits très regrettables, l'avenir de l'OAC comme institution ne semble pas sérieusement compromis, ce qui est, en fin de comptes, une bonne nouvelle.

B. Situation de l'OAC dans le cadre constitutionnel espagnol et catalan ; éléments principaux de sa configuration

La configuration légale de l'OAC est difficile à comprendre si l'on ne tient pas compte de l'organisation territoriale de l'Espagne établie dans la Constitution espagnole de 1978. Il s'agit d'un modèle tendanciellement fédéral qui a donné lieu à la création de 17 Communautés autonomes (dont la Catalogne) dotées de pouvoirs législatifs plus ou moins larges dans diverses matières, exercés par leurs parlements ou assemblées législatives. Les articles 148 et 149 de la Constitution établissent, par un système de double liste, les différentes matières dans lesquelles les Communautés autonomes peuvent assumer des compétences législatives (ce qui doit être déclaré dans le Statut d'autonomie de la Communauté, norme de rang quasi-constitutionnel qui est la clé de voûte de l'ordre juridique propre de la Communauté), les matières dans lesquelles

l'État central a une compétence législative exclusive, et celles où la compétence législative est partagée, l'État central établissant les bases du cadre légal que les Communautés autonomes peuvent développer.

Dans ce modèle, l'État central a la compétence législative exclusive en matière d'administration de justice (article 149.5 de la Constitution), de droit pénal et de droit de la procédure judiciaire, notamment pénale (article 149.6), et de sécurité intérieure (article 149.29), bien que la création de corps de police propres des Communautés autonomes soit admise par la Constitution. Par contre, la première des compétences législatives exclusives des Communautés autonomes (article 148.1) et la principale est la configuration et la réglementation de leur propre organisation institutionnelle.

Dans ce cadre constitutionnel, le Parlement de la Catalogne n'était évidemment pas compétent pour créer une institution rattachée au pouvoir judiciaire ou disposant de pouvoirs propres au pouvoir judiciaire ; ni non plus d'attribuer à l'OAC des pouvoirs (notamment d'enquête) propres à la Police judiciaire ; ni d'altérer les règles de la procédure judiciaire pénale ou administrative.

En conséquence, l'OAC est configurée légalement comme un organisme de contrôle externe du secteur public catalan, dont les caractéristiques principales sont les suivantes :

- l'OAC est une entité de droit public dotée de la personnalité juridique et de la pleine capacité pour agir (article 1.1 de la LOAC) ;

- il est rattaché au Parlement catalan, seule institution à laquelle l'OAC doit rendre compte, via une Commission parlementaire spécifique et, principalement, au moyen d'un rapport annuel d'activité, afin de garantir l'indépendance de l'institution vis-à-vis des administrations qui feront l'objet de ses enquêtes (articles 1.1, 12 et 22 de la LOAC) ;

- son Directeur est nommé par le Parlement, avec un quorum renforcé (trois cinquièmes parties en premier tour ; majorité absolue en deuxième tour), pour une période unique de 9 ans, ce qui le met à l'abri des aléas de la politique et des modifications de majorité parlementaire (articles 8 et 9 de la LOAC) ; il est également protégé légalement de toute révocation, celle-ci pouvant intervenir que pour les motifs concrets spécifiés dans l'article 11.1 de la LOAC ;

- l'OAC jouit de l'autonomie budgétaire, son budget étant consolidé avec le budget du Parlement de la Catalogne et ceux des autres institutions qui y sont rattachées.

Le préambule de la LOAC signale expressément que « La création de l'Office anti-fraude répond pour la première fois à ce que propose l'article 6 de la Convention des Nations Unies contre la corruption, approuvée à New York le 31 octobre 2003, qui garantit l'existence d'un organe spécialisé et indépendant chargé de prévenir la corruption. »

Quant aux fonctions de l'OAC, elles sont définies dans les articles 1.2 et 3 à 7 de la LOAC.

II. Le cadre conceptuel : corruption non criminelle. Fonctions de l'OAC. Limites

A. Concept de corruption. Corruption non criminelle

Cependant, avant d'analyser en détail lesdites prévisions légales, il est utile de prendre une perspective élargie et de nous situer brièvement au plan conceptuel.

Et là, force est de constater, avant tout, que le cadre législatif espagnol (et notamment le Code pénal) existant au moment de la création de l'OAC ne contenait pas de définition légale générale et large de la corruption dans le secteur public. Le mot « corruption », avant sa modification par la Loi organique 1/2015, du 30 mars, n'apparaissait dans le Code pénal que dans deux articles :

- l'article 286bis, qui, à lui seul, formait la section 4 du chapitre XI du titre XIII (délits patrimoniaux et contre l'ordre socio-économique) du Livre II, et qui définissait et règlementait les délits de « corruption entre particuliers »,

- et l'article 445, correspondant au chapitre X du titre XIX (Délits contre l'Administration Publique), qui définissait et règlementait les «délits de corruption dans les transactions commerciales internationales», afin d'incorporer au droit espagnol les prévisions de la Convention de l'OCDE pour

la lutte contre la corruption des agents publics étrangers dans les transactions commerciales internationales, adoptée à Paris le 17/12/1997.

En 2015, la Loi organique 1/2015 susmentionnée a modifié le cadre législatif pénal, développant la section dédiée à la corruption entre particuliers, qui en vient à s'intituler « Corruption dans les affaires » (articles 286bis à 286quater) et incorpore la corruption d'agents publics étrangers.

Face à ces définitions concrètes de la corruption dans le Code pénal, il est utile de rappeler une définition bien plus générale de la corruption, qui est celle utilisée dans le Rapport anticorruption de l'Union européenne (RAC-UE) , où nous pouvons lire : « À l'instar des instruments juridiques internationaux, le présent rapport définit la corruption au sens large comme un "abus de pouvoir aux fins d'un profit personnel". Cette définition couvre donc des actes de corruption spécifiques et les mesures spécifiquement arrêtées par les États membres pour prévenir ou sanctionner des actes définis comme tels par la législation, mais vise également une série de domaines et de mesures qui ont une incidence sur le risque de corruption et sur la capacité à le maîtriser. »

La définition de corruption habituellement utilisée à l'OAC est en fait une version légèrement modifiée de cette définition : la corruption est entendue comme toute utilisation de ressources publiques pour l'obtention d'un bénéfice privé, en utilisant à son tour le mot « ressources » dans son acception la plus large (ressources financières, évidemment, mais aussi information, possibilités positionnelles d'action, etc.).

Cette définition délimite un périmètre, très large, de ce que nous pourrions considérer une "zone grise", à l'intérieur de laquelle (dans certains cas, en intersection avec laquelle) il est possible de situer des "zones sombres" qui correspondraient aux délits concrets, catégorisés dans le Code pénal, associés, directement ou de façon instrumentale, à la corruption, à savoir (et sans prétendre du tout faire une énumération exhaustive ni une analyse juridique pénale qui dépasserait largement le cadre de cet article) :

- la violation de secrets : chapitre IV du titre XIX du Code pénal (articles 413 à 418) ;

- la corruption (au sens strict : offre / sollicitation de pots-de-vin): chapitre V du titre XIX (délits contre l'administration publique) du Code pénal (articles 419 à 427bis) ;

- le trafic d'influence : chapitre VI du titre XIX du Code pénal (articles 428 à 431) ;

- la malversation ou le détournement de ressources publiques : chapitre VII du titre XIX du Code pénal (articles 432 à 435) ;

- les fraudes à l'encontre de l'administration : chapitre VIII du titre XIX du Code pénal (articles 436 à 438) ;

- les négociations et activités interdites aux fonctionnaires et les abus dans l'exercice de leurs fonctions : chapitre IX du titre XIX du Code pénal (articles 439 à 444) ;

- la prévarication administrative : chapitre I du titre XIX du Code pénal (articles 404 à 406) ;

- et les délits de corruption dans les affaires, susmentionnés.

Or, des principes essentiels qui régissent le droit pénal (principe d'intervention minimale ; principe d'interprétation restrictive ; présomption d'innocence ; règle in dubio pro reo ; etc.), établis dans la Constitution voire même, en amont, dans la Convention de sauvegarde des droits de l'homme et des libertés fondamentales adoptée à Rome le 4/11/1950, il découle une conséquence assez incontestable : ces « zones sombres » auxquelles nous avons fait allusion (délits relatifs à la corruption catégorisés dans le Code pénal) sont soumises à une dynamique restrictive, et n'ont, en tout cas, pas du tout tendance à élargir leur périmètre. Par contre, la « zone grise », qui engloberait tous les faits, situations ou actions qui raisonnablement pourraient s'inscrire dans le périmètre défini par la définition large de corruption susmentionnée, obéit à une dynamique d'expansion dérivée du développement et de l'approfondissement des interactions de tous ordres entre le secteur public et le secteur privé.

L'établissement ou le développement de règlementations dans des secteurs entiers de l'activité économique ; l'activité des pouvoirs publics comme acteurs économiques majeurs ; la conception des marchés publics, non seulement comme une activité économique quantitativement très importante,

mais également comme un instrument essentiel de politique économique, sociale, voire même environnementale ; ou le développement de formules de partenariat public-privé, constituent autant de domaines de risque où l'interaction d'intérêts privés avec l'intérêt général que doivent défendre les pouvoirs publics peut, assez facilement, dériver en une utilisation des ressources publiques aux fins d'un profit privé, c'est-à-dire en corruption au sens large.

Les faits, situations ou actions susceptibles d'être placés dans le périmètre de cette « zone grise », hors des « zones sombres » qui délimitent, restrictivement, les délits relatifs à la corruption, constituent ce que nous pouvons appeler la corruption non criminelle.

La prévention et la lutte (nous verrons tout de suite en quels termes et avec quels instruments) contre cette corruption non criminelle constituent la mission de l'OAC.

B. Fonctions de l'OAC. Domaine d'activité et limites

L'article 1.2 de la LOAC établit la finalité de l'OAC dans les termes suivants : « La finalité de l'Office Anti-fraude de la Catalogne est de prévenir et d'enquêter sur de possibles cas concrets d'utilisation ou de destination frauduleuse de fonds publics ou de tout bénéfice irrégulier dérivé de conduites comportant un conflit d'intérêts ou l'utilisation aux fins d'un bénéfice privé d'informations provenant de fonctions propres du personnel au service du secteur public. Relèveront également des finalités de l'Office Anti-fraude le conseil et l'émission de recommandations pour l'adoption de mesures contre la corruption, les pratiques frauduleuses et les comportements portant atteinte à l'intégrité et la transparence dans l'exercice des fonctions publiques, tout en coopérant avec les autorités compétentes et en collaborant dans la formation dans ce domaine du personnel au service du secteur public, et aussi encourager l'adoption de toutes mesures pertinentes à l'atteinte de la transparence dans gestion du secteur public. »

Cette finalité de l'OAC se décline ensuite dans les articles 3 à 6 de la LOAC qui font référence, respectivement, aux fonctions générales de l'OAC (article 3), aux fonctions spécifiques dans le domaine du secteur public de l'Administration autonome catalane, la Generalitat (article 4), aux fonctions dans le domaine des universités publiques catalanes (article 5) et, finalement, dans le domaine du secteur public de l'Administration locale (article 6).

Ces dispositions, d'une technique législative assez perfectible, semblent étendre le domaine d'action fonctionnel de l'OAC de façon extraordinairement large. En ce sens, les articles 4 et 6 font référence à la prévention et l'enquête de « conduites contraires à la probité ou aux principes d'objectivité, d'efficacité et de soumission pleine à la loi et au droit », principes constitutionnels qui régissent toute l'activité des administrations publiques (article 103.1 de la Constitution).

Au sens littéral, ces deux dispositions semblent autoriser l'OAC à enquêter et à se prononcer sur toute question ou conflit de légalité, voire même sur des situations de mauvaise gestion des affaires publiques, indépendamment de l'existence ou non dans le cas concret d'un élément de corruption. Cependant, la pratique suivie depuis le tout début de la mise en place de l'OAC, à partir d'une interprétation systématique et intégrée des dispositions des articles 1 et 3 à 6 de la LOAC, a été de limiter son action aux cas où apparaît, ne serait-ce que sur la base d'indices, l'existence d'un tel élément de corruption (l'obtention d'un bénéfice privé dérivé de l'usage de ressources publiques).

Si nous considérons maintenant le domaine d'activité de l'OAC d'un point de vue subjectif, ces fonctions se projettent et s'exercent sur le secteur public catalan, défini à l'article 2 de la LOAC comme incluant :

- l'administration de la Generalitat, y compris les organismes, les entités reliées et les entreprises publiques dépendantes de ces organismes ;

- les entités locales, dans le respect du principe constitutionnel d'autonomie locale (article 140 de la Constitution) ;

- les universités publiques, dans le respect du principe constitutionnel d'autonomie universitaire (article 27.10 de la Constitution) ;

- les fondations ou consortiums contrôlés par le secteur public catalan ; s'agissant d'entités de cette nature non contrôlées par le secteur public catalan, l'activité de l'OAC est limitée à leur activité pour compte du secteur

public catalan ;

- les entités privées ayant la condition de bénéficiaires de subventions ou de concessionnaires de services publics, ou auxquelles ont été attribués des marchés publics ; dans ces cas, de nouveau, l'activité de l'OAC est limitée à vérifier la destination et l'utilisation des subventions, ou à contrôler la gestion la gestion comptable, économique et financière des services publics ou l'exécution des marchés publics.

Du point de vue fonctionnel, le domaine d'activité de l'OAC est délimité dans les termes suivants par l'article 7 de l'OAC :

« 1. Il est entendu, en tout cas, que les fonctions de l'Office Anti-fraude sont sans préjudice de celles propres à l'Intervention Générale de la Generalitat de la Catalogne, le Síndic de Greuges [Médiateur de la Catalogne], la Sindicatura de Comptes [Cour des Comptes catalane], la Cour des Comptes [de l'État espagnol] ou les institutions équivalentes de contrôle, supervision et protectorat des personnes juridiques publiques et privées instrumentales, ni celles qui correspondent aux organes, nécessaires ou complémentaires, de contrôle des entités locales.

2. L' Office Anti-fraude ne peut pas exécuter les fonctions revenant à l'autorité judiciaire, le parquet et la police judiciaire, et ne peut enquêter sur les mêmes faits qui font l'objet de leurs enquêtes. Au cas où l'autorité judiciaire ou le parquet entament une procédure pour déterminer la relevance pénale de faits faisant à la fois l'objet d'enquêtes de l'Office Anti-fraude, celui-ci doit interrompre immédiatement son activité et apporter immédiatement toutes les informations dont elle dispose, et fournir tout l'appui nécessaire à l'autorité compétente. »

Cette disposition légale est complétée par celle de l'article 21.2 de la LOAC qui dispose que si l'OAC observe au cours d'une procédure des indices permettant de qualifier comme potentiellement délictuels les comportements ou les faits qui font l'objet de la procédure, elle doit communiquer immédiatement l'affaire à l'organe compétent, au parquet ou à l'autorité judiciaire.

Ces prévisions légales configurent les principes qui régissent l'interaction entre l'OAC et le parquet, principes dont la concrétisation opérationnelle a pris la forme d'un accord de collaboration entre le parquet supérieur de la Catalogne et l'OAC signé le 15 décembre 2010. Il convient de signaler que ce mécanisme de transmission des affaires entre le parquet et l'OAC fonctionne de façon bidirectionnelle : à diverses reprises des dossiers transmis au parquet car l'OAC considérait les faits ou comportements objets de l'enquête comme potentiellement délictuels ont été renvoyés de nouveau à l'OAC par le parquet, celui-ci ayant considéré que lesdits faits n'avaient pas de pertinence sur le plan pénal, ce qui a donné lieu à la reprise de l'activité de l'OAC.

III. Aspects organiques et opérationnels

A. Organisation de l'OAC

Pour l'accomplissement de ses fonctions, l'OAC est structuré en trois grandes unités : la Direction Prévention, la Direction Enquêtes et la Direction Analyse.

L'organigramme, défini dans les articles 8 à 15 des NARI, est dirigé par la Direction de l'Office, qui compte, dépendant directement du Directeur, le Cabinet de Direction, le Département Administration, Ressources Humaines et Budget, le Département Relations Institutionnelles, Visibilité et Participation, et le Département Secteur Privé, Gestion Éthique et Responsabilité Sociale.

L'activité et les fonctions concrètes de la Direction Prévention, décrites dans l'article 13 des NARI, sont axées sur la création de valeurs sociales, de cadres réglementaires, de mesures de promotion et de sensibilisation et de mécanismes de responsabilité et de reddition de comptes, dans le but de prévenir et d'entraver tout comportement contraire à la probité et à l'intégrité personnelle ; cette Direction dispense également des conseils et une assistance aux organismes publics et privés pour la mise en place d'initiatives de transparence et de bonne gouvernance.

La Direction Enquêtes est chargée de l'investigation, de la constatation et de la documentation de cas concrets d'utilisation ou destination illégales de fonds publics ou de toute autre mise à profit irrégulière dérivée de comportements entraînant des conflits d'intérêts ou l'utilisation, pour leur propre bénéfice, d'informations dérivées des fonctions du personnel au

service du secteur public, et des comportements allant à l'encontre de la probité ou contraires aux principes d'objectivité, d'efficacité et d'obéissance pleine et entière à la loi et au droit (article 14 des NARI).

Enfin, la Direction Analyse recueille, organise, structure et traite l'information générée dans son domaine d'activité par l'OAC, en détermine l'importance, réalise un suivi proactif des actions du secteur public, gère les contenus obtenus et veille à la sécurité et à l'intégrité des systèmes et des données obtenus (article 15 des NARI).

A signaler que ces trois Directions interviennent, en différentes phases de la procédure, dans la gestion des dénonciations présentées devant l'OAC.

B. Cycle opérationnel de l'OAC

Ainsi, si nous suivons chronologiquement ce que nous pourrions appeler le cycle opérationnel de l'OAC, celui-ci commence par l'intervention de la Direction Analyse, qui traite en premier lieu toute plainte, dénonciation ou communication reçue à l'OAC, en en faisant une première évaluation ou analyse préalable de vraisemblance (article 16 de la LOAC). La Direction Analyse propose également au Directeur l'ouverture d'office de dossiers sur la base d'informations obtenues de sources publiques (principalement les médias), d'analyses de domaines de risque, d'évaluations ou d'enquêtes préexistantes.

Dans le cas de dénonciations, la procédure de l'OAC (article 16.3 de la LOAC) prévoit la possibilité de déclarer secrète l'identité du dénonciateur, secret qui ne sera levé que sur demande d'une autorité judiciaire.

Les résultats possibles de cette première phase d'analyse sont au nombre de trois :

- le classement sans suite du dossier dans les cas de manque de compétence de l'OAC ; de manque d'un minimum d'indices ou de vraisemblance des faits analysés ; ou, particulièrement, de manque dans lesdits faits d'un élément de corruption (au sens large susmentionné), notamment dans les cas où les faits dénoncés posent strictement des problèmes d'interprétation ou d'application du cadre légal ou de mauvaise gestion publique ;

dans certains cas exceptionnels malgré le classement du dossier des recommandations ont été adressées à l'entité publique concernée par les faits analysés ;

- la communication du dossier au parquet lorsque dès cette phase l'on dispose de suffisamment d'indices permettant de considérer les faits analysés comme potentiellement délictuels ;

- et l'ouverture d'une enquête de l'OAC.

Dans ce dernier cas, le dossier passe à la Direction Enquêtes dont l'activité est sujette aux principes de confidentialité et réserve maximale, d'efficacité, de congruence, de proportionnalité et de célérité (articles 18 de la LOAC et 22 des NARI). La possibilité d'adopter des mesures conservatoires est expressément prévue aux articles 20 de la LOAC et 29 des NARI.

Signalons que l'OAC dispose, dans cette phase, de pouvoirs d'enquête remarquablement larges bien que strictement limités au périmètre de son domaine subjectif d'activité auquel nous avons déjà fait référence. Dans ce domaine, l'article 17.1 de la LOAC autorise l'Office à « … accéder dans le domaine qui est de son ressort à toute information détenues par des organes, organismes publics ou personnes physiques et juridiques, publiques ou privées. »

Quant au résultat final de l'enquête, de nouveau, plusieurs possibilités :

- face à des faits ou comportements établis par l'enquête qualifiables comme délictuels, le dossier et toute la documentation et information disponibles sont transférés au parquet ou à l'autorité judiciaire ;

- si l'enquête met en lumière des infractions ou d'autres irrégularités administratives, l'OAC transmet à l'entité publique concernée un rapport raisonné proposant l'imposition de sanctions disciplinaires ou l'adoption de mesures correctives de toute autre nature; l'organisme public dispose alors d'un délai de 30 jours pour informer l'OAC des mesures adoptées ou des raisons pour lesquelles les recommandations n'ont pas été suivies (article 21 de l'OAC) ; ce rapport raisonné de l'OAC n'a pas de force contraignante vis-à-vis de l'organisme public destinataire, qui peut ne pas en tenir compte ; cependant, dans cette hypothèse (dans la pratique assez peu fréquente),

l'OAC signalera cette circonstance dans son rapport annuel, soumis et présenté chaque année devant la Commission parlementaire compétente ;

- lorsque l'enquête conclut à l'existence de conduites non répréhensibles voire légalement admissibles mais éthiquement discutables, l'OAC adresse à l'entité publique concernée des recommandations préventives ;

- enfin, l'enquête est close par classement sans suite du dossier lorsque aucun fait répréhensible n'a pu être établi.

Une fois la phase d'enquête conclue, le dossier passe pour finir à la Direction Prévention, responsable du suivi à plus long terme des résultats de l'enquête : application effective des mesures ou recommandations proposées aux entités publiques ; problématiques ponctuelles surgies ; etc.

Ce suivi fournit à la Direction Prévention un retour d'information extrêmement précieux pour concevoir et cibler les actions concrètes de formation et de sensibilisation adressées au secteur public.

IV. Interactions entre l'OAC et le parquet. Limites du droit pénal

A. Un cas d'école : l'affaire Bagó

Une affaire concrète dans laquelle est intervenu l'OAC illustre à la perfection l'interaction entre l'OAC et le parquet ainsi que les limites structurelles de l'efficacité des instruments juridico-pénaux face à certaines formes diffuses de corruption (relevant du concept de corruption non criminelle abordé ci-dessus).

Les faits concernant cette affaire, connue dans les médias comme l'affaire Bagó , sont, en synthèse, les suivants.

M. B, maire d'une commune côtière catalane entre 1979 et 1991, et entrepreneur, fondateur, président et actionnaire de référence du groupe S, avait également été le fondateur et promoteur, en 1984, d'un consortium dans la santé, le Consortium de Santé et d'Assistance Sociale de la Catalogne (CSC).

Ce Consortium, devenu une organisation extrêmement étendue et complexe (intégrée en 2012 par 94 entités dont 31 mairies, 2 entités régionales, 21 fondations, 3 associations, 18 autres consortiums, 7 entités de droit public, 7 sociétés publiques et 5 autres entités), était l'entité mère de nombreuses sociétés, parmi lesquelles CSC, S.A. et CSCCIG, S.A. offraient, principalement à des communes ayant un hôpital ou d'autres installations sanitaires analogues, un service de management intégral desdites installations.

La commune de Badalona ayant fait appel à ce service de management intégral pour gérer l'hôpital municipal, un directeur fut désigné, dans le cadre de ce contrat de management intégral, par la société filiale du CSC présidée par M. B.

Or il s'est avéré qu'en 2012, ledit hôpital recevait et payait, de facto, le service de restauration du groupe S sur la base d'un marché public passé irrégulièrement en 1993 et depuis longtemps révolu, sans qu'aucune procédure de passation de ce marché n'ait été suivie postérieurement.

Considérant que cette situation, à l'évidence irrégulière, était susceptible d'être qualifiée comme un délit de trafic d'influence, l'OAC avait transmis l'affaire au parquet en janvier 2013.

Le parquet finit cependant par classer l'affaire. L'ordonnance de clôture du dossier contient toutefois les attendus et considérations extrêmement durs suivants :

«*… en même temps que M. B occupait les plus hautes instances dirigeantes de l'entité locale publique CSC et des sociétés publiques CSC, S.A. et CSCCIG, S.A. qui en dépendaient, il était également président et conseiller de diverses sociétés intégrées dans le holding d'entreprises […] contrôlé par lui et sa famille. Des sociétés du holding familial […] ont pris part et se sont vues attribuer des marchés par les entités intégrantes du consortium CSC dont le management était, dans certains cas, exercé par CSCCIG, S.A.*

Ceci représente clairement une atteinte frontale à l'encontre des dispositions en matière d'incompatibilités, […].

[…] Il est contraire à toute logique que ledit M. B ai pu occuper des postes dans des entités publiques liées au CSC, l'une desquelles offre des services de management à des hôpitaux parmi lesquels est inclus le conseil et la gestion de la passation de marchés publics, et, en même temps, diriger un conglomérat

d'entreprises qui ont pu prendre part à la passation de marchés de services par lesdites entités sans qu'aucune réaction des organes de contrôle n'ai eu lieu. Si l'on ajoute à ceci les liens solides de M. B avec un large réseau de relations politiques, l'on peut bien comprendre la stupeur des citoyens face à ces faits [...], ainsi que l'incompréhension face à un cadre juridique administratif objectivement insuffisant à l'heure d'empêcher la possibilité de situations comme celle décrite, qui porte atteinte au sens commun et à la bonne gouvernance des institutions. Cependant le cadre [juridique] pénal est régit par ses propres critères, [...], et la portée pénale de cette situation doit être établie objectivement et concrètement vis-à-vis de conduites concrètes.

... [dans le cas d'espèce] l'on n'a pas pu vérifier, de façon suffisamment fondée tel que l'exige le domaine pénal et au-delà de simples soupçons circonstanciels, des éléments indiquant que les irrégularités formelles détectées aient été conscientes, intentionnées et dues à des motivations détournées, [...], ni forcées ou obtenues [...] par M. B, [...], ou provoquées, sans équivoque, par une influence illicite de celui-ci sur l'administrateur (qui nie toute influence) qui constituerait du trafic d'influence visé aux art. 428 et suivants du CP.

Il n'empêche qu'il est particulièrement pénalisant qu'ait pu exister et se prolonger dans le temps sans aucune réaction administrative une situation où à l'évidence des intérêts publics et privés coexistaient en la personne de M. B en conflit évident, à partir de sa double position (de par ses postes de direction au sein du CSC et entités en dépendant et par le holding d'entreprises contrôlé par lui-même et sa famille), permettant ainsi que ses entreprises privées puisse prendre part librement à la passation de marchés par les entités participant au consortium CSC ou objet d'un contrat de management intégral avec CSCCIG, S.A. Cependant, en matière pénale il est nécessaire d'établir des preuves qui vont au-delà de ce qui est simplement circonstanciel. Et comme il a été déjà dit, tel n'est pas le cas, au-delà de soupçons pleinement justifiés. »

B. De l'anecdote au fait général : les limites du droit pénal

Au-delà des répercussions médiatiques et juridiques de cette affaire, nous pouvons en extraire une importante conclusion : l'existence de limites à l'efficacité du droit pénal et des poursuites pénales confrontées à des situations et des faits comme ceux que nous avons vus, qui sont indéniablement perçus comme de la corruption, mais sont suffisamment diffus et peu concrets pour que cette même situation floue et dilution objective des responsabilités constitue un obstacle difficilement surmontable à la nécessité, inhérente à toute procédure judiciaire pénale, d'étayer avec un minimum de solidité une accusation.

Dans le cas considéré, il semble clair que la réalisation et la perpétuation dans le temps d'une situation juridico-publique irrégulière (le marché irrégulièrement attribué et perpétué bien au-delà de son délai original) de laquelle découle un bénéfice privé a été le fruit d'une dynamique positionnelle au coeur de laquelle se trouvent les différents acteurs : il n'était probablement nul besoin de payer un pot-de-vin, ni même de donner des ordres ou d'influencer de quelque façon que ce soit le directeur de l'hôpital, placé à ce poste par le CSC, pour qu'il s'abstienne de prioriser la passation (et donc, la régularisation, conformément au droit) du marché irrégulier préexistant.

La complexité de certaines structures organisationnelles publiques (ou, également, publico-privées, appelées à se développer dans un avenir très proche) peut arriver même à court-circuiter et rendre totalement inefficaces les dispositions du cadre légal du régime d'incompatibilités auquel est soumis tout responsable ou travailleur public.

Et si nous en revenons à l'armature conceptuelle sur la corruption non criminelle que nous avons exposée ci-dessus, force est de constater que le droit pénal et les instruments de réaction pénale par eux seuls peuvent, dans ces « zones grises », s'avérer impuissants à donner une réponse que la société demande.

Et c'est ici précisément que l'on peut trouver la justification et la raison d'être d'une institution comme l'OAC : éviter que cette « zone grise » ne soit un véritable espace d'impunité en servant de mécanisme de réaction, de correction et de prévention face à ce genre de situations, mécanisme doué, évidemment, d'une "capacité de frappe" infiniment moindre que celle du

parquet ou de la juridiction pénale (l'OAC, comme nous l'avons vu, ne peut, par lui-même, ni accuser ni condamner pénalement personne, ni même imposer juridiquement aux opérateurs publics les solutions préconisées aux irrégularités détectées), mais cependant, depuis une position institutionnelle d'auctoritas, apte à promouvoir, de façon indirecte, la reconduction de situations irrégulières ou dysfonctionnelles vers un cadre de probité, de transparence et de bonne gouvernance.

Conclusion

Sur le plan sociologique, l'on constate ces dernières années, en Espagne et en Catalogne, une véritable situation d'hypersensibilité de la société vis-à-vis de la corruption. Mois après mois, depuis près de 5 ans, les baromètres du Centre d'Investigations Sociologiques montrent que la corruption figure parmi les premières préoccupations des citoyens et au nombre des principaux problèmes du pays. En ce sens, le RAC-UE fait état d'une situation apparemment paradoxale : alors que les expériences personnelles de corruption sont rares en Espagne (1 à 3% des réponses), la perception sociale d'une corruption généralisée est très étendue (95% des réponses). Il existe donc une perception de corruption généralisée qui ne répond pas à la réalité. Les causes de ce phénomène seraient évidemment à chercher dans l'écho médiatique, souvent hypertrophié, de nombreux scandales politiques et, également, dans une grande mesure, dans les dramatiques effets sociaux-économiques de la crise en Espagne depuis 2010.

Cependant, le mot corruption est un terme polysémique, utilisé indistinctement par les médias et par la société pour désigner des réalités très diverses, depuis des comportements délictuels (souvent n'ayant rien à voir, techniquement, avec la corruption - fraude fiscale, par exemple), des situations légales mais éthiquement contestables, voire même certains effets de la crise économique (le creusement des inégalités ; le sauvetage financier des banques ; etc.).

Dans ce contexte social, la « stupeur des citoyens » (pour paraphraser l'ordonnance du parquet citée ci-dessus) devant le manque de réponse des pouvoirs publics face à de situations perçues, de façon tout à fait justifiée, comme de la corruption, pose un grave problème.

À maux multiformes, multiples remèdes. Il est évident que la lutte contre la corruption exige le renforcement des instruments pénaux (parquets, juridictions et forces de l'ordre spécialisés ; cadre légal adapté aux innovations délictuelles ; etc.). Mais ne miser que sur l'une des approches, si importante et nécessaire soit-elle, peut mener à des résultats insatisfaisants.

Le modèle et l'approche de l'OAC dans la lutte contre la corruption, que nous pourrions qualifier de soft law enforcement, présentent l'intérêt d'être strictement complémentaires de l'approche classique (répressive pénale), et permettent d'attaquer le phénomène, d'une autre façon et sous un autre angle, en évitant que ne subsistent des "angles morts" que la corruption pourrait mettre à profit en toute impunité.

Notes :

1 L'accord politique conclu, le 21 novembre 2006, entre le PSC, ERC et ICV, et qui donna lieu à ce deuxième gouvernement tripartite catalan, prévoyait la création de « l'Office Anti-fraude avec l'objectif de prévenir et enquêter de possibles cas d'usage ou de déviation frauduleuse de fonds publics ou toute autre bénéfice illicite dérivé de comportements comportant un conflit d'intérêts ou l'utilisation particulière d'informations provenant des propres fonctions. En ce sens, [l'Office] aura aussi comme fonctions coopérer avec les autorités compétentes, collaborer dans la formation du personnel et conseiller dans le domaine de la lutte contre la fraude. »

2 Rapport de la Commission au Conseil et au Parlement européen - Rapport ant-icorruption de l'UE, du 3 février 2014, COM(2014) 38 final ; accessible, sur ce lien (juin 2016).

3 Cette affaire est décrite de façon très succincte et anonymisée, comme cas d'étude dans l'annexe A (page 163) de l'Etude sur la corruption dans le secteur sanitaire (Study on Corruption in the Healthcare Sector, HOME/2011/ISEC/PR/047-A2), publié en octobre 2013 par la Commission Européenne ; accessible sur ce lien (juin 2016).

De nombreux médias s'en firent l'écho à l'époque (entre 2012 et 2014), notamment le journal El País. L'article publié le 12/03/2014 dans El País, accessible sur ce lien (juin 2016), retrace (en espagnol) les tenants et les aboutissants de l'affaire et cite textuellement divers passages de l'ordonnance du Parquet de classement sans suite de l'affaire.

1La résolution / rapport de l'OAC, du 17/01/2013, transmettant l'affaire au Parquet (en catalan), publiée par le député éco-socialiste catalan M. David Companyon, est accessible sur ce lien (juin 2016).

4 Les baromètres du Centre d'Investigations Sociologiques, organisme indépendant relevant du Ministère de la Présidence espagnol sont réalisés mensuellement et visent principalement à mesurer l'état de l'opinion publique espagnole à un moment déterminé. Ils sont accessibles (en espagnol) sur ce lien (juin 2016).

5 Op. cit. en note 2, page 7.

LE RÔLE COMPLÉMENTAIRE DU RÉSEAU JUDICIAIRE EUROPÉEN ET D'EUROJUST DANS LA LUTTE CONTRE LA CRIMINALITÉ TRANSFRONTALIÈRE

FLORIN-RĂZVAN RADU

DOCTEUR EN DROIT, EXPERT NATIONAL DÉTACHÉ AUPRÈS D'EUROJUST AU SECRÉTARIAT DU RÉSEAU JUDICIAIRE EUROPÉEN

Les opinions exprimées dans cet article n'engagent que l'auteur et ne reflètent pas nécessairement l'opinion d'Eurojust ou celle du (secrétariat du) Réseau judiciaire européen.

Le Réseau judiciaire européen (RJE) et Eurojust ont un objectif commun, celui de faciliter la coopération judiciaire en matière pénale entre les États membres de l'Union européenne. Mais, leurs fonctions et moyens d'atteindre ce but sont différents.

Depuis sa création en 2002[1], EUROJUST cohabite, en tant que « partenaire privilégié », avec le Réseau judiciaire européen (en matière pénale), créé en Juin 1998[2]. La raison de cette coexistence se trouve justement dans leur complémentarité. En effet, le RJE est une structure flexible et décentralisée, représentée par les points de contact qui fonctionnent toujours dans les juridictions des pays membres, ayant le rôle d' « intermédiaires actifs » pour faciliter l'entraide judiciaire et la coopération en matière pénale ; Eurojust est un organe de l'Union européen (bientôt une agence), jouissant de la personnalité morale et disposant d'un siège (à la Haye) et d'un budget propre, avec une organisation centralisée, représentée par les bureaux nationaux et un secrétariat.

La nécessité de maintenir les deux structures et de clarifier leurs relations est précisée dans le cinquième paragraphe du préambule de la décision 2008/976/JAI du Conseil du 16 décembre 2008 concernant le Réseau judiciaire européen[3]. D'ailleurs, les deux structures sont mentionnées dans les traités et, par conséquent, au-delà des possibles débats doctrinaires, leur coexistence ne peut pas être remise en discussion par un acte juridique de force inférieure.

Ainsi, la coopération entre Eurojust et le Réseau judiciaire européen a été pour la première fois réglementée au niveau du droit primaire par le traité de Nice[4] qui l'avait introduite à l'article 31 (1) c) du Traité sur l'Union européenne (Troisième partie, Titre VI). Le besoin de préserver cette coexistence a été une fois de plus confirmé par le traité de Lisbonne[5]. *De lege lata*, après la réforme des traités, la coopération entre Eurojust et le RJE est réglementée au niveau primaire par les dispositions de l'article 85 du traité sur le fonctionnement de l'Union européenne (TFUE)[6].

Quels sont les fonctions et le fonctionnement du RJE (I) et d'Eurojust (II) ? Laquelle des deux structures est « la mieux placée » pour traiter une affaire de coopération judiciaire en matière pénale ? (III)

I. Fonctions et fonctionnement du Réseau judiciaire européen

Le Réseau judiciaire européen (RJE) est le premier réseau de coopération judiciaire, en étant, de ce point de vue, un pionnier et un modèle pour les réseaux similaires qui ont été créés plus tard[7] dans l'Union européenne et au-delà de l'Europe. Il fut créé par l'Action commune 98/428 JAI du Conseil du 29 juin 1998

afin de mettre en oeuvre la recommandation 21 du Programme d'action relatif à la criminalité organisée approuvé par le Conseil européen le 17 juin 1997. L'article 2, paragraphe 1er de l'Action commune prévoit : « *Le Réseau judiciaire européen est composé, compte tenu des règles constitutionnelles, des traditions juridiques et de la structure interne de chaque État membre, des autorités centrales responsables de la coopération judiciaire internationale, des autorités judiciaires ou d'autres autorités compétentes ayant des responsabilités spécifiques dans le cadre de la coopération internationale, soit en général, soit pour certaines formes graves de criminalité, telles que la criminalité organisée, la corruption, le trafic de drogue ou le terrorisme.*»

Dix ans après, sa base juridique a été renforcée par l'Action commune de juin 1998, abrogée et remplacée par la Décision 2008/976/JAI du Conseil du 16 décembre 2008 (ci-après nommée « la décision concernant le RJE » ou « la décision »), qui maintient l'organisation décentralisée et flexible du RJE et la plupart des dispositions de l'Action commune tout en apportant certains éléments nouveaux, comme nous allons détailler ci-dessous.

Conformément aux dispositions de l'article 2, paragraphe 1er de la décision, « Le Réseau judiciaire européen est composé, compte tenu des règles constitutionnelles, des traditions juridiques et de la structure interne de chaque État membre, des autorités centrales responsables de la coopération judiciaire internationale, des autorités judiciaires ou d'autres autorités compétentes ayant des responsabilités spécifiques dans le cadre de la coopération internationale. » On peut observer une différence de rédaction entre le texte de l'article 2 (1) de l' Action commune et l'article 2 (1) de la décision, mais cette différence est seulement de forme et n'affecte pas le fond de la compétence du réseau, qui reste la même, vu que l'article 4 (1) précise le rôle des points de contact du RJE, qui « *sont des intermédiaires actifs chargés de faciliter la coopération judiciaire entre les États membres, en particulier dans le cadre de la lutte contre les formes graves de criminalité.* » Néanmoins, l'article 1 de la décision et le préambule prévoient clairement que le Réseau créé par l'Action commune 98/428/JAI continue à fonctionner conformément aux dispositions de la décision. Par conséquent, le RJE est compétent dans le domaine de la coopération judiciaire en matière pénale en général et notamment dans le cadre de la lutte contre les formes graves de criminalité.

Les nouveautés majeures introduites par la décision de 2008 sont les correspondants nationaux (article 2 paragraphes 3 et 4 de la décision), qui doivent être désignés par chaque État membre parmi les points de contact, les correspondants chargés des aspects techniques du RJE (article 2 paragraphes 4 et 5), et la règlementation particulière du secrétariat chargé de la gestion du réseau (article 2 paragraphe 8), qui dispose d'un budget propre, partie du budget d'Eurojust (article 11 de la décision).

A. Les points de contact du Réseau judiciaire européen

Les principales fonctions des points de contact du RJE, telles qu'elles sont prévues par l'article 4 de la décision, sont :

- de se mettre à la disposition des autorités judiciaires locales et autres autorités compétentes de leur État membre, des points de contact des autres États membres, ainsi que des autorités judiciaires locales et autres autorités compétentes des autres États membres, pour leur permettre d'établir les contacts directs les plus appropriés ;

- de fournir aux autorités judiciaires locales de leur État membre, aux points de contact des autres États membres et aux autorités judiciaires locales des autres États membres les informations juridiques et pratiques nécessaires pour leur permettre d'établir de façon efficace une demande de coopération judiciaire ou pour améliorer la coopération judiciaire en général ;

- de participer, à leur niveau respectif, à l'organisation des sessions de formation sur la coopération judiciaire à l'intention des autorités compétentes de leur État membre, le cas échéant en coopération avec le Réseau européen judiciaire de formation, et de promouvoir cette organisation.

Le correspondant national a, au-delà de ses tâches en tant que point de contact, le rôle d'assurer une meilleure coordination entres les points de contact nationaux et le contact, en premier chef, avec le secrétariat du RJE. Il peut également donner, sur demande, un avis sur la désignation des nouveaux points de contact.

Conformément à l'article 4 (5) de la décision, « *le correspondant*

chargé des aspects techniques du Réseau judiciaire européen, qui peut également être un point de contact au sens des paragraphes 1 à 4, veille à ce que les informations concernant son État membre et visées à l'article 7 soient fournies et mises à jour conformément à l'article 8. »

Les points de contact du réseau exercent leurs fonctions dans leur propre pays de façon complémentaire aux fonctions primaires en tant que juge/procureurs ou représentants des autorités centrales.

Cependant, afin de créer un cadre de confiance mutuelle, le réseau se réunit régulièrement dans différentes formations. Ainsi, l'article 5 de la décision prévoit au moins trois réunions plénières par an. Deux de ces réunions sont organisées dans l'État membre qui détient la présidence semestrielle du Conseil de l'Union européenne et l'une peut, selon la décision concernant le RJE, « se tenir dans les locaux du Conseil à Bruxelles ou dans les locaux d'Eurojust à La Haye. » Depuis 2010, afin de souligner une fois de plus les relations privilégiées entre le RJE et Eurojust et vu que le secrétariat du RJE se trouve à la Haye, au sein du secrétariat d'Eurojust, cette réunion, connue sous le nom de « réunion ordinaire » (« regular meeting »), se tient tous les ans, en février, au siège d'Eurojust. En conformité aux dispositions de la décision, au moins trois points de contact par État membre sont invités aux réunions plénières qui ont lieu aux pays membres, et deux points de contact par État membre sont conviés aux réunions ordinaires.

Dans les lignes directrices sur le fonctionnement du RJE[8], document sans force obligatoire adopté par le RJE depuis 2010, il est également précisé le nombre des participants des pays candidats à l'Union européenne, pays associés ou pays tiers.

Au moins une fois par an, sont organisées des réunions de correspondants nationaux et des réunions des correspondants chargés des aspects techniques du RJE (article 6 de la décision).

Le RJE a approuvé l'organisation, avec co-financement du budget du secrétariat du RJE, des réunions nationales et régionales du réseau.

L'objectif du RJE de faciliter la coopération judiciaire et notamment le contact direct entre les autorités judiciaires des États membres de l'Union européenne est atteint pas seulement par l'intermédiaire des points de contact, mais de plus en plus par le biais des outils de télécommunication créés et mis à jour par le RJE.

B. Les outils internet du Réseau judiciaire européen

Même bien avant la décision de 2008, le RJE a fait de son site internet[9] une source essentielle d'information et un assistant très efficace et moderne pour les praticiens de la coopération judiciaire en matière pénale, notamment avec ses outils électroniques comme l'Atlas judiciaire européen[10], les fiches belges[11] et le Compendium[12]. Après l'entrée en vigueur de la décision, ces outils ont toujours été améliorés et mis à jour. Un nouvel outil, la bibliothèque judiciaire (« *Judicial Library* »)[13] a été créé en 2011 afin de mettre en oeuvre les conclusions du Conseil des 7 et 8 octobre 2010[14], et d'autres sections ou sous-sections, comme celle dédiée aux relations avec les pays tiers et les autres réseaux ou celle concernant la transposition de la législation de l'Union européenne dans les législations nationales.

La gestion du RJE, y compris de son site internet avec ses outils, est assurée par son secrétariat, qui représente l'unité administrative. Le secrétariat, dirigé par le Secrétaire du RJE, est une unité autonome au sein du secrétariat d'Eurojust[15], qui bénéficie d'un budget propre pour les activités liées à l'administration du réseau, partie de celui d'Eurojust[16].

i. L'Atlas judiciaire européen

En raison du principe du contact direct entre les autorités judiciaires des États Membres, l'Atlas judiciaire européen est désormais un outil presque indispensable pour identifier les autorités compétentes dans les pays requis/d'exécution. La version initiale de l'Atlas a été mise à jour et, depuis février 2015, cet outil contient les autorités compétentes, pas seulement pour l'entraide judiciaire dite « classique » et le mandat d'arrêt européen, mais également pour les autres instruments juridiques de reconnaissance mutuelle, comme la décision cadre sur le gel des avoirs, la décision cadre sur la confiscation, la décision cadre sur les sanctions pécuniaire, etc..

ii. Les fiches belges

Les fiches belges répondent aux exigences de l'article 7 (1) c) de la décision du Conseil concernant le RJE, de mettre à la disposition des praticiens des informations concises concernant les systèmes judiciaires et procéduraux des États Membres. Conçues initialement seulement pour l'entraide judiciaire, les fiches belges sont maintenant en cours de révision complète afin de contenir des informations concernant toutes les formes de coopération judiciaire en matière pénale. La révision des fiches belges devrait être finalisée en Juin 2016.

iii. Le Compendium

Le Compendium est un outil conçu pour aider les praticiens à rédiger des demandes d'entraide ainsi qu'un mandat d'arrêt européen. À partir de juillet 2016, le Compendium sera disponible dans une version tout à fait nouvelle, plus « user-friendly », qui aidera les praticiens à rédiger et à envoyer également d'autres demandes /décisions de coopération judiciaire mettant en oeuvre le principe de la reconnaissance mutuelle.

iv. La bibliothèque judiciaire

La bibliothèque judiciaire contient les textes des instruments juridiques de coopération judiciaire pénale, les formulaires prévus par les différentes décisions-cadre ou directives, les notifications et déclarations des pays membres, des manuels et guides sur la coopération, différents rapports, etc. Cette base de données est très utile pour ceux qui veulent en savoir plus sur certains instruments de coopération judiciaire.

II. Organisation, objectifs et fonctions d'Eurojust

Eurojust a été mentionnée pour la première fois au niveau du droit primaire dans le traité de Nice. À l'époque, le traité sur l'Union européenne, modifié par le traité de Nice, avait prévu à l'article 29 (Troisième partie, Titre VI) « *une coopération plus étroite entre les autorités judiciaires et autres autorités compétentes des États membres, y compris par l'intermédiaire de l'Unité européenne de coopération judiciaire (Eurojust), conformément aux articles 31 et 32* ».

Sur cette base primaire, Eurojust a été créée comme un organe de l'Union européenne par la décision 2002/187/JAI du Conseil du 28 février 2002, doté de la personnalité morale. Son acte fondateur a été modifié pour la première fois en 2003[17] et, d'une manière plus substantielle, par la décision 2009/426/JAI du Conseil du 16 décembre 2008[18] (ci-après nommée « la décision concernant Eurojust » ou « la décision »).

Cependant, depuis 2009, la mission d'Eurojust est précisée dans l'article 85 du Traité sur le fonctionnement de l'Union européenne (TFUE), dans sa forme après les modifications apportées par le Traité de Lisbonne. Ainsi, en conformité au premier paragraphe de l'article 85 du TFUE, « *La mission d'Eurojust est d'appuyer et de renforcer la coordination et la coopération entre les autorités nationales chargées des enquêtes et des poursuites relatives à la criminalité grave affectant deux ou plusieurs États membres ou exigeant une poursuite sur des bases communes, sur la base des opérations effectuées et des informations fournies par les autorités des États membres et par Europol. (...).* »

Eurojust se trouve maintenant dans une situation qu'on peut définir comme transitoire, car son cadre normatif d'organisation et de fonctionnement au niveau de la législation européenne secondaire est toujours représenté par la décision du Conseil (avec les modifications successives) adoptée sur la base de l'ancien traité sur l'Union européenne. Mais, elle a une nouvelle réglementation au niveau de la législation primaire (article 85 du TFUE), qui exige l'adoption, par le Parlement européen et le Conseil, conformément à la procédure législative ordinaire, d'un règlement déterminant la structure, le fonctionnement, le domaine d'action et les tâches d'Eurojust.

Nous allons d'abord présenter l'organisation et le fonctionnement d'Eurojust en conformité aux dispositions de la décision du Conseil en vigueur, puis, nous aborderons quelques éléments contenus dans la proposition de règlement du Parlement européen et du Conseil relatif à l'Agence de l'Union européenne pour la coopération judiciaire en matière pénale (Eurojust)[19].

A. Organisation et fonctionnement d'Eurojust

La décision concernant Eurojust, modifiée par la décision du 16 décembre 2008, prévoit que « *chaque État membre détache auprès d'Eurojust, conformément à son système juridique, un membre national qui a la qualité de procureur, de juge ou d'officier de police ayant des prérogatives équivalentes.* » (Article 2, paragraphe 1). Néanmoins, chaque État membre doit nommer un

adjoint et un assistant du membre national (article 2, paragraphe 1 b). Le membre national est tenu de fixer son lieu de travail habituel au siège d'Eurojust. Son adjoint et son assistant peuvent également fixer leur lieu de travail habituel au siège d'Eurojust. En outre, les États membres peuvent détacher des experts nationaux auprès de leurs représentations nationales à Eurojust.

Eurojust dispose d'un secrétariat dirigé par un directeur administratif.

B. Les objectifs d'Eurojust

Les objectifs d'Eurojust sont règlementés dans l'article 3 de la décision. Ces objectifs généraux sont :

- **de promouvoir et d'améliorer la coordination entre les autorités compétentes des États membres** concernant des enquêtes et des poursuites dans les États membres, en tenant compte de toute demande émanant d'une autorité compétente d'un État membre et de toute information fournie par un organe compétent en vertu de dispositions arrêtées dans le cadre des traités ;

- **d'améliorer la coopération entre les autorités compétentes des États membres**, notamment en facilitant l'exécution des demandes de coopération judiciaire et des décisions dans ce domaine relatives notamment à des instruments donnant effet au principe de reconnaissance mutuelle ;

- **de soutenir, par ailleurs, les autorités compétentes des États membres** pour renforcer l'efficacité de leurs enquêtes et de leurs poursuites.

En plus, Eurojust peut apporter son soutien à des enquêtes ou des poursuites concernant un seul État membre et un État tiers si un accord instaurant une coopération en vertu de l'article 26 bis, paragraphe 2 de la décision a été conclu avec ledit État ou si, dans un cas particulier, il y a un intérêt essentiel à apporter ce soutien ou elle peut apporter son soutien à des enquêtes ou des poursuites concernant ce seul État membre et la Communauté.

C. Compétence d'Eurojust

La compétence matérielle générale d'Eurojust, conformément à l'article 4 paragraphe 1 de la décision, vise les types de criminalité et les infractions pour lesquelles Europol a, à tout moment, compétence pour agir et les infractions commises en liaison avec ces types de criminalité. Toutefois, le deuxième paragraphe de l'article 4 permet une compétence complémentaire d'Eurojust élargie aux autres infractions, à la demande d'une autorité compétente d'un État membre afin d'apporter son concours à des enquêtes ou à des poursuites.

D. Les tâches d'Eurojust

Les tâches d'Eurojust sont exercées soit par ses membres nationaux, soit par le collège d'Eurojust composé des 28 membres nationaux.

i. Les tâches exercées par d'Eurojust exercées par l'intermédiaire de ses membres nationaux

En conformité aux dispositions de l'article 6 de la décision, un membre national d'Eurojust peut demander, de manière motivée, aux autorités compétentes des États membres concernés :

- d'entreprendre une enquête ou des poursuites sur des faits précis ;

- d'accepter que l'une d'elles puisse être mieux placée pour entreprendre une enquête ou des poursuites sur des faits précis ;

- de réaliser une coordination entre les autorités compétentes des États membres concernés ;

- de mettre en place une équipe d'enquête commune en conformité avec les instruments de coopération pertinents ;

- de lui fournir toute information nécessaire pour accomplir ses tâches ;

- de prendre des mesures d'enquête spéciales ;

- de prendre toute autre mesure justifiée par l'enquête ou les poursuites.

Eurojust assure l'information réciproque des autorités compétentes des États membres concernés sur les enquêtes et les poursuites dont elle a connaissance. Elle assiste, à leur demande, les autorités compétentes des États membres en vue d'assurer la meilleure coordination possible des enquêtes et des poursuites. Elle apporte son concours afin d'améliorer la coopération entre les autorités compétentes des États membres. Elle coopère avec le Réseau judiciaire européen et le consulte, y compris en utilisant sa base documentaire et en contribuant à l'améliorer. Elle apporte, dans les cas visés à l'article 3, paragraphes 2 et 3, et avec l'accord

du collège, son soutien à des enquêtes et des poursuites concernant les autorités compétentes d'un seul État membre.

ii. Les tâches d'Eurojust exercées en tant que collège

Les tâches d'Eurojust en tant que collège sont détaillées dans l'article 7 de la décision. Une partie de ces tâches sont communes à celles qui peuvent être exercées et tant que membre national, auxquelles s'ajoutent des tâches spécifiques, qui peuvent être exercées seulement en tant que collège. Ainsi, seul le collège peut fournir des avis à Europol sur la base des analyses qu'il a effectuées ou peut fournir un soutien logistique.

L'un des rôles les plus importants du collège est prévu au deuxième paragraphe de l'article 7, qui consiste à rendre, par écrit, un avis non contraignant sur les conflits de compétence lorsque deux membres nationaux ou plus ne peuvent s'accorder sur la manière de résoudre un tel conflit.

Néanmoins, le collège peut rendre, par écrit, des avis non contraignants en cas de concurrence entre plusieurs mandats d'arrêt européens ou en cas de difficultés ou de refus récurrents concernant l'exécution de demandes de coopération judiciaire et de décisions dans ce domaine relatives notamment à des instruments donnant effet au principe de reconnaissance mutuelle.

iii. Les pouvoirs particuliers des membres nationaux d'Eurojust

Les pouvoirs particuliers de membres nationaux d'Eurojust sont réglementés aux articles 9bis - 9septies de la décision concernant Eurojust. Chaque État membre doit définir la nature et l'étendue des pouvoirs qu'il confère à son membre national en étant obligé de conférer à son membre national au moins les pouvoirs décrits à l'article 9 ter et, sous réserve de l'article 9sexies, les pouvoirs décrits aux articles 9 quater et 9quinquies, dont il disposerait au niveau national.

L'article 9ter règlemente les pouvoirs ordinaires des membres nationaux, de « *recevoir les demandes de coopération judiciaire et les décisions dans ce domaine, relatives notamment à des instruments donnant effet au principe de reconnaissance mutuelle, à les transmettre, à les faciliter, à fournir des informations supplémentaires y ayant trait et à assurer le suivi de leur exécution* ».

L'article 9quater prévoit les pouvoirs que les membres nationaux peuvent exercer en leur qualité d'autorités nationales compétentes en accord avec l'autorité nationale compétente ou à sa demande, comme ceux d'émettre et compléter des demande de coopération judiciaire et des décisions dans ce domaine, d'exécuter dans leur État membre de telles demandes ou décisions, d'ordonner dans leur État membre des mesures d'enquête jugées nécessaires lors d'une réunion de coordination organisée par Eurojust, d'autoriser et de coordonner des livraisons contrôlées dans leur État membre.

En cas d'urgence « et dans la mesure où il ne leur est pas possible d'identifier ou de contacter l'autorité nationale compétente en temps voulu », l'article 9quinquies permet aux membres nationaux d'autoriser et de coordonner des livraisons contrôlées dans leur État membre et d'exécuter dans leur État membre des demandes de coopération judiciaire ou des décisions dans ce domaine.

L'article 9sexies précise que les membres nationaux devraient avoir le pouvoir de faire une proposition à l'autorité nationale compétente comme celle d'exercer les pouvoirs prévus aux articles 9quater et 9quinquies lorsque l'attribution de ces pouvoirs à un membre national est contraire aux règles constitutionnelles ou aux aspects fondamentaux du système de justice pénale.

L'article 9septies règlemente la participation des membres nationaux aux équipes commune d'enquête visées à l'article 13 de la convention relative à l'entraide judiciaire en matière pénale entre les États membres de l'Union européenne ou dans la décision-cadre 2002/465/JAI du Conseil du 13 juin 2002. À cet égard, les membres nationaux d'Eurojust peuvent participer aux équipes communes d'enquête qui ne bénéficient pas de financement du budget de l'Union européenne, et ils doivent être invités à participer à celles financées par le budget de l'Union européenne.

En ce qui concerne la durée du mandat des membres nationaux, la décision du Conseil impose une durée minimale de 4 ans, qui peut être renouvelée par l'État membre d'origine.

Il convient de rappeler que les dispositions de l'article 85 du TFUE prévoient parmi les tâches d'Eurojust (qui peuvent être comprises dans les futurs règlements du Parlement européen et du Conseil, qui devraient être

adoptés conformément à la procédure législative ordinaire) :

« *a) le déclenchement d'enquêtes pénales ainsi que la proposition de déclenchement de poursuites conduites par les autorités nationales compétentes, en particulier celles relatives à des infractions portant atteinte aux intérêts financiers de l'Union ;*

b) la coordination des enquêtes et poursuites visées au point a) ;

c) le renforcement de la coopération judiciaire, y compris par la résolution des conflits de compétences et par une coopération étroite avec le Réseau judiciaire européen. »

À cet égard, nous pouvons regretter que, dans l'état actuel des négociations[20] sur le règlement concernant Eurojust, on n'a pas mis en valeur toutes les possibilités offertes par l'article 85 (1) a) et c) du TFUE. Ainsi, la proposition de règlement se limite aux dispositions de la décision en vigueur du Conseil en ce qui concerne le déclenchement d'enquêtes pénales et le rôle d'Eurojust en ce qui concerne la résolution des conflits de compétence. À notre avis, l'article 85 du TFUE permettait d'aller plus loin pour ce qui est de la résolution de conflits de compétence en donnant à Eurojust la possibilité réelle de résoudre ces conflits par une décision contraignante du collège, et pas seulement la possibilité d'émettre un avis consultatif comme la proposition de règlement le prévoit dans la réglementation actuelle. Dans le même sens, l'article 85 du TFUE envisage la possibilité d'Eurojust de déclencher des enquêtes pénales et pas seulement de demander aux autorités nationales de déclencher telles enquêtes, comme c'est prévu dans la proposition de règlement, qui, encore une fois, reprend la solution législative déjà en vigueur.

Évidemment, les négociations au Conseil et au Parlement européen impliquent des compromis nécessaires que nous comprenons très bien. Même si le futur règlement est moins ambitieux que le TFUE le permettait, son adoption, que nous souhaitons rapide, apporterait des clarifications nécessaires sur l'organisation et le fonctionnement d'Eurojust, y compris une meilleure séparation des tâches opérationnelles du collège d'Eurojust de celles de gestion par la création du conseil exécutif (*Executive Board*) d'Eurojust.

Néanmoins, l'un des avantages majeurs représentés par la nouvelle base juridique sera l'application directe du règlement, par comparaison à la décision du Conseil, ce qui contribuera à une uniformisation en ce qui concerne les pouvoirs des membres nationaux.

III. « Qui est le mieux placé » pour traiter une affaire de coopération judiciaire en matière pénale ? Le rôle du RJE au sein du System National de Coordination Eurojust (SNCE)

A. Quelle structure est mieux placée pour traiter d'une affaire de coopération judiciaire en matière pénale ?

La réponse à la question de savoir « qui est le mieux placé » entre Eurojust et le RJE pour traiter une affaire de coopération judiciaire en matière pénale n'est pas du tout simple. Depuis 2002, les praticiens de la coopération judiciaire pénale, ainsi que le RJE et Eurojust, essayent toujours de trouver les meilleures réponses. L'explication simpliste, « le RJE est compétent pour des affaires bilatérales (parfois on ajoute « simples ») et Eurojust pour des affaires multilatérales complexes », est souvent incorrecte, car il y a des affaires purement bilatérales pour lesquelles Eurojust est compétente et des affaires complexes, même multilatérales, où le RJE peut aider.

Pour apporter une réponse correcte à cette question, il faut lire et interpréter systématiquement les deux décisions du Conseil relatives respectivement à Eurojust et au RJE. Évidemment, les praticiens de la coopération judiciaire en matière pénale peuvent apporter leur importante contribution à la clarification des moyens complémentaires des deux structures. À cet égard, dans certains États membres de l'Union européenne, des guides, des lignes directrices ou des lettres circulaires ont été élaborés par les autorités nationales compétentes. En plus, le RJE et Eurojust ont travaillé ensemble dans les années passées afin de trouver quelques réponses pratiques à cette question. Le résultat de ce travail commun est dans un document du groupe de travail conjoint RJE-Eurojust intitulé « *Assistance à la coopération en matière pénale pour les praticiens* » (Joint Paper EJN/Eurojust « *Assistance in international cooperation in criminal matters for practitioners* »), qui est publié sur les pages internet du RJE[21] et d'Eurojust[22].

Dans le document commun RJE-Eurojust, on présente brièvement les deux structures et leurs manières spécifiques de travail, et on synthétise comment le RJE et Eurojust peuvent être utilisés. Ainsi :

- le RJE peut être utilisé pour identifier les autorités compétentes à l'étranger afin de permettre une communication directe ; pour faciliter la coopération judiciaire ; pour faciliter l'échange d'informations entre les autorités judiciaires ; pour obtenir des informations sur les mesures d'enquête ;

- Eurojust peut être utilisée pour faciliter la coopération judiciaire ; pour aider à prévenir ou à résoudre les conflits de compétence ; pour coordonner les enquêtes ou poursuites ; pour organiser et soutenir des réunions de coordination et des centres de coordination ; pour faciliter et soutenir les équipes communes d'enquête ; pour coordonner et faciliter les demandes de coopération judiciaire de et vers les États tiers.

De notre point de vue, il y a, évidement, des « zones » de compétence bien délimitées, presque exclusives pour Eurojust – comme la coordination des enquêtes (y compris l'organisation des réunions de coordination), la prévention et l'aide à résoudre les conflits de compétence, l'intervention en cas de refus répétés d'exécuter une demande de coopération, ou en cas de retards injustifié dans l'exécution des demandes, ou en cas de concours de demandes. Dans ces zones, c'est assez clair, c'est Eurojust « qui est la mieux placée ».

D'autre part, il est aussi clair que le RJE est le meilleur placé afin d'identifier une autorité compétente pour l'exécution d'une demande de coopération ou pour fournir des informations concises sur les procédures et les législations nationales applicables aux différentes formes de coopération judiciaire en matière pénale.

Des problèmes d'interprétation apparaissent sur la compétence de l'une ou de l'autre des deux structures notamment en ce qui concerne la « facilitation de la coopération judiciaire » en général, où, le cas échéant, chacune peut être compétente. Sur ce point, les choses sont bien plus compliquées que des délimitations simplistes comme « *le RJE pour les affaires simples, Eurojust pour les affaires complexes* » ou « *le RJE pour identifier les autorités compétentes, Eurojust pour résoudre un problème lié à la coopération* ».

Par exemple, il peut y avoir une situation où l'affaire est « simple » mais les retards répétés pour exécuter la demande imposent l'intervention d'Eurojust, ou, vice-versa, il peut y avoir une affaire très complexe, mais qui ne nécessite pas de coordination entre plusieurs États membres, pour laquelle il suffit de consulter les points de contact ou le site du RJE afin de faciliter l'exécution des demandes de coopération judiciaire.

B. Le système national de coordination Eurojust

Depuis l'entrée en vigueur de la nouvelle décision du Conseil concernant Eurojust, un autre instrument peut aider à identifier la structure « la mieux placée », il s'agit du système national de coordination Eurojust (SNCE) prévu à l'article 12 de ladite décision où le RJE est représenté, dans chaque État membre, au moins par le correspondant national et jusqu'à trois points de contact. Ainsi, le SNCE facilite, dans chaque État membre, l'accomplissement des tâches d'Eurojust, y compris « en contribuant à déterminer si un dossier doit être traité avec l'aide d'Eurojust ou du Réseau judiciaire européen » (article 12 para. 5 b de la décision concernant Eurojust).

Ce thème toujours actuel des relations RJE-Eurojust a d'ailleurs été à l'agenda de la 46ème réunion plénière du RJE (Amsterdam et La Haye, 7-9 juin 2016).

Conclusion

Le Réseau judiciaire européen et Eurojust sont, en tant que partenaires privilégiés, deux structures complémentaires, qui, chacune avec sa propre méthode de travail, peuvent faciliter la coopération judiciaire en matière pénale entre les États membres de l'Union européenne, notamment contre la criminalité transfrontalière.

Leur partenariat privilégié, qui découle de leur objectif général commun, est renforcé par le fait que le secrétariat du RJE fait partie du secrétariat d'Eurojust et le correspondant national du RJE et d'autres points de contact font partie du SNCE dans chaque État membre, assurant ainsi les synergies nécessaires entre les deux structures.

Les efforts des autorités nationales compétentes pour la formation des magistrats, en ce qui concerne la coopération judi-

ciaire en matière pénale, doivent se pencher de plus en plus sur les rôles des deux structures afin d'aider les autorités judiciaires nationales de bénéficier au maximum des possibilités et des outils offerts par Eurojust et le Réseau judiciaire européen.

Notes :

1 Décision du Conseil du 28 février 2002 instituant Eurojust afin de renforcer la lutte contre les formes graves de criminalité (2002/187/JAI), JO L 63 du 6 mars 2002, p. 1-13.

2 Action commune du 29 juin 1998 adoptée par le Conseil sur la base de l'article K.3 du traité sur l'Union européenne concernant la création d'un Réseau judiciaire européen (98/428/JAI), JO L 191 du 07/07/1998 p. 0004 - 0007

3 Décision 2008/976/JAI du Conseil du 16 décembre 2008 concernant le réseau judiciaire européen, JO L 348 du 24.12.2008, p. 130-134.

4 Traité de Nice modifiant le traité sur l'Union européenne, les traités instituant les Communautés européennes et certains actes connexes, JO C 80, 10.3.2001, p. 1–87.

5 Traité de Lisbonne modifiant le traité sur l'Union européenne et le traité instituant la Communauté européenne, signé à Lisbonne le 13 décembre 2007, JO C 306, 17.12.2007, p. 1–271.

6 Version consolidée du traité sur le fonctionnement de l'Union européenne, JO C 326, 26.10.2012, p. 47–390.

7 Par exemple, au sein de l'UE, le réseau judiciaire européen en matière civile et commerciale (créé par la décision du Conseil 2001/470/CE), le réseau des points de contact en ce qui concerne les personnes responsables de génocide, de crimes contre l'humanité et de crime de guerre (créé par la décision du Conseil 2002/494/JAI), le réseau d'experts pour les équipes communes d'enquête (ECA), créé en juillet 2005 par le document du Conseil 11037/05 ou, au-delà de l'UE, IberRed (le réseau euro-américain de coopération judiciaire ou le SEEPAG – South East European Prosecutors Advisory Group).

8 Ces lignes directrices peuvent être trouvées sur le site du RJE : http://www.ejn-crimjust.europa.eu/ejn/EJN_StaticPage.aspx?Bread=8

9 www.ejn-crimjust.europa.eu

10 http://www.ejn-crimjust.europa.eu/ejn/AtlasChooseCountry.aspx?Type=2

11 http://www.ejn-crimjust.europa.eu/ejn/EJN_FichesBelges.aspx

12 http://www.ejn-crimjust.europa.eu/ejn/EJN_ChooseCompendium.aspx

13 http://www.ejn-crimjust.europa.eu/ejn/libcategories.aspx

14 Conclusions du Conseil du 7 et 8 octobre 2010 sur le suivi de la mise en oeuvre des instruments mettant en oeuvre le principe de la reconnaissance mutuelle des décisions judiciaires en matière pénale (document 13405/10.

15 Voir les dispositions de l'article 25bis de la décision du Conseil concernant Eurojust (version consolidée) et le considérant 20 de ladite décision.

16 Voir aussi l'article 11 de la décision du Conseil relatif au RJE.

17 Décision 2003/659/JAI du Conseil du 18 juin 2003 modifiant la décision 2002/187/JAI instituant Eurojust afin de renforcer la lutte contre les formes graves de criminalité, JO l 245 du 29 septembre 2003, p. 44-45.

18 Décision 2009/426/JAI du Conseil du 16 décembre 2008 sur le renforcement d'Eurojust et modifiant la décision 2002/187/JAI instituant Eurojust afin de renforcer la lutte contre les formes graves de criminalité, JO 138 du 4 juin 2009, p. 14-30.

19 COM (2013) 535 final.

20 Orientation générale du Conseil de l'UE sur la proposition de règlement (document 6643/15 du 27 février 2015; on attend l'opinion du Parlement Européen.

21 http://www.ejn-crimjust.europa.eu/ejn/PartnersDetail.aspx?Id=1

22 http://eurojust.europa.eu/about/Partners/Pages/ejn.aspx

OUVRAGES RÉCENTS

L'ENFER DE LA CRIMINALITÉ FINANCIÈRE

AUTEUR : FRÉDÉRIC COMPIN

EDITEUR : JET D'ENCRE

Présentation de l'éditeur

Et si Dante n'avait rien vu ? Le capitalisme financier, vecteur de moult perversions, s'arrête-t-il aux portes de l'enfer économique et social, faisant de la criminalité financière le moyen le plus sûr d'extorquer la plus-value collective ? Tel un cri, cet ouvrage veut ouvrir les yeux et informer les consciences que la criminalité financière n'est autre que l'instrument de domination d'un système économique dont la

finalité consiste à blanchir des capitaux et à échapper à l'impôt, tout en asservissant les masses et en servant les puissants.

Frédéric Compin signe un ouvrage incisif et sans concessions pour le monde de la finance, et y dénonce avec acuité deux fléaux majeurs de ce siècle : la fraude fiscale et le blanchiment d'argent.

SYNTHÈSE DU RAPPORT INTÉRIMAIRE SOCTA 2015

ELENA PELLISER

DOCTORANTE EN DROIT À L'UNIVERSITÉ DE STRASBOURG - UMR DRES,

Le Conseil de l'UE a rendu public le 16 mars 2015 le rapport intérimaire SOCTA pour 2015, qui constitue une mise à jour du rapport de situation 2013 sur la criminalité grave et organisée dans l'UE. Les rapports SOCTA sont des documents stratégiques qui permettent d'orienter les politiques de lutte contre la criminalité grave et organisée dans l'UE.

Les **principaux constats** du Rapport intérimaire SOCTA 2015, suivis d'une analyse des principaux **éléments catalyseurs de la criminalité** et d'un **état des lieux des principaux secteurs criminels**, sont exposés ci-après. Le lecteur est renvoyé au texte du rapport pour l'analyse sectorielle détaillée, sur le site http://www.statewatch.org/news/2015/mar/eu-europol-interim-SOCTA-7271-15.pdf (en anglais uniquement). Les **préconisations** figurent en toute fin.

I Principaux constats

La criminalité grave et organisée dans l'UE demeure une menace dynamique et substantielle. Si les principales dimensions de cette menace demeurent globalement semblables à celles qui avaient été exposées dans le rapport SOCTA 2013, les trajets, *modi operandi* et technologies exploitées par les criminels continuent de se diversifier et d'évoluer.

- Le **marché des stupéfiants et drogues illicites** reste le premier marché criminel, avec pour principale préoccupation l'apparition permanente de nouvelles substances psychoactives jusque-là inconnues, ainsi que la flexibilité et l'adaptabilité extrêmes dont font preuves les GCO dans les activités sont concernées par les drogues de synthèse et la production de ces nouvelles substances. On note que la production de ces dernières, notamment le conditionnement, l'emballage et l'étiquetage, se font de plus en plus dans l'UE, avec une tendance à rapprocher la production des consommateurs. Les groupes criminels organisés (GCO) travaillant dans la production et la distribution de différents types de drogue continuent d'avoir accès à des ressources financières significatives, d'investir stratégiquement dans des technologies et de faire appel à la corruption afin de maximiser le profit et d'éviter d'être détectés.
- Les **produits de contrefaçon**, en particulier ceux qui violent les réglementations sanitaires et de sécurité, restent une préoccupation significative pour les Etats membres. Des pesticides contrefaits font l'objet de trafic vers les pays de l'UE, en quantité toujours croissante, et constituent donc un risque significatif pour la santé des Européens et pour l'environnement.
- Les **atteintes aux biens commises en bande organisée**, qui sont très visibles pour les citoyens et menacent de saper la confiance publique dans la capacité des services répressifs à lutter contre les GCO, sont particulièrement apparentes. Sur ces deux années, de nombreux Etats membres ont été témoins d'une hausse significative dans ce secteur.
- L'aide **aux migrations illégales** demeure un secteur

très profitable, où interviennent un grand nombre de groupes organisés, et représente un marché de croissance, d'autres groupes étant attirés par cette activité et se détournant donc de celles qu'ils menaient jusque-là. Les transferts de migrants irréguliers par la mer, en Méditerranée centrale et orientale, a connu une croissance exponentielle l'an dernier. L'augmentation globale du nombre de migrants irréguliers parvenant sur le territoire de l'UE entraîne une augmentation encore plus forte des services des passeurs proposés par des GCO, liés aux déplacements secondaires au sein de l'UE et à la transition vers un séjour légal dans les Etats membres. Dans l'intervalle, le trafic des êtres humains, une activité en pleine expansion, continue d'affecter les Etats membres, qu'ils soient pays source ou de destination. Les trafiquants facilitent de plus en plus l'entrée sur le territoire de l'UE pour leurs victimes en utilisant de manière abusive les procédures d'asile et en recourant à Internet pour faire la publicité des services d'exploitation sexuelle et de main-d'oeuvre que peuvent rendre leurs victimes.

- La **cybercriminalité** demeure très dynamique et les acteurs criminels agissant dans ce secteur innovent en permanence, tant dans leur mode de fonctionnement que dans les produits qu'ils proposent. La cybercriminalité couvre toute une gamme d'activités criminelles diverses. Les cyber-attaques et la cybercriminalité à but lucratif entraînent la diffusion de données privées et constituent une menace significative pour l'économie européenne. La fraude aux cartes de paiement a des conséquences dommageables sur le plan financier, et ne cesse d'augmenter d'une année sur l'autre. Les vols croissants permettent de diffuser des volumes significatifs d'informations relatives aux cartes de paiement et de données personnelles sur Internet, lui-même de plus en plus utilisé par les GCO pour leur fraude aux cartes de paiement. Les délinquants qui sévissent dans l'exploitation sexuelle des enfants et la diffusion de contenus pédopornographiques s'adaptent rapidement pour exploiter les nouvelles technologies ou de nouveaux modes de fonctionnement afin de tenter d'entrer en contact avec leurs victimes potentielles. Ceci a abouti à l'émergence de nouvelles tendances dans la sollicitation en ligne et l'exportation commerciale sexuelle des enfants dans le cyberespace.

- Le **modèle économique du crime en tant que service** est de plus en plus adopté par des GCO et des acteurs criminels à titre individuel, hors du cyberespace où il avait d'abord été créé. Dans ce cadre, divers services et outils sont proposés qui permettent aux GCO de mener leurs activités. Les facilitateurs pour l'immigration illégale s'appuient sur des contrefacteurs de documents, les GCO chargés de la distribution des produits stupéfiants acquièrent des armes pour intimider ou exercer leur contrôle, et les fraudeurs aux cartes de paiement peuvent accéder à des volumes de données considérables sur des informations compromises relatives aux cartes de paiement. Tous ces services et biens servent à entretenir une activité criminelle grave et organisée et permettent aux groupes et criminels individuels d'étendre leurs activités et de cibler plus de victimes. Le modèle économique du crime comme service est en passe de devenir un **catalyseur clé pour la criminalité organisée**, dont il amplifie l'impact et la portée.

- Dans ce modèle, le point-clé est la capacité des acteurs criminels à communiquer et à interagir dans le cadre d'un espace criminel occulte partagé. Une bonne partie de cette **interaction a lieu désormais en ligne**. Internet continue de permettre aux GCO d'accéder à de larges gisements de victimes, de dissimuler les activités criminelles et de les réaliser avec un impact plus grand et moins de risques de détection. Les faux-monnayeurs qui fabriquent des euros de contrefaçon se fournissent en matières premières sur les marchés en ligne, les groupes organisés qui sévissent dans la traite des êtres humains utilisent des plates-formes en ligne pour faire la publicité des services de leurs victimes et les blanchisseurs de capitaux exploitent l'accès immédiat aux systèmes financiers globaux mondiaux pour faire circuler et dissimuler les flux de profits illicites. Les acteurs criminels ont utilisé Internet pour créer un **milieu criminel globalisé**, un marché où on peut se procurer virtuellement tous les biens et services criminels nécessaires.

- Le **commerce en ligne de**

drogues, de produits contrefaits, d'armes illégales et autres biens illégaux ne cesse de s'étendre. Les GCO utilisent les **marchés en ligne** pour distribuer leurs produits à une gamme de plus en plus large de clients, attirés par ces services du fait de l'apparence d'anonymat et de la capacité à commander ces produits de chez soi. Les marchés en ligne permettent également à des criminels de devenir distributeur de biens illégaux sans avoir à passer par l'infrastructure de trafic qui était jusque-là nécessaire et que les criminels organisés devaient entretenir.

- Ce **milieu criminel virtuel** menace de plus en plus de devenir un espace commun pour le crime organisé et le terrorisme. En l'absence de liens structurels clairs entre les organisés et le terrorisme, il convient de se garder de surestimer la convergence de ces phénomènes. Toutefois, les **terroristes** ont accès aux mêmes services criminels qui pourraient potentiellement utiliser ou obtiennent les mêmes outils pour leurs crimes, tels que les armes, commercialisés sur les plates-formes en ligne qui sont le fonds de commerce de ce monde criminel virtuel.

- Le nombre de GCO impliqués dans plus d'un secteur criminel, que l'on appelle également des **groupes polycriminels (ou multicartes)**, continue d'augmenter. La majorité de ces GCO combine des types de crimes similaires, tels que le trafic de différentes drogues et stupéfiants, ou sont impliquées dans différents types d'atteinte aux biens commises en bande organisée. En dépit de la perturbation de plusieurs gros réseaux criminels à grande échelle ces dernières années, rien ne semble indiquer que le nombre global de groupes criminels diminue.

- **Des lacunes significatives persistent en matière de renseignement** concernant diverses activités criminelles. On ne sait pas clairement quelle est l'envergure du phénomène de trafic d'armes et le niveau d'implication des GCO dans cette activité. De même, le **niveau d'organisation criminelle**, pour ce qui est de la commercialisation de contrefaçons et des biens ne répondant pas aux normes ainsi que du trafic illicite de déchets, est dans une large mesure inconnu. Les connaissances parcellaires sur les mécanismes et acteurs impliqués dans le blanchiment de capitaux constituent une lacune substantielle dans le paysage du renseignement.

II Principaux catalyseurs de la criminalité

Les catalyseurs de la criminalité sont les facteurs pertinents qui ont une influence sur la nature sur l'impact des activités criminelles graves et organisées.

La **situation économique** joue un rôle clé dans ce domaine. Les réorientations des marchés criminels sont souvent causées par des modifications de la situation économique. Ainsi, dans certains Etats membres, entre 2012 2014, le vol de carburant a augmenté du fait des cours élevés du pétrole. Aujourd'hui, le pétrole est au plus bas, ce qui devrait réduire les bénéfices pour les groupes criminels pratiquant cette activité.

Divers secteurs criminels sont affectés par la **situation géopolitique** en Europe et dans son voisinage. La situation en Ukraine pourrait, à l'avenir, avoir des conséquences pour les activités criminelles graves et organisées dans l'UE. Les conflits armés sont un vecteur essentiel pour la prolifération des armes de petit calibre, même longtemps après qu'ils se soient terminés, et offrent un flux régulier d'armes pour les trafiquants. L'insécurité qui règne actuellement en Irak, en Libye et en Syrie est un catalyseur clé pour les réfugiés émigrants qui s'efforcent de rejoindre l'UE.

Les GCO suivent **des trajets bien établis et utilisent les infrastructures de transport** pour se livrer à leurs trafics. Les grands ports tels qu'Anvers, Rotterdam et Hambourg donnent accès au marché européen à la fois pour les marchandises légales et illégales qui arrivent sur des porte-conteneurs de très grande capacité. Les Balkans de l'Ouest demeurent une région clé pour le transit de migrants irréguliers et de produits illicites en provenance de Turquie et d'Afrique du Nord et à destination de l'UE. L'Afrique de l'Ouest reste une région importante pour le transit de cocaïne à destination de l'UE.

Les GCO exploitent les **liens ethniques nationaux avec les diasporas** dans tout le continent. Celles-ci leur donnent des opportunités d'infiltrer des structures commerciales légales et d'établir des réseaux de contacts dans de nombreux Etats membres. Les groupes criminels qui pratiquent les atteintes aux

biens commis en bande organisée s'appuient souvent sur des diasporas pour le soutien logistique et pour recruter de nouveaux membres.

La **corruption** est utilisée par les GCO pour atteindre et influencer d'autres personnes qui occupent des postes clés. Elle peut prendre diverses formes, par exemple le versement de pots-de-vin, les conflits d'intérêts, le trafic d'influence, la collusion ou le népotisme, la distorsion à la concurrence légitime et l'érosion de la confiance dans les autorités nationales. Les GCO et s'efforcent souvent de corrompre des personnes possédant des connaissances spécifiques ou ayant accès à des bâtiments sécurisés, pour que les produits illicites échappent aux contrôles frontaliers et de sécurité.

Les **structures commerciales légales** permettent aux GCO d'opérer dans l'économie légale et de mélanger les profits illégaux aux profits légaux. Les groupes criminels possèdent ou établissent des structures commerciales légales, en infiltrent ou persuadent les dirigeants de coopérer par des pots-de-vin ou des menaces.

Les GCO tirent également profit de la **tolérance sociale** à l'égard de certains crimes. La vente de cannabis, de drogues psychoactives et de produits de contrefaçon de luxe sont les activités qui sont le plus tolérées au niveau social, selon l'idée largement répandue que ce sont des crimes sans victimes.

Les GCO se livrent à une **analyse des profits et des risques** lorsqu'ils souhaitent pénétrer différents marchés criminels. Dans la plupart des cas, ils sélectionneront les marchés où les profits sont élevés et les risques faibles. Ainsi, la contrefaçon de produits, la fraude et la production et distribution de produits psychoactifs génèrent des profits élevés mais entraînent des risques faibles.

Dans de nombreux cas, les GCO sont à même de réagir rapidement aux **changements législatifs**. Ainsi, l'interdiction de certaines substances entraînera la création de nouvelles substances psychoactives dont les formules ne sont pas couvertes par la législation nationale, ou qui utiliseront des substances anté-précurseurs non encore repérées. De nouvelles dispositions législatives à cet égard dans certains Etats membres compliquent de plus en plus la tâche des services répressifs chargés de lutter contre la production et la distribution de nouvelles substances psychoactives. Les GCO exploitent également le manque d'harmonisation entre les Etats membres dans divers pans de législation. Les frontières juridictionnelles sont pour l'essentiel sans importance pour les GCO et dans de nombreux cas, au contraire, elles facilitent même leurs activités, en particulier dans le secteur de la cybercriminalité.

Internet est un catalyseur significatif. Cependant, les activités criminelles facilitées par Internet ne devraient pas être confondues avec la cybercriminalité conventionnelle. Les infractions perpétrées grâce à Internet, par exemple la distribution de marchandises illicites sur des marchés en ligne, sont considérées non comme de la cybercriminalité, mais comme des délits facilités par Internet. Qu'il s'agisse de produits de contrefaçon, d'armes, de drogue, de documents d'identité frauduleux, d'animaux appartenant à des espèces protégées, de cartes de crédit contrefaites et de fausse monnaie, ou encore de matières premières et de données volées, tout peut s'acheter sur les marchés en ligne. En outre, Internet sert également à faire la publicité de services illicites tels que l'expertise professionnelle, les services liés à l'aide de l'immigration illégale et des contenus à caractère pédopornographique.

Les marchés illégaux en ligne hébergée dans le **Darknet** ont créé des sous-cultures et des communautés virtuelles au sein desquelles clients et fournisseurs peuvent échanger leurs expériences, donner leur avis sur des produits et services. Internet donne aux criminels l'impression de l'anonymat, et leur permet de commettre leurs infractions à distance, car la détection et la poursuite de ces dernières devient beaucoup plus difficile et complexe. Le recours à des serveurs proxy, à des réseaux assurant l'anonymat, à des monnaies virtuelles, à des plates-formes bancaires alternatives et l'adoption croissante de technologies informatiques dans le Cloud continueront d'avoir des conséquences pour les investigations et enquête des services répressifs. Ces évolutions posent des difficultés en ce qui concerne le recueil de preuves numériques forensiques et la collaboration dans des enquêtes où interviennent plusieurs juridictions.

III. Etat des lieux sectoriel

- **Cannabis**

La résine de cannabis est produite en Europe et acheminée vers l'Europe en large quantité depuis le **Maroc**. **L'Espagne**

le trafic de produits contrefaits en direction de l'UE.

Les produits sont pour l'essentiel originaires de Chine et d'Asie du Sud-Est.

De grands ports européens tels que Rotterdam, Anvers, Hambourg et Gioia Tauro sont des points d'entrée clés pour les produits de contrefaçon, qui pénètrent en Europe à la faveur du transport par conteneurs.

Le port et la zone de libre-échange de Tanger Med, au Maroc, commencent à émerger comme une plaque tournante clé pour l'expédition et devraient devenir vraisemblablement un point de passage important pour le transit de produits contrefaits à destination de l'UE.

- **Fausse monnaie : billets en euros**

Les matières premières pour la production de faux billets en euros sont de plus en plus vendues sur des marchés en ligne, que ce soit sur le Web de surface ou sur le Darknet.

La production de faux billets en euros fabriqués par un groupe criminel organisé basé dans la région de Naples a abouti à une augmentation du nombre de faux billets en circulation.

L'Italie demeure le centre de production de faux billets en euros en Europe.

On a relevé un recul notable de la production de faux billets en euros en Amérique latine.

- **Aide à l'immigration illégale**

L'an dernier, l'aide à l'immigration illégale par la mer par le centre et l'est de la Méditerranée a connu une augmentation exponentielle.

L'augmentation globale du nombre de migrants irréguliers entrant sur le territoire de l'UE se traduit par une demande encore plus grande pour les services d'aide proposés par des GCO en vue d'organiser la suite des déplacements sur le territoire européen et la transition vers une résidence légale dans les Etats membres.

L'aide à l'immigration illégale touche tous les Etats membres, qu'ils soient un point d'entrée vers l'Europe, un pays de transit ou de destination.

Le passage par le centre de la Méditerranée est devenu le principal point d'entrée de l'immigration illégale vers l'UE, notamment pour les Syriens qui arrivent en Italie en provenance de la Lybie via l'Egypte.

La pression migratoire à la frontière extérieure de l'UE le long de l'Est de la Méditerranée demeure forte, avec des flux migratoires toujours plus élevés en Mer Egée, et des tentatives de passage le long des frontières terrestres turco-bulgare et turco-grecque. Le nombre de migrants tentant d'entrer dans l'UE le long des frontières maritimes bulgare et roumaine (Mer noire) est en hausse.

Les passeurs facilitent les déplacements secondaires de migrants irréguliers du sud vers le nord et de l'est vers l'ouest le long de routes reliant les « hotspots » tels que Budapest, Milan, Francfort, Paris, Bruxelles ou Calais.

- **Traite des êtres humains**

Les trafiquants utilisent de plus en plus abusivement les règles concernant l'asile pour faire entrer leurs victimes sur le territoire de l'UE.

Ils utilisent de plus en plus Internet pour faire la publicité des services sexuels et de travail que peuvent fournir leurs victimes.

Les victimes proviennent de plus en plus des pays d'Europe centrale et orientale, et les pays de destination principaux sont l'Autriche, la Belgique, la France, l'Allemagne, la Grèce, l'Italie, les Pays-Bas, l'Espagne et le Royaume-Uni.

- **Atteintes aux biens commises en bandes organisées**

Dans de nombreux Etats membres, le nombre de cambriolages d'habitations commis par des groupes criminels itinérants très mobiles est en augmentation, ce qui impacte gravement un nombre élevé d'Européens, à quoi viennent s'ajouter les vols de véhicules à moteur et les vols de métaux (en diminution), le trafic illicite d'oeuvres d'art et les vols de cargaisons.

Les pays riches en vestiges archéologiques et oeuvres culturelles, comme la Grèce et Chypre, ou à proximité de zones de conflit sont plus exposés au risque de vol/trafic d'oeuvres d'art.

Les pays les plus exposés aux vols de cargaison sont l'Allemagne, les Pays-Bas et le Royaume-Uni ainsi que, dans une moindre mesure, la France, l'Italie et l'Espagne.

- **Trafic d'armes**

Le trafic intracommunautaire d'armes à feu converties ou remilitarisées demeure l'une des principales sources d'armes à feu illégales qui viennent ali-

est le principal point d'entrée pour ce type de trafic.

Le cannabis végétal est produit dans divers Etats membres sur des sites de culture à l'air libre et sous abri. Cependant, les **Pays-Bas** demeurent un pays clé d'origine pour ce type de produit.

- **Cocaïne**

Les GCO ont de plus en plus recours à la corruption systématique tout au long de la chaîne du trafic pour faire parvenir la cocaïne sur le territoire européen. Ces groupes, qui entretiennent des réseaux étendus d'employés, agents publics et sociétés commerciales légales corrompues dans divers Etats membres, sont à même de faire pénétrer leurs produits par différents points d'entrée, notamment les grands ports et aéroports.

La cocaïne provient d'un certain nombre de pays d'Amérique latine, notamment le Brésil, la Colombie, l'Équateur et le Pérou.

La région des Caraïbes, ainsi que Dubaï et l'Afrique de l'Ouest, sont des régions de transit clé pour le trafic de cocaïne en direction de l'Europe.

Il semblerait que la cocaïne fasse également l'objet de trafics vers l'Espagne via le Maroc, en empruntant des trajets, des méthodes de transport et des réseaux de passeurs déjà établis pour le trafic de cannabis.

Les GCO se servent des zones de libre-échange comme plaques tournantes pour coordonner les filières de fournitures mondiales de drogue.

La cocaïne provient également en Europe, bien qu'en de moindres quantités, via les Balkans de l'Ouest, par l'intermédiaire de GCO « multicartes ».

Les principaux points d'entrée de la cocaïne sur le territoire européen sont l'Espagne, les Pays-Bas, la Belgique et la France.

Sur le territoire de l'UE, la cocaïne est fréquemment transportée par des passeurs qui empruntent des vols intérieurs dans l'espace Schengen.

- **Héroïne**

L'anhydride acétique, le principal précurseur pour la production d'héroïne, continue d'être « exporté » depuis l'UE : les GCO s'en procurent sur le territoire européen et le font passer à des laboratoires en dehors de notre continent, où il servira à la production d'héroïne.

Les routes des Balkans demeurent les plus fréquentées pour le trafic d'héroïne à destination de l'UE.

L'Irak commence à émerger comme pays de transit significatif pour l'héroïne à destination de l'UE, acheminée via la Turquie.

L'Afrique de l'Ouest et l'Afrique de l'Est sont des régions de transit pour l'héroïne destinée à l'Europe. Des passeurs d'héroïne voyageant sur des compagnies aériennes partent de plus en plus d'Afrique de l'Est.

Le marché de l'héroïne en Fédération de Russie et en Asie centrale demeure d'une taille significative, et est probablement plus important que celui de l'UE.

- **Drogues de synthèse et nouvelles substances psychoactives**

La capacité de production et la disponibilité de MDMA dans l'UE ont augmenté de manière significative ces dernières années. Les comprimés de MDMA contiennent souvent des concentrations dangereusement élevées de substances actives.

La production de nouvelles substances psychoactives, notamment le conditionnement, l'emballage et l'étiquetage, se fait de plus en plus sur le territoire européen.

Les drogues de synthèse sont produites dans de nombreux Etats membres, même si on relève une grande hétérogénéité dans les substances produites et les niveaux de production.

Les Pays-Bas et la Belgique sont des centres de production clé pour diverses drogues de synthèses qui font aussi ensuite l'objet de trafic vers d'autres Etats membres et au niveau international, notamment les comprimés de MDMA, d'amphétamine et de méthamphétamine.

Des quantités significatives de drogues de synthèse produites dans différents Etats membres sembleraient faire l'objet d'un trafic vers des destinations extérieures à l'UE. Toutefois, les informations sont incomplètes en ce qui concerne l'ampleur précise de ce trafic et les destinations finales des drogues concernées.

- **Contrefaçon**

Peu de changements sont intervenus par rapport à la situation en 2013.

Les GCO utilisent les zones franches, telles que Tanger Med au Maroc, pour orchestrer

menter les GCO et autres criminels.

Au nombre des principales sources d'armes illégales dans l'UE figurent l'offre nationale, le trafic intracommunautaire et le trafic en provenance des pays des Balkans de l'Ouest.

Des armes et pièces d'armes illégales sont également régulièrement importées des Etats-Unis.

- **Infractions portant atteinte à l'environnement**

Le renseignement est encore peu au fait de l'ampleur de l'activité et des *modi operandi* des GCO et autres criminels opérant dans ce secteur.

Le trafic illicite de déchets dans l'UE semblerait l'oeuvre d'un petit nombre de GCO. Toutefois, des déchets illicites font souvent l'objet de trafic par les entreprises de traitement des déchets en marge de leurs activités légales dans leur secteur.

Le trafic illégal de déchets, en particulier les déchets des ménages, se déroule principalement sur le territoire des Etats membres ou entre Etats membres voisins.

Les déchets électroniques sont souvent acheminés clandestinement par conteneur en Afrique de l'Ouest et, dans une moindre mesure, en Asie du Sud-Est.

Les Etats membres de l'UE sont pays de destination, d'origine et de transit pour les espèces menacées, qui sont acheminées par diverses voies en fonction de leur origine.

- **Crimes de nature financière ou économique**

Des changements législatifs dans certains Etats membres peuvent inciter des GCO pratiquant actuellement la fraude au moyen des TIC à se réorienter.

Ce type de fraude a un impact significatif sur les économies des Etats membres qui, en 2012, avaient chiffré les pertes sous forme de TVA non acquittée à 177 milliards d'euros.

Les GCO qui fraudent les droits et accises, qui opéraient jusque-là dans le trafic de produits tels que l'alcool, le tabac et le carburant, se réorientent de plus en plus vers l'utilisation frauduleuse des mécanismes de suspension temporaire de droits pour importer ces biens légalement mais ne pas payer les droits et accises ensuite.

La fraude par le biais des TIC est souvent réalisée grâce à des sociétés créées par les fraudeurs.

Si l'on en croit le nombre d'usines illicites signalées, la Pologne demeure le principal point européen de fabrication illicite de tabac, mais on trouve aussi un nombre significatif d'usines illicites en République tchèque et en Slovaquie, ainsi qu'en Fédération de Russie et en Ukraine.

- **Blanchiment de capitaux**

La tendance émergente concerne le blanchiment de type « trade-based » (échange physique de biens) par des GCO ou des criminels individuels en liens avec les grandes plateformes financières asiatiques telles que Hong-Kong, Macao et Singapour.

On ne dispose que de peu d'informations encore sur les principaux acteurs et *modi operandi* associés au blanchiment, dont les opérations se complexifient en permanence.

Pour ce qui est du trafic d'argent en espèces, l'euro prédomine. Les mules qui transportent les espèces sont en général des hommes, et les nationalités chinoise et nigériane prédominent.

- **Cybercriminalité à but lucratif et cyber-attaques**

Ces deux dernières années ont été marquées par une augmentation du nombre et de la sophistication des cyber-attaques, facilitées par le mode de fonctionnement « multicartes » des GCO.

Parmi les menaces graves émergentes, on notera les attaques ciblées et persistantes contre des réseaux critiques, mais aussi l'apparition de maliciels qui s'attaquent aux banques, au commerce en ligne.

- **Fraude aux cartes de paiement**

Cette activité demeure très profitable pour les GCO et criminels qui la pratiquent. Les techniques innovent et se complexifient à mesure que les établissements améliorent leur sécurité informatique.

Une nouvelle tendance émerge : la prise en otage des données contre une rançon. L'utilisation du Darknet pour l'exploitation sexuelle et la pédopornographie constitue une menace très élevée qui mérite une attention particulière.

Les enfants visés plus particulièrement sont dans les pays en développement, en particulier d'Asie du Sud-Est.

Les compétences linguistiques jouent un grand rôle dans la détermination du territoire d'action des criminels : plus ils parlent de langues, plus le gisement de victimes potentielles est important.

- **Groupes criminels organisés**

Le nombre de GCO multicartes est en constante augmentation, et ils adoptent de plus en plus le modèle économique du crime en tant que service, tant en matière de cybercriminalité qu'en-dehors de ce secteur.

La très grande majorité des membres de GCO opérant dans l'UE sont de nationalités européennes, les GCO étant plurinationaux.

Très agiles, les GCO achètent les compétences nécessaires à leurs activités auprès de « free lance » qui n'appartiennent pas au GCO mais collaborent avec lui.

Les GCO coopèrent entre eux occasionnellement, dans le cadre d'une filière d'activité criminelle.

IV. Lignes d'action et priorités recommandées

- **Produits de contrefaçon ayant un impact pour la santé publique et la sécurité**

Affaiblir les GCO impliqués dans la production et la distribution de produits de contrefaçon et de qualité insuffisante violant les réglementations sanitaires et de sécurité

- **Cybercriminalité**

Combattre la cybercriminalité commise par des groupes organisés et générant de gros profits (par exemple la fraude en ligne), les cyber-délits qui causent de graves préjudices à leurs victimes (exploitation sexuelle des enfants, par exemple) et ceux qui affectent des infrastructures et systèmes d'information critiques dans l'UE.

- **Aide à l'immigration illégale**

Réduire l'abus des canaux légaux d'immigration par les GCO, notamment l'utilisation de documents frauduleux pour faciliter l'immigration illégale. Affaiblir les GCO opérant aux principaux points d'entrée dans l'UE et ceux qui pratiquent l'aide à grande échelle de l'immigration illégale.

- **Fraude aux échanges intracommunautaires**

Affaiblir la capacité des GCO et spécialistes de ce type de fraude.

Blanchiment

Intensifier l'investigation des activités financières des GCO et promouvoir des possibilités supplémentaires de récupération d'actifs.

- **Cambriolages et vols en bande organisée**

Cibler les groupes criminels organisés itinérants qui se livrent à ces activités dans plusieurs Etats membres.

- **Production de drogues de synthèse et de nouvelles substances psychoactives**

Réduire la production de ces drogues dans l'UE et affaiblir la capacité des GCO impliqués dans ces activités.

- **Traite des êtres humains**

Affaiblir les GCO impliqués dans la traite intracommunautaire d'êtres humains aux fins de l'exploitation sexuelle et pour le travail, notamment ceux qui utilisent des structures commerciales légales pour faciliter *ou dissimuler leurs activités criminelles.*

SOCTA 2013	SOCTA intérimaire 2015
. Produits de contrefaçon ayant un impact pour la santé publique et la sécurité . Cybercriminalité . Aide à l'immigration illégale . Fraude aux intérêts financiers de l'UE (TVA) . Blanchiment d'argent . Production de drogues de synthèse et trafic multicartes . Traite des êtres humains	. Produits de contrefaçon ayant un impact pour la santé publique et la sécurité . Cybercriminalité . Aide à l'immigration illégale . Fraude aux intérêts financiers de l'UE (TVA) . Blanchiment d'argent . Cambriolages et vols en bande organisée . Production de drogues de synthèse et trafic multicartes . Traite des êtres humains

COMPTE RENDU DE LA RÉUNION « IDENTITÉ SÉCURISÉE : UN ENJEU ÉCONOMIQUE ET SÉCURITAIRE MAJEUR, LA FRANCE EN RETARD »

Le 24 mai 2016 à Paris, à l'initiative de l'association FITS1, forum international des technologies et de la sécurité, et avec l'aide de SIA2, Secure Identity Alliance, les principaux acteurs de l'identité numérique, notamment Anne Bouverot, Présidente de Morpho (Safran), Didier Trutt, président-directeur général de l'Imprimerie Nationale, Frédéric Trojani, directeur général délégué de Gemalto, Philippe Goujon, député, rapporteur de la commission des lois constitutionnelles, Guillaume Poupard, directeur général de l'Agence nationale de sécurité des systèmes d'information (Anssi), Thierrry Derville, délégué ministériel aux industries de sécurité, se sont réunis pour évoquer la problématique de l'identité sécurisée. Ils ont constaté qu'il s'agissait d'un enjeu économique et sécuritaire essentiel pour la France, qui en dépit d'atouts importants, accuse un retard préoccupant dans la mise en oeuvre des politiques publiques devant garantir à chacun une identité sûre.

Voici un résumé des conclusions, partagées par la plupart des participants.

I. Un enjeu économique majeur

L'économie numérique ne pourra se développer sans que l'identité des utilisateurs ne soit établie en ligne pour acheter, vendre, voter, recevoir des aides individuelles, gérer un dossier santé numérique, déclarer ses revenus et payer ses impôts, signer un contrat, etc. Il faut une identité numérique forte. Chaque utilisateur doit avoir à sa disposition des dispositifs adaptés permettant d'établir ou de vérifier sans risque de fraude ou d'erreur l'identité déclinée sur le net.

Des exemples étrangers montrent que disposer d'une identité numérique sécurisée permet des progrès significatifs dans la modernisation de l'administration et des services publics et autorise d'importantes économies pour les finances publiques (2 milliards d'euros environ par an au Royaume- Uni).

L'identité, et notamment la biométrie, est aujourd'hui le support d'une industrie florissante. De nombreux marchés s'ouvrent à l'étranger : en Inde, en Afrique, dans les pays de l'est européen, etc.

II. Un enjeu de souveraineté et de sécurité nationale

La fraude à l'identité semble devenir une pratique courante : accès frauduleux aux prestations sociales ou de santé, titres d'identité et titres de séjour frauduleux, utilisation de faux titres par des organisations criminelles et terroristes, usurpation d'identité, etc. Le coût direct pour les finances publiques dépasse sans doute plusieurs milliards d'euros.

La sécurité des transports, et en particulier des voyages aériens, passe par la vérification de l'identité des passagers. La mise en place du PNR (Passenger Name Record) n'a de sens que si

les identités des voyageurs qui sont insérées dans la base sont authentiques.

La carte d'identité est le passeport de l'espace Schengen qui ne pourra fonctionner durablement que si ce titre est sécurisé et si l'identité qu'il établit est forte.

L'industrie de l'identité est une industrie souveraine. Elle est aujourd'hui en France, sous le contrôle d'intérêts français et, aux États-Unis, l'administration américaine n'hésite pas à imposer des contraintes très fortes aux entreprises non américaines qui souhaitent investir dans ce domaine.

III. La France en retard malgré ses atouts

La France est très en retard par rapport à de nombreux pays européens :16 États de l'Union européenne ont aujourd'hui une carte d'identité électronique, ce chiffre sera porté à 23 prochainement. Les pays de l'Europe du nord prennent une avance déterminante en identité électronique. En dépit de sa tradition politique, hostile à la délivrance de titres d'identité, la Grande-Bretagne développe une politique active, sous direction publique, pour doter les Britanniques d'une identité numérique sécurisée.

L'Inde comme de nombreux États africains ont engagé une politique volontariste pour doter leur citoyens d'une identité sûre indispensable à toute politique de développement : ni les procédures démocratiques, ni la scolarisation des enfants, ni l'attribution d'aides individuelles ou de prestations de santé ne peuvent être mises en oeuvre de façon rationnelle sans que les citoyens soient dotés d'une identité incontestable, établie souvent en recourant aux techniques de la biométrie.

Dans ce secteur, les entreprises françaises sont très performantes au niveau mondial et remportent de nombreux marchés : à ce titre, le retard français à utiliser des techniques vendues à l'étranger est souvent jugé paradoxal par nos partenaires.

Si les États ne mettent pas en place des procédures permettant d'établir une identité forte, les GAFA (Google, Apple, Facebook, Amazon) s'en chargeront pour répondre à la demande des acteurs économiques. À titre d'exemple, les acteurs de l'économie collaborative (prêter ou louer sa maison, sa voiture, organiser le co-voiturage, etc.) cherchent, pour des raisons évidentes, à s'assurer de l'identité des utilisateurs, et auront recours aux services d'identité numérique qu'on leur proposera.

Sauf à mettre en place au plus vite un régime incitatif et opérationnel d'identité numérique forte, la France ne pourra pas tenir les engagements qu'elle a pris au sein de l'Union européenne pour promouvoir une identité numérique forte et interopérable, élément essentiel du marché unique (règlement européen sur l'identification électronique et les services de confiance (eIDAS).

La loi votée en 2012, même partiellement censurée par le Conseil Constitutionnel, n'interdit pas la mise en place d'un titre d'identité électronique. En effet, la censure tient très précisément aux caractéristiques de la loi qui cherchait à combiner des finalités difficiles à concilier d'identité et de sécurité. Elle laisse des marges de manoeuvre au législateur pour élaborer de nouveaux textes sur l'un ou l'autre de ces deux thèmes.

Le coût pour les finances publiques de la mise en place d'une carte d'identité sécurisée peut être réduit si, à l'image de nombreux pays européens, on revient sur la gratuité complète du titre (par exemple en rendant onéreux son remplacement).

Notes :

1 https://www.fits-forum.org

2 https://www.secureidentilylliance.org

© Toute reproduction ou utilisation des articles de la revue du *GRASCO* est interdite sans l'autorisation préalable du *GRASCO* et ne peut être effectuée qu'en vue de l'utilisation qui aura été acceptée par le GRASCO

La Revue du GRASCO doit être citée de la manière suivante : L.R.D.G., année, n° xx, p. xxx

COMPTE RENDU DE LA TABLE RONDE SUR LA LUTTE CONTRE LE FINANCEMENT DU TERRORISME EN FRANCE

ORGANISÉE PAR L'ASSOCIATION DES ÉTUDIANTS DU MASTER 2 JURISTE SÉCURITÉ FINANCIÈRE, LE 19 MAI 2016 DANS LA SALLE DES CRIÉES DU PALAIS DE JUSTICE DE PARIS

La table ronde sur la lutte contre le financement du terrorisme a réuni Bruno Dalles, Directeur du Service Tracfin, Vincent Soulignac, Responsable Sanctions Financières Internationales et Lutte contre la Corruption d'HSBC France et Thibault de Montbrial, avocat au barreau de Paris et fondateur du centre de réflexion sur la sécurité intérieure. Les débats ont été animés par Chantal Cutajar, directrice du Master, directrice du GRASCO et directrice générale du CEIFAC, le Collège européen des investigations financières. Elle a précédé la remise des diplômes aux étudiants de la promotion « Michel Sapin 2014-2015 » par Bruno DALLES, directeur de TRACFIN en lieux et place de son parrain, ministre des Finances et des Comptes Publics.

Le choix du sujet a été dicté par l'actualité ainsi que par l'intérêt des étudiants appelés à exercer les fonctions de compliance officer au sein de divers établissements bancaires, d'assurances ou de l'industrie et donc à occuper des postes-clé dans cette lutte qui devient de plus en plus intense et complexe.

Les organisateurs remercient très sincèrement Yves Charpenel, Premier Avocat Général à la Cour de cassation, Chantal ARENS, Première Présidente de la cour d'appel de Paris, et Pascal Le Luong, Secrétaire général de la Première présidence de la Cour d'appel de Paris qui ont permis que la table ronde se déroule dans ce lieu prestigieux de la Salle des Criées du Palais de Justice de Paris. Ils remercient également Eric Chavent et la société ERI/Arrow Institute qui a apporté son soutien financier et logistique à l'organisation de la table ronde.

En guise d'introduction, Chantal Cutajar a rappelé la genèse du Master. Tout a débuté en 2001, à l'issue d'un colloque consacré à la lutte contre le blanchiment d'argent dans sa double dimension préventive et répressive réunissant des responsables des services juridiques des banques, assurances, mais aussi des avocats, des commissaires aux comptes, des experts comptables. Un consensus s'est dégagé autour de l'idée qu'il serait

utile de mettre en place une formation en matière de prévention du blanchiment et du financement du terrorisme, nous étions, au lendemain des attentas du 11 septembre.

C'est ainsi qu'a été porté sur les fonts baptismaux en 2004 le premier diplôme universitaire « Prévention des fraudes et du blanchiment » grâce à un partenariat étroit de nombreux professionnels et notamment celui du Service central de prévention de la corruption alors dirigé par Claude Mathon.

Dès l'année suivante, le ministère de l'Éducation nationale et de l'Enseignement supérieur homologuait le diplôme qui devenait une spécialité du Master droit des affaires. La formation a ensuite évolué pour répondre à la demande des services de conformité, de pouvoir disposer de juristes spécialisés dans le champ de la conformité.

Mais qu'est-ce que la conformité ?

Les établissements financiers et les entreprises transnationales sont confrontés à un enjeu majeur et à des risques nouveaux.

L'enjeu, pour l'entreprise est de mettre en cohérence ses valeurs, ses actions et ses projets avec les normes sociales et particulièrement avec les règles juridiques. L'un de ses actifs les plus importants est sa réputation. Il s'agit bien d'un risque de nature juridique qui expose les entreprises à des sanctions judiciaires, administratives ou disciplinaires mais également à des pertes financières qui peuvent se révéler gigantesques. Mais ce risque juridique est bien différent du risque de litige auxquels sont confrontés les services juridiques. Or, la crise de confiance qui touche toutes les catégories d'investisseurs depuis 2008 a mis les financiers au banc des accusés. Des entreprises sont condamnées à l'étranger pour corruption à des amendes très élevées et sont *blacklistées* par des ONG ou des fonds de pension avec de plus en plus d'impact dans la population. Des législations d'application extraterritoriales telles que le FCPA américain ou le UKBA britannique font peser sur les entreprises un risque pénal financier, économique mais également humain. Même la Chine vient de se doter d'une législation extraterritoriale sur le modèle américain. Dans un tel contexte, on comprend bien que la conformité va bien au-delà des exigences posées par le droit. Elle renvoie à des valeurs sociales qui transcendent le champ du légal et du licite.

Elle renvoie aussi à l'aptitude d'une entreprise à mettre en place des dispositifs, des process et des programmes qui doivent lui permettre de créer une culture de la conformité qui soit en adéquation avec les valeurs qu'elle souhaite respecter et aux objectifs qu'elle s'est fixée. Le développement de cette culture ne se traduit pas par une soumission mécanique à la loi et c'est pourquoi le juriste est un acteur majeur de la conformité. Il est en effet le mieux formé non seulement pour garantir la conformité de l'organisation par rapport à un système de normes et de valeurs, mais aussi parce qu'il sait concilier cet impératif avec la gestion du risque juridique dans un environnement où il faut bien le reconnaître, la soumission de l'entreprise à la norme juridique n'est ni automatique ni systématique et cela même si cette norme est clairement identifiée et correctement interprétée. Dans un tel contexte, le responsable de la conformité tient désormais un rôle essentiel au sein de l'entreprise. Mais c'est un rôle difficile parce qu'il doit en effet tenir le rôle de facilitateur au quotidien et savoir instaurer un climat de confiance. Tel est le profil des femmes et des hommes que nous voulons former au service d'une certaine conception de la

vie des affaires où l'éthique occupe une place centrale.

Chantal Cutajar : Comme c'est toujours le cas lorsqu'un attentat survient, la question du financement du terrorisme est propulsée en avant de la scène. Devant les représentants du GAFI en février 2015, Michel Sapin s'exprimait ainsi : « *L'argent est partout et tout le temps le nerf de la guerre : les terroristes ont, pour continuer à agir, besoin des financements indispensables à l'achat d'armes, de véhicules, de caches. La lutte internationale contre le financement du terrorisme est un rempart fondamental de la paix et de la sécurité dans le monde* ». La question de la compréhension du phénomène est centrale, parce qu'on ne peut bien lutter que si l'on connaît parfaitement l'adversaire. à l'occasion du G20 à Antalya, les 15 et 16 novembre 2015, le GAFI a rendu public un bilan de l'ensemble de ses travaux concernant les principaux schémas et sources de financement du terrorisme.

Question de Chantal CUTAJAR : Quelle est, de votre point de vue, qui peut être différent parce que vous parlez d'endroits différents, la définition du financement du terrorisme ? Quels sont les axes principaux de la lutte que vous déduisez de la situation actuelle ?

Thibault de Montbrial : Pour ma part, je pense qu'on doit plutôt qualifier les terroristes d'ennemis que d'adversaires. Le terrorisme est un moyen utilisé par des gens qui sont dans une logique de conquête planétaire au nom d'un projet politique :

l'islam radical sunnite. Pour ce faire, ils tentent d'affaiblir les démocraties occidentales. Les attaques terroristes perpétrées ces dernières années n'ont nécessité que de faibles moyens financiers (exemple : les paiements effectués pour les attentats du 13 novembre sont tous de l'ordre de 1000 euros). Ces dépenses pouvant être effectuées à l'aide des nouveaux moyens financiers.

Bruno Dalles : L'incrimination de financement du terrorisme a été créée le 15 novembre 2001 non pas pour l'islamisme mais pour l'ETA. Le financement du terrorisme, ce n'est pas nécessairement du blanchiment de capitaux, l'origine des fonds peut être licite. Le terrorisme c'est la guerre du pauvre : celui qui fait du terrorisme, c'est celui qui fait la guerre avec des petits moyens. La lutte contre le financement du terrorisme passe par l'établissement de liens entre les personnes, l'identification des associations de malfaiteurs et l'identification des personnes en voie de radicalisation ou qui reviennent de théâtres d'opération.

Vincent Soulignac : Les services de Conformité ont toujours dû s'adapter aux menaces en matière de criminalité financière, y compris le financement du terrorisme. Nous avons sans cesse besoin de renforcer les compétences et connaissances en la matière. Nous avons besoin d'avoir une sensibilité transversale sur ces problématiques, d'un point de vue juridique comme opérationnel, de bon sens et de curiosité.

Question de Chantal Cutajar : Pouvez-vous préciser ce que nous attendons des futurs Compliance officers ?

Bruno Dalles : Afin d'être efficaces, nous n'avons pas besoin d'obtenir un grand nombre de déclarations de soupçons peu approfondies, mais des déclarations de soupçons de qualité. Tracfin tente de venir en aide aux compliance officers en publiant des lignes directrices sur ce sujet. Pour être efficace, nous avons également besoin de coopérer à l'international. Une

information qui paraît anodine peut, une fois recoupée avec d'autres éléments, devenir une information cruciale. Une question se pose : devons-nous mettre en place une surveillance de masse ou bien nous focaliser sur quelques milliers d'individus présentant un risque important ?

Question de Chantal Cutajar : Qu'en est-il de la question du gel des avoirs ?

Vincent Soulignac : Le gel des avoirs obéit à une logique différente de la prévention du blanchiment. En matière de gel, les établissements financiers sont tributaires des informations (noms, date de naissance, homonymes connus etc.) données par les pouvoirs publics afin de détecter les personnes visées par les mesures de gel.

Ces deux logiques ne sont pas contraires, elles sont complémentaires. Une logique d'échange d'informations pour alimenter les cellules de renseignements financiers et les établissements financiers doit être suivie pour atteindre l'objectif fixé. Toutefois, il faut garder à l'esprit que le champ de vision des établissements financiers est limité principalement à la relation d'affaires.

Question de Chantal Cutajar : Qu'en est-il de la mise en place de la 4ème directive et quelles sont les mesures préconisées ?

Bruno Dalles : La transposition de la 4ème directive devrait arriver dans les prochains mois, au plus tard à la fin de l'année. La première mesure concerne la qualification de PPE nationales. Le deuxième domaine visé concerne les jeux et les casinos avec qui il faudra travailler pour faire évoluer leurs pratiques. Enfin, la 4ème directive permet une meilleure communication entre les cellules de renseignements financiers.

Question de Chantal Cutajar : L'un des freins principaux à cet échange de renseignements n'est-elle pas la nécessaire protection des données personnelles dans un État démocratique ?

Thibault de Montbrial : Il n'y a pas d'antagonisme entre la sécurité et la liberté : si vous n'êtes pas en sécurité, vous ne pourrez pas exercer vos libertés, même si elles ne vous ont pas été ôtées. Le renseignement financier est un élément essentiel d'un puzzle, mais ce n'est qu'une pièce. Le plus difficile, ce n'est pas le recueil, c'est l'analyse. Le risque c'est de se retrouver avec des instruments, qui compte-tenu du zèle des uns et des autres, aboutissent à ce que les cellules de renseignements se retrouvent submergées d'informations et ne soient plus en mesure de les traiter. Cette information ne servant plus qu'à comprendre les évènements, une fois qu'ils ont eu lieu. Les clients, personnes morales comme personnes physiques, ont l'impression que les établissements financiers, sous couvert de ce qui est demandé par les cellules de renseignements, ont tendance à recueillir des informations pas complètement essentielles à l'objectif poursuivi. Le risque d'atteinte aux libertés est là.

Vincent Soulignac : Il appartient aux banquiers d'interroger leurs clients dans le cas où certains éléments ne leur paraitraient pas cohérents avec la connaissance que les banquiers ont de ceux-ci. C'est ce qu'exige la loi. Cela ne veut pas dire que toute information doit et va être remontée à Tracfin. Pour être exploitable, la remontée d'informations doit être pertinente et c'est ce qui est attendu de TRACFIN et des superviseurs.

Bruno Dalles : La logique de conformité se retrouve en conflit avec d'autres logiques, comme la logique commerciale. C'est pourquoi la place de la conformité n'est pas la même dans tous les établissements.

Questions des participants

Nous avons des difficultés à identifier les associations potentiellement à risque, pouvez -vous nous éclairer là-dessus ?

Bruno Dalles : C'est un sujet compliqué pour tout le monde. Sur les typologies liées au financement via les associations il y aura des précisions dans les prochains rapports d'activité Tracfin. Avec d'autres partenaires assujettis, nous travaillons au recentrage sur les associations. En effet, sur les associations en termes de gestion, d'abus de confiance, de détournement de fonds, il y a beaucoup de choses à dire. Il faut avoir une réflexion sur les contrôles globaux des associations en plus de la vérification des mouvements de fonds.

Y aura-t-il une possibilité d'échange d'informations entre les différents assujettis ?

Bruno Dalles : Les possibilités d'échanges d'informations permises par la législation ne sont pas toutes forcément connues et correctement utilisées. Toutefois, permettre une trop grande possibilité de déclaration ne serait pas profitable, nous assisterions à des déclarations en cascade, au détriment de la pertinence de certaines d'entre elles.

Les établissements financiers pourront-ils avoir accès au fichier S ?

Bruno Dalles : Non car le fichier S a pour objectif de porter une attention particulière sur certains individus, ce qui n'est pas demandé aux établissements de crédit.

Est-ce cohérent pour l'Europe de conclure des accords avec la Turquie ?

Thibault de Montbrial : Concernant le double jeu de la Turquie sur ces questions, celle-ci a un agenda complexe qui n'est pas du tout le nôtre. La façon dont la Turquie utilise la carte des migrants comme un levier de pression sur l'Europe n'est qu'un des maux auxquels nous faisons face.

En tant qu'établissement bancaire, comment pouvons-nous intégrer aujourd'hui ces questions de géopolitique ?

Vincent Soulignac : Au-delà du risque légal (responsabilité pénale, civile, disciplinaire) qui pèse sur un établissement de crédit, il y a également le risque de réputation. De manière générale, un établissement bancaire essaie de gérer son risque de manière globale. Toutes les dimensions/composantes du risque contribuent à la définition d'une politique de gestion des risques que va suivre l'établissement.

Les américains ont levé les sanctions à l'encontre de l'Iran, les établissements de crédit vont-ils commencer à faire des affaires dans cette zone géographique ?

Vincent Soulignac : Ce n'est pas parce que les pouvoirs publics disent qu'il faut y aller qu'il n'y a pas de risque. Les gouvernements peuvent lever les sanctions, mais le secteur privé est toujours responsable de la gestion de ses risques et, sans aucun doute, sera tenu responsable s'il échoue.

Bruno Dalles : L'Iran est toujours sur la liste noire du GAFI. De plus, sa solvabilité est remise en cause depuis la chute du prix du pétrole. Enfin, il reste des tensions au sein de l'appareil politique iranien. En conclusion, les risques de faire des affaires en Iran restent très élevés malgré la levée des sanctions.

Quels sont les moyens à utiliser dans le cadre de la détection de la fraude documentaire ?

Bruno Dalles : Je pense qu'aujourd'hui un partenariat public/privé pourrait être envisagé à ce

sujet. Les banques devraient pouvoir avoir accès à une base publique ou mutualisée qui leur permettrait de vérifier si le document est un original. Les instances publiques sont d'accord sur le principe, c'est à la fédération des banques de prendre en main la mise en place de ce projet.

Comment les services de Tracfin prennent-ils en compte les évolutions technologiques du monde financier (blockchain, financement participatif…) ?

Bruno Dalles : Tracfin a alerté depuis longtemps sur la menace que représentent les nouveaux outils qui se développent. Il faut penser à assujettir ces nouveaux établissements spécifiques qui se développent et à les accompagner dans la détection qui sort parfois du cadre habituel.

Chantal Cutajar : À titre de conclusion, pourrais-je solliciter chacun d'entre vous sur une préconisation que vous appelleriez de vos voeux ?

Bruno Dalles : Nous avons besoin de gens formés pour équiper les services de lutte anti-blanchiment. Plus on aura de gens formés, plus on aura d'assujettis partenaires qui feront bien leur travail.

Thibault de Montbrial : On est en train de sortir de 70 ans de paix et dans les années qui viennent on va vraiment changer de mode de vie au quotidien sur les questions de sécurité, d'identité, de violence. À ce titre, ma préconisation serait : le changement d'état d'esprit et la résilience.

Vincent Soulignac : Face aux menaces existantes et nouvelles, le secteur financier a besoin de personnes compétentes et des profils diversifiés. Nous ne pouvons avoir des dispositifs efficaces que si nous avons des collaborateurs curieux ou « aguerris », disposant d'une certaine ouverture d'esprit et désireux d'adopter une transversalité dans la gestion des problématiques de criminalité financière.

Les étudiants se sont dits flattés et honorés que Bruno Dalles ait accepté d'être le parrain de leur promotion (2015-2016).

Le bureau de l'association du Master (Marie-Laure Bazi, Christelle Bour, Blandine Julé et Vincent Paolantoni)

association.m2jsf@gmail.com

FORUM DE NÎMES

ENVIRONNEMENT
NOUVELLES MENACES, NOUVEAUX DEFIS

11, 12 et 13 octobre 2016
Hôtel Atria - Nîmes

FITS : L'environnement face à la criminalité
IPSE et UpM : Le changement climatique et la Méditerranée

Remise du prix GAIA par Med 21
pour la sauvegarde et la sécurité environnementale
en Méditerranée

FiTS

nîmes métropole

IPSE

Union pour la Méditerranée
Union for the Mediterranean
الإتحاد من أجل المتوسط

En partenariat avec

saur

ECO EMBALLAGES

IFAW

WWF

/IRONN

THOMSON REUTERS

Organisé par

FFO FRANCE FORUM ORGANISATION

ENVIRONNEMENT
NOUVELLES MENACES, NOUVEAUX DEFIS

Sécurité et Criminalité environnementale sont les thèmes des conférences internationales organisées chaque année à Nîmes sous le patronage du Forum international des technologies et de la sécurité (FITS) et de Nîmes métropole.

Les intervenants sont des femmes et des hommes politiques, d'anciens ministres français et étrangers, des juristes de renom, des magistrats, des avocats spécialisés, des journalistes de grands média, des policiers, des gendarmes, des industriels, des armateurs.

PROGRAMME

Tables rondes

MARDI 11 OCTOBRE 2016

Le crime environnemental

14h45 – 16h **Un an de lutte contre la criminalité environnementale**
16h30 – 18h **Zoom sur le trafic d'espèces sauvages**

MERCREDI 12 OCTOBRE 2016

Le crime environnemental

9h – 0h30 **Prévention, réparation, répression de la criminalité environnementale**
11h – 12h30 **Compliance et criminalité environnementale**

L'eau dans le monde méditerranéen

L'impact du changement climatique sur la stabilité régionale en Méditerranée : l'exemple de l'eau

14h 45 – 16 h **Le partage de l'eau : conflits et coopération**
16h30 – 18h **L'eau : un enjeu de sécurité global § régional**

JEUDI 13 OCTOBRE 2016

L'eau dans le monde méditerranéen

8h30 – 10h **Les grands défis liés à l'eau en méditerranée : gérer la rareté**
10h30 – 12 h **Un outil de démocratie (hydro-diplomatie)**
13h30 – 15 h **L'eau ; un enjeu économique et de développement territorial**

Remise du prix GAIA 2016 PAR MED 21

INSCRIPTIONS : contact@nimesforum.fr