LA REVUE DU GRASCO

www.grasco.eu
www.larevuedugrasco.eu

N°27— Juillet 2019

Parution trimestrielle
Gratuite
ISSN 2272-981X

EDITORIAL

CHANTAL CUTAJAR

DIRECTRICE DU GRASCO

L'indépendance du parquet européen à l'épreuve de la nomination de son Procureur

L'indépendance du Parquet européen est une condition sine qua non de sa pérennité et de celle de l'État de droit. Le rapport intérimaire de Monica Macovei (PPE, roumaine) sur le projet de Parquet européen insistait sur le fait que ce Parquet destiné à lutter contre la fraude au budget européen devait être pleinement indépendant des gouvernements nationaux et des institutions européennes et sous contrôle démocratique. Il est crucial, jugeaient les députés, que ce Parquet soit soustrait à toute pression politique.

Rappelons que le 12 octobre 2017, les ministres de 20 États membres[1] ont adopté, dans le cadre d'une coopération renforcée, le règlement instituant le Parquet européen, chargé de lutter contre la fraude aux fonds européens et à la TVA dans ses dimensions transfrontalières et qui doit être opérationnel en 2020.

La garantie de son indépendance est inscrite à l'article 6 § 1 du règlement. Elle se traduit d'une part par l'injonction faite à l'ensemble des membres du parquet, y compris le personnel administratif, d'agir dans l'intérêt de L'Union dans son ensemble. Ils ne doivent solliciter ni accepter d'instructions d'aucune personne extérieure au Parquet européen, d'aucun État membre, d'aucune institution, d'aucun organe ou organisme de l'Union. D'autre part, les États membres et les institutions, organes ou organismes de l'Union doivent respecter l'indépendance du Parquet européen et ne pas chercher à l'influencer dans l'exercice de ses missions. Il est clair que le choix des hommes et des femmes sera déterminant.

La nomination du procureur européen ainsi que des procureurs délégués dans les États membres est soumise à une procédure censée garantir leur indépendance. Mais des textes à leur mise en œuvre, il y a un pas qui pourrait bien, s'il est franchi, décrédibiliser l'institution avant même qu'elle n'ait vu le jour.

En effet, la procédure qui doit amener à la désignation imminente

SOMMAIRE

ÉDITO 1

INTERVIEW :

JEAN-PAUL LABORDE, AMBASSADEUR ITINÉRANT DE L'ASSEMBLÉE PARLEMENTAIRE DE LA MÉDITERRANÉE, DIRECTEUR DU CENTRE D'EXPERTISE SUR LA LUTTE CONTRE LE TERRORISME, TITULAIRE DE LA CHAIRE CYBERSÉCURITÉ/CYBERDÉFENSE SAINT-CYR, SOGETI, THALES 5

NICOLE COCHET, DIRECTRICE GÉNÉRALE DU GROUPEMENT D'INTÉRÊT PUBLIC "JUSTICE COOPÉRATION INTERNATIONALE " (GIP JIC) 9

DOCTRINE JURIDIQUE :

BLANCHIMENT : LA PREUVE DE L'ORIGINE ILLICITE DES FONDS FACILITÉE, PAR PHILIPPE PETITPREZ 15

DOCTRINE SCIENCES CRIMINELLES :

LA CYBERCRIMINALITÉ BOURSIÈRE, PAR ALEXANDRE NEYRET ET ELISE NAIGEON- DE SANTI 22

LA THALASSOCRATIE CRIMINELLE, CLÉ DE COMPRÉHENSION DE LA CRIMINALITÉ ORGANISÉE TERRESTRE ?, PAR FLORIAN MANET 35

LA STRATÉGIE DU CRIME ORGANISÉ TRANSNATIONAL ET LES FAUX MÉDICAMENTS, PAR BERNARD LEROY 43

COMPLIANCE/CONFORMITÉ :

LE SORT DE LA RELATION D'AFFAIRES APRÈS UNE DÉCLARATION DE SOUPÇON, PAR MAMADOU DIALLO 52

ACTUALITÉ JURIDIQUE

ACTUALITÉS EN MATIÈRE DE CYBERPREUVE, PAR MYRIAM QUÉMÉNER 58

du procureur européen qui doit être **nommé d'un commun accord** par le Parlement européen et le Conseil a été jalonnée d'événements qui démontrent la difficulté de certains représentants des États à respecter ce principe d'indépendance. Elle se trouve aujourd'hui, au moment où nous publions ces lignes, dans une situation de blocage.

Pourquoi ?

Tout a bien commencé avec la publication le 19 novembre 2018 par la Commission européenne, de l'avis de vacance pour le poste de chef du Parquet européen[2]. Les candidatures ont d'abord été évaluées par les douze membres du comité de sélection chargés d'établir une liste restreinte de candidats qualifiés[3]. Début janvier 2019, le comité a procédé à une première présélection de 11 candidats qui ont été auditionnés le mercredi 30 et jeudi 31 janvier 2019. Le 4 février 2019, le comité a transmis au Parlement européen et au Conseil de l'UE une liste restreinte de 3 candidats pour occuper le poste de chef du Parquet européen.

Figurent, en première position, l'ancien procureur en chef de la Direction nationale anticorruption de Roumanie, Laura Codruţa Kövesi, ensuite le procureur général français, Jean-François Bohnert et, enfin l'Allemand, Andrés Ritter.

Le choix du comité de sélection de placer en première position Laura Codruta Kövesi n'est pas anodin et démontre l'indépendance des membres du comité de sélection.

Cette magistrate roumaine a en effet, joué un rôle décisif, en tant que procureur en chef de la Direction nationale anticorruption (DNA) entre 2013 et 2018, pour la mise en place des mesures de sauvegarde dans le cadre du « Mécanisme de coopération et de vérification (MCV) », imposées à la Roumanie lors de son adhésion à l'Union européenne le 1er janvier 2007 et destinées à combler les lacunes de la réforme judiciaire et de la lutte contre la corruption. En 2017, les progrès réalisés par la Roumanie étaient si importants que la Commission avait annoncé vouloir clôturer le MCV avant la fin de son mandat.

Mais en 2018, Laura Codruta Kövesi a été démise de ses fonctions par le nouveau ministre de la Justice, Tudorel Toader. Cette révocation s'inscrit dans l'offensive des partis politiques majoritaires au Parlement, visant à limiter drastiquement l'efficacité de la lutte contre la corruption, l'indépendance de la justice et la séparation des pouvoirs elle-même. C'est ainsi que plusieurs enquêtes ont été remises en cause, des décisions définitives de la Cour suprême ont été annulées, des personnes condamnées pour corruption ont été libérées sous prétexte de désengorger les prisons. Ces changements, constatés par le dernier rapport « MCV » ont atteint leur point d'orgue avec la création d'une section spéciale d'enquête sur les magistrats, placée hors de tout contrôle du procureur général et qui a suscité une vague de protestation de la part des magistrats roumains. La Commission européenne a immédiatement réagi et demandé au gouvernement roumain de se remettre sur le chemin des recommandations du MCV sans « *inverser les progrès accomplis ces dernières années* ».

Ce choix en faveur de Laura Kövesi ne pouvait pas convenir au ministre roumain de la Justice Tudorel Toader. En violation du principe d'indépendance, il a envoyé une lettre à ses collègues européens pour les dissuader de nommer Laura Codruţa Kövesi à la tête du Parquet européen. Mieux encore, des mesures de rétorsion à l'égard de la magistrate ont été prises telle qu'une citation à comparaître devant la section spéciale le mardi 26 février, alors qu'elle devait se rendre à Bruxelles le même jour pour être auditionnée. Ces comportements ont conduit le 14 février, la porte-parole de la Commission européenne, Margaritis Schinas, à rappeler que les trois candidats présélectionnés pour le poste de chef du Parquet européen devaient être traités « *équitablement* ». Elle a indiqué que la Commission suivrait de près le processus de nomination et rappelé que le chef du Parquet européen devait être nommé rapidement, afin de ne pas retarder la mise en place de l'organe, prévue en 2020.

Subissant ces pressions, le Coreper[4], qui réunit les ambassadeurs des États membres auprès de l'UE, a placé en première position, le magistrat français Jean-François Bohnert. Certes, il ne s'agit que d'un vote interne et indicatif uniquement destiné à permettre aux ambassadeurs du trio des prochaines Présidences du Conseil de l'UE, à savoir la Finlande, la Croatie et le Portugal – l'Allemagne ayant été exclue puisqu'elle a aussi un candidat - d'aller négocier avec le

Parlement européen.

La politisation du processus de désignation apparaissait ainsi au grand jour.

Ceci a amené les groupes S&D et GUE/NGL au Parlement européen à demander que le vote sur le classement des candidats pour le poste de chef du Parquet européen se tienne publiquement en commission LIBE et non à huis clos, en réunion des coordinateurs comme cela était prévu.

Le 27 février 2019 le Parlement européen désigne Laura Codruţa Kövesi comme candidate favorite avec 26 voix, le Français Jean-François Bohnert s'est placé en seconde position avec 22 voix, suivi de l'Allemand Andrés Ritter, qui n'a obtenu qu'une seule voix.

Le ministre roumain de la Justice, Tudorel Toader, n'a pas pour autant désarmé et n'a pas hésité, dans une lettre, publiée le 6 mars dans le *Financial Times*, à exposer ses arguments contre la nomination de Laura Kövesi, expliquant qu'il n'avait « *rien de personnel contre Laura Codruţa Kövesi* », mais que, « *d'après tous les éléments de preuve* » *en sa possession* « *émanant des juges, des procureurs et d'autres sources crédibles* », *Madame Kövesi* « *ne devrait pas être nommée à ce poste d'une importance capitale* ».

Nous sommes toujours, à l'heure où nous publions ces lignes, dans une situation de blocage. Elle pourrait se résoudre à la faveur du retrait annoncé mais pas encore acté, du candidat français. Il est pour le moins curieux qu'aucun média généraliste n'ait fait état de ce processus de désignation pour le moins chaotique et qui jette le discrédit sur une institution que les européens attendent de longue date et qui démontre malheureusement que le chemin qui doit conduire à l'édification d'une véritable Europe de la Justice est semé d'embûches. Le courage politique des membres du Conseil européen devrait les amener à résister aux pressions du gouvernement roumain et à désigner Laura kövesi. Il y va réellement de la crédibilité de la future institution judiciaire européenne.

Notes :

1 Allemagne, Autriche, Belgique, Bulgarie, Croatie, Chypre, République tchèque, Estonie, Finlande, France, Grèce, Italie, Lettonie, Lituanie, Luxembourg, Portugal, Roumanie, Slovaquie, Espagne et Slovénie. Depuis Malte (20 août 2018) et les Pays-Bas (1er août 2018) ont adopté le règlement.

2 Les critères de sélection comprennent, entre autres, au moins quinze années d'expérience professionnelle en tant que membre actif du ministère public ou du corps judiciaire et au moins cinq années d'expérience en tant que procureur chargé d'enquêter sur des délits financiers. L'avis de vacance précise aussi que le candidat devra pouvoir exercer un mandat complet de 7 ans et acte la prolongation à 70 ans de l'âge de la retraite.

3 Ces douze personnalités ont été choisies parmi d'anciens membres de la Cour de justice et de la Cour des comptes européenne, d'anciens membres nationaux d'Eurojust, des membres des juridictions nationales suprêmes, des procureurs et des juristes, dont une proposée par le PE.

4 Le Comité des représentants permanents.

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— http://www.larevuedugrasco.eu

Adresse mail : information@grasco.eu

Directrice de la revue du GRASCO : Chantal CUTAJAR

Rédactrice en chef : Jocelyne KAN

Rédacteur adjoint—Conception : Sébastien DUPENT

COMITÉ SCIENTIFIQUE DU GRASCO

FALLETTI François

Ancien magistrat, il a exercé plus de 15 ans au sein de la Direction des affaires criminelles et des Grâces du ministère de la Justice dont il a été le directeur de 1993 à 1996. Il a ensuite été procureur général près les cours d'appel de Lyon, Aix en Provence et Paris. Avocat général à la cour de cassation, il a été le membre français de l'Unité Eurojust à La Haye (2004-2008). Il a également exercé les fonctions de président de l'association internationale des procureurs (2007-2010), de secrétaire général de l'association internationale des procureurs francophones (2009-2018), et assuré la mission de conseiller spécial auprès de Madame le Commissaire européen pour la Justice (2016-2017). Docteur en droit, diplômé de Sciences-po Paris, il est l'auteur de plusieurs ouvrages, notamment du "précis de droit pénal et de procédure pénale" (PUF 7e édition 2018) coécrit avec Frédéric Debove. Il est aujourd'hui avocat au Barreau de Lyon.

LABORDE Jean-Paul

Conseiller honoraire à la Cour de cassation et ancien Directeur exécutif du comité des Nations Unies chargé de la lutte contre le terrorisme avec rang de Sous-Secrétaire général. Il est actuellement ambassadeur itinérant de l'Assemblée parlementaire de la Méditerranée, Directeur du Centre d'expertise sur la lutte contre le terrorisme, titulaire de la Chaire Cyber à l'École de St-Cyr Coëtquidan et Conseiller spécial de l'Initiative mondiale de lutte contre le crime transnational organisé.

LEBLOIS-HAPPE Jocelyne

Professeur à L'Université de Strasbourg et chargée de cours à l'Université Albert-Ludwig de Fribourg-en-Brisgau (Allemagne). Elle est membre du groupe European Criminal Policy initiative et du groupe d'experts sur la politique pénale de l'UE auprès de la commission européenne.

MATHON Claude

Avocat général honoraire à la Cour de cassation (chambre criminelle). Après avoir Développé une carrière essentiellement comme procureur de la République, il a dirigé le Service Central de prévention de la Corruption (2001). Spécialisé en intelligence économique, il a présidé à la rédaction de trois rapports : « Entreprise 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 ».

PRADEL Jean

Ancien magistrat (de 1959 à 1969), il obtient l'agrégation en droit privé et en sciences criminelles en 1969. D'abord affecté à la Faculté de droit de Tunis, il devient professeur à la Faculté de droit à Poitiers (1972). Depuis 2003, il est professeur émérite de l'Université de Poitiers. Il est directeur honoraire de l'institut de sciences criminelles de Poitiers. Il a présidé l'Association française de droit pénal. Il participe à de nombreux congrés internationaux. Il est l'auteur de nombreux ouvrages, notamment - Droit pénal général, Procédure pénale, Droit pénal comparé, Droit pénal spécial en collaboration avec M. Danti-Juan, Droit pénal européen avec G. Corsten et G. Vermeulen.

SORDINO Marie-Christine

Professeur à l'Université de Montpellier, Directrice de l'Équipe de droit pénal (EDPM-UMR 5815), Directrice du Master 2 Droit pénal fondamental et du Master 2 Pratiques pénales. Elle est auteur de nombreux ouvrages dont Mutations du droit pénal, entre affirmation de valeurs et protection des libertés ?, Faculté de droit et science politique de l'Université de Montpellier, coll. Actes de colloque, décembre 2017 ; Lanceur d'alerte : innovation juridique ou symptôme social ?, Faculté de droit et science politique de l'Université de Montpellier, coll. Actes de colloque, décembre 2016 ; Innovation numérique et droit pénal économique et financier : enjeux et perspectives, Faculté de droit et science politique de l'Université de Montpellier, coll. Actes de colloque, mai 2016 . Elle est cotitulaire de la chronique « Sanctions » au Bulletin Joly des entreprises en difficulté (BJE), titulaire de la chronique « Droit de la concurrence », RSC et expert auprès d'organismes nationaux et internationaux.

STRICKLER Yves

Docteur de l'Université de Strasbourg, Maître de conférences à Toulouse, Professeur à Nancy, puis à Strasbourg, il exerce depuis 2010 à l'Université Côte d'Azur. Membre du Haut Conseil de la Magistrature de la Principauté de Monaco, il dirige à Nice l'Institut fédératif de recherche "interactions".

STORCK Michel

Professeur émérite à l'Université de Strasbourg.

INTERVIEW

JEAN-PAUL LABORDE,

AMBASSADEUR ITINÉRANT DE L'ASSEMBLÉE PARLEMENTAIRE DE LA MÉDITERRANÉE, DIRECTEUR DU CENTRE D'EXPERTISE SUR LA LUTTE CONTRE LE TERRORISME, TITULAIRE DE LA CHAIRE CYBERSÉCURITÉ/CYBERDÉFENSE SAINT-CYR, SOGETI, THALES

PROPOS RECUEILLIS PAR JOCELYNE KAN, RÉDACTRICE EN CHEF DE LA REVUE DU GRASCO

L.R.D.G. : Quelles sont les missions du Centre d'expertise sur la lutte contre le terrorisme (CELT) et de la Chaire Cybersécurité/Cyberdéfense Saint-Cyr, Sogeti, Thales ?

Le Centre d'expertise sur la lutte contre le terrorisme (CELT) a été créé à l'initiative des Écoles de Saint-Cyr en décembre 2015, en partenariat avec la Direction exécutive du comité contre le terrorisme du Conseil de Sécurité de l'ONU (DECT), la Fondation Saint-Cyr et la SNCF.

Il est actuellement sous ma direction. Il organise des colloques sur les sujets les plus sensibles de la lutte contre le terrorisme, publie les actes de ceux-ci, des newsletters et il abritera bientôt une thèse sur ces questions. Il aide en particulier à réfléchir sur le rôle des Armées dans cette lutte et plus particulièrement de l'Armée de Terre. Il le fait, en considération des nouvelles menaces, à l'extérieur et à l'intérieur de la France, en insistant sur la liaison entre les deux théâtres d'opérations. Ainsi, hors du territoire français, avec par exemple l'opération Barkhane au Sahel et, sur le territoire français, les nouvelles attributions de l'Armée de Terre dans l'opération Sentinelle, la création d'un commandement Terre pour le territoire national au sein de l'Armée de Terre et des fonctions de plus en plus importantes dans l'appui aux autorités civiles et des compétences militaires y compris par exemple en matière de secours et de médecine de guerre comme ce fût le cas lors des attentats du 13 novembre 2015. Tout cela est possible grâce à la place du CELT aux Écoles de St-Cyr qui lui permet ce regard unique. Ce positionnement lui permet également de se projeter, au plan international, avec sa participation, en autres, à divers évènements de

l'ONU, de l'Assemblée parlementaire de la Méditerranée ou encore de l'Initiative mondiale de lutte contre la criminalité transnationale organisée.

La Chaire Cybersécurité/Cyberdéfense des Écoles de Saint-Cyr Coëtquidan en partenariat avec Sogeti a inauguré le 2 juillet 2012, la Chaire de Cyberdéfense et Cybersécurité Saint-Cyr, Sogeti, Thales. En faisant converger les mondes militaire et civil dans la préoccupation essentielle de la sécurité des systèmes d'information, mais aussi dans le cadre de la formation au leadership dans ce domaine, elle permet de mieux anticiper les futures cybermenaces, de présenter des solutions innovantes pour relever les défis juridiques liés à la lutte contre ces menaces ainsi que ceux qui sont en relation avec les nouvelles utilisations de l'intelligence artificielle.

L.R.D.G. : Comment mieux identifier, comprendre et prévenir la menace terroriste et ses évolutions ?

Plusieurs degrés de réponses permettent de mieux cibler la menace terroriste actuelle. Tout d'abord évidemment, il faut disposer d'un excellent outil du renseignement tant à l'extérieur qu'à l'intérieur du pays. La Direction du Renseignement militaire (DRM), la Direction générale de la sécurité extérieure (DGSE), la Direction générale de la sécurité intérieure (DGSI), la Direction générale de la Gendarmerie nationale (DGGN) et le Service central du renseignement territorial (SCRT) ainsi que tous les services de terrain, y compris le Service national du renseignement pénitentiaire (SNRP), permettent d'obtenir d'excellentes informations. Mais ce n'est pas tout, il faut ensuite bien croiser ces informations pour obtenir un renseignement fiable. Il faut aussi échanger ce renseignement avec les services d'autres pays également menacés par le terrorisme, qu'ils soient du Sud, du Nord, de l'Est ou de l'Ouest du Globe. Le maître mot en la matière s'appelle « Confiance » en ayant avec ces services des relations sûres. En effet, les menaces varient et sont très fluctuantes et pour les appréhender au plus près, il faut encore et toujours croiser le renseignement. Par exemple, hier les combattants terroristes étrangers allaient rejoindre la Syrie et l'Irak, alors qu'aujourd'hui ils sont au Sahel, en Asie du Sud-Est, en Asie du Sud et en Asie centrale. Certains reviennent directement en Europe et il faut les suivre. Mais, il semble qu'actuellement, la menace endogène est la plus dangereuse ; toutefois, il ne faut pas baisser la garde sur les combattants terroristes étrangers les plus aguerris qui sont aujourd'hui à l'étranger. Donc, il faut bien comprendre que la menace est multiforme et qu'il faut être prêt à la contrer sur plusieurs fronts. Cela implique une grande coordination et une excellente coopération internationale, en commençant par les pays de l'Union européenne mais en sachant qu'il faut étendre cette coopération bien au-delà, avec, en particulier, les services des pays des zones où l'on a identifié la présence de combattants terroristes étrangers. Il faut aussi impliquer la société civile sans laquelle rien ne pourra se faire. En France, c'est un point très important à développer, les citoyens restant souvent dans leur coin et les autorités également. Enfin, il faut aussi avoir à l'esprit que le renseignement ne suffit pas ; il faut aussi combattre l'impunité en traduisant les terroristes en justice pour faire bien prendre conscience qu'il convient de ne jamais oublier les victimes et que les principes de l'État de droit sont toujours premiers.

L.R.D.G. : Quelle menace potentielle présentent les personnes suivies pour radicalisation et le risque lié aux revenants ?

Sur le premier point, il est une constante qu'il faut toujours garder à l'esprit : la radicalisation s'effectue presque toujours, en plusieurs étapes. Il est rare qu'une personne se radicalise du jour au lendemain. Dans l'affaire de Strasbourg par exemple, on voit bien que le terroriste avait un réseau, des appuis, etc. Il faut, à cet effet, souligner le rôle déterminant du nouveau Service national du renseignement pénitentiaire, en particulier vis-à-vis des terroristes incarcérés et qui risquent de sortir bientôt après avoir purgé leurs peines ainsi que des délinquants membres de la petite criminalité organisée qui risquent de se radicaliser.

En ce qui concerne le second point, il faut diviser les revenants en deux groupes distincts. Il y a « les revenants directs » qui

reviennent de Syrie ou d'Irak sans faire de détours dans d'autres pays, ils sont très bien repérés et identifiés ; tous font l'objet d'un suivi judiciaire. Par contre, les plus dangereux sont, à mon sens, ceux qui ne rentrent pas tout de suite et vont continuer à commettre des actes terroristes dans d'autres pays ou à s'aguerrir ailleurs pour retourner plus tard lorsque nous ne les attendrons plus.

L.R.D.G. : Que regroupe la notion de cyberterrorisme et comment se manifeste le terrorisme sur les réseaux ?

Attention : il convient d'être très prudent et de ne pas faire d'amalgame. Pour l'instant, nous n'avons pas de preuve qu'il y ait eu de cyberterrorisme au sens pénal du terme. En tout cas, s'il existait, ce serait tout simplement un acte de terrorisme tel que nous en connaissons la définition dans les textes actuels commis à l'aide des moyens cyber.

Pour l'instant, il n'y a pas eu d'attaque directe. Hélas, cela ne veut pas dire qu'il n'y en aura pas dans l'avenir ! Par contre l'utilisation des outils tels qu'Internet ou encore des messageries cryptées constitue des méthodes souvent utilisées par les organisations terroristes pour recruter leurs troupes ou encore pour perpétrer leurs attaques. Cela est fréquent et continue de l'être. Il faut être très vigilant et à cet égard, la loi sur le renseignement du 24 juillet 2015 est un outil important. Toutefois, il reste toujours difficile d'établir un juste équilibre entre les renseignements nécessaires à notre protection et le respect de la vie privée. Nos principes démocratiques sont, hélas mis à rude épreuve par ces attaques terroristes qui nous obligent à prendre des mesures qui, inévitablement, restreignent nos libertés… mais n'est-ce pas à ce prix que nous protégeons nos concitoyens ? En tout cas, cet exercice est, il faut l'avouer, périlleux.

L.R.D.G. : Quelles sont les recommandations du CELT sur la lutte contre le terrorisme et la radicalisation ?

Il faut, à tout prix, s'occuper des jeunes, les former, leur donner des outils de réflexion sur leur avenir ou leur non avenir s'ils s'engagent sur les pentes du terrorisme. Avant tout, il faut qu'ils acquièrent une capacité de jugement, un vrai libre arbitre. Pour les délinquants plongés dans la criminalité organisée de moyenne importance, le problème est certes plus complexe car ils sont déjà impliqués dans une criminalité souvent violente. Il faut les détecter dès le départ et en particulier en prison. En tout cas, s'ils sont difficilement récupérables. Il ne faut pas baisser les bras et leur démontrer qu'en tout cas il n'y a pas d'avenir en optant pour cette voie…, c'est une voie de mort. Et ensuite, il faut bien utiliser la répression et les infractions-obstacles telles que l'association de malfaiteurs à visée terroriste pour prévenir toute action de leur part lorsque les faits sont prouvés.

L.R.D.G. : Y a-t-il un lien entre le terrorisme et la criminalité organisée ?

Même si les buts de ces organisations criminelles sont différents, il y a des liens de fait entre criminalité organisée et organisations terroristes. Ces dernières ont un besoin évident de soutenir leurs troupes, de maintenir leurs communications, de soudoyer l'environnement humain, etc., mais leur but ultime est effectivement de semer la terreur dans la population générale ou de contraindre un gouvernement à faire ou ne pas faire quelque chose alors que le crime organisé a pour but d'obtenir un avantage financier ou tout autre avantage matériel. En tout cas, les trafics en tout genre alimentent les conflits et, par effet, induit le terrorisme bien que les actes terroristes en eux-mêmes ne coûtent pas très cher.

L.R.D.G. : Au mois de janvier 2019, dans un entretien au Parisien, le directeur de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a déclaré redouter une « succession d'attaques massives » estimant que tous les éléments techniques sont réunis pour un « cyber Pearl Harbor ». D'après vous, nos entreprises sont -elles prêtes à surmonter une telle situation ?

Certes, nos entreprises doivent être prêtes mais aussi nos administrations, nos armées, la société civile. C'est tout un ensemble qu'il faut mettre en place. En outre, je voudrai insister sur un aspect qui révolutionne notre pensée et nos façons de faire : il faut un partenariat public-privé

dans cette lutte contre la cybercriminalité. Par exemple, dans nos armées, il est évident que pour les systèmes d'armes, les avions, les navires de guerre, la collaboration public-privé est indispensable tout en respectant les règles d'éthique indispensables. C'est pourquoi les Chaires offrent des lieux de rencontre et de collaboration neutres et pour lesquels l'éthique peut être plus facilement respectée qu'évidemment dans le cadre de rapports professionnels entre public et privé.

L.R.D.G. : Les réponses judiciaires en matière de terrorisme et de cybercriminalité sont-elles adaptées ?

En matière de terrorisme elles le sont, absolument. On voit bien la réactivité du parquet de Paris qui coordonnait toutes les procédures. Il faut espérer qu'avec le nouveau parquet national antiterroriste, la réponse du parquet pourra être encore plus réactive et plus coordonnée qu'actuellement et que les moyens qui seront mis à sa disposition seront à la hauteur des réponses attendues bien que le parquet de Paris ait parfaitement répondu aux attentes et aux défis auxquels il a dû faire face durant ces dernières années.

Pour ce qui est de la cybercriminalité, les réponses, au niveau national sont encore trop disséminées, voire éparpillées. Il n'y a pas moins de 470 infractions dénombrées pour les couvrir. Les policiers et les gendarmes, sous l'impulsion de l'ANSSI, ont déjà bien avancé. Pourtant, il semble que l'autorité judiciaire n'ait pas pris toute la mesure de la menace lorsque des cybercriminels lui sont déférés. Il faut sensibiliser davantage les magistrats par de la formation continue mais aussi en augmentant la formation initiale à l'École Nationale de la Magistrature qui ne propose pas encore assez de modules sur ces sujets critiques. En effet, si l'on réfléchit bien au sujet, il vaut mieux aujourd'hui faire un détournement à la banque par cyberattaque que par vol à main armée. Les peines prononcées ne seront pas du tout les mêmes et il faut que ça change !

L.R.D.G. : La coopération internationale pénale doit-elle être améliorée pour lutter contre le terrorisme et la cybercriminalité ?

Je dirai que la coopération internationale contre le terrorisme peut et doit toujours être améliorée. Cependant, après les attaques à New-York, celles de Madrid, Londres et plus récemment Paris, les instruments internationaux de lutte contre le terrorisme sont en place tant au niveau international que régional pour une coopération véritable. Il en est de même pour les résolutions contraignantes du Conseil de sécurité des Nations Unies. Il faut aussi souligner que, dorénavant, aucun État dans le monde ne peut se permettre de soutenir le terrorisme international tel que défini par ces divers instruments et résolutions, d'autant que l'Assemblée générale de l'ONU a également adopté une stratégie mondiale de lutte contre le terrorisme.

Pour la cybersécurité ou la cyberdéfense, nous n'en sommes pas encore là hélas... Le groupe d'experts de l'ONU peine à se mettre d'accord sur des fondamentaux tandis que le Conseil de l'Europe, avec la convention contre la cybercriminalité et les négociations de son protocole sur la coopération internationale en matière pénale, fait des progrès. On pourrait aussi utiliser la Convention contre la criminalité transnationale organisée aussi appelée Convention de Palerme...mais hélas, la prise de conscience de la communauté internationale sur la cybercriminalité n'est pas encore au niveau auquel il le faudrait.

Il faut nous unir tous pour que cette prise de conscience soit rapide car les dégâts commis par la cybercriminalité sont énormes et on ne peut y faire face qu'ensemble. Rappelons-nous les dégâts déjà commis sur nos hôpitaux ou nos entreprises. Il faut seulement espérer que, contrairement à ce qui se passe la plupart du temps, nous n'attendrons pas de devoir faire face à une attaque massive telle que décrite par le Directeur de l'ANSSI avant d'agir. Hélas, la communauté internationale est toujours dans un mode réaction et non d'action, comme on a pu le voir sur le terrorisme. Mobilisons-nous pour qu'il en soit autrement pour la cyber !

INTERVIEW

NICOLE COCHET,

DIRECTRICE GÉNÉRALE DU GROUPEMENT D'INTÉRÊT PUBLIC "JUSTICE COOPÉRATION INTERNATIONALE " (GIP JIC)

PROPOS RECUEILLIS PAR JOCELYNE KAN, RÉDACTRICE EN CHEF DE LA REVUE DU GRASCO

L.R.D.G. : Comment le Groupement d'Intérêt Public "Justice Coopération Internationale " (GIP JCI) est-il composé et quelles sont ses missions ?

Je commencerai, si vous le voulez bien, par un très bref rappel historique. Justice Coopération Internationale (JCI) est l'émanation de l'association ACOJURIS (Agence de coopération juridique internationale), elle-même successeur de l'association ARPEJE (Association pour le Renouveau des Échanges Juridiques avec l'Europe centrale et orientale), l'une et l'autre résultant d'une initiative du ministère de la Justice visant à assurer sa présence sur la scène de la coopération judiciaire internationale. Celle-ci, alors naissante, a pris, à partir des années 2000 et du développement de l'espace judiciaire européen, une importance de plus en plus grande : d'abord entre les États membres, ensuite en direction des pays candidats à l'accession à l'Union européenne, puis encore en direction des pays dits du voisinage.

C'est pour mettre le monde judiciaire dans son ensemble mieux en mesure de répondre à cette montée en puissance qu'a été décidée en 2012 la transformation d' ACOJURIS en un Groupement d'intérêt public, Justice Coopération Internationale (JCI), en vue d'associer le plus grand nombre d'acteurs aux activités de la coopération judiciaire internationale.

JCI compte six membres fondateurs : le ministère de la Justice (avec ses directions, services, écoles non autonomes et agences), ses écoles indépendantes (l'École nationale de la magistrature, l'École nationale de l'administration pénitentiaire) et les principales professions judiciaires (avocats, notaires et huissiers, aujourd'hui commissaires de justice), qui sont membres du Groupement via leurs institutions représentatives : le Conseil National des Barreaux (CNB), le Conseil Supérieur du Notariat (CSN) et la Chambre nationale des huissiers de justice (CNHJ), devenue au 1er janvier 2019, la Chambre nationale des commissaires de justice.

JCI a ainsi vocation à appuyer l'ensemble des acteurs du monde judiciaire, y compris ceux qui ne sont pas membres du Groupement, dans leurs activités de coopération. Mobilisant auprès d'eux une expertise pluridisciplinaire, il peut prétendre se voir confier, en gré à gré, ou remporter, après mise en concurrence, puis mettre en oeuvre, des programmes de coopération juridique et judiciaire correspondant à la stratégie de coopération internationale du ministère de la Justice, largement partagée par ses

membres, et auxquels ceux-ci souhaitent participer.

La technicité de l'équipe JCI, forte de dix-huit membres à son siège, mais également des experts internationaux à long terme installés dans les pays bénéficiaires, eux-mêmes appuyés par des assistants nationaux pris en charge dans le cadre des projets en matière de préparation et de gestion de projets, lui permet d'accompagner les pays bénéficiaires des projets dans leur démarche de modernisation et de professionnalisation de leurs systèmes judiciaires. II s'agit de les aider à les réformer, dans la perspective de les voir se rapprocher des standards de l'État de droit tout en facilitant l'accès de leurs citoyens aux droits fondamentaux. En même temps, cette coopération nous offre les moyens d'un rayonnement de notre système juridique et judiciaire, et un retour en termes de connaissance des systèmes étrangers, et de ceux qui les mettent en oeuvre. C'est un enrichissement, mais également un instrument de facilitation et d'amélioration de la coopération opérationnelle avec les États concernés, tant dans le domaine pénal que dans le domaine civil.

JCI exerce tout d'abord une veille continue et efficace sur les programmes de coopération judiciaire proposés par les bailleurs de fonds internationaux, qui sont essentiellement l'Union européenne, l'Agence française de développement, la Banque mondiale, l'UNICEF, le Programme des Nations unies pour le développement, pour être en mesure d'informer tout partenaire potentiellement concerné sur celles de ces propositions susceptibles de les intéresser.

Si la décision d'accepter une offre formulée de gré à gré ou de concourir pour les offres soumises à concurrence, est prise, JCI doit, avec l'appui des partenaires internes intéressés, construire le projet, souvent sur la base d'une mission exploratoire conduite et organisée soit de sa propre initiative, soit de concert avec le bailleur de fonds. Une fois construit, le projet doit encore être soutenu auprès des bailleurs et bénéficiaires. Enfin, lorsqu'il est retenu, JCI le met en oeuvre avec l'appui du ou des experts à long terme internationaux qui lui sont détachés ou des institutions participantes, et des experts nationaux qu'il a recrutés sur place.

Dans ce contexte, le groupement assure l'organisation et la logistique des activités prévues par le plan de travail : missions d'expertise à moyen terme et court terme, visites d'études en France ou dans d'autres pays européens.

Il n'est pas indifférent de mentionner que JCI, qui reçoit les fonds de la part du bailleur, porte de ce fait la responsabilité administrative, financière et logistique de leur emploi. Cela permet aux membres et institutions parties prenantes de se libérer des tâches administratives liées au fonctionnement du projet, pour consacrer toute leur énergie aux apports conceptuels et substantiels liés à la mise en oeuvre des activités et à la réalisation des apports promis aux bénéficiaires.

Parallèlement, cela oblige le Groupement à une rigueur et un suivi administratif et financier sans faille des projets. En effet, tout manquement que révèleraient les contrôles effectués par le bailleur de fonds pendant le cours d'un projet ou après sa clôture (jusqu'à sept ans après celle-ci, s'agissant des projets financés par l'Union européenne) est sanctionné par le refus de prise en charge de toute dépense qui serait jugée insuffisamment justifiée.

L.R.D.G. : Quels sont les partenaires du Groupement d'Intérêt Public "Justice Coopération Internationale " ?

Ces partenaires sont très divers. J'ai déjà évoqué un certain nombre d'entre eux.

Ce sont d'abord bien sûr, en interne, nos membres, mais, au-delà, c'est plus largement l'ensemble des institutions françaises partenaires et leurs experts dont JCI sollicite les compétences dans le cadre des missions d'expertise et de l'accompagnement des visites d'études.

Je souligne à nouveau que le Groupement n'est pas exclusivement dédié au service de ses seuls membres. Il a vocation à apporter son appui à toute institution judiciaire qui souhaite participer à un projet d'envergure, mais ne dispose pas de la ressource technique qui lui permettrait de le préparer et le soutenir, et/ou manque des moyens logistiques, administratifs et comptables adaptés pour gérer les fonds alloués et pouvoir en répondre financièrement devant le bailleur. JCI peut ainsi intervenir par exemple pour le Conseil d'État, le Conseil constitutionnel, le Défenseur des

droits…dès lors que le projet est dans le champ de sa mission générale, la coopération judiciaire, et une large part de la coopération juridique.

Ce sont aussi les bailleurs de fonds, partenaires essentiels, puisque JCI n'a pas de fonds propres, ni n'est destinataire de dotations spécifiques qui lui permettraient d'initier de manière autonome des actions de coopération. En dehors de quelques rares opportunités de participer à des projets ouverts sur des fonds bilatéraux, sous l'égide, par exemple, du Centre de crise du ministère de l'Europe et des Affaires étrangères, le groupement oeuvre quasi exclusivement dans le cadre des projets qu'il remporte ou lui sont confiés par des bailleurs internationaux.

En 2018, c'est l'Union européenne qui a financé 81% des projets mis en oeuvre. Elle est le partenaire financier principal de JCI, même si cette part est en légère baisse par rapport à l'année précédente.

Un autre financeur important de JCI est l'Agence française de développement (AFD) qui, ayant pris en charge les questions de gouvernance à la suite des réformes intervenues dans l'organisation de l'aide au développement, met en oeuvre à ce titre, notamment, des projets de construction d'infrastructures judiciaires en Afrique, qui s'accompagnent de volets d'assistance technique souvent confiés à JCI. Ces projets portent, par exemple, sur la formation de juges, des procureurs et des greffiers, sur l'organisation pénitentiaire, ou encore sur l'organisation et la gestion d'un tribunal.

JCI met également en oeuvre, à l'occasion, des projets financés par des institutions internationales (UNODC, UNICEF).

Mais JCI ne travaille pas seul, et la plupart des projets à long terme sont conduits en consortium avec d'autres opérateurs. Il s'agit alors soit de projets de très gros volume, soit de projets pluridisciplinaires, qui engagent une expertise autre que judiciaire, comme par exemple les projets sécurité associant les compétences « Police » et les compétences « Justice ».

Ces partenaires importants sont, en premier lieu, les autres opérateurs publics français : Essentiellement Expertise France (opérateur généraliste), et CIVIPOL (opérateur du ministère de l'Intérieur).

Il s'agit aussi d'autres partenaires européens : espagnols (les opérateurs FIIAPP et AECID), allemands (IRZ- opérateur Justice du ministère fédéral- et GIZ-opérateur généraliste-), hollandais (l'opérateur CILC), autrichiens, mais également des institutions judiciaires belges, italiennes, lettones, croates et autres – ministères de la Justice, Cours suprêmes ou Conseils supérieurs des juges, Instituts de formation – qui participent en direct aux projets sans l'intermédiaire d'opérateurs.

Des alliances avec des partenaires opérateurs privés peuvent aussi advenir à leur demande pour répondre à leur souhait d'afficher une participation de l'opérateur public « Justice » français à leur projet. Mais, encore faut-il que cet affichage soit compatible avec les devoirs et contraintes de l'opérateur public, et qu'il s'agisse d'une participation effective, et non pas seulement de pure façade.

Dans l'éventail des possibles en matière de partenariats, et de structure, localisation et contenu des projets, le Groupement opère les choix des projets auxquels il doit concourir ou participer comme pilote ou comme partenaire d'un autre chef de file, en conjuguant trois préoccupations : satisfaire ses membres et leurs priorités stratégiques tant thématiques que géographiques ; cultiver ses partenariats avec les autres opérateurs ; maintenir son portefeuille de projets à un niveau qui assure son équilibre financier, sans pour autant outrepasser les capacités de gestion et de suivi de l'équipe, sous peine de majorer dangereusement les risques encourus. Ces risques sont le risque financier bien sûr, mais aussi celui d'une prestation de moindre qualité, dont résulterait non seulement une perte de la confiance des bailleurs, mais aussi celle des pays et institutions bénéficiaires. Or, la satisfaction de ces partenaires finaux est à la fois l'objectif même des interventions de JCI et une clé du maintien de sa réputation de qualité et de sérieux dans la conduite des projets.

L.R.D.G. : Combien de projets intra-européens et hors Union européenne le Groupement d'Intérêt Public "Justice Coopération Internationale " a-t-il réalisés et sont actuellement en cours ?

JCI a démarré ses activités en 2012 en reprenant celles d'ACOJURIS, qui avait en portefeuille à l'époque une quinzaine de projets focalisés sur les pays nouveaux entrants ou candidats à l'entrée

dans l'Union européenne (Pologne d'abord, puis Roumanie, Bulgarie et Croatie notamment) avec cette particularité de ne traiter alors aucun projet intra-européen.

Depuis 2012, ont été lancés et mis en oeuvre 93 projets, dont un gros tiers de projets intra-européens, les autres étant mis en place hors Europe, dans les pays dits du voisinage – Balkans en particulier – et au-delà, avec une prééminence pour les zones Maghreb, Afrique, Moyen-Orient et Afrique subsaharienne.

Actuellement, le portefeuille de JCI compte 39 projets, étant à souligner que parmi ceux-ci : 16 d'entre eux sont des projets nouveaux ou en cours de lancement ; 18 des 41 projets du portefeuille 2018 s'étant terminés au cours des quatre derniers mois de cette année passée. La durée moyenne d'un projet de 18 à 36 mois, oblige en effet à un constant renouvellement, ce qui exige donc un travail de prospection continu.

À titre d'exemples, en ce qui concerne les projets récents ou actuellement en cours hors Union européenne, les thématiques essentielles traitées portent sur : le renforcement de l'efficacité des tribunaux (Moldavie), ou plus largement du secteur de la justice en général (Algérie) ; l'amélioration de l'administration de la justice (Égypte) ; l'appui à la restauration de l'État de droit (Centrafrique), ou à la justice et à la sécurité (Niger) ; aux réformes de la justice (Ukraine) ; le renforcement de la formation des magistrats, des greffiers, ou des personnels pénitentiaires (Géorgie, Maroc, Tunisie, Algérie, Côte d'Ivoire)....

Les projets intra-européens, plus courts et nettement plus ciblés, portent sur : les enfants victimes ; la lutte contre le terrorisme ; la prévention de la radicalisation des mineurs ; la prévention contre le racisme et l'intolérance ; l'organisation des greffes des tribunaux ; le fonctionnement des services d'Inspection des juridictions ; la mise en oeuvre de certains règlements européens en matière civile....

L.R.D.G. : Quels sont les points forts du Groupement d'Intérêt Public "Justice Coopération Internationale " en matière de lutte contre la criminalité organisée, la corruption, le blanchiment d'argent et le terrorisme ?

La force de JCI, pour opérer dans les domaines que vous énoncez, tient d'abord à sa capacité de recourir à un large éventail d'expertise, capacité qu'il tire de la diversité de ses membres et partenaires potentiels internes. Outre le vivier des magistrats judiciaires et administratifs et des avocats spécialisés, le Groupement peut, dans ces matières, aller puiser l'expertise présente dans les organismes spécialisés tels que la Haute Autorité pour la transparence de la vie publique (HATVP), la Cellule française de lutte contre le blanchiment de capitaux et le financement du terrorisme (TRACFIN), l'Agence de gestion et de recouvrement des avoirs saisis et confisqués (AGRASC) et, depuis peu, l'Agence française anticorruption (AFA), structures qui sont toutes dirigées par des magistrats ou des magistrats honoraires.

Pour ce qui est de la lutte contre la criminalité organisée et le terrorisme, nous pouvons faire appel au parquet de Paris, au vu de sa compétence nationale en matière de terrorisme, et bientôt au parquet national antiterroriste qui se met actuellement en place. Sont également sollicités, les magistrats du siège du tribunal de grande instance de Paris, les magistrats du siège et du parquet de la Cour d'appel de Paris, en particulier les juges de la Cour d'assises. Les magistrats des Juridictions interrégionales spécialisées (JIRS) de Marseille, Lyon ou Bordeaux sont également sollicités.

L'autre force de JCI réside dans sa capacité, précédemment évoquée, à nouer des partenariats européens avec d'autres opérateurs publics sur des thématiques précises, telles les techniques d'audit, la conception et la mise en oeuvre de formations spécialisées, ainsi que la formulation de recommandations qui prennent en compte les meilleurs pratiques européennes. Ces alliances contribuent au renforcement de JCI, qui, plus armé et plus expérimenté, peut remplir son rôle de support en répondant au mieux aux besoins et attentes des bénéficiaires.

Après avoir participé comme partenaire junior à des projets menés en Serbie et au Kosovo sur la lutte contre la criminalité organisée et sur une meilleure transparence du Parquet au Kosovo, JCI a l'occasion, depuis le début de 2019, de fédérer toute l'expertise spécialisée évoquée plus haut dans le cadre d'un programme de lutte contre la criminalité organisée et la corruption en Bosnie-Herzégovine (projet EU4Justice), pour le compte de l'Union européenne. Ce programme transversal et multidisciplinaire vise à renforcer les capacités des parquets bosniens en matière de conduite

d'enquêtes complexes ayant souvent une dimension transfrontalière.

Ce projet concrétise par ailleurs un engagement de plus en plus important de JCI pour étendre l'influence de la France dans les Balkans et lutter de manière plus efficace contre la criminalité organisée dans cette zone, et les effets qu'elle entraîne sur le territoire national. Cette priorité affichée nous conduit actuellement à nous positionner autant que possible sur les offres de tous projets « justice » proposés dans la zone, offres qui, compte tenu des perspectives à plus ou moins long terme des pays des Balkans à accéder à l'Union européenne, mettent toutes la lutte contre la corruption et la criminalité organisée au coeur de leurs préoccupations .

La lutte contre le terrorisme, priorité essentielle de la stratégie ministérielle, pousse également JCI à s'intéresser de prés à tous les projets susceptibles d'intensifier les moyens de cette lutte dans la zone très sensible de l'Afrique subsaharienne. Nous avons pour cela l'atout de ce que JCI est assez connu et dispose d'une image positive dans la région, auprès des bailleurs et des bénéficiaires. Par ailleurs, la France a une expertise reconnue en matière d'entraide pénale internationale, et JCI peut s'appuyer sur le réseau des ambassades et sur la présence, au sein de ce réseau, de plusieurs magistrats de liaison français dont notre ministère s'attache à intensifier la présence dans les pays les plus concernés.

L.R.D.G. : Quel bilan faites-vous des activités du Groupement d'Intérêt Public "Justice Coopération Internationale " depuis votre nomination en qualité de directrice générale le 1er juillet 2016, et avez-vous des préconisations à formuler ?

Le Groupement d'Intérêt Public (GIP) a connu au cours de sa première période de vie une croissance très forte qu'il a fallu discipliner en adaptant la structure interne aux exigences de la gestion très rigoureuse, impérative en raison de l'importance de la responsabilité financière pesant sur JCI vis-à-vis de ses bailleurs.

L'équipe est aujourd'hui solidement structurée, très réactive et dynamique. C'est un premier point positif du bilan de ces trois dernières années.

L'activité est soutenue. De nouveaux projets viennent succéder en portefeuille aux anciens ; fait notable et éminemment satisfaisant. JCI reçoit maintenant régulièrement de la part de ses bailleurs, des offres tendant à lui confier des projets en gré à gré. Sur le plan « commercial », donc, la situation actuelle apparaît également satisfaisante.

JCI est connu, mais paradoxalement, il l'est davantage auprès de ses partenaires extérieurs qu'il ne l'est à l'intérieur du monde judiciaire français. J'ai pu constater, notamment à l'occasion de diverses rencontres récentes au sein même du corps de la magistrature, dont je fais moi-même partie, l'ignorance complète de beaucoup sur les activités du Groupement, quand cette ignorance ne porte pas sur son existence même. Travailler à développer la connaissance des activités de JCI non seulement parmi les magistrats judiciaires, mais beaucoup plus largement, en ciblant tout autant les magistrats administratifs, les magistrats consulaires, que les avocats, huissiers, notaires, et les juristes en général, sans omettre le monde universitaire, doit être pour JCI un objectif.

Ce faisant, il s'agit certes d'accroître l'ouverture du monde judiciaire à l'international mais c'est aussi une démarche primordiale pour maintenir, développer et renouveler un vivier d'experts qui est pour JCI la ressource première et la condition sine qua non de son activité et de la qualité de celle-ci. Pour une large part, cette qualité, je le répète, tient à la mobilisation de véritables spécialistes du monde judiciaire et juridique, trop souvent absents, chez d'autres opérateurs, au bénéfice de consultants dont certains sont très compétents, mais dont beaucoup manquent de la connaissance fine des procédures et des fonctionnements pratiques, qui est l'apanage de professionnels de la justice.

Je l'ai dit au début de mon propos, et je vais conclure par là également, c'est par sa capacité à continuer de fournir cette expertise de qualité, et par la technicité, la précision et la rigueur dans le montage et la mise en oeuvre des projets, que JCI pourra conserver et asseoir définitivement sa place dans le paysage changeant de l'assistance technique internationale.

Sans y être très ancien, JCI a déjà vu ce paysage se réorganiser, et sont aujourd'hui en chantier de nouveaux changements. En effet, après le regroupement de plusieurs opérateurs qui a présidé à la fondation d'Expertise France, c'est aujourd'hui le rapprochement de l'Agence Française de développement et d'Expertise

France qui se met en place. Quelle que soit la configuration à venir, il convient d'y préserver, pour JCI, son statut actuel d'opérateur « métier » autonome, non par revendication gratuite d'indépendance, mais parce que son autonomie est indispensable à la très grande spécificité des conditions de mobilisation de l'expertise justice, aussi bien publique que privée.

Autonome et, en quelque sorte, obligé à l'excellence, JCI est en bonne position pour gagner par lui-même de beaux projets, l'exemple récent de la Bosnie-Herzégovine en fait, entre autres, la démonstration.

Mais, il ne suffit pas que le Groupement soit en mesure de remporter des projets par lui-même. Sur le marché à la fois concurrentiel et mouvant de la coopération internationale, où changent à la fois l'organisation des opérateurs, mais aussi celle de la structure des projets, il serait bon que JCI puisse être pleinement associé, en premier lieu par Expertise France, aux gros projets transversaux impliquant de façon significative l'expertise Justice, en étant convié à véritablement co-construire la ou les composantes ou sous-composantes du projet qui en relèvent.

L'objet premier de cette préconisation n'est pas de rechercher, pour JCI, la garantie d'une pérennité sereine résultant de l'allocation de ces nouveaux projets ou tranches de projets, encore qu'une telle situation ne nuirait assurément à personne. Il s'agit essentiellement d'assurer que la coopération judiciaire française dans le domaine de la justice pourra continuer d'apporter á ses bénéficiaires la même plus value de qualité. C'est d'une particulière importance pour les projets portant sur les thématiques lourdes de la criminalité organisée, de la corruption et du terrorisme, que nous avons plus spécialement évoquées. Préoccupants et prioritaires, ces sujets doivent être traités à la hauteur des enjeux de coopération opérationnelle dont ils sont porteurs.

OUVRAGES RÉCENTS

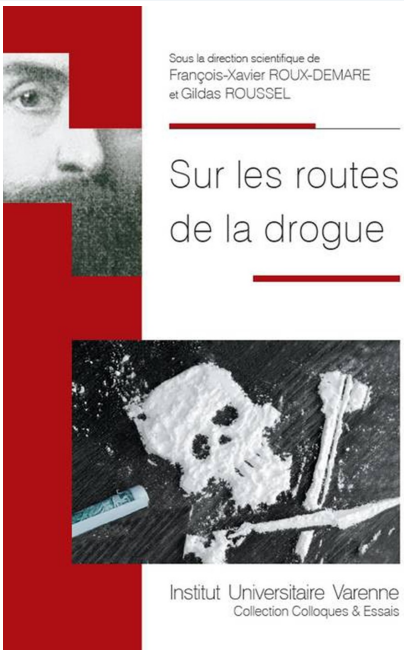
SUR LES ROUTES DE LA DROGUE

SOUS LA DIRECTION DE FRANÇOIS-XAVIER ROUX-DEMARE ET GILDAS ROUSSEL

ÉDITEUR : INSTITUT UNIVERSITAIRE VARENNE

Présentation de l'éditeur

Cet ouvrage propose une appréhension pluridisciplinaire de la question du trafic de stupéfiants avec un regard des universitaires et des professionnels sur les problématiques principales soulevées dans le contexte législatif répressif français. De l'identification à la lutte contre le trafic de stupéfiants, les auteurs apportent un regard sur ce phénomène de notre société, facteur d'addiction et mettant en jeu les politiques de santé publique. Juristes (universitaires, avocat, magistrats, commissaire en chef de la marine), médecins (neurologue, radiologue, psychiatre, médecins légistes), sociologue et économiste ont ainsi réfléchi sur cette question des routes de la drogue.



Gildas ROUSSEL *est maître de conférences et co-directeur du master 2 Magistrature à l'Université de Brest.*

François-Xavier ROUX-DEMARE *est doyen de la faculté de droit de Brest, maître de conférences, directeur du master 2 Droit des personnes vulnérables et co-directeur du master 2 Magistrature. Ils enseignent le droit pénal et la procédure pénale.*

BLANCHIMENT : LA PREUVE DE L'ORIGINE ILLICITE DES FONDS FACILITÉE

PHILIPPE PETITPREZ

AVOCAT GÉNÉRAL À LA COUR DE CASSATION

Par deux arrêts destinés à être publiés au bulletin (Crim. 6 mars 2019, n° 18-81.059 et Crim. 20 mars 2019, n° 17-85.664), la chambre criminelle de la Cour de cassation a statué pour la première fois sur l'application des dispositions légales (art. 324-1-1 du Code pénal et 415-1 du Code des douanes) qui facilitent la preuve du blanchiment en instaurant une présomption de l'origine illicite des fonds. D'une part, la mise en oeuvre de cette présomption est laissée à l'appréciation souveraine des juges du fond, à condition de suffisamment caractériser les conditions de fait ou de droit faisant supposer la dissimulation de l'origine ou du bénéficiaire effectif des biens ou revenus faisant l'objet de l'opération de blanchiment (1er arrêt). D'autre part, les juges du fond doivent rechercher si les conditions d'application de la présomption sont réunies, mais n'ont pas à identifier et caractériser l'infraction d'origine qui, en matière de blanchiment douanier, ne peut être que la conséquence d'un délit sous-jacent prévu par le Code des douanes ou la législation sur les stupéfiants (2e arrêt).

Dans le cadre de la lutte contre le blanchiment, infraction de conséquence, les magistrats et enquêteurs sont souvent confrontés à la difficulté de faire la preuve de l'infraction sous-jacente ou infraction d'origine. Cette démonstration est néanmoins facilitée par les dispositions légales qui instaurent une présomption de l'origine illicite des fonds, qu'il s'agisse du délit général de blanchiment défini par l'article 324-1 du Code pénal ou du blanchiment douanier prévu et réprimé par l'article 415 du Code des douanes.

Rappelons que l'article 324-1 du Code pénal qualifie de blanchiment le fait de :

- de faciliter, par tout moyen, la justification mensongère de l'origine des biens ou des revenus de l'auteur d'un crime ou d'un délit ayant procuré à celui-ci un profit direct ou indirect.

- d'apporter un concours à une opération de placement, de dissimulation ou de conversion du produit direct ou indirect d'un crime ou d'un délit.

De son côté, l'article 415 du Code des douanes incrimine spécifiquement le blanchiment, délit douanier de 2e classe, défini comme le fait de procéder à une opération financière entre la France et l'étranger ou d'importer, exporter ou transférer des fonds que l'auteur sait provenir, directement ou indirectement, soit d'un délit prévu au Code des douanes, soit d'une infraction à la législation sur les stupéfiants.

C'est d'abord la loi n° 2013-1117 du 8 décembre 2013 relative à la lutte contre la fraude fiscale et la grande délinquance économique et financière, qui, en insérant dans le Code pénal un nouvel article 324-1-1 a édicté une présomption de la provenance délictueuse des fonds en

matière de blanchiment, lorsque la personne mise en cause n'est pas en mesure de justifier de leur origine régulière. Cette présomption a été étendue au blanchiment douanier par 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 édictant le nouvel article 415-1 du Code des douanes.

La chambre criminelle de la Cour de cassation a eu l'occasion, dans les deux arrêts précités, de faire application pour la première fois de la présomption d'origine illicite des biens ou fonds objets du blanchiment. D'une part, le simple constat du caractère anormal de l'opération, entendu au sens large, permet de faire jouer la présomption de l'origine illicite des fonds (I). D'autre part, dans le cadre de la mise en oeuvre de cette présomption, les services répressifs sont dispensés d'identifier et de caractériser l'infraction d'origine (II).

I. Le caractère « anormal » de l'opération est entendu au sens large

Il convient, après avoir rappelé les conditions d'application de la présomption (A), de remarquer que la chambre criminelle se montre souple dans l'appréciation du caractère suspect de l'opération qui, sans revêtir nécessairement un caractère complexe, doit tout au moins ne répondre à aucune justification objective (B).

A. Les conditions d'application de la présomption

L'article 324-1-1 du Code pénal dispose que « pour l'application de l'article 324-1, les biens ou les revenus sont présumés être le produit direct ou indirect d'un crime ou d'un délit dès lors que les conditions matérielles, juridiques ou financières de l'opération de placement, de dissimulation ou de conversion ne peuvent avoir d'autre justification que de dissimuler l'origine ou le bénéficiaire effectif de ces biens ou revenus ».

Bien qu'il soit fait référence à l'article 324-1 en son entier, cette présomption ne concerne pas l'aide à la justification mensongère de l'origine des biens et revenus incriminée au premier alinéa de cet article, mais uniquement l'incrimination de blanchiment par concours à une opération portant sur le produit d'un crime ou d'un délit, prévue à l'alinéa 2 du même article[1].

Ce texte institue un renversement de la charge de la preuve en matière de blanchiment, sans modifier les éléments constitutifs de l'infraction eux-mêmes. Il ne s'agit donc pas d'une présomption de constitution du délit, mais d'une présomption portant sur l'origine des fonds, présomption simple qui peut être renversée[2].

L'article 415-1 du Code des douanes, inspiré largement de l'article 324-1-1 du Code pénal, prévoit quant à lui que « 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 ».

La présomption légale est édictée dans des termes voisins mais pas exactement similaires, étant observé que la principale différence réside dans l'intention prêtée à la personne mise en cause. En matière de blanchiment de droit commun, les enquêteurs et les juges doivent, en analysant les conditions matérielles, juridiques ou financières de l'opération, se demander si la personne mise en cause a voulu masquer l'origine des fonds en général (éventuellement pour une autre raison que le fait qu'elle soit frauduleuse), tandis que dans le cadre du blanchiment douanier il faut, en étudiant les mêmes circonstances, s'interroger sur le point de savoir si l'auteur a voulu dissimuler « l'origine illicite » des fonds et si l'on peut raisonnablement supposer la nature spécifique de l'infraction d'origine : un délit douanier ou d'un trafic de stupéfiants[3].

Là encore, le dispositif ne fait qu'alléger la charge de la preuve de l'origine des fonds, sans modifier les éléments constitutifs de l'infraction de blanchiment douanier. En pratique, comme le relève Madame Cutajar, « dès lors que le service d'enquête aura mis en lumière suffisamment d'éléments permettant de présumer que des sommes ont un lien direct ou indirect avec une infraction en matière de stupéfiants ou d'un délit douanier, l'infraction de délit douanier de blanchiment pourra être

retenue, sous réserve que les autres éléments matériels du délit prévu à l'article 415 du Code des douanes soient réunis. Le nouvel article 415-1 opère un renversement de la charge de la preuve de l'infraction concernant l'origine illicite des fonds. Cette présomption simple pourra donc être combattue par la preuve contraire apportée par tout moyen »[4].

Compte tenu des termes communs aux deux articles, faisant référence aux « conditions matérielles, juridiques ou financières de l'opération » il est permis de se demander si, pour faire jouer la présomption d'origine illicite, l'opération analysée doit revêtir ou non, dans ses modalités d'organisation, un certain degré de complexité.

B. Une opération pas nécessairement complexe mais sans justification objective

Il a été indiqué au cours des débats parlementaires qui ont précédé l'adoption de la loi du 6 décembre 2013 que le nouvel article 324-1-1 devait permettre, « dans l'hypothèse où les circuits financiers sont inutilement complexes ou sans rationalité économique, de renverser la charge de la preuve, en obligeant le mis en cause à apporter la preuve de l'origine licite des sommes en jeu »[5].

Mais si, en évoquant les « conditions matérielles, juridiques ou financières » de l'opération, il est clair que le législateur a voulu viser avant tout les montages financiers complexes dépourvus de toute justification économique, il n'a pas entendu exclure pour autant les situations de simple transport d'argent liquide.

Comme le relève la circulaire DACG du 23 janvier 2014[6] (relative à la présentation de la loi n° 2013-1117 en date du 6 décembre 2013 relative à la lutte contre la fraude fiscale et la grande délinquance économique et financière), la présomption légale ne peut jouer que si « les conditions de réalisation de l'opération ne répondent à aucune justification économique ou patrimoniale. C'est donc la justification de l'opération qui est centrale dans ce texte et non la complexité du montage en elle-même, cette complexité pouvant répondre de manière parfaitement légitime à des impératifs économiques. Dans la mesure où l'article 324-1-1 du Code pénal n'affecte que la charge de la preuve de l'existence d'une infraction sous-jacente, il s'ensuit que si la personne mise en cause justifie de considérations juridiques, patrimoniales ou économiques permettant d'expliquer le montage, la présomption ne jouera pas, mais il restera possible d'établir par ailleurs que les biens ou revenus proviennent directement ou indirectement d'un crime ou d'un délit ».

Relevons par ailleurs qu'une jurisprudence constante admet qu'une opération de transport de fonds puisse constituer un blanchiment.

Il en est ainsi du transport dans les bagages d'un commerçant, contrôlé à l'aéroport de Roissy, de plusieurs centaines de milliers d'euros emballés dans des paquets cadeaux provenant des délits de travail dissimulé et de fraude fiscale et destinés à être transférés en Chine[7].

De même, l'incrimination de blanchiment a été retenue à la suite de la découverte par les agents des douanes à un péage autoroutier d'importantes sommes d'argent liquide supportant des traces de cocaïne, dans une cache aménagée derrière le parechoc d'un véhicule circulant dans le sens Italie-Espagne[8].

En présence d'un simple transport de fonds, la question est celle de savoir quels sont les éléments à partir desquels les juges peuvent retenir le caractère suspect de l'opération. La référence par le législateur aux « conditions matérielles » fait songer immédiatement aux procédés plus ou moins élaborés permettant de dissimuler une somme d'argent (mallette à double fond, billets glissés dans les vêtements, cache aménagée dans un véhicule...).

On verra que c'est le cas dans la deuxième affaire, puisque l'argent transporté était caché sous soufflet du levier de vitesse d'un véhicule.

Pourtant, le caractère anormal de l'opération est entendu au sens large par la chambre criminelle, le premier des deux arrêts commentés illustrant concrètement les conditions dans lesquelles les enquêteurs et les magistrats sont admis à faire jouer la présomption.

En l'occurrence, un ressortissant allemand, qui déclarait venir de Suisse et se rendre à Strasbourg, a été contrôlé par

les agents des douanes, dans le train entre Bâle et Mulhouse. Alors que ce dernier déclarait ne pas transporter de sommes, titres ou valeurs, le contrôle a révélé qu'il était en possession de 49 500 € en espèces. Cette somme d'argent, composée essentiellement de coupures de 500 € n'était pas cachée mais simplement contenue dans une enveloppe glissée dans sa poche.

Au cours de l'enquête, les autorités allemandes ont fait savoir qu'une enquête était ouverte contre l'intéressé pour escroquerie aux prestations sociales ayant généré un préjudice de plus de 50 000 €. Lui-même a fourni des explications différentes et peu rationnelles au sujet du but de son voyage et de l'origine des fonds, indiquant notamment qu'ils provenaient de la vente d'un bien immobilier appartenant à son épouse et que celle-ci lui avait confié cet argent pour acheter un camion, version qui a été démentie par cette dernière.

Invité à prouver l'origine des fonds qu'il transportait, le prévenu n'a jamais justifié, ni immédiatement, ni au cours de la procédure, la provenance de la somme d'argent transportée.

Condamné en appel à la peine de six mois d'emprisonnement avec sursis pour blanchiment, outre une amende douanière pour le délit de transfert non déclaré de sommes d'argent (articles L. 152-1, L. 152-4 du Code monétaire et financier, 464 et 465 du Code des douanes), le prévenu faisait valoir, au stade du pourvoi en cassation, qu'aucune condition de fait ou de droit laissant supposer la dissimulation de l'origine ou du bénéficiaire effectif de la somme litigieuse n'avait été constatée par la cour d'appel lui permettant de mettre en oeuvre la présomption légale.

La chambre criminelle approuve le raisonnement de la cour d'appel de Colmar en relevant que « pour appliquer la présomption d'origine illicite des fonds, prévue par l'article 324-1-1 du Code pénal, l'arrêt, qui a relevé, notamment, les incohérences dans le récit fait par le prévenu de son voyage entre l'Allemagne et la France, l'absence de justification des raisons de celui-ci et l'importance de la somme non déclarée, énonce que les conditions matérielles de l'opération de dissimulation de la somme de 49 500 euros en possession de laquelle M. H. a été trouvé lors de son passage à la frontière entre la Suisse et la France ne peuvent avoir d'autre justification que de dissimuler l'origine ou le bénéficiaire effectif de cette somme » et « qu'en prononçant ainsi, par des motifs relevant de son appréciation souveraine des faits, la cour d'appel a justifié sa décision ».

Il n'est donc pas nécessaire que les fonds transportés aient été dissimulés pour que l'opération soit considérée comme douteuse. Ce sont, en l'espèce, toutes les circonstances entourant l'opération, appréciées souverainement par les juges, qui pouvaient faire objectivement douter de son caractère normal : l'attitude du mis en cause au moment du contrôle, les incohérences et contradictions dans ses déclarations, l'importance de la somme non déclarée susceptible de représenter le produit d'infractions commises à l'étranger et les justifications peu crédibles de son transfert vers la France.

Mais le principal intérêt d'un système de présomptions est, comme on va le voir, d'épargner aux enquêteurs et magistrats une démonstration de la nature exacte de l'infraction sous-jacente.

II. Dans la mise en oeuvre de la présomption, les services répressifs sont dispensés de désigner l'infraction d'origine

Pour rester compatible avec la présomption d'innocence, la présomption d'origine illicite, qui suppose une démonstration préalable des conditions de fait ou de droit ayant pour finalité de rendre opaque l'opération en cause, est doublement délimitée (A). Mais dès lors qu'elle peut être mise en oeuvre, cette présomption dispense les magistrats et enquêteurs de désigner l'infraction d'origine (B).

A. Nécessité d'une démonstration préalable

Avant de faire jouer la présomption, il faut établir préalablement l'existence d'une opération de placement de dissimulation ou de conversion ou encore d'une opération financière entre la France et l'étranger. Ensuite il faudra réunir les conditions de fait ou de droit laissant supposer la dissimulation de l'origine ou du bénéficiaire effectif des biens et revenus (blanchiment de droit commun) ou encore l'origine illicite des fonds (blanchiment douanier).

Envisageant les conditions de fait ou de droit auxquelles il sera possible de songer à l'avenir, M. Segonds indique dans le répertoire de droit pénal et de procédure pénale[9] que « pour l'essentiel, elles se ramènent aux caractéristiques anormales de l'opération de placement, de dissimulation ou de conversion : localisation entière ou partielle de l'opération considérée à l'étranger sans que rien ne justifie économiquement ou juridiquement l'extranéité constatée, duplicité des personnes physiques (simple prête-nom, gérant de fait, gérant de paille...) ou des personnes morales (société dormante, société écran ou encore éphémère), des actes juridiques (faux contrat) ou des écritures comptables (faux bilan, fausse facture...). Autant de caractéristiques qui pourront ainsi laisser supposer la dissimulation de l'origine ou du bénéficiaire effectif des biens ou des revenus ».

Il convient d'observer que la présomption d'origine illicite n'est pas contraire à la présomption d'innocence. Comme le constate M. Létocart[10], « la présomption de l'article 324-1-1 du Code pénal est doublement encadrée : d'une part, son caractère « simple » permet à la personne mise en cause de rapporter la preuve contraire, d'autre part sa mise en oeuvre est conditionnée par l'établissement de conditions de l'opération litigieuse qui ne peuvent avoir pour objet que de dissimuler l'origine ou le bénéficiaire effectif des fonds ».

C'est d'ailleurs parce que la présomption légale est doublement encadrée que le renversement de la charge de la preuve n'est pas entaché d'inconstitutionnalité. Saisie d'une question prioritaire de constitutionnalité portant sur la conformité de ce texte avec la Constitution, la chambre criminelle a dit n'y avoir lieu à renvoi au Conseil constitutionnel au motif que « d'une part, la présomption d'illicéité, instituée par le texte contesté, de l'origine des biens ou revenus sur lesquels porte le délit de blanchiment prévu par l'article 324-1 du Code pénal, n'est pas irréfragable, et, d'autre part, nécessite, pour être mise en oeuvre, la réunion de conditions de fait ou de droit faisant supposer la dissimulation de l'origine ou du bénéficiaire effectif de ces biens ou revenus »[11].

Ajoutons que, jusqu'à présent, aucune question prioritaire de constitutionnalité n'a été soulevée à l'occasion de l'application des dispositions de l'article 415-1 du Code des douanes. Mais il est permis de reprendre les mêmes considérations puisque ce texte ne fait qu'édicter une présomption simple qui peut être combattue par le prévenu et suppose la réunion d'éléments permettant de présumer non seulement l'origine illicite des fonds mais également un délit sous-jacent qui ne peut être qu'un délit douanier ou de droit commun en matière de stupéfiants.

Dès lors que sont réunis les éléments de fait ou de droit permettant de faire jouer la présomption, l'infraction d'origine n'a pas à être désignée ni à plus forte raison caractérisée.

B. Il n'est pas nécessaire d'identifier et de caractériser l'infraction d'origine

Les faits exposés dans la deuxième affaire étaient les suivants : Les agents des douanes ont procédé à proximité de la frontière belge au contrôle d'un véhicule circulant dans le sens nord-sud, mis à disposition par une tierce personne. Après que les deux occupants de ce véhicule aient répondu par la négative aux questions portant sur les déclarations obligatoires, les douaniers ont procédé à une fouille de leurs effets personnels et du véhicule, qui leur a permis de constater la présence d'un GPS, de six téléphones portables, d'une cache aménagée mais vide sous la banquette arrière et d'une somme totale de 122.300 € en billets de banque, outre des produits anabolisants.

C'est dans une cavité située sous le soufflet du levier de vitesse qu'ont été découverts deux paquets transparents thermo-soudés contenant chacun une liasse de cent billets de banque de 500 €. Le reste de l'argent était réparti dans les sacoches et les portefeuilles détenus par les occupants du véhicule.

Un test de détection olfactif de produits stupéfiants sur les liasses de billets a été effectué par l'équipe cynophile et s'est avéré positif.

À l'issue de l'enquête au cours de laquelle les intéressés ont donné des explications variables, des poursuites ont été engagées par voie de comparution immédiate devant le tribunal correctionnel de Lille pour transfert non déclaré de sommes d'argent et blanchiment douanier, outre la détention sans justificatif d'anabolisants.

Condamnés en première instance,

les prévenus ont été relaxés en appel du chef de blanchiment douanier, étant observé que la prévention ne visait que le blanchiment en lien avec une infraction douanière et non en lien avec un trafic de stupéfiants.

La cour d'appel de Douai a relevé que les prévenus avaient été poursuivis pour blanchiment en lien avec un délit douanier non visé dans la prévention et a considéré, un peu hâtivement, que ce délit ne pouvait être que celui de celui de transfert de capitaux sans déclaration. Pour entrer partiellement en voie de relaxe, du chef de blanchiment douanier, elle a constaté de manière lapidaire qu'un tel délit, « eu égard à sa nature », ne pouvait tenir lieu de provenance des fonds.

Sur pourvoi formé par la procureure générale, l'arrêt a été cassé en ses dispositions relatives au blanchiment douanier. La chambre criminelle a énoncé « qu'en statuant ainsi, alors qu'il lui appartenait de rechercher si les conditions matérielles de l'opération de dissimulation des sommes en possession desquelles les prévenus ont été trouvés, ne pouvaient avoir d'autre justification que de dissimuler leur origine illicite et permettaient donc de présumer, en l'absence de preuve contraire apportée par les prévenus, que ces fonds étaient le produit direct ou indirect d'un délit du Code des douanes, seul délit visé à la prévention, la cour d'appel, qui n'avait pas à identifier et caractériser le délit d'origine, a violé les dispositions susvisées ».

Deux enseignements importants peuvent être tirés de cette décision :

En premier lieu, les juges doivent analyser toutes les circonstances de l'opération laissant présumer l'origine illicite des fonds susceptibles de représenter le produit d'une infraction douanière ou d'un trafic de stupéfiants. Il est vrai qu'en l'espèce, seul un délit douanier était visé au titre de l'infraction d'origine. La cour d'appel n'y a pas pensé, mais les indices recueillis par les enquêteurs laissaient bien entrevoir la commission d'un délit douanier, celui de contrebande de marchandises prohibées, en l'occurrence des stupéfiants.

En second lieu et en tout état de cause, il n'est nécessaire ni de désigner, ni de caractériser en tous ses éléments constitutifs le délit d'origine. Il suffit de relever des indices suffisants rendant vraisemblable le fait que les fonds provenaient d'une infraction sous-jacente spécifique, c'est à dire un délit douanier ou en matière de stupéfiants, sans obligation de viser une qualification précise.

Cette solution a été critiquée par la doctrine. Ainsi M. Azoulay considère que « si l'on pouvait comprendre, en soumettant la lettre de l'article 324-1-1 du Code pénal à une interprétation stricte, que le champ d'application de la présomption fût plus large en ce qu'elle concerne un délit ou un crime de droit commun, et que celui de l'article 415-1 du Code des douanes était plus restreint puisque circonscrit aux seuls délits douaniers ou à une infraction à la législation sur les stupéfiants, les juges du droit ont inversé le postulat en ce que la réalité de l'infraction de conséquence en matière douanière permet de considérer comme acquise une infraction principale demeurant jusqu'ici seulement vraisemblable »[12].

M. Detraz considère que « c'est a priori de manière tout à fait critiquable que la décision rapportée soulage le juge du fardeau de l'identification et de la caractérisation de l'infraction d'origine ». Se livrant à une comparaison avec le recel, « dont l'infraction d'origine doit elle aussi être pleinement mise en évidence » il considère qu'il s'agit « pour le recel comme pour le blanchiment, du seul moyen sérieux pour le juge de s'assurer de l'existence d'une telle infraction primordiale : il ne peut se contenter d'observer que, "à vue de nez", il y a bien un crime ou un délit à la racine des faits. Aussi bien lui appartient-il de poser l'hypothèse d'une ou de plusieurs qualifications déterminées pour ensuite en vérifier la pertinence (...). Une fois cette opération intellectuelle accomplie avec succès, l'infraction originaire est établie »[13].

L'interprétation par la Cour de cassation de l'article 415-1 du Code des douanes est pourtant conforme à l'intention du législateur. Quelle serait l'utilité d'un mécanisme de présomption si l'infraction d'origine doit être malgré tout désignée ? Le renversement de la charge de la preuve aboutit au contraire, en présence d'éléments de fait ou de droit qui rendent vraisemblables le lien avec un délit douanier ou un trafic de stupéfiants, à imposer au mis en cause lui-même de démontrer que les fonds transportés ont

une origine licite ou tout au moins qu'ils ne sont pas le produit de ces infractions.

Il appartiendra, dans l'avenir, aux magistrats et enquêteurs, dans le cadre de la lutte contre le blanchiment des capitaux, de se saisir de ces nouvelles facilités probatoires.

Notes :

1 Voir en ce sens A. Lepage, P. Maistre du Chambon et R. Salomon, Droit pénal des affaires, 5e édition, LexisNexis, § 431.

2 Circulaire DACG de présentation de la loi n° 2013-117 du 6 décembre 2013, n° JUS D 1402112C.

3 Voir la note de Stéphane Detraz sous l'arrêt du 20 mars 2019, La Semaine Juridique Edition Générale n° 17, 29 Avril 2019, 457.

4 Chantal Cutajar - Le volet « Lutte contre le blanchiment et le financement du terrorisme » À propos de la loi n° 2016-731 du 3 juin 2016, La Semaine Juridique Edition Générale n° 26, 27 Juin 2016, 739.

5 Assemblée nationale, rapports n° 1348 et 1349 faits au nom de la commission des lois par M. Yann Galut.

6 Circulaire précitée, note 2

7 Crim. 6 décembre 2017, n° 16-84.310.

8 Crim. 4 mai 2016, n° 15-80.990.

9 Répertoire de droit pénal et de procédure pénale – Blanchiment – Marc Segonds, § 97.

10 Aurélien Létocart « La revitalisation du traitement judiciaire du blanchiment - À propos de l'article 324-1-1 du Code pénal », La Semaine Juridique Edition Générale n° 30-35, 27 Juillet 2015, 899.

11 Crim. 9 décembre 2015, n° 15-90.019.

12 Warren Azoulay - « Blanchiment douanier : de la vraisemblance d'illicéité à la présomption de culpabilité » - Dalloz actualité, 9 avril 2019.

13 Voir le commentaire précité, note 3.

OUVRAGES RÉCENTS

AFRICA CONNECTION

LA CRIMINALITÉ ORGANISÉE EN AFRIQUE

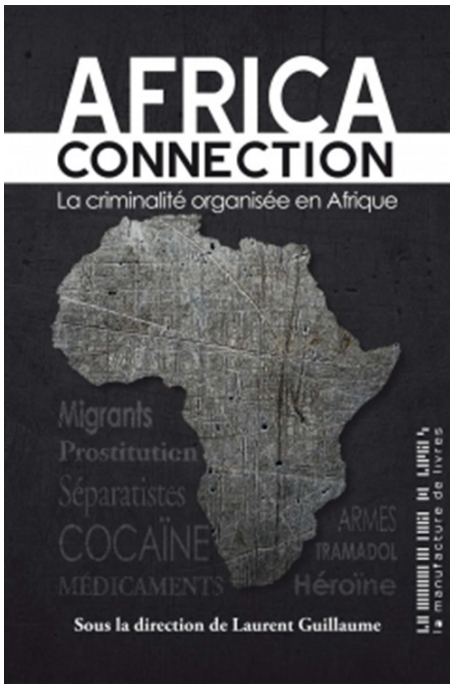
SOUS LA DIRECTION DE : LAURENT GUILLAUME

ÉDITEUR : LA MANUFACTURE DE LIVRES

Présentation de l'éditeur

Trafics d'êtres humains, de stupéfiants ou d'armes, exploitation des migrants ou des matières premières : la criminalité organisée en Afrique est née des désordres de la décolonisation, a grandi sous la guerre froide puis avec la mondialisation. Elle constitue aujourd'hui le précipité de ce que Michel Foucault a qualifié d'illégalisme d'État, véritable gangrène d'un continent.

Laurent Guillaume, ancien policier aujourd'hui consultant



pour divers organismes internationaux, a réuni pour cet ouvrage des spécialistes universitaires et consultants de terrain. Dans cette étude unique, ils nous proposent de découvrir la frontière des trafics, entre légalité et illégalité. Ils éclairent les dynamiques sociales et politiques qui animent ces réseaux pour comprendre leur organisation matérielle et humaine.

LA CYBERCRIMINALITÉ BOURSIÈRE

ALEXANDRE NEYRET

ADJOINT AU DIRECTEUR DES ENQUÊTES DE L'AUTORITÉ DES MARCHÉS FINANCIERS (AMF)

ELISE NAIGEON- DE SANTI

MAGISTRATE DÉTACHÉE

Ce travail ne reflète en aucun cas la position officielle de l'Autorité des marchés financiers. Les auteurs s'expriment à titre uniquement personnel. Les idées et opinions développées dans le cadre de cet article ne sauraient engager en aucune façon l'Autorité des marchés financiers.

Dans notre monde actuel, tout est devenu numérique, connecté, et donc potentiellement en proie aux attaques informatiques. De fait, depuis deux décennies, un changement de paradigme a été opéré consistant à ne plus considérer le risque cyber comme un risque spécifique parmi tant d'autres (à la croisée des chemins entre risque informatique et risque opérationnel) mais bien comme un vecteur de risque beaucoup plus générique, voire un méta-risque[1]. Le « cyber » a permis l'exploitation nouvelle de schémas frauduleux anciens, tout en facilitant l'émergence de nouveaux modes opératoires délictueux.

La cybercriminalité a ainsi envahi notre monde[2]. Le secteur financier, avec des crimes d'envergure (comme le piratage[3] du système de paiement SWIFT[4] de la Banque du Bangladesh pour 80 millions d'euros ou les « exploits » du groupe baptisé FIN7 avec un vol pour plus d'un milliard d'USD en 5 ans[5] de cartes de crédit), n'y échappe pas, tout comme la sphère boursière. Dès juillet 2017, dans sa cartographie des risques[6], l'Autorité des marchés financiers (AMF) a souligné l'importance des risques de nature cyber et de la cybercriminalité boursière, et en septembre 2017, la US Securities and Exchange Commission[7] (SEC) a créé au sein de sa filière répressive une unité spécialisée, la « cyberunit »[8]. Mais si l'on appréhende assez facilement la notion de cybercriminalité financière, qu'entend-t-on exactement par la cybercriminalité boursière ?

S'il n'existe pas de définition juridique communément acceptée de la cybercriminalité, on peut cependant avancer celle-ci[9] : « *la cybercriminalité regroupe toutes les infractions pénales tentées ou commises à l'encontre ou au moyen d'un système d'information et de communication, principalement Internet* ». Cette définition, qui varie selon les pays et les organismes[10], souligne que les systèmes d'information et de communication peuvent être à la fois la cible aussi bien que le vecteur de comportements illégaux.

Il est alors tentant de définir la cybercriminalité boursière comme l'ensemble des abus de marché possédant une composante cyber c'est-à-dire « tentés *ou commis à l'encontre ou au moyen d'un système d'information et de communication* ».

Nous développerons ici l'aspect cyber des trois principaux abus de marché, définis par le Code Monétaire et Financier (CMF) : les opérations d'initié (I), la manipulation de cours (II) et la diffusion

d'information fausse ou trompeuse (III). En revanche, nous n'aborderons pas les sujets liés aux cryptomonnaies[11] qui mériteraient un développement à part entière et liés aux escroqueries aux investissements par Internet[12].

I. Les cyber-manquements d'initiés

Les délits d'initiés, tels que définis à l'article L.465-1 du CMF[13], se caractérisent par l'utilisation/transmission d'une information privilégiée : précise, non publique et susceptible d'avoir une influence sur le cours.

Quoi de plus naturel pour un pirate que de subtiliser des informations confidentielles (et donc potentiellement privilégiées) sauvegardées dans des systèmes informatiques ? En effet, une fois en possession d'une telle information, il est facile d'en tirer profit soit en réalisant des transactions sur le titre avant que son cours n'évolue une fois l'information rendue publique, soit en la revendant à qui se chargera d'intervenir sur les marchés financiers.

Le périmètre d'attaque est d'ores et déjà très vaste (A) avec un mode opératoire relativement « classique » mais dont les évolutions possibles sont nombreuses (B).

A. Un périmètre d'attaque réellement très large

i. La chaîne d'acteurs détenteurs d'informations privilégiées

De nombreux acteurs (financiers ou non) peuvent détenir des informations privilégiées à des moments différents. Ainsi, lors de la préparation d'une opération de fusion-acquisition d'une société acquéreuse sur une société cible, toute une chaîne d'acteurs sera potentiellement au courant : la société acquéreuse, la société cible, les banques conseils, les cabinets d'avocats mais aussi les « *dataroom providers* »[14], les cabinets comptables, les cabinets de conseil, les régulateurs boursiers, les diffuseurs d'informations financières, les agences de relations publiques, potentiellement les agences de traduction (dans le cas d'une opération internationale) voire les bourses elles-mêmes. Les cybercriminels auront tôt fait de tester toute la chaîne afin de choisir le maillon faible comme cible.

- **Les émetteurs**

En 2013, un groupe de cybercriminels dénommé FIN4[15], aurait[16] visé plus de 100 sociétés dont la plupart dans le domaine de la santé et de la pharmacie afin de subtiliser les accès aux boîtes mail des dirigeants pour en extraire des informations confidentielles relatives à de potentielles transactions de fusion-acquisition[17].

En 2016, un technicien informatique employé chez Expedia a compromis les ordinateurs et les boîtes mail de plusieurs dirigeants exécutifs afin de subtiliser des informations confidentielles relatives aux résultats financiers afin de réaliser des transactions sur les actions en amont des annonces officielles, et a ainsi réalisé un profit de 350 000 USD[18].

- **Les banques**

D'août 2014 jusqu'à avril 2017, un consultant IT[19] dénommé RIVAS[20] s'est approprié de manière répétée des informations privilégiées dans le système de suivi des possibilités de fusions-acquisitions ou de rachat d'une banque, et a divulgué ces informations à des connaissances qui en ont fait usage sur les marchés, pour un profit de plus de 5 millions d'USD.

- **Les cabinets d'avocats**

Entre mars et septembre 2015, trois hackers chinois[21] ont pénétré le réseau informatique interne de deux éminents cabinets d'avocats new-yorkais afin d'y dérober des informations privilégiées contenues dans leurs mails, relatives à des opérations de fusion-acquisition, et d'utiliser ces dernières pour traiter sur les marchés financiers pour un profit avoisinant les 3 millions d'USD.

- **Les diffuseurs d'informations**

En 2005, deux employés d'une société ukrainienne d'investissement Lohmus Haavel & Viisemann[22] se sont frauduleusement introduits dans le site Internet sécurisé du diffuseur d'information financière Business Wire pour subtiliser 360 communiqués financiers non encore rendus publics, et ainsi effectuer des transactions sur les marchés financiers sur plus de 200 valeurs, pour 7,8 millions d'USD de profit.

Entre 2010 et 2015, deux hackers ukrainiens Ivan Turchynov and Oleksandr Ieremenko[23] se sont introduits dans les réseaux informatiques de deux diffuseurs d'informations financières pour y subtiliser près de 100 000 annonces de résultats financiers de sociétés avant que celles-ci ne soient publiquement diffusées. Turchynov et Ieremenko ont même créé un serveur

secret sur lequel des traders pouvaient sélectionner des shopping lists d'annonces déjà obtenues et émettre des voeux concernant des annonces à obtenir. Les traders associés étaient d'une trentaine de nationalités variées (Russie, Ukraine, Malte, Chypre, France, US) et ont utilisé ces informations privilégiées pour effectuer des transactions sur les actions, les options et d'autres instruments financiers d'une douzaine de compagnies différentes. Ils partageaient les gains financiers avec les deux hackers[24]. Le profit s'est élevé à 100 millions d'USD.

Entre janvier 2012 et février 2016, Mr Oakes[25], un consultant informatique, a accédé à des informations confidentielles d'un diffuseur d'information financière à Melbourne, relatives à des recommandations d'achat d'actions par des analystes financiers. Il a ainsi acheté en 70 occasions des actions de 52 compagnies différentes, avant de les revendre avec profit une fois les recommandations rendues publiques.

- **La bourse**

En février 2011, il a été révélé que des cybercriminels avaient réussi à compromettre une application de la bourse Nasdaq OMX[26] dénommée « Director's Desk » qui permettait le partage d'informations (en grande partie privilégiées) entre membres du conseil d'administration des sociétés cotées (plus de 300 sociétés).

- **Le régulateur boursier**

Le 20 septembre 2017, la SEC a révélé une intrusion datant de 2016 dans son système règlementaire de déclarations EDGAR[27]. Le 15 janvier 2019, la SEC a inculpé à nouveau le hacker ukrainien Ieremenko[28], déjà condamné en 2015 (cf supra), pour avoir subtilisé plus de 157 résultats financiers ayant permis à ses complices de dégager plus de 4 millions d'USD de profits.

ii. L'informatisation des données

Si le changement de paradigme cyber n'a pas modifié la nature des informations privilégiées, sauf à considérer les cyberattaques comme des informations privilégiées en soi (cf. infra), l'informatisation de toutes les données a en revanche fondamentalement élargi le périmètre d'attaque. À titre d'exemple, la connaissance, avant parution officielle, des indicateurs, indices ou données économiques peut être qualifiée d'information privilégiée pour les instruments financiers concernés. Or, ces indicateurs sont calculés par des acteurs privés (indice de confiance des ménages américains MCSI très observé aux États-Unis est calculé par des chercheurs de l'Université du Michigan) comme par des acteurs publics (les chiffres du chômage calculés par Pôle emploi et la DARES) et il n'est pas garanti que le protocole de production et de transmission de ces indicateurs soit parfaitement sécurisé. Un récent exemple finlandais du 21 novembre 2018[29], avec des cyberattaques sur un site officiel hébergeant des données potentiellement sensibles du ministère des Affaires économiques et du Travail, montre que ces scenarii ne sont pas de la fiction. Ils le sont d'autant moins que les systèmes d'information des organismes publics semblent particulièrement menacés à travers le monde, du fait de l'obsolescence des technologies existantes, ainsi que du futur départ à la retraite des responsables en charge de la maintenance de ces systèmes[30].

Devant l'impact potentiel d'une cyberattaque sur le cours d'une société victime, on pourrait envisager une cyberattaque non pas comme un moyen de dérober une information privilégiée mais plutôt comme l'information privilégiée elle-même. L'analyse des cas EQUIFAX[31] (cf. notes de fin : connaissance en interne de « cyber-incidents » utilisée avant la communication au public pour commettre des délits d'initiés) et du très surprenant MW vs SAINT JUDE MEDICAL[32] confirme ce point de vue. Pourquoi ne pas imaginer dès lors qu'une telle cyberattaque ne soit commanditée par une personne (ou par le responsable de la cyberattaque lui-même !) ayant préalablement vendu des titres de cette société, afin de bénéficier de la chute du cours provoquée par la révélation de la cyberattaque ?

B. Du mode opératoire : analyse et perspective

i. Le mode classique des attaques des cybercriminels

Le mode classique des attaques par courriel (« hameçonnage » ou « hameçonnage ciblé»[33]), très connues du monde de la sécurité informatique, reste encore parmi les plus privilégiés par les pirates pour s'infiltrer dans les réseaux informatiques. Simples d'implémentation et peu coûteuses, ces attaques permettent de cibler facilement le facteur humain, maillon faible de toute organisation, et de « télécharger » des programmes malveillants (« malware ») extrêmement sophistiqués, permettant un accès à distance discret

et permanent aux systèmes informatiques, et wdonc potentiellement à toutes les informations qu'ils contiennent. Depuis quelques années, les attaquants usurpent même l'identité des régulateurs boursiers pour mieux tromper leurs victimes : la SEC en 2017[34], l'AMF en 2019[35], l'Australian Sécurities & Investment Commision (« ASIC ») en 2019[36].

Les attaques sont également facilitées par les services d'approvisionnement que procure le Dark Web aux cybercriminels[37], même si certaines sources avancent qu'il pourrait perdre en attrait au profit d'autre medium de type Telegram[38] :

- procuration de données confidentielles (adresses email éventuellement associées à des mots de passe de personnes clés comme des avocats[39] ou des dirigeants) permettant de mener des campagnes d'hameçonnage ciblé (à partir d'une identité usurpée) ou des attaques de type « *credential stuffing* »[40]. Ce phénomène est d'autant plus inquiétant au vu des fuites de données massives de ces dernières années (Yahoo, Uber, Equifax parmi tant d'autres connues ou non),

- embauche « à la carte » de hackers et/ou achat de malware « clé en main » pour compromettre un compte mail personnel, professionnel ou le réseau informatique d'une cible potentielle,

- recrutement d'employés de la société cible concernée (« insiders ») pour fournir un accès au réseau informatique de leur société[41].

Enfin, il existerait même plus spécifiquement sur le Dark Web des forums d'échange spécialisés permettant directement l'achat et la revente d'informations privilégiées[42].

ii. Les points d'accès potentiels pour les cybercriminels

Cependant, les points d'accès potentiels pour les cybercriminels sont de plus en plus nombreux avec le développement des ordinateurs portables, des smartphones et maintenant des objets connectés[43] ainsi que de la migration massive des entreprises dans le Cloud[44]. Si certains dangers sont connus (connexions à distance non sécurisées[45] et accès Wifi[46], équipements mobiles utilisés à des fins personnelles et professionnelles avec le risque de télécharger des malwares sur des sites compromis ou sur les réseaux sociaux[47]), d'autres le sont sans doute beaucoup moins, comme les vulnérabilités offertes par les objets connectés commandés à la voix dont certains ont montré qu'ils pouvaient enregistrer des conversations à notre insu[48] (même l'assistant expert vocal des smartphones semble être susceptible d'être compromis[49]).

De manière plus générale, les récentes controverses ou affaires liées au cyberespionnage russe ou chinois (éditeur antivirus Kaspersky[50] fournissant un accès aux ordinateurs des entreprises américaines, micropuces chinoises sur les serveurs informatiques produits en Chine pour les entreprises américaines[51], condamnation de deux hackers chinois d'APT10 pour intrusion et vol d'informations confidentielles[52], tentative d'espionnage russe du 4 octobre 2018 où des équipements d'interception du trafic Wi-Fi avaient été découverts dans le coffre d'une voiture banalisée près d'un bâtiment hollandais sensible[53]) attestent de la réalité du vol de données numériques (et donc potentiellement d'informations privilégiées) à plus ou moins grande échelle et de manière plus ou moins sophistiquée.

II. Les cybermanipulations de cours

A. Plusieurs variétés de manipulations de cours

La présentation de ces dernières, définies notamment à l'article L.465-3-1 du CMF[54], ne saurait dès lors être exhaustive, et on se contentera ici de fournir des lignes directrices.

Les principaux procédés manipulatoires, qui ne sont pas mutuellement exclusifs, et visant à fixer le cours d'un instrument financier à un niveau anormal ou artificiel à la hausse sont :

1) L'émission d'ordres d'achat de taille significative n'ayant pas vocation à être exécutés, pour signaler un fort intérêt acheteur au reste du marché et ainsi l'entraîner à ajuster ses cotations à la hausse ;

2) L'achat d'action de manière agressive à des prix de plus en plus élevés, ce qui va mécaniquement augmenter le cours (un peu à la manière d'une enchère) ;

3) La diffusion de fausses rumeurs visant à entraîner le marché à spéculer à la hausse sur ce titre.

Une fois le cours de l'instrument suffisamment élevé (« pump »), il suffit de revendre (« dump ») avec profit (en amont des autres investisseurs et de la chute du

cours), les titres acquis au préalable à bas coût. Dans les cas 2 et 3 précités, on parle de « pump &dump » ou technique dite de la bouilloire.

La compromission des comptes de trading va permettre la mise en place des stratégies 1 et 2 (B) et certains cas avérés de cyber-manipulation de cours soulignent le caractère sophistiqué des groupes cybercriminels, qui pourraient un jour s'attaquer aux algorithmes eux-mêmes (C).

Les vecteurs de diffusion numériques/cyber (emails, faux-site, réseaux sociaux) vont permettre celle de la stratégie 3, qui en tant que telle, peut également relever de la cyberdiffusion de fausse information (cf. infra III).

B. Compromissions des comptes de trading de particuliers

Les cas suivants constituent tous des cas de « pump & dump » où des comptes de trading de particuliers ont été compromis pour permettre la manipulation de cours par des achats (ou des ventes) agressif (ve)s suivant la 2ème stratégie (précitée point A.) :

- BROCO[55] : d'août 2009 jusqu'à décembre 2009, Valery Maltsev, président de Broco Investment, a manipulé le cours d'au moins 38 actions grâce à la compromission de comptes de trading de particuliers pour un gain de 255 000 USD,

- NAGAICEVS[56] : de juin 2009 à août 2010, un trader letton, Igors Nagaicevs, a manipulé le prix de plus de 100 actions du NYSE et du NASDAQ grâce à la compromission de comptes de trading de particuliers pour un profit de 850 000 USD,

- WILLNER[57] : de septembre 2014 à aout 2016, Joseph P. Willner a manipulé le cours de plusieurs actions à l'aide des transactions effectuées par son complice à partir de plus de 110 comptes de trading usurpés pour en tirer un profit de 700 000 USD sur son compte de trading personnel,

- MUSTAPHA[58] : en avril et en mai 2016, Idris Dayo Mustapha a compromis de nombreux comptes de trading de particuliers et utilisé ces derniers pour traiter avec profit sur son compte personnel pour 68 000 USD.

La problématique de la sécurisation des applications et des comptes de trading semble être beaucoup plus importante que prévue puisqu'une toute récente étude de juillet 2018[59] a montré que de nombreuses applications de trading, même parmi des acteurs américains renommés, étaient beaucoup moins sécurisées que leurs homologues de paiement bancaire. À Hong-Kong, devant l'ampleur de la menace, amplifiée par l'évolution des habitudes et des technologies, les autorités locales ont proposé dès 2016 des revues de la cybersécurité des systèmes de trading mobiles et/ou par Internet[60], ainsi que des nouvelles guidelines relatives notamment au trading sur les messageries instantanées[61].

C. Des groupes cybercriminels très sophistiqués

Les cas SWIFT (cf supra), SHALON et ENERGOBANK révèlent la sophistication des groupes cybercriminels spécialisés dans la finance/la bourse.

Le cas SHALON de 2012[62], baptisé « Securities fraud on cyber steroids », se révèle à la fois illustratif de la stratégie 3 (précitée point A.), et emblématique de la cybercriminalité, puisque les adresses courriels des victimes des campagnes promotionnelles malveillantes avaient été auparavant subtilisées à la banque JP Morgan et que cette manipulation boursière, dont le profit s'élève à 2,8 millions d'USD, s'inscrivait dans le cadre beaucoup plus vaste des activités « cyber » d'un groupe criminel international et organisé, ayant dégagé plus de 100 millions d'USD de profits illégaux.

Pour le cas ENERGOBANK[63], il s'agit d'une attaque menée en février 2015, contre des systèmes de trading professionnels de la banque russe ENERGOBANK, grâce à un malware dénommé CORKOW[64], lequel a permis de placer des ordres sur les marchés financiers pour un montant notionnel avoisinant les 500 millions d'USD, provoquant des fluctuations importantes sur la parité Dollar/Rouble, laquelle a ainsi varié de plus de 15% en l'espace de quelques instants. Aucun profit malhonnête ne semble avoir été spécifiquement dégagé mais la banque a déclaré des pertes pour 3,2 millions d'USD.

Cette sophistication des groupes cybercriminels spécialisés dans la finance/la bourse est remarquable car elle allie une expertise informatique de très haut niveau à une connaissance aigüe des mécanismes financiers, démultipliant les impacts potentiels sur l'intégrité

des marchés. On peut ainsi citer parmi ces groupes : Corkow[65] (cf supra), Carbanak[66] dont le cerveau a été arrêté tout récemment en Espagne début 2018, Cobalt[67], FIN4 (cf. supra), FIN7 dont trois membres ont également été arrêtés en Aout 2018[68], Lazarus[69]…

Comment ne pas imaginer dès lors qu'un cybercriminel, certes doué, ne puisse sciemment compromettre les algorithmes d'une société pour manipuler le cours de certains instruments, à des fins économiques ou de déstabilisation, en envoyant des ordres de vente massifs en série ? Les algorithmes sont en effet au coeur des échanges financiers modernes et représentent l'immense majorité des transactions et des ordres[70]. Cette hypothèse n'est pas si irréaliste puisque la DARPA (« The Defense Advanced Research Projects Agency ») y travaille dans son projet « Financial Markets Vulnerabilities Project »[71]. Rappelons à cet égard l'achat malencontreux en l'espace d'une demi-heure de plusieurs milliards d'USD d'actions américaines par Knight Capital, société spécialisée dans le trading à haute fréquence, suite à une erreur informatique dans un de ses algorithmes, laquelle a coûté plus de 440 millions d'USD, entraînant d'ailleurs sa fusion ultérieure avec la société Getco[72].

III. La cyberdiffusion de fausse information

La diffusion de fausse information, définie notamment à l'article L.465-3-2 du CMF[73], est une technique de manipulation boursière vieille comme le monde, si l'on songe à l'annonce de la fausse mort de Napoléon orchestrée en février 1814 au London Stock Exchange afin de faire augmenter les bons du Trésor anglais[74].

Les motivations des diffusions de fausses informations sont souvent économiques[75] (le criminel cherche à tirer un profit de l'opération) mais elles peuvent être aussi activistes[76], vu la symbolique idéale et l'impact potentiellement important sur la valorisation des sociétés visées. Sans aucun doute, du sabotage économique de la part d'un concurrent ou de la déstabilisation étatique et terroriste pourraient aussi être envisagées.

Aujourd'hui, nul ne peut contester, et ce d'autant plus avec tous les débats actuels autour des « fake news »[77] et des nouvelles lois ad-hoc[78], qu'à l'ère numérique avec les sites Internet, les réseaux sociaux (B) et les courriels, la diffusion de fausses informations est devenue beaucoup plus facile, plus rapide, et avec une portée beaucoup plus large, donc avec un impact sur les marchés financiers, automatisés et dopés à l'information instantanée et aux rumeurs[79], beaucoup plus important. Les diffuseurs d'informations sont les plus touchés et le périmètre d'attaque, à l'instar des cyberdélits d'initié est très large (A), et le type de fausse information est quant à lui de plus en plus varié (C), pour un risque plutôt limité (D).

A. Cibles et périmètre d'attaque

i. Les acteurs de la chaîne de diffusion les plus visés

La cyberdiffusion de fausse information peut, comme les cyber-manquements d'initiés, toucher plusieurs acteurs de la chaîne financière de diffusion, mais les premiers visés sont surtout les émetteurs, les diffuseurs d'information financière spécialisée comme Bloomberg ou Reuters voire parfois les régulateurs boursiers qui recueillent certaines déclarations obligatoires relatives aux sociétés cotées.

Ainsi, le 22 novembre 2016[80], un faux communiqué de presse usurpant l'identité de Vinci (avec une adresse courriel similaire à l'officielle et un site Internet miroir) et alléguant de la découverte de fraudes comptables a été envoyé aux journalistes. L'information a été rapidement relayée par Bloomberg entrainant quasi instantanément[81] la chute du cours du titre de 19%, soit une perte momentanée de capitalisation d'environ 7 milliards d'euros. Des revendications activistes ont été avancées en fin de journée par courriel.

D'autres cas, aux motivations activistes déclarées, ont révélé un mode opératoire quasiment identique :

- Cas de la banque italienne Banca Intesa San Paolo le 24 avril 2015[82] avec une baisse de 4% du cours de l'action en l'espace de 8 minutes suite à un faux communiqué annonçant des malversations comptables.

- Cas de la société anglaise G4S[83], mais dont le cours n'a que très peu bougé en l'absence de reprise du faux communiqué (indiquant toujours les mêmes malversations comptables !) par Bloomberg.

- Cas de la société minière australienne Whitehaven Coal dont le cours chuta de 9% le 7 janvier 2013[84] suite à un faux communiqué de la banque ANZ annonçant l'annulation

d'un prêt à cette première pour des raisons environnementales. L'instigateur de cette campagne a été arrêté et condamné[85].

L'un des premiers cas connus, et un des rares ayant permis un profit criminel démontré, est celui d'EMULEX le 24 août 2000[86] où un jeune étudiant de 23 ans, grâce à un faux communiqué, a fait chuter le cours de la société de près de 60% en 18 minutes, et a empoché un profit de 241 000 USD. Le lecteur intéressé pourra consulter également les cas TWITTER du 14 juillet 2015[87], IMMUNOVACCINE du 3 mars 2015[88] et FINGERPRINTS CARDS du 11 octobre 2013[89].

Il apparaît évident à la lumière de tous ces cas au mode opératoire très similaire, que la question de la diffusion de l'information financière « officielle » est cruciale. À la suite de l'incident VINCI, l'AMF a d'ailleurs établi dans son communiqué de presse du 23 février 2017[90] des bonnes pratiques pour les émetteurs et les agences de presse, visant d'une part, à clarifier le canal officiel de diffusion de l'information de l'émetteur pour mieux s'assurer de son authenticité, et d'autre part, à renforcer les procédures de sensibilisation et de cybersécurité des agences de presse pour éviter tout piratage en amont (réception d'un faux communiqué considéré comme vrai par les journalistes dans les cas ci-dessus) ou en aval (diffusion d'un faux communiqué directement dans les systèmes d'information de l'agence de presse ou du diffuseur).

Malheureusement, le régulateur boursier, de par la crédibilité et la capacité de dissémination qu'il apporte, n'est pas plus à l'abri des tentatives de diffusions de fausses informations. Trois cas ont ainsi affecté la plateforme réglementaire électronique EDGAR de la SEC en publiant de fausses déclarations d'offres de rachat sur les sociétés afin de faire bondir les volumes échangés et les cours des actions concernées (qui tend naturellement à s'ajuster vers le prix de l'offre) et matérialiser pour le cybercriminel un gain économique sur des produits dérivés (options ou CFD[91]) acquis au préalable : IDTI le 12 avril 2016[92], FITBIT le 10 novembre 2016[93] et AVON le 14 mai 2015[94].

ii. Les classes d'actifs visés

La diffusion de fausse information ne se limite pas à un émetteur en particulier, elle peut potentiellement toucher toutes les classes d'actifs (actions, crédit, taux d'intérêts, taux de change, matières premières, énergie, immobilier…).

Prenons par exemple les principaux facteurs influençant le prix d'une sous-famille des matières premières plutôt confidentielle comme le bétail : les maladies affectant les cheptels, les conditions météorologiques extrêmes des pays producteurs, les habitudes de consommation et le pouvoir d'achat des pays consommateurs. Il semble facile d'imaginer une fausse information pour chacun de ces facteurs et ainsi, à condition de trouver le moyen de dissémination ad-hoc (chaque marché ayant ses habitudes et ses sources particulières d'informations), manipuler le prix des futures[95] relatifs au bétail[96].

De même, la classe d'actifs « crédit », en ce qui concerne les sociétés et les émetteurs souverains, est fortement influencée par les évaluations émises par les agences de notation. Ces dernières, parfois victimes d'erreurs informatiques[97], constituent une cible idéale pour les cybercriminels. Ainsi, le 10 novembre 2011[98], Standard & Poor's, par l'intermédiaire d'un mail envoyé à certains de ses abonnés, a indiqué par erreur que la note de la dette souveraine française avait été abaissée, entraînant une forte secousse sur les marchés en pleine crise de la dette de la zone euro.

B. Les réseaux sociaux

Twitter, comme l'ensemble des réseaux sociaux, est le terrain de jeu rêvé pour la diffusion de fausses informations: quasi-anonymat, rapidité, possibilité de toucher un large public notamment grâce à de très nombreux faux comptes, parfois robotisés (« bots ») et louables à la commande, que les « réseaux sociaux » s'évertuent à détecter et à supprimer[99]. Ces « social bots » semblent si capables d'influencer l'opinion que la DARPA (cf. supra) s'en est émue dès 2015[100]. Depuis les dernières élections américaines, et la controverse de l'éventuelle ingérence russe par ces mêmes robots sociaux (« social bots »), le sujet a pris de l'ampleur[101].

La SEC a d'ailleurs émis des alertes spécifiques visant à mettre en garde les investisseurs particuliers contre les rumeurs et recommandations provenant des medias sociaux, et propices à des manipulations de type « pump&dump »[102]. La contribution de Twitter à ces dernières semble même corroborée par des études scientifiques[103].

Ainsi, plusieurs cas ont utilisé la capacité de diffusion des réseaux sociaux à des fins économiques (campagnes promotionnelles de

type « pump&dump » dans l'iconique cas CYNK où le cours d'une société a été multiplié par 500[104], ou dissémination de faux tweets usurpant l'identité de l'analyste reconnu Muddy Waters par un trader écossais du nom de Craig[105]) ou terroristes (compromission du compte Twitter de l'Associated Press le 23 avril 2013 par la Syrian Electronic Army[106] annonçant des explosions à la Maison Blanche et la blessure de Barack Obama, entraînant une chute instantanée des marchés de 1%).

C. De la « Fake news » aux « fake data », « deep fake » et « botadvisor »

i. Des données modifiées ou corrompues

Les cas précédents présentaient des fausses informations fabriquées de toute pièce comme des faux communiqués financiers, proches de la création d'une rumeur classique (« fake news »). Mais dans un monde boursier toujours plus automatisé et accroc aux données, comment ne pas imaginer que ces dernières, comme les indices et indicateurs économiques sensibles pour les cyber-manquements d'initiés définis supra, ne soient pas subtilisées, mais plutôt modifiés ou corrompues (« fake data ») ? Une récente étude d'Accenture[107] montre à quel point l'intégrité des données est un facteur de risque critique pour les institutions financières.

Ce risque est d'ailleurs d'autant plus important qu'une grande partie des données financières est concentrée entre les mains de diffuseurs majeurs d'informations financières comme Bloomberg ou Reuters (plus de 50% de part de marché à eux deux), et que la cybersécurité de ces acteurs et des modes d'acheminement de leurs données aux clients reste une question essentielle, qui pour l'instant ne semble pas avoir reçu l'attention qu'elle mérite.

ii. L'utilisation malveillante de l'intelligence artificielle

L'imminence de l'intelligence artificielle[108] ouvre également de nouvelles perspectives. La possibilité offerte, et facilement accessible grâce aux nombreux tutoriels disponibles sur l'Internet public, de pouvoir falsifier des vidéos en « faisant *dire n'importe quoi à n'importe qui n'importe comment*» (« deepfake ») rend la fausse information plus crédible et donc sa diffusion encore plus efficace[109]. D'ores et déjà, les gouvernements, notamment américains, s'inquiètent du potentiel de désinformation de cette nouvelle menace dans le cadre des élections[110]. Même si aujourd'hui, les vidéos ne semblent pas encore parfaites[111], combien de temps avant qu'une rumeur sur les médias sociaux ne circule avec une vidéo soi-disant cachée du gouverneur de la FED ou de la BCE discutant en privé d'une hausse des taux directeurs ou d'une vidéo montrant un activiste reconnu et suivi dévoilant sa prochaine cible ?

Enfin l'apparition de robots « intelligents », propres à simuler sous certaines conditions le comportement humain de manière réaliste, rendra la détection des « social bots », et donc de la diffusion de fausse information, encore plus ardue. De même, la présence toujours plus nombreuse de robots conseillers, dans les relations entre particuliers et prestataires financiers, pose également la question de la cybersécurité de ces robots, qui, une fois compromis, pourraient être le vecteur de diffusion de fausse information ou de fausses recommandations d'investissements sur des instruments financiers.

D. Peu de moyens pour de gros impacts avec un risque faible

Devant cette criminalité, nécessitant parfois peu de moyens (un faux communiqué « crédible », un nom de domaine, une adresse courriel ad-hoc, un site internet, une liste de diffusion de journalistes) et facilement anonyme, les enquêteurs ont souvent plus de chances d'aboutir en suivant le fil d'Ariane laissé par les transactions boursières du cybercriminel, s'il en a réalisé.

En effet, il existe sur Internet de nombreuses ressources en libre accès permettant au cybercriminel novice de se perfectionner dans la fabrication de son « hoax » boursier[112]. Il est ensuite possible pour le fraudeur de conserver son anonymat soit par l'utilisation d'un Wifi public, soit par l'utilisation de VPN[113] ou du réseau TOR[114], et ce d'autant plus que les contrôles d'identité demandés lors de l'enregistrement de nom de domaine ou de l'hébergement de site Internet sont quasiment inexistants. L'utilisation de moyens de paiement comme les cartes prépayées ou les cryptomonnaies[115] permet enfin de payer ces services sans rompre son anonymat.

Pour le cybercriminel, l'investissement et les risques restent plutôt faibles alors que l'impact est potentiellement très important, pouvant s'élever à plusieurs centaines de millions voire des milliards d'euros de capitalisation boursière momentanément perdue. Les coupe-circuits mis en place dans

les bourses permettent néanmoins de stopper une chute trop importante, dont l'effet se résorbe quasi instantanément lorsque la supercherie est découverte.

En conclusion, on soulignera qu'au-delà des abus de marché, les cas de compromission de la bourse elle-même existent et attestent de la réalité de la menace cyber. Dans un sondage réalisé en 2013 auprès de 46 bourses[116], l'IOSCO (« International Organisation of Securities Commission ») rapportait que plus de la moitié avait déjà subi une cyberattaque dans l'année (jugées sans effet sur le bon fonctionnement du marché et n'entraînant qu'un faible coût). Les cyberattaques les plus courantes sont celles utilisant des malwares et des dénis de service (DoS)[117]. On peut ainsi mentionner les cas suivants[118] : de 2007 à 2011 des hackers russes ont réussi à compromettre le NASDAQ[119] ; en 2011 la Bourse de Hong-Kong[120] a été touchée ; en 2012, une vague d'attaques par déni de service distribué (« DDoS ») menée par des activistes[121] a touché les bourses américaines NYSE, NASDAQ et BATS ; en 2014, la Bourse de Varsovie a subi une cyberattaque d'envergure revendiquée par des terroristes[122].

La cybercriminalité boursière touche ainsi toute la chaîne des acteurs du monde financier avec des conséquences extrêmement importantes dans des échelles de temps réduites. Les cybercriminels, aux motivations économiques ou activistes, peuvent être des particuliers ou des groupes organisés hautement sophistiqués. L'évolution des technologies modernes (Dark Web, réseaux sociaux, intelligence artificielle, objets connectés (IoT), Cloud...) et le recours massif à l'automatisation et aux données propres à la finance, démultiplient d'autant plus la surface d'attaque, les points d'entrée et les moyens mis à la disposition des cybercriminels. Cette cybercriminalité boursière reste attractive dans le contexte actuel malgré la prise de conscience généralisée du risque cyber et l'apparition de nouvelles lois ad-hoc[123].

Notes :

1. https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline
2. Dans la 13ème édition de son rapport sur les risques mondiaux en 2018, le World Economic Forum place les deux risques de cyberattaques et de vols/pertes massifs de données parmi les cinq risques majeurs en termes de probabilité de survenance en compagnie des risques environnementaux comme les catastrophes naturelles, les conditions météorologiques extrêmes et les risques dus aux changements climatiques ; et en 6ème position en termes de gravité après les armes de destruction massive (sic !), les risques environnementaux précédemment cités et les crises de pénurie d'eau.
3. https://www.nettitude.com/wp-content/uploads/2016/12/Nettitude-SWIFT-Threat-Advisory-Report-client.pdf

   https://www.mwrinfosecurity.com/assets/swift-whitepaper/mwr-swift-payment-systems-v2.pdf

   1.https://www.securityinsider-wavestone.com/2016/06/retour-sur-laffaire-swift-synthese-des.html
4. SWIFT (Society for Worldwide Interbank Financial Telecommunication) est une société privée détenue par ses membres dont l'objet est d'assurer le fonctionnement d'un réseau international de communication électronique entre acteurs des marchés (baptisé aussi SWIFT par extension), dont notamment les banques, qui s'échangent des messages standardisés relatifs aux opérations financières (ordres d'achat et de vente, confirmations d'exécutions de transactions, instructions de règlement-livraison, ordres de paiement...).
5. https://www.justice.gov/opa/pr/three-members-notorious-international-cybercrime-group-fin7-custody-role-attacking-over-100

   https://www.fireeye.com/blog/threat-research/2018/08/fin7-pursuing-an-enigmatic-and-evasive-global-criminal-operation.htm

   https://www.lemonde.fr/pixels/article/2018/08/02/les-etats-unis-accusent-trois-ukrainiens-d-avoir-pirate-15-millions-de-cartes-de-credit_5338611_4408996.html
6. AMF, Cartographie des risques 2017, 3 juillet 2017.
7. Homologue américain de l'AMF.
8. https://www.sec.gov/news/press-release/2017-176
9. http://www.justice.gouv.fr/include_htm/pub/rap_cybercriminalite.pdf
10. https://tel.archives-ouvertes.fr/tel-01470150/document section I « définition de la cybercriminalité ».
11. Intrusion et vol sur les plateformes d'échanges, fraudes aux ICO, manipulation de cours... Les récentes évolutions législatives, et notamment la loi PACTE adoptée à l'Assemblée nationale le 11 avril 2019, offrent un nouveau régime pour les crytpo-actifs en France avec une régulation optionnelle par l'AMF. https://www.amf-france.org/Reglementation/Dossiers-thematiques/Fintech/Vers-un-nouveau-regime pour-les-crypto-actifs-en-France
12. qui relèvent plus de l'escroquerie classique.
13. qui consistent d'après l'article L.465-1 du CMF, pour une personne « à faire usage d'une information privilégiée en réalisant, pour elle-même ou pour autrui, soit directement, soit indirectement, une ou plusieurs opérations ou en annulant ou en modifiant un ou plusieurs ordres passés par cette même personne avant qu'elle ne détienne l'information privilégiée, sur les instruments financiers émis par cet émetteur ou sur les instruments financiers concernés par ces informations privilégiées ». L'information privilégiée est définie d'après les alinéa 1 à 4 de l'article 7 du règlement (UE) n° 596/2014 mais principalement par : « une information à caractère précis qui n'a pas été rendue publique, qui concerne, directement ou indirectement, un ou plusieurs émetteurs, ou un ou plusieurs instruments financiers, et qui, si elle était rendue publique, serait susceptible d'influencer de façon sensible le cours des instruments financiers concernés ou le cours d'instruments financiers dérivés qui leur sont liés ».
14. Fournisseurs d'accès au dataroom, « chambre de données », espace physique ou virtuel utilisé pour stocker un volume important d'informations (généralement à caractère confidentiel) que seules les personnes autorisées peuvent consulter via un accès à distance.
15. baptisé ainsi par FireEye dans son rapport détaillé en 2014 « Hacking The Street, FIN4 likely playing the market.
16. L'usage du conditionnel est de mise dans la mesure où les résultats de l'enquête menée par la SEC ne sont pas connus
17. https://www.reuters.com/article/us-hackers-insidertrading/exclusive-sec-hunts-hackers-who-stole-corporate-emails-to-trade-stocks-idUSKBN0P31M720150623?feedType=RSS&feedName=topNews
18. https://www.sec.gov/litigation/complaints/2016/comp-pr2016-256.pdf

19. Technologie de l'information (ie chargé de conseiller, accompagner, suivre les sociétés et leurs salariés dans l'utilisation des nouvelles technologies).

20. https://www.justice.gov/usao-sdny/pr/five-individuals-charged-participating-three-insider-trading-schemes-generating-more-5

21. https://www.sec.gov/litigation/complaints/2016/comp-pr2016-280.pdf

22. https://www.sec.gov/litigation/complaints/comp19450.pdf

23. https://www.justice.gov/usao-nj/pr/hacker-sentenced-30-months-prison-role-largest-known-computer-hacking-and-securities

    https://www.sec.gov/litigation/complaints/2015/comp-pr2015-163.pdf

    https://www.sec.gov/litigation/litreleases/2016/lr23471.htm

    https://www.sec.gov/litigation/litreleases/2016/lr23530.htm

24. Allant même jusqu'à leur donner accès aux comptes de trading en gage de leur bonne foi.

25. https://asic.gov.au/about-asic/media-centre/find-a-media-release/2018-releases/18-136mr-it-consultant-charged-with-gainingunauthorised-access-to-data-and-insider-trading/

26. https://www.reuters.com/article/us-nasdaq-hacking-idUSTRE79J84T20111020

    https://arstechnica.com/information-technology/2014/07/how-elite-hackers-almost-stole-the-nasdaq/

27. EDGAR (« Electronic Data Gathering, Analysis, and Retrieval ») traite 1,7 million de déclarations réglementaires électroniques par an.

28. https://www.sec.gov/news/press-release/2019-1

    https://www.sec.gov/litigation/complaints/2019/comp-pr2019-1.pdf

    Nessim Aît-Kacimi, Comment les cyberpirates ukrainiens font trembler WallStreet, Article des Echos, 13 mars 2019.

29. https://yle.fi/uutiset/osasto/news/cyber-attack_shuts_finnish_ministry_jobs_site/10518762

30. http://www.globalsecuritymag.fr/Les-cyberattaques-visant-les,20190306,85113.html

31. Jun Ying, Chief Information Officer (CIO) d'une business unit d'Equifax et qui devait succéder au CIO global de la compagnie, a commis un manquement d'initié en utilisant sa connaissance d'une perte massive (mais encore confidentielle) de données personnelles subie par Equifax pour vendre ses stock-options avant que la compagnie ne dévoile publiquement dans un communiqué en Septembre 2017 ce cyber-incident, dans lequel 148 millions de citoyens US ont vu leur données personnelles comme leur numéro de sécurité social fuiter. https://www.sec.gov/litigation/complaints/2018/comp-pr2018-40.pdf

32. Si le cadre juridique n'est pas nécessairement celui du manquement d'initié, le cas de Muddy Waters avec Saint Jude Medical est aussi intéressant puisque le premier annonçait publiquement que les appareils médicaux du deuxième (notamment les pacemakers) présentaient de graves lacunes en termes de cybersécurité et étaient susceptibles de succomber à des cyberattaques (notamment effectuées et filmées par une compagnie de cybersécurité spécialisée dans le domaine médical). Muddy Waters espérait bien entendu profiter de la chute du cours engendrée par la dissémination publique de cette information pour tirer bénéfice de ses positions à la vente sur Saint Jude Medical. https://www.marketwatch.com/story/short-seller-muddy-waters-renews-claims-of-st-jude-medical-cyber-vulnerabilities-2016-10-19

33. Plus connu sous le terme anglais de « phishing » est une approche par laquelle les cyber escrocs poussent la victime à révéler des informations personnelles (mots de passe, numéros de carte de crédit...) via des e-mails contrefaits ou dirigeant sur un site web contrefait.

34. En mars 2017, FireEye aurait découvert une campagne d'hameçonnage ciblé, émanant du groupe FIN7, visant des individus en charge des déclarations réglementaires sur la plateforme EDGAR de la SEC chez onze sociétés cotées. L'adresse du mail envoyé (EDGAR

    <filings@sec.gov>) usurpait la véritable adresse de la plateforme tandis qu'un document malicieux Word y était attaché

    http://fortune.com/2017/03/07/sec-phishing/

    https://www.fireeye.com/blog/threat-research/2017/03/fin7_spear_phishing.html

35. Un article du Times of Malta du 25 février 2019 établit d'ailleurs un lien possible entre cette campagne de courriels ciblés usurpant l'identité de l'AMF et la récente cyberattaque de la Banque de Valette (Malte), ayant débouché sur un profit de 13 millions d'euros. https://www.timesofmalta.com/articles/view/20190225/local/how-bov-hackers-got-away-with-13-million.702800

36. https://asic.gov.au/online-services/service-availability/scams-targeting-asic-customers/

37. http://itzashita.ru/wp-content/uploads/2017/05/RedOwl_Intsights_Report.pdf

38. Télégram est une application de messagerie sécurisée, dont les messages cryptés peuvent s'autodétruire (messages textes et images temporaires ; https://www.undernews.fr/hacking-hacktivisme/telegram-le-nouveau-medium-de-choix-de-la-cybercriminalité.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+undernews%2FoCmA+%28UnderNews%29

    https://research.checkpoint.com/telegram-cyber-crimes-channel-choice/

39. https://www.repknight.com/wp-content/uploads/2018/01/White-Paper-Securing-the-Law-Firm-January-2018-Website-LM.pdf

40. Le « credential stuffing » est une pratique qui consiste à utiliser les identifiants volés d'un compte sur un site Internet piraté pour essayer d'accéder de manière automatisée à plusieurs comptes sur divers autres sites Internet (à l'aide de botnets notamment, ie réseau de programmes connectés à Internet qui communiquent avec d'autres programmes similaires pour l'exécution de certaines tâches). Cette pratique permet ainsi d'accéder à tous les comptes pour lesquels la victime initiale du premier compte piraté utilise le même mot de passe.

41. http://itzashita.ru/wp-content/uploads/2017/05/RedOwl_Intsights_Report.pdf

42. http://itzashita.ru/wp-content/uploads/2017/05/RedOwl_Intsights_Report.pdf

43. Près de 8,4 milliards en 2017 et presque 20,4 milliards en 2020.

44. http://globbsecurity.fr/office-365-ligne-de-mire-cybercriminels-44303/

    https://www.solutions-numeriques.com/cyberattaques-office-365-et-google-g-suite-de-plus-en-plus-vises/

45. HAGER, S. Les voyageurs d'affaire, portes d'entrée des hackers Option Finance n° 1467. 18 juin 2018.

46. https://www.techradar.com/news/networking/wi-fi/why-you-should-avoid-hotel-wi-fi-like-the-plague-1292555/2

47. En effet, selon un rapport de l'entreprise de cybersécurité Bromium, la cybercriminalité impliquant les réseaux sociaux est en forte hausse. Le rapport indique qu'une compromission d'entreprise sur cinq a un lien avec un maliciel distribué par un réseau social. https://www.bromium.com/social-media-platforms-cybercrime-economy/

48. Des Google Home ou des Amazon Alexa disposés dans des bureaux d'exécutifs pourraient facilement obtenir des informations privilégiées...

49. http://thehackernews.com/2017/09/ai-digital-voice-assistants.html

50. https://www.pcworld.com/article/3235484/what-the-kaspersky-antivirus-hack-really-means.html

51. https://www.lemonde.fr/pixels/article/2018/10/04/espionnage-la-chine-accusee-d-avoir-installe-des-micropuces-dans-des-serveurs-utilisespar-apple-et-amazon_5364769_4408996.html

    https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

52. https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion

53. https://www.lemonde.fr/pixels/article/2018/10/04/les-pays-bas-revelent-une-operation-d-espionnage-russe-sur-leur-territoire_5364712_4408996.html

54. qui consiste d'après l'article L.465-3-1 du CMF par : « le fait, par toute personne, de réaliser une opération, de passer un ordre ou d'adopter un comportement qui donne ou est susceptible de

donner des indications trompeuses sur l'offre, la demande ou le cours d'un instrument financier ou qui fixe ou est susceptible de fixer à un niveau anormal ou artificiel le cours d'un instrument financier » et/ou « le fait, par toute personne, de réaliser une opération, de passer un ordre ou d'adopter un comportement qui affecte le cours d'un instrument financier, en ayant recours à des procédés fictifs ou à toute autre forme de tromperie ou d'artifice. »

55. https://www.sec.gov/litigation/complaints/2010/comp21452.pdf
56. https://www.sec.gov/litigation/complaints/2012/comp22238.pdf
57. https://www.sec.gov/litigation/complaints/2017/comp-pr2017-202.pdf
58. https://www.sec.gov/litigation/complaints/2016/comp-pr2016-127.pdf
59. https://ioactive.com/wp-content/uploads/2018/08/Are-You-Trading-Stocks-Securely-Exposing-Security-Flaws-in-TradingTechnologies.pdf

    https://www.sfc.hk/edistributionWeb/gateway/EN/consultation/openFile?refNo=17CP4
60. https://www.sfc.hk/edistributionWeb/gateway/EN/circular/intermediaries/supervision/doc?refNo=16EC46
61. https://www.sfc.hk/edistributionWeb/gateway/EN/circular/doc?refNo=18EC30
62. https://www.justice.gov/opa/pr/attorney-general-and-manhattan-us-attorney-announce-charges-stemming-massive-network

    https://www.reuters.com/article/hacking-indictment-idUSL1N13518P20151110

    https://www.sec.gov/litigation/complaints/2015/comp-pr2015-152.pdf
63. https://www.silicon.fr/corkow-la-cyberattaque-qui-a-fait-devisser-le-rouble-russe-138989.html
64. https://www.welivesecurity.com/2014/02/27/corkow-analysis-of-a-business-oriented-banking-trojan/

    https://www.group-ib.ru/brochures/Group-IB-Corkow-Report-EN.pdf
65. https://www.virusbulletin.com/uploads/pdf/magazine/2016/VB2016-Boutin-Cherepanov.pdf
66. Les hackers du groupe Carbanak ont débuté leurs méfaits fin 2013 avec leur logiciel Anunak qui ciblait les transferts financiers et les réseaux ATM (pour Asychronous Transfer Mode) des institutions financières. L'année suivante, ils sortaient une version plus sophistiquée d'Anunak, connue sous le nom de Carbanak, utilisée jusqu'en 2016. Puis, ils ont lancé une vague de cyberattaques encore plus sophistiquées avec le logiciel Cobalt Strike qui leur permettait d'ordonner aux guichets automatiques de « sortir » de l'argent à des moments déterminés à l'avance. https://www.lesechos.fr/2018/03/cybercriminalite-le-cerveau-du-gang-des-carbanak-arrete-987505

    https://www.europol.europa.eu/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain
67. Dans leur blog, les auteurs soulignent que le groupe Cobalt a principalement pour cibles les banques mais aussi toutes les institutions financières et qu'il pourrait se montrer particulièrement intéressé par les bourses, comme prédit par le FinCERT de la banque centrale russe.http://blog.ptsecurity.com/2017/08/cobalt-group-2017-cobalt-strikes-back.html. Ce groupe Cobalt semble toujours extrêmement actif.(https://www.romania-insider.com/financial-institutions-cyber-attacks/)
68. https://www.justice.gov/opa/pr/three-members-notorious-international-cybercrime-group-fin7-custody-role-attacking-over-100
69. D'après cet article du 1er avril 2019, la société chinoise 360 Security a publié un rapport sur les activités du groupe de menace persistante et avancée (APT) Lazarus (alias Hidden Cobra, Dark Seoul, APT38) relatives aux plateformes de cryptomonnaie. Les détournements de fonds se seraient ainsi multipliés, notamment avec la dernière compromission en date de la plateforme DragonEX en mars 2019. En analysant cette attaque, les chercheurs ont identifié un faux logiciel de trading nommé Worldbitbot utilisé par les attaquants, contenant un code malveillant, qui a été distribué au personnel interne des plateformes d'échanges de cryptomonnaie, sous prétexte de proposer une promotion sur ledit logiciel. Une porte dérobée a ainsi pu être installée sur les machines, permettant aux attaquants d'obtenir la clé privée du portefeuille, et d'opérer sur les réseaux compromis pendant des mois https://news.8btc.com/alert-lazarus-hacker-group-continues-targeting-crypto-using-faked-trading-software
70. Suivant les classes d'actifs considérées, ils étaient déjà responsables sur la période 2014-2016 d'au moins 50% à 80% des échanges quotidiens de futurs sur la bourse d'échange américaine du Chicago Mercantile Exchange, tandis que sur les marchés d'actions américains, le trading haute fréquence, qui est une sous famille du trading algorithmique, représente au moins 50% des échanges quotidiens depuis une dizaine d'années.
71. https://technologyevangelist.co/2017/12/18/security-darpa-hft-financial-markets
72. Maintenant Virtu Financial.
73. qui est principalement définie par l'article L.465-3-2 du Code Monétaire et Financier : « le fait, par toute personne, de diffuser, par tout moyen, des informations qui donnent des indications fausses ou trompeuses sur la situation ou les perspectives d'un émetteur ou sur l'offre, la demande ou le cours d'un instrument financier ou qui fixent ou sont susceptibles de fixer le cours d'un instrument financier à un niveau anormal ou artificiel. ». L'article 12.1c) du règlement européen MAR est encore plus explicite : « que ce soit par l'intermédiaire des médias, dont l'Internet, ou par tout autre moyen. »
74. https://www.thehistorypress.co.uk/articles/napoleon-is-dead-the-great-stock-exchange-fraud-of-1814/
75. Il ne semble pas que dans le domaine particulier de la cybercriminalité boursière, les motivations des attaquants soient fondamentalement différentes de celle de la cybercriminalité classique où ¾ des attaques sont motivées par un profit économique (source : https://www.hackmageddon.com)
76. On reviendra sur cet aspect dans l'analyse des cas. Un exemple d'activistes fameux est celui des « Yes Men », aux États-Unis. C'est une organisation activiste environnementale spécialisée dans la production de fausses nouvelles qui a ciblé des multinationales, en particulier pétrolières. En 2010, le géant américain Chevron a été victime d'un canular très sophistiqué, avec une campagne publicitaire détournée et faisant croire qu'il endossait la responsabilité de plusieurs catastrophes environnementales. En 2011, c'était au tour du conglomérat industriel américain GE, -accusé à l'époque de bénéficier de faveurs fiscales indues-, d'être visé par un faux communiqué des Yes Men, annonçant qu'il allait restituer 3,2 milliards de dollars au fisc. Ces derniers étaient allés jusqu'à organiser une fausse conférence de presse à Washington, en se faisant passer pour des représentants de la Chambre de commerce, jusqu'à ce qu'un membre de la vraie Chambre débarque et dévoile le pot-aux-roses.
77. https://www.lemonde.fr/pixels/article/2018/08/24/les-grandes-entreprises-de-la-silicon-valley-se-rencontrent-pour-parler-de-la-desinformation_5345665_4408996.html
78. http://www.culture.gouv.fr/Actualites/Les-enjeux-de-la-loi-contre-la-manipulation-de-l-information
79. L'automatisation algorithmique couplée à la recherche à tout prix de la rapidité, la propension naturelle des acteurs de la finance à se tenir informés des rumeurs, et l'existence d'algorithmes spécifiques dont les ordres de trading sont directement dépendants du contenu circulant sur les media officiels et/ou sociaux, que ce soit simplement de la lecture automatisée (sans intervention humaine) du contenu des pages web ou des comptes Twitter de sources officielles ou des signaux plus complexes basés sur l'analyse de l'activité même de Twitter (analyse des sentiments, des hashtags ou des comportements...) rend les marchés financiers encore plus susceptibles de succomber à ce type de manipulation.
80. https://www.lemondeinformatique.fr/actualites/lire-vinci-degringole-en-bourse-suite-a-un-hoax-66589.html

    https://www.lemonde.fr/economie-francaise/article/2016/11/23/comment-le-groupe-vinci-victime-d-un-hoax-a-chute-en-bourse_5036269_1656968.html
81. en 7 minutes
82. https://money.cnn.com/2015/04/24/investing/italian-bank-hoax/

https://www.linkiesta.it/it/article/2015/04/24/il-finto-comunicato-che-ha-fatto-tremare-il-titolo-di-intesa-sanpaolo/25628/

http://www.ilgiornale.it/news/politica/email-far-crollare-mercato-i-no-tav-attaccano-banca-italiana-1120580.html

83. http://www.telegraph.co.uk/finance/markets/11226463/G4S-shares-knocked-by-elaborate-hoax-regarding-companys-finances.html

84. https://www.australianmining.com.au/news/fake-press-release-wipes-314-million-off-whitehaven/

85. https://www.smh.com.au/national/nsw/jonathan-moylan-avoids-jail-term-for-fake-anz-media-release-about-whitehaven-coal-20140725zwwe7.html

86. https://www.sec.gov/litigation/litreleases/lr16671.htm

87. https://www.theguardian.com/technology/2015/jul/14/twitter-shares-fake-story-bloomberg

88. https://www.reuters.com/article/immunovaccine-regulator-hoax/trades-in-immunovaccine-shares-to-be-undone-after-hoax-spurs-30-pctjump-idUSL1N0W523G20150303

https://www.benzinga.com/news/15/02/5283736/immunovaccine-up-24-on-deal-with-gilead-sciences

89. https://www.reuters.com/article/us-fingerprint-samsung/swedish-tech-company-caught-in-hoax-samsung-bid-idUSBRE99A07N20131011

https://qz.com/134493/one-fake-press-release-created-200-million-today-and-another-one-made-it-disappear/

90. AMF, l'AMF présente l'avancement de ses travaux à la suite de la diffusion d'une fausse information relative au titre Vinci, 23 février 2017.

91. Le CFD (« Contract for Difference ») est un produit dérivé qui permet une exposition identique aux variations de l'action multipliée par un effet de levier fixé à l'avance.

92. https://www.sec.gov/litigation/complaints/2016/comp-pr2016-95.pdf

93. https://www.sec.gov/litigation/complaints/2017/comp23836.pdf

94. https://www.sec.gov/litigation/complaints/2015/comp-pr2015-110.pdf

95. Un futur ou contrat à terme est un contrat standardisé négocié sur un marché organisé permettant de s'assurer ou de s'engager sur un prix pour une quantité déterminée d'un produit donné (le sous-jacent) à une date future.

96. Des futurs relatifs au bétail sont échangés notamment au Chicago Mercantile Exchange (CME).

97. https://www.francetvinfo.fr/economie/bourse/marches/les-trois-plus-grosses-bourdes-des-agences-de-notation_25721.html

98. https://lexpansion.lexpress.fr/actualite-economique/standard-poor-s-reprimande-pour-avoir-degrade-la-france-par-erreur_1548720.html

99. En 2018, Facebook avait supprimé plus d'un quart de ses comptes car prétendument faux. https://www.cnet.com/news/facebook-deleted-583-million-fake-accounts-in-the-first-three-months-of-2018/

En 2017, une étude révélait qu'au moins 15% des comptes Twitter pouvaient être des bots!

https://www.cnbc.com/2017/03/10/nearly-48-million-twitter-accounts-could-be-bots-says-study.html

Toutes les applications « réseaux sociaux » sont touchées, ainsi Whatsapp supprime-t-elle 2 millions de comptes par mois pour lutter contre les fausses informations.

https://www.lemonde.fr/pixels/article/2019/02/07/whatsapp-supprime-2-millions-de-comptes-par-mois-pour-lutter-contre-les-fausses-informations_5420513_4408996.html

100. https://arxiv.org/abs/1601.05140

101. https://www.vox.com/2018/1/23/16923276/facebook-twitter-russia-interference-congress-release-the-memo

102. https://www.sec.gov/oiea/investor-alerts-bulletins/ia_rumors.html

103. https://www.sec.gov/oiea/investor-alerts-bulletins/ia_rumors.html

104. https://seekingalpha.com/article/2274553-cynk-technology-promoters-push-market-cap-to-655-million-despite-39-in-assets-and-norevenue-100-percent-downside?page=1

http://promotionstocksecrets.com/cynk-aftermath-putting-together-pieces-puzzle/

https://www.sec.gov/litigation/complaints/2015/comp-pr-2015-157.pdf

105. https://www.sec.gov/litigation/complaints/2015/comp-pr2015-254.pdf

106. https://www.reuters.com/article/net-us-usa-whitehouse-ap/hackers-send-fake-market-moving-ap-tweet-on-white-house-explosionsidUSBRE93M12Y20130423

https://www.washingtonpost.com/news/worldviews/wp/2013/04/23/syrian-hackers-claim-ap-hack-that-tipped-stock-market-by-136billion-is-it-terrorism/?utm_term=.e0629cdeaadf

107. Ainsi, d'après un sondage réalisé auprès de 800 sociétés, plus de la moitié n'aurait pas de système en place robuste pour valider et assurer la qualité de leurs données, alors que la plupart d'entre elles reconnaissent qu'un usage de plus en plus soutenu est fait de ces données pour automatiser les décisions d'investissement, entrainant un risque de manipulation élevé . https://www.finextra.com/newsarticle/31978/fake-data-will-make-banks-vulnerable-accenture?utm_medium=dailynewsletter&utm_source=2018-4-23&member=42526

108. ou à tout le moins de techniques sophistiquées d'apprentissage ou de machine learning.

109. https://www.lemonde.fr/pixels/article/2018/02/04/du-porno-aux-fausses-informations-l-intelligence-artificielle-manipule-desormaisvideo_5251535_4408996.html

http://lirelactu.fr/source/courrier-international/b64b4654-ada4-4f5a-b0d6-4966dea55a41

110. https://edition.cnn.com/2019/01/28/tech/deepfake-lawmakers/index.html

https://www.washingtonexaminer.com/news/white-house/the-deep-fake-threat

111. https://www.ft.com/content/8e63b372-8f19-11e8-b639-7680cedcc421

112. Au moins un document est disponible « Pranktheprakster.pdf », véritable manifeste et bible contenant tout le monde opératoire ainsi que toutes les étapes et astuces pour réussir son hoax boursier : pourquoi et comment élaborer et diffuser un faux communiqué de presse financier, obtenir les emails des journalistes, créer des faux sites, envoyer des mails d'une fausse adresse en exploitant les faiblesses du protocole SMTP avec Telnet sans oublier de rester anonyme...

113. VPN pour « Virtual Private Network ». C'est un réseau privé « virtuel » qui permet de créer un lien direct et sécurisé entre deux ordinateurs distants. Des sociétés proposent donc des services VPN en établissant un VPN entre votre ordinateur et un serveur de cette société. Lors de la connexion à l'Internet sur votre ordinateur, seule l'adresse IP de ce serveur sera visible. Bien entendu, les sociétés proposant des services de type VPN peuvent ou non enregistrer vos connexions et donc votre adresse IP d'origine.

114. TOR pour « The Onion Router ». C'est un réseau informatique mondial et décentralisé dont les serveurs sont aussi appelés noeuds. Ce réseau permet d'anonymiser l'origine des connexions à Internet (la fameuse adresse IP d'origine) en faisant rebondir les échanges sur différents noeuds, qui ne connaissent que l'adresse IP du noeud précédant et suivant. TOR propose également à ses utilisateurs un ensemble de services cachés, en cachant l'identité du serveur qui les héberge. Ce serveur recevra une adresse en onion et ne sera accessible qu'avec TOR. C'est une partie du fameux Dark Web.

115. Même si certains paiements réalisés par Bitcoins peuvent être tracés, il ressort que les plateformes d'échange bitcoins/FIAT ne sont pas toutes exigeantes en termes de KYC « Know Your Customer ». La législation européenne est en train de changer à cet égard mais l'harmonisation mondiale est encore loin.

116. https://www.iosco.org/research/pdf/swp/Cyber-Crime-Securities-Markets-and-Systemic-Risk.pdf

117. Une attaque par déni de service vise à rendre un serveur ou une infrastructure indisponible.

118. Si les systèmes de trading (« core engine » ou « matching engine ») sont compromis, on imagine aisément les cybercriminels tirer profit de cette compromission en augmentant ou diminuant « artificiellement » le prix respective-

ment de leur vente ou de leur achat. Les attaques dont on parle semblent se limiter à des compromissions du réseau interne/externe « corporate » de la société qui gère la Bourse. Il est aussi évident au vu de l'importance de ces infrastructures que le secret défense s'impose.

119. https://www.justice.gov/sites/default/files/opa/press-releases/attachments/2015/02/18/drinkman_vladimir_et_al_indictment_comp.pdf

https://www.justice.gov/opa/pr/russian-national-charged-largest-known-data-breach-prosecution-extradited-united-states

https://arstechnica.com/information-technology/2013/07/nasdaq-is-owned-five-men-charged-in-largest-financial-hack-ever/

120. https://www.akamai.com/de/de/multimedia/documents/content/ddos-attacks-against-global-markets-white-paper.pdf

https://www.ft.com/content/f448a9b6-c33a-11e0-9109-00144feabdc0#axzz2kSbxNfZ2

121. cf. note 120

122. https://thehill.com/policy/cybersecurity/221806-hackers-breach-the-warsaw-stock-exchange

123. Relatives à la cybersécurité, à la protection des données personnelles ou aux « fake news ».

OUVRAGES RÉCENTS

ISO 37001

SYSTÈME DE MANAGEMENT ANTI-CORRUPTION

AUTEURS : CHARLES BARATIN ET FRANÇOIS SIBILLE

ÉDITEUR : AFNOR

Présentation de l'éditeur

La corruption reste un véritable fléau mondial. De nature occulte et pouvant revêtir des formes très variées, elle est difficile à quantifier, néanmoins le FMI estime que, chaque année, entre 1.500 et 2.000 milliards de dollars de pots-de-vin sont versés dans le monde, soit entre 2% et 3% du PIB mondial... Au vu de l'ampleur du phénomène et de ses conséquences désastreuses, il est urgent d'agir à tous les niveaux. La norme ISO 37001 a pour but de définir des exigences et fournir des recommandations concernant la mise en oeuvre et l'amélioration d'un système de management anti-corruption, quel que soit le type de corruption auquel l'organisme – public ou privé - peut être amené à faire face au travers de ses

activités. Sous la forme de questions simples et pragmatiques, l'ouvrage fait un tour d'horizon de l'ISO 37001 : les définitions, le contexte d'émergence, la motivation à mettre en place une telle approche, le cadre réglementaire... Il met notamment en valeur les synergies avec la Loi Sapin 2 (loi sur la transparence, la lutte contre la corruption et la modernisation de la vie économique) votée en France en 2016. L'objectif est de couvrir la norme et son contexte, avec en toile de fond un déroulé du livre qui va suivre une logique de PDCA, et de rapprocher deux catégories d'experts : les professionnels des systèmes de management et les spécialistes juridiques. Les deux auteurs ont acquis une expérience pionnière en France sur ce sujet. La réalisation de cet ouvrage traduit leur volonté de partager ces retours d'expériences avec pragmatisme, simplicité et pédagogie

LA THALASSOCRATIE CRIMINELLE, CLÉ DE COMPRÉHENSION DE LA CRIMINALITÉ ORGANISÉE TERRESTRE ?

FLORIAN MANET

COLONEL DE LA GENDARMERIE NATIONALE, COMMANDANT LA SECTION DE RECHERCHES DE BRETAGNE

Dans l'imaginaire collectif, la malveillance exercée en mer se résume principalement à des actes de piraterie, à des transports de substance illicites, à la traite d'êtres humains à des pollutions maritimes et, éventuellement, à la pêche illégale. Or, la réalité est plus complexe et plus diverse. C'est ignorer le contexte contemporain de la maritimisation, ce mouvement irréfragable qui rend les territoires de plus en plus dépendants des espaces océaniques.

Les premières manifestations de la criminalité organisée apparaissent précisément en mer méditerranée, durant l'antiquité. Les raids lancés à partir d'embarcations grecques ou romaines précédent les menées des « grandes compagnies[1] » du XVIIème siècle ou encore les agissements des mafias italiennes du XIXème siècle. Force est de constater un profond déficit conceptuel de cette criminalité qui prend la mer... pour démultiplier, sur les territoires, son pouvoir de nuisance et de déstabilisation de l'ordre public socio-économique. Telle une hydre polymorphe, elle s'ancre sur des espaces distants, souvent localisés dans des continents différents, qu'elle relie, notamment, par la voie maritime. La thalassocratie criminelle[2] désigne, alors, une structure criminelle transnationale tributaire du vecteur ou de l'espace maritime pour assouvir sa volonté de puissance. Ainsi, en écho aux propos du célèbre géographe portuaire, André VIGARIÉ, qui énonce qu' « Il faut avoir présent à l'esprit que la maritimisation du monde est un phénomène irréversible et croissant ; les nations se tournent de plus en plus vers la mer ; elles développent sans cesse leurs intérêts ». La criminalité organisée contemporaine s'inscrit totalement dans cette logique de développement.

Cependant, de nombreuses difficultés aveuglent l'enquêteur et le magistrat. Ceci a pour effet direct de taire cette réalité flagrante et, de fait, d'en minimiser l'impact. Certes, par exemple, les critères de compétence juridique, le cadre légal, le vocabulaire ou encore les logiques de milieu ne facilitent point l'appréhension de scènes d'infractions parfois très éloignées. Ces dernières impliquent des acteurs inhabituels et internationaux connectés avec les espaces terrestres.

Identifier les filières primaires d'approvisionnement en biens illicites, volés, contrefaits ou violant des embargos ; identifier les rouages compromis de ces échanges illicites globalisés au sein des chaînes logistiques intégrées et connectées avec un hinterland criminel ancré dans la profondeur des territoires ; comprendre les mécanismes internationaux de blanchiment des trafics illicites ; sécuriser les approvisionnements stratégiques d'économies globalisées, en flux tendus, tels se résument les enjeux actuels de la lutte contre la criminalité organisée. Dans un contexte de maritimisation universelle, l'investigation judiciaire ne peut passer sous silence un milieu couvrant 70 % d'un globe abusivement appelé

« terre », un vecteur logistique par lequel transite 90 % de nos biens et des fonds marins qui acheminent 99 % de nos échanges numériques. Énoncée de manière synthétique, la stabilité des territoires comme la sûreté des mobilités humaines résident dans la maîtrise du lien terre-mer, à la fois sous l'angle économique, logistique, politique mais aussi sécuritaire. Il s'agit de l'espace à plus fort développement pour l'humanité, à côté du cyberespace et du spatial.

I. La criminalité maritime, une *terra incognita* ?

La criminalité maritime et portuaire est un champ d'étude à défricher. Usuellement, la lutte contre la délinquance est appréhendée de manière géo-centrée, même si, notamment en matière de stupéfiants, des perspectives océaniques ouvrent régulièrement les enquêtes judiciaires sur les vecteurs maritimes. Le maritime embrasse la criminalité dans une perspective spatiale des plus ouvertes : il invite à un regard global, à la fois au sens de la mondialisation mais aussi dans une logique d'une filière entière, du producteur au consommateur.

A. Le chiffre noir de la criminalité maritime

Un chiffre noir[3] maintient cette criminalité maritime confidentielle.Cette approche restrictive est renforcée par l'absence d'indicateurs statistiques propres à l'environnement maritime. Les principes méthodologiques usuels sont conçus pour des espaces terrestres, finis et circonscrits à des compétences territoriales des services d'enquête et des tribunaux. Or, dans le domaine maritime comme pour d'autres modes de transport terrestre, les sources d'erreurs peuvent être importantes. En effet, comment localiser dans l'espace un vol ou une agression sexuelle commise lors d'une croisière ? Où vont porter plainte les victimes pour ces faits ? Dans leur pays d'origine ? Lors de l'escale suivante ? Ou encore à l'escale terminus ? Tout cela illustre les limites de l'approche statistique bien souvent fondamentale dans la prise en compte d'une réalité criminelle.

B. Les difficultés à caractériser la criminalité maritime

Les difficultés à caractériser cette activité criminelle sont liées à la spécificité du milieu maritime et portuaire. Analyser ces difficultés revient à décrire la nature de l'écosystème maritimo-portuaire, en appréhender les enjeux de sécurité et suggérer les contraintes qui s'imposeront, ensuite, à toutes actions répressives.

Le fait maritime impose un changement d'échelle radical : c'est se confronter à l'immensité océanique, au gigantisme de la construction navale comme à ceux des flux de fret (matières premières ou biens de consommation) diffusés par voie maritime. La route empruntée par les portes conteneurs entre l' « usine du monde », la Chine, et les ports européens du *Northern range*[4] nécessite une quarantaine de jours de mer. Une durée identique nécessaire pour rallier en multicoque la côte pacifique colombienne avec les atolls tahitiens.

De plus, une organisation administrative particulière caractérise l'entreprise maritime. La multiplicité d'intervenants, bien souvent internationaux, rend difficile l'identification des responsabilités au sein de la chaîne logistique et de l'expédition maritime : shipowner, armateur, fréteur, affréteur, consignataires, investisseurs, institutions bancaires, compagnies d'assurance, acteurs étatiques (gendarmerie maritime, douanes, affaires maritimes,...). Cette opacification organisationnelle se trouve accrue par les changements de propriétaires de la coque ou du fret. Sans compter les changements d'immatriculation sous des pavillons[5] pouvant être exotiques. Ces process maritimes démultiplient les possibilités classiques observées à terre. La dimension internationale est congénitale à l'expédition maritime : un équipage est la somme de multiples talents de nationalité différente, par exemple. De fait, cela suggère des coopérations internationales permanentes, établies avec des pays peu rodés à la coopération policière ou à l'entraide pénale internationale. Rappelons que 60 % des registres de pavillons relèvent du Liberia, du Panama, des Îles Marshall, de Singapour ou encore de Hong Kong.

Enfin, les spécificités de l'aventure maritime conjuguées à l'internationalisation des liaisons maritimes ont généré un cadre légal singulier : le droit de la mer. Longtemps immuable, cette branche du droit public international a été progressivement codifié au fil des siècles jusqu'à obtenir un (relatif) consensus[6] international au travers d'une constitution de la mer : la

Convention des Nations unies du droit de la mer signée à Montégo Bay, en Jamaïque, le 10 décembre 1982. Figurant comme l'un des instruments juridiques les plus importants du XXème siècle, son champ d'application est vaste et couvre l'ensemble de l'espace marin et de ses utilisations : la navigation et le survol, l'exploration et l'exploitation des ressources, la conservation des ressources biologiques, la protection et la préservation du milieu marin et la recherche scientifique marine. Les enseignements majeurs sont, d'une part, la territorialisation de l'espace océanique en reconnaissant la ligne des douze miles nautiques[7] comme délimitation des eaux territoriales de l'État côtier et, d'autre part, le pavillon arboré par les navires. Corrélativement, les notions de « passage inoffensif[8] » dans la mer territoriale ou de « passage en transit » dans les détroits servant à la navigation internationale concrétisent le principe immuable de la liberté de navigation. L'essentiel de la compétence en matière de souveraineté contre une menace humaine malveillante autre qu'environnementale est comprise entre 0 et 12 miles nautiques. L'action douanière est élargie à la zone contiguë d'une largeur de 12 miles nautiques aussi.

C. Des difficultés générées par la maritimisation contemporaine

L'analyse de la criminalité maritime s'intègre dans les enjeux d'une maritimisation généralisée et irréversible d'économies globalisées. On constate le dévoiement de l'expédition maritime et du commerce international par les organisations criminelles. Comment envisagent-elles ces potentialités infinies ? Comment s'opère ce mécanisme ? Envisageons cette étude au travers de plusieurs focus : le vecteur, l'infrastructure portuaire et enfin les espaces océaniques.

i. Le vecteur de la maritimisation

Le navire symbolise l'aventure maritime et ses caractéristiques. Il cristallise la recherche d'investisseurs susceptibles d'immobiliser un capital-risque important motivé par la perspective d'un gain à moyen terme. À titre d'illustration, le porte-conteneur CMA CGM BOUGAINVILLE[9] est évalué à l'achat à 150 millions de dollars. Fournisseur de services, il est inséré dans un écosystème complexe conditionnant sa rentabilité : la crise de 2008 a affecté le modèle économique des grandes unités et provoqué une recomposition de la flotte mondiale. Des transferts de propriété de navires sur le marché de l'occasion de deuxième voire troisième main facilitent ainsi l'acquisition de vecteurs par des armateurs peu regardant sur la raison sociale des commanditaires, le but étant de gagner des marchés quels qu'ils soient. C'est un mécanisme[10] susceptible de contribuer à la criminalisation de l'expédition maritime. Camouflage idéal de biens illicites par ses multiples caches où, par la navigation maritime, le navire est aussi malgré lui un ambassadeur : il projette des réalités géopolitiques inspirées par ses escales sur d'autres territoires non préparées. Le niveau de sûreté du port de départ constitue un critère de vigilance du port de destination.

ii. L'infrastructure portuaire

Ensuite, le port interface les gens de mer et le commanditaire, transformateur et consommateur établis à terre. Connectant des routes maritimes et un hinterland, c'est aussi un lieu de fragilité dans la chaîne logistique du fait de la rupture de charge du fret. Cette réorganisation de la cargaison massifiée génère implicitement une forte tension logistique, financière, sécuritaire et … criminelle. Pour tous, il s'agit de s'assurer de l'arrivée à bon port de ses biens et de leur bonne redirection dans un flux prédéterminé. Ces plates-formes logistiques multimodales nécessitent des intervenants de toute nature afin de gérer des millions de données à forte valeur économique. Rappelons qu'un porte-conteneurs transporte l'équivalent ferroviaire de 100 kilomètres. Ces enjeux suggèrent la pression exercée sur des organisations criminelles et les perspectives de corruption des intervenants licites de la chaîne logistique.

iii. Les espaces océaniques

Enfin, couvrant 70 % du globe, l'espace océanique est régi par les lois naturelles et les règles de la navigation. Le contrôle des « autoroute des mers » ou des gisements de richesses halieutiques, minérales… constituent des enjeux géopolitiques majeurs au travers de conflits d'usage dont peuvent s'emparer des organisations criminelles. La liberté de navigation et l'immensité océanique entretiennent un sen-

timent d'impunité. D'autant plus que les mers ont été longtemps définies comme res communis (la chose commune) ou res nullius (la chose n'appartenant à personne). Cela suffit-il pour que certains s'arrogent le titre de maître pour se les approprier à leur profit exclusif ? Cela aiguise de fait les intérêts particuliers d'opérateurs illicites qui les considèrent comme un théâtre d'opération criminelle ou un vecteur de leurs activités répréhensibles.

II. Une criminalité maritime aux caractéristiques propres

L'éco-système maritime façonne une criminalité aux caractéristiques propres dont l'influence se mesure aussi à terre.

A. La criminalité maritime génère un impact global

La manifestation de la criminalité maritime a un impact durable et irréversible sur l'écosystème terrestre. Ainsi, la pollution maritime générée par l'avarie du roulier Grande America, le 15 mars 2019, a menacé de souiller les côtes charentaises pourtant distantes de 350 km. Il produira des effets jusqu'à épuisement des produits contenus dans l'épave. La surpêche épuise la ressource halieutique, compromettant le renouvellement des stocks, affectant les équilibres nourriciers et financiers pour les acteurs locaux.

Le degré de maritimisation des sociétés détermine l'intensité de l'effet d'amplification sur l'écosystème terrestre. Ainsi, en juin 2017, le rançongiciel Petya a contraint à une reprise manuelle des terminaux portuaires opérés par MAERSK dans 76 pays, ce qui provoqua une désorganisation majeure de l'économie mondiale. De même, les aléas climatiques ou techniques génèrent des modifications des plans de continuité d'activité préjudiciable aux économies en flux tendus, tributaires d'importation, par voie maritime, de matières premières ou de biens manufacturés. Les conséquences financières d'un défaut d'approvisionnement des chaînes de montage automobiles sont effectivement considérables. Dans ce village global tributaire de la maritimisation des économies comme des modes de vie, le frémissement observé sur un espace peut avoir ailleurs des conséquences majeures.

B. La criminalité maritime stimule une hybridation criminelle

Le développement de l'activité criminelle génère des convergences d'intérêts entre organisations licites et illicites qui finissent par échanger des savoir-faire et des compétences. Les frontières entre légal/illégal, État/privé et civil/militaire s'atténuent, banalisant davantage les menaces criminelles. Ce mélange opportuniste est qualifié d'hybridation criminelle. Il s'exprime de multiples manière[11]. D'une façon restrictive, Alain Bauer considère que l'hybridation « entre opérateurs politiques et organisations criminelles » est le croisement d'une criminalité politique et d'une criminalité de profit. Ceci s'illustre par la piraterie maritime où la motivation financière peut se muer en finalité politique. Par différence, Xavier Rauffer se montre plus souple dans la compréhension du phénomène. L'hybride serait un « individu ou un groupe évoluant entre banditisme et terrorisme », « un terroriste qui tourne gangster après avoir perdu ses illusions ou son fanatisme »....

Cette réalité trouve à s'appliquer dans la criminalité maritime où il est observé, dans une certaine mesure, des rapprochements entre les différents réseaux. Certains savoir-faire peuvent alimenter plusieurs trafics. Ainsi, des navires de pêche peuvent être notamment utilisés pour le trafic de drogue, d'armes voire le terrorisme. La patron pêcheur dévoie sa pratique professionnelle en se livrant à la pêche, sur des gisements fermés, au-delà des quotas ou des tailles autorisées de capture, employant une main d'oeuvre non déclarée et blanchissant in fine le produit de ses campagnes. L'activité maritime peut aussi contribuer à financer le terrorisme.

C. La criminalité maritime est connectée avec la délinquance terrestre

La continuité criminelle terre-mer caractérise la criminalité maritime. L'homme ne peut élire durablement domicile en mer : la terre demeure un refuge pour les gens de mer qui y trouvent leur commanditaire ou leur consommateur. C'est, d'ailleurs, la finalité de l'expédition maritime pour les passagers comme pour le fret. C'est aussi l'espace de valorisation du profit tiré de l'exploitation de la mer (ressources halieutiques ou

matières fossiles). Enfin, il s'agit du lieu de ressourcement des membres d'équipage comme celui de la maintenance des machines. D'ailleurs, observons que les bénéfices de cette entreprise de capital-risque sont majoritairement réinvestis à terre dans des placements moins risqués : « la sécurisation du gain et son exportation hors du système de risques qui l'a généré » comme l'exprime Yan Giron[12].

Les spécificités du transport maritime attisent l'intérêt d'organisations criminelles qui se muent en thalassocratie criminelle. Elles ont pressenti, avec lucidité, l'effet démultiplicateur du fait maritime. Un voilier transporte aisément une tonne de cocaïne, un conteneur emporte 4 véhicules volés, etc. Les biens extraits des mers, produits de la mer comme hydrocarbures et autres terres rares assurent des revenus substantiels car intégrés dans une économie de la rareté.

D. La marétique révolutionne l'évaluation du risque maritime

La marétique[13] révolutionne l'évaluation du risque maritime En effet, l'univers mental des gens de mer désignait, auparavant, la terre comme un refuge, un lieu de sécurité en comparaison de l'adversité des éléments naturels. Or, aujourd'hui, le navire devient un objet connecté, bientôt autonome, dont la programmation ou la maintenance s'effectuent depuis la terre.

Cette déshumanisation de l'aventure maritime s'accompagne d'une dépendance accrue aux SCADA[14] : un gouvernail dispose d'une adresse IP tout comme la propulsion. Et si un vers malveillant était introduit à bord lors d'une opération de maintenance et s'opérait à la mer ? De même, la sécurité de la navigation maritime repose sur un maillage de balises virtuelles équipées de la technologie AIS (Système d'Identification Automatique) indiquant les obstacles à la navigation. Qu'en sera-t-il si l'une d'entre elles émet un signal falsifié ?

La démocratisation contemporaine de la cyber-malveillance introduit une stratégie du faible au fort renversée : des cyberpirates investissant quelques centaines d'euros sont en mesure de causer des préjudices s'élevant à plusieurs dizaines de millions d'euros et de provoquer une désorganisation du commerce international. La terre devient alors synonyme de lieu de compromission d'une expédition maritime.

III. Les manifestations maritimes du capitalisme criminel

Les menaces directes exercées sur le vecteur et l'espace maritime se résument à cinq grands items susceptibles de se combiner entre eux : cybermenaces, atteinte à la sécurité[15] et sûreté maritime (dont les trafics illicites), atteintes à l'environnement naturel, terrorisme (prolifération). Ces menaces s'insèrent dans l'environnement maritime considéré, d'une part, comme un théâtre des opérations criminelles et d'autre part, comme un vecteur du crime. Le fait maritime constitue un fournisseur de services, un générateur d'opportunités et un démultiplicateur du projet criminel.

A. Un théâtre d'opérations criminelles

Les espaces océaniques constituent des terrains de jeu d'envergure pour des organisations criminelles. Elles exploitent avec agilité les lacunes du droit international codifiant et régulant un milieu hétéromorphe où les potentialités semblent infinies malgré des difficultés d'accès. Ainsi, la pêche illégale désigne une pratique dérégulée et dévoyée d'exploitation des richesses naturelles présentes dans les océans. Elle s'inscrit dans une logique de rente de richesses pensées comme indéfiniment renouvelables même si toutes ne sont pas exploitées ni découvertes. Or, l'économie bleue s'inscrit dans une logique de rareté voire de pénurie. Sous des atours uniformes, tous les espaces maritimes ne se valent pourtant pas : la richesse des gisements comme les critères d'accessibilité diffèrent d'un point à l'autre des 360 millions de km2. La FAO[16] (Organisation des Nations unies pour l'alimentation et l'agriculture) estime que la pêche illégale représente 20 à 30 % des prises mondiales. Ce qui se traduit par un chiffre d'affaire évalué à plus de 10 à 20 milliards de dollars par an. Aujourd'hui, 61,3 % des stocks halieutiques mondiaux sont exploités à leur seuil maximum de renouvellement tandis que 28,8 % sont surexploités. Derrière cette activité ancestrale se dissimule un écosystème particulièrement prolifique susceptible d'être connecté à la criminalité

organisée et d'alimenter une économie souterraine concurrençant l'autorité légitime de l'État. La pratique régulière du sur-quota et des prises en sous-taille génère des infractions relatives au droit du travail, à la fraude sociale, à la traite d'êtres humains, au blanchiment et d'atteintes graves à l'environnement. Son impact déborde des limites de la région maritime pour se répandre sur l'ensemble de la chaîne avale de transformation et de commercialisation des produits de la mer. La reconnaissance d'un « crime halieutique » renforcerait les effets répressifs d'une approche nécessairement multi-sectorielle, partenariale et internationale. D'autres atteintes graves à l'environnement maritime telles les pollutions maritimes volontaires ou résultant d'une fortune de mer illustrent les limites d'une action répressive en mer : difficultés de la constatation et de l'identification des auteurs de l'infraction.

Les océans sont aussi le cadre d'expression de la violence. Même si ce phénomène n'a pas changé de nature au fil des siècles, sa définition s'est progressivement codifiée et stabilisée. L'article 101 de la Convention sur le droit de la mer définit la piraterie maritime[17] comme « *un acte illicite de violence ou de détention ou de déprédation commise par l'équipage ou des passagers d'un navire (...) agissant à des fins privées (...) en haute mer* ». Agissant hors des eaux territoriales et hors de toute revendication politique, elle illustre le rapport inversé du faible au fort, ce que rend possible le milieu maritime à la différence des agissements à terre. Un sommaire boutre somalien peut alors défier et prendre l'ascendant sur un *super tanker* affrété par les *majors*. C'est bien là l'état d'esprit du pirate comme le suggèrent les étymologies grecques (*peiratês*) qui désignent « *un brigand, un bandit qui court les mers pour attaquer les navires* » et latine qui enrichit cet héritage de la notion de « *tenter sa chance à l'aventure* ». Par ailleurs, « *la souplesse de l'instrument donne une prime au maître de la mer, libre d'attaquer à de multiples endroits* »[18]. Même si, vus de la terre, les océans paraissent des espaces vides, la menace[19] peut se révéler alors intense sur de très vastes espaces stratégiques au point d'imposer aux flottes de commerce internationales la reconfiguration des routes maritimes. Enfin, les perspectives actuelles liées au contexte du terrorisme envisagent des scénarii de « Bataclan sur mer » où un navire à passagers serait victime d'une attaque[20] à la mer perpétrée par des organisations radicales.

Au delà de la violence faite aux personnes, les mers sont aussi l'arène où s'exprime la compétition inter-étatique dans laquelle s'immiscent aussi des structures criminelles. Tributaires de flux maritimes, des puissances peuvent être tentées d'enfreindre des embargos internationaux. Ainsi, l'actualité démontre les capacités de dissimulation offertes par des opérations maritimes apparemment banales mêmes si elles demeurent complexes. Des enquêtes récentes ont mis en lumière la contrebande d'hydrocarbures entre la Libye et des pays d'Europe du sud, sur fond d'instabilité politique au Maghreb. La mer méditerranée a, de fait, connecté autour d'un projet criminel des organisations libyennes et des structures mafieuses italiennes. Frauduleusement extrait d'une raffinerie libyenne par des navires de pêche, le pétrole était ensuite transbordé en haute mer à bord de tankers avant un déchargement sur des ports européens. Il approvisionnait alors le réseau de pompes à essence. Sur une période d'un an, il a été estimé le détournement de 80 millions de litres achetés à moins de 50 % du prix du marché. Outre l'infraction de contrebande, apparaissent des fraudes sociales et fiscales ou des escroqueries à la TVA d'ampleur. En filigrane, se dessinent des soupçons de financement du terrorisme.

B. Un vecteur du crime

Les espaces océaniques peuvent être perçus comme le support logistique d'un commerce criminel. Il est insidieusement inséré dans une chaîne logistique mondiale en pleine expansion, dont serait tributaire la santé économique des États. La thalassocratie criminelle détourne de son usage conventionnel les navires (navire de pêche, plaisance, commerce, plate-forme off-shore ...) et exploite à son profit les capacités de transport des conteneurs de 20 ou 40 pieds. Le transport maritime est très avantageux pour des opérateurs illicites : faible coût du transport, capacité d'emport démultiplié par rapport aux autres modes, dissimulation assurée dans la massification du fret,

dilatation des distances et du temps au regard du terrestre ainsi que la fragmentation organisationnelle entre le port origine et le port destination. La mer supporte l'acheminement des biens illicites vers la zone de commercialisation, parfois bien éloignée de la zone de production comme de prédation. C'est dans les porte-conteneurs que le fret illicite se légalise dans les flux licites de biens.

Les mers supportent une variété infinie de trafics illicites : narcotrafic, biens contrefaits, volés ou sous l'effet d'un embargo, déchets, oeuvres d'art, faune ou flore, produits alimentaires… Cette fonction logistique insérée dans la géo-économie terrestre sous-tend un capitalisme criminel dont la détection s'avère problématique. C'est à ce titre que la thalassocratie criminelle affecte l'équilibre des territoires ainsi que la sûreté des mobilités. Certes, les flux physiques comme numériques affectant les biens sont canalisés au sein de chaînes logistiques multimodales particulièrement normées et standardisées.

Cette géo-économie maritime s'apprécie sous un triple prisme. Tout d'abord, la réticularité de l'économie, qui se mesure à l'aune du niveau d'insertion ou d'interconnexion dans les réseaux physiques comme virtuelles d'opérateurs de transport. Elle traduit le dynamisme commercial dont la capacité de transport hebdomadaire de flux conteneurisés, le nombre de connexions régulières, la présence d'acteurs (commissionnaires, courtiers d'assurance ou encore sièges sociaux) constituent autant de critères d'évaluation. Ensuite, la centralité : la zone portuaire (incluant la ville portuaire) constitue un point de convergence, un centre logistique d'intérêt régional, national voire international en fonction de ses qualités ou de son rayonnement. Enfin, on parle aussi de nodalité : le port est un noeud de communication particulièrement complexe qui possède une fonction de carrefour au coeur d'un réseau de relations, internationales notamment.

Dans ce contexte général se développe un capitalisme criminel très dynamique et souvent insoupçonné. L'enjeu est alors de déterminer son degré d'insertion dans cette géo-économie dont finalement le port et – in fine - le navire constituent un maillon faible dans la chaîne logistique et un point physique de convergence du fret illicite.

L'analyse des situations géopolitiques des organisations logistiques amont et aval au transport maritime constitue un préalable à l'évaluation du risque. Elle explicite le niveau de sûreté des opérations et installations logistiques, le degré de loyauté des acteurs licites locaux, la disponibilité de produits illicites ou encore le dynamisme de l'économie souterraine locale ou régionale. Celle-ci peut expliquer la présence de sacs contenant de la cocaïne dans des lots conteneurisés de bananes ou de produits de la mer congelés par exemple. Elle justifie l'exportation de véhicules volés dans les métropoles européennes qui s'écoulent ensuite en Afrique ou ailleurs depuis les ports du Northern range européen. De plus, il convient de cartographier sur ce hub logistique - comprenant l'avant-port, le port et l'hinterland – le relationnel développé par des acteurs illicites. Ainsi, leur pouvoir d'influence, molle ou dure, et leur capacité d'agir seront évalués. Cette analyse pointera les ressorts propres à cette économie criminelle composée d'intervenants multiples distinguant des prestataires de service (logistique, financier, ..) se mettant à disposition, de manière directe ou indirecte, de commanditaires. C'est ainsi que la thalassocratie criminelle se connecte avec les organisations criminelles terrestres.

En effet, les organisations criminelles ont vite perçu les atouts des espaces océaniques et la puissance de la mondialisation contemporaine. La maritimisation emporte avec elle inéluctablement les opérateurs illicites, partageant avec eux sa force, son intensité et ses perspectives prometteuses. Comment imaginer une prospérité illicite sans le recours à un océan ou un navire ?

Aux côtés du cyberespace et du spatial, la mer demeure l'espace au plus fort potentiel de développement. Supportant 90 % du commerce international, 99 % des transmissions numériques, elle offre des effets démultiplicateurs pour toutes entreprises licites comme illicites. Dans ce contexte émerge un acteur de poids, objet de multiples conventions internationales, mais non signataires de ces normes : la thalassocratie criminelle. Moteur d'une économie souterraine dynamique, cette hydre intercontinentale déploie, continuellement, ses membres sur tous les continents qu'elle relie,

insidieusement, s'immisçant dans des vecteurs maritimes. Les espaces océaniques supportent, malgré eux, des trafics illicites de toutes natures. Par leur intensité et leur diversité, ils sont susceptibles de mettre en danger les équilibres socio-économiques des territoires ainsi que la sûreté des mobilités humaines comme celle des matières premières ou des biens de consommation.

Lutter contre cette thalassocratie criminelle, c'est développer une meilleure compréhension des mécanismes criminels à l'oeuvre sur les territoires. Au préalable, changeons instamment notre manière d'appréhender ces phénomènes. Élargissons davantage notre approche de l'économie souterraine. Ce nouveau regard, thalassocentré, permet d'embrasser de manière globale le capitalisme criminel qui se nourrit des circuits complexes d'une économie-monde. De fait, les filières illicites émergeront précisément dans leur complétude : de l'ouvrier au commanditaire sans omettre les prestataires de service ; des mécanismes frauduleux de génération de capitaux aux circuits de blanchiment les plus divers. Pour ce faire, il convient d'élargir notre focale selon deux axes majeurs : la fertilisation croisée du renseignement et l'enrichissement d'un partenariat national comme international. Connecter la thalassocratie à la géo-économie criminelle invite à une fusion de l'intelligence qu'il soit de nature judiciaire comme administrative, national comme international. La nécessaire convergence des cultures propres à la défense nationale[21] avec celle de la sécurité intérieure doit s'enrichir d'une approche économique et logistique. Cet effort suggère donc un partenariat étroitement développé entre acteurs publics comme privés, nationaux comme internationaux.

Notes :

1. In Les cahiers de la sécurité de l'INHES, janvier-février 2009, Les organisations criminelles.
2. In Le crime en bleu, essai de thalassopolitique, Florian MANET, édition Nuvis, mai 2018
3. Le chiffre noir désigne l'ensemble des crimes qui ne sont pas connus du système pénal. Il ne s'auto-alimente pas. Pour qu'un service de police ait connaissance d'une infraction, il faut qu'une victime ou un témoin lui rapporte les faits. Sont exclus les infractions relevées à l'initiative des services (contrôle de vitesse, usage de produits stupéfiants,...).
4. Le northern range ou rail du nord, deuxième façade maritime mondiale, désigne une rangée portuaire long de 800 kilomètres, de Dunkerque à Hambourg en passant par Anvers et Rotterdam. Il exerce une influence internationale. Rotterdam, le champion européen des ports de commerce, est relié à plus de 1000 ports répartis sur les cinq continents. De même, supportant majoritairement un flux d'importation, Rotterdam relie au monde plus de 150 millions de consommateurs, établis à proximité du Rhin et de ses affluents. Cette dorsale européenne s'étend jusqu'à plus de 500 kilomètres de la mer du nord. Grâce à de puissantes infrastructures logistiques et de transport routier, ferroviaire ou aérien, elle bénéficie, en moins de 24 heures, des marchandises et productions débarquées à Rotterdam.
5. Pierre ANGELLELI évoque un double mouvement: le flagging out ou dépavillonement et le flag shopping ou recherche d'un mieux disant pour l'armateur in thèse en sciences économiques soutenue à l'université des Antilles et de la Guyane en 2012, « la libre immatriculation des navires : un gain pour les petites économies insulaires? », disponible sur https://halshs.archives-ouvertes.fr/tel-00697681/document
6. 119 États signent dés le premier jour la CNUDM. Il faudra, cependant, attendre le 16 novembre 1994 pour que cette convention entre en vigueur, les 60 ratifications ayant été obtenues. Aujourd'hui encore, des grandes puissances n'ont toujours pas ratifié ce texte même si elles en appliquent les principes.
7. Un mile nautique correspond à 1.852 kilomètres. 12 miles nautiques équivallent à 19 kilomètres, 200 miles à 370 kilomètres.
8. Article 19 de la CNUDM.
9. Ce porte-conteneurs de la compagnie française CMA-CGM a été mis à flot le 25/08/2015. Long de 398 mètres, il transporte plus de 17 000 conteneurs sur la ligne maritime French Asia Line. Tous les 77 jours il escale au Havre.
10. Toxicité de la surcapacité maritime par Yan Giron et Caroline Britz dans Sécurité globale n° 13 / 2018-1.
11. Mémoire de droit pénal sous la direction du professeur Yves Mayaud – Université de Panthéon-Assas, L'hybridation criminelle, 2014 par Marc-Antoine Fioc.
12. Ibid.
13. Contraction entre maritime et numérique, ensemble des systèmes d'information et de traitement de données relatif aux activités maritimes et portuaires
14. Le SCADA (Supervisory Control and Data Acquisition) est un système de télégestion à grande échelle permettant de traiter en temps réel un grand nombre de télémesures et de contrôler à distance des installations techniques.
15. La sécurité ou safety désigne les risques liées à l'activité tandis que la sûreté ou security concerne la malveillance.
16. Ou Food and Agriculture Organization of the United Nations.
17. Cette violence exercée dans les eaux territoriales se nomme « brigandage ».
18. In La lutte pour l'empire de la mer sous la direction d'Hervé COUTEAU-BEGARIE, Economica, 1995.
19. Le Golfe de Guinée ou la mer des Célèbes ou de Sulu en Asie demeurent des points d'attention.
20. De tels agissements ont déjà eu lieu au cours de l'histoire comme le détournement de l'Achille Lauro en 1985 par une organisation palestinienne
21. Les conventions internationales attribuent aux marines de guerre des pouvoirs de police en haute mer.

LA STRATÉGIE DU CRIME ORGANISÉ TRANSNATIONAL ET LES FAUX MÉDICAMENTS

BERNARD LEROY

DIRECTEUR DE L'INSTITUT INTERNATIONAL DE RECHERCHE ANTI-CONTREFAÇON DE MÉDICAMENTS (IRACM)

Ce n'est qu'à partir du milieu des années 80 que la communauté internationale a commencé à prendre conscience de la menace des faux médicaments pour la population mondiale. Aujourd'hui, le risque de consommer – involontairement - un faux médicament s'aggrave de façon exponentielle pour tout patient du « village terre ». Ce risque peut devenir un réel danger pour la vie de chacun, mais aussi globalement, pour la santé publique mondiale.

Le crime organisé transnational a très vite perçu l'intérêt d'investir ce domaine et son potentiel, dans le contexte de la mondialisation et du développement d'Internet.

L'exploitation de cette problématique accroît le pouvoir financier du crime organisé, mais aussi son emprise au niveau local et intercontinental.

I. Le phénomène des faux médicaments

A. Les faux médicaments en chiffres

Aujourd'hui, le trafic de faux médicaments a atteint une ampleur sans précédent au niveau mondial. Des centaines de milliers d'enfants, de femmes et d'hommes sont victimes de la cupidité de criminels organisés en réseaux. La contrefaçon de médicaments contre le paludisme et la tuberculose serait à elle seule responsable de 700 000 morts par an (chiffre 2009 – International Policy Network).

En Afrique, les taux de médicaments falsifiés varient entre 30 % et 70 % selon les pays[1]. 30% en Amérique Latine et 1% dans les pays développés selon l'Organisation mondiale de la santé (OMS), qui estime que le chiffre d'affaires mondial du trafic de faux médicaments aurait atteint 45 milliards de dollars en 2006 et 75 milliards en 2010. On avance maintenant le chiffre de 200 milliards.

À noter que 50 % des médicaments vendus sur des sites internet dissimulant leur adresse physique sont faux ou pour le moins non conformes (OMS) et 95% des sites internet vendant des médicaments sont illégaux.

Le spectre des classes thérapeutiques concernées est très vaste : traitement des maladies graves telles que le paludisme, le diabète, l'hépatite, la tuberculose, le sida, entre autres. Dès lors, les faux médicaments se retrouvent parmi les produits antibiotiques, les vaccins, les anticancéreux[2] et les médicaments dits de confort. De manière intelligente, les trafiquants ciblent en priorité les maladies touchant le plus grand nombre pour garantir le maximum de bénéfices.

En France, le crime organisé sévit sur Internet et cible en priorité les troubles de l'érection, la recherche d'amaigrissants ou d'anabolisants.

Les faux médicaments sont des produits très dangereux du fait de l'absence de principe actif dans 1/3 des cas, d'ingrédients insuffisants dans 20% des produits ou de présence de produits toxiques. De surcroît, le recours aux faux médicaments aggrave le développement d'un phénomène très inquiétant actuellement en pleine croissance : la résistance d'infections aux antimicrobiens (Assurance maladie

obligatoire des indépendants - RAM)[3]. Les véritables médicaments utilisés pour soigner deviennent inefficaces et certains micro-organismes deviennent alors résistants à la plupart des antimicrobiens. Sur un million de décès annuels dus au paludisme, 200 000 morts auraient pu être évités si les malades avaient été soignés avec de vrais médicaments (OMS).

Globalement donc, les faux médicaments créent des résistances, entraînent l'aggravation et la chronicisation des maladies et provoquent la mort.

B. Même les médicaments vétérinaires sont concernés

Les trafiquants s'intéressent également aux produits vétérinaires comme l'atteste la multiplication des saisies de faux médicaments vétérinaires[4]. Les risques existent aussi bien parmi les médicaments destinés aux animaux domestiques qu'aux animaux d'élevage. Le trafic procède des mêmes méthodes que celui des faux médicaments à usage humain (faible dosage en principe actif, trafic par conteneurs et sur Internet, etc.)

L'Afrique semble être le continent le plus touché. Des contrôles effectués dans 20% des États africains au début des années 2000 ont révélé plus de 30% de faux. Une étude menée dix ans plus tard en Côte d'Ivoire a montré une aggravation à 40%. L'Organisation Mondiale de la Santé Animale (OIE) et La Global Alliance for Livestock Veterinary Medecines (GALVmed) de leur côté chiffrent à 67% le pourcentage de faux médicaments vétérinaires utilisés en Afrique de l'Ouest.

À noter que le trafic de faux médicaments vétérinaires ne menace pas seulement l'animal, mais aussi l'homme consommateur de viande et l'environnement.

Comme pour la santé humaine, le trafic de médicaments vétérinaires falsifiés est le fait de gangs criminels internationaux visant les pays en développement (les produits saisis sont le plus souvent en provenance d'Asie et à destination de l'Afrique subsaharienne) mais aussi les pays développés. Des affaires récentes en Pologne, France, Grande-Bretagne l'attestent. En 2011, il a été mis fin à un trafic qui a écoulé 2,5 tonnes de médicaments illicites auprès de 4 000 clients au Royaume-Uni pour un chiffre d'affaires de 13,5 millions de Livres Sterling.

La falsification de médicaments vétérinaires peut même constituer une source de financement majeure pour les organisations terroristes. Ainsi, 700 000 animaux auraient reçu des médicaments contrefaits par un laboratoire clandestin créé par l'IRA à Miami dans les années 90.

On constate également que certains produits vétérinaires tels que la kétamine ou la tilétamine sont détournés comme produits dopants à usage humain.

II. L'implication du crime organisé transnational

Le crime organisé, toujours en quête de nouveaux champs de profit, a très vite focalisé sur ce domaine qui présente un double intérêt exceptionnel : une criminalité très avantageuse avec peu de risques côté sanctions et en revanche, de grands bénéfices possibles. Une criminalité attractive donc, rentable et dépourvue de risques. L'immense majorité des lois nationales ne s'intéresse pas aux méfaits résultant des faux médicaments mais seulement aux violations de la propriété intellectuelle à travers des dispositions affublées d'échelles de peines ridicules. Par contre, le trafic de faux médicaments apporte un fort retour sur investissement et est 10 à 20 fois plus rentable que la drogue.

Si l'on considère les facilités offertes, la mise à profit de la mondialisation avec ses flux généralisés, sa flexibilité et la rapidité des échanges, la tentation était trop grande.

Globalement, on peut distinguer l'utilisation de 4 types de réseaux de distribution des faux médicaments par les réseaux criminels :

- le trafic intercontinental de grande envergure par conteneurs,
- le trafic mondial via Internet et les envois postaux,
- le trafic de médicaments périmés via le reconditionnement/repackaging,
- le trafic mettant à profit des lacunes de la réglementation européenne sur les importations parallèles.

L'Institut de Recherche Anti-Contrefaçon de Médicaments (IRACM) a entrepris en 2013 la première étude mondiale sur les relations entre organisations criminelles et contrefaçon de médicaments[5], ce qui a apporté de nombreuses informations sur : l'intérêt de groupes criminels dits multicartes pour cette délinquance, l'existence de formes diverses et hétérogènes de trafic, le développement de pratiques loin des idées reçues.

A. Typologie des organisations concernées

De nombreux types de groupes criminels se retrouvent impliqués dans le trafic de faux médicaments, et 3 formes d'organisations s'y distinguent :

i. Des organisations de petite taille (deux à cinq personnes)

Elles sont souvent le fait d'individus opportunistes motivés par des gains à court terme qui proposent des produits ciblés à des prix attractifs.

ii. Des organisations transnationales de taille moyenne

Leur profil criminel est variable. Il peut s'agir de structures issues du grand banditisme (affaire Wuppertal), d'affairistes opportunistes utilisant des techniques sophistiquées dans la gestion de leur organisation (affaire Arnaud B.) ou encore d'acteurs plus directement impliqués dans l'industrie pharmaceutique (affaire Gillespie).

iii. L'implication d'organisations transnationales de grande envergure

Cette implication a été mise en évidence par deux cas significatifs :

- L'affaire RxNorth où un distributeur canadien avait organisé en parallèle de ses activités un système complexe d'importation de médicaments contrefaits « made in China » à destination des États-Unis en les faisant transiter par Hong Kong, le Moyen-Orient, le Royaume-Uni et les Bahamas.

- La filière dite « jordano-syrienne » constitue un exemple encore plus complexe. Elle a débuté en 2003 à l'occasion de l'invasion américaine en Irak et s'est transformée au gré des opportunités en de multiples sous-réseaux sur la région (Jordanie, Territoires palestiniens, Égypte, Syrie), puis s'est déplacée vers la zone occidentale avec un médicament anti-cancer contrefait dont la filière a transité par de nombreux pays (Égypte, Turquie, Suisse, Grande-Bretagne) avant d'atteindre enfin le marché américain. Ce cas, peu médiatisé, semble avoir été parmi les plus importants et il n'est pas certain que ce réseau criminel de contrefaçon de médicaments ne soit pas toujours en activité.

Le crime organisé chinois a un rôle particulièrement stratégique, et il convient de distinguer des affaires criminelles chinoises qui concernent le marché occidental (affaire Kevin Xu, un homme d'affaires qui s'était spécialisé dans l'export), des affaires qui concernent surtout le marché local avec des acteurs souvent liés au milieu de la santé[6]. Par ailleurs, des structures étrangères viennent parfois monter des sociétés locales destinées à former des réseaux transnationaux à partir de cette région leader dans la fabrication de faux médicaments.

Dans le cadre du trafic par conteneurs, il faut souligner l'importance des filières en place notamment à partir de la Chine et de l'Inde à destination de l'Afrique et du Moyen-Orient.

B. La cybercriminalité : un territoire sans frontières

Sur Internet, deux types de structures criminelles existent[7].

La première catégorie regroupe les réseaux en ligne opportunistes qui peuvent être mis en place de manière ad hoc en les greffant sur les flux « réels » en phase de distribution vers le consommateur final.

La seconde catégorie d'organisations est exclusivement dédiée aux activités de distribution en ligne avec des techniques d'affiliation globalisées et de promotion agressive sur des moteurs de recherche ou par l'intermédiaire de spams. L'affaire la plus significative d'organisation cybercriminelle de ces dernières années implique les programmes d'affiliations russes Glavmed et SpamIt. Les affiliés de ces deux réseaux bénéficiaient de pharmacies en ligne « préfabriquées » et une dizaine d'affiliés de SpamIt gagnaient plus de 1 million de dollars de commissions sur leur site.

C. Des organisations criminelles complexes d'envergure

Pour des raisons évidentes, l'approfondissement de la connaissance de ce domaine se heurte à de nombreuses difficultés.

i. La mafia italienne et importations parallèles

Malgré l'implication validée d'organisations criminelles italiennes dans la contrefaçon de produits de luxe (fausses montres, faux vêtements de marque par exemple) ou dans le secteur de la santé (trafic d'organes humains), leur présence dans l'organisation de trafics de médicaments contrefaits est restée longtemps difficile à prouver. Une évolution est en train de se produire. La mafia italienne, par exemple, est capable de voler de faux tonnages de vrais médicaments[8], de décupler les quantités et, après reconditionnement/repackaging chez des distributeurs parallèles situés en Europe de l'Est, d'inonder les pharmacies authentiques d'Europe de l'Ouest (Affaire dite de l'Herceptine). En effet, la nouvelle réglementation européenne a libéralisé les règles en termes de choix des distributeurs pour ce qui est des ventes à l'étranger. La mafia italienne a immédiatement choisi de mettre à

profit ces dispositions pour appuyer la création de réseaux de distribution conformes en Europe de l'Est et écouler, via ces derniers, dans les pharmacies authentiques britanniques, allemandes, hollandaises, danoises et finlandaises, les faux médicaments qu'ils élaborent à partir de vols dans les circuits normaux[9].

Le phénomène pose la question de l'implication de la mafia dans certaines zones stratégiques telles que les ports.

ii. Les triades chinoises

Quant aux triades chinoises, l'analyse de leur implication reste délicate à établir, tant les travaux de recherche en Chine continentale sont complexes à conduire.

iii. Les organisations terroristes

L'implication d'organisations terroristes est là aussi un élément difficile à prouver malgré de nombreux rapports qui s'efforcent d'appréhender le blanchiment d'argent lié au trafic de médicaments contrefaits. Mais les explications en question sont souvent en relation avec des enjeux géopolitiques plus vastes qui jettent le trouble sur l'objectivité de telles analyses (exemple du Hezbollah). Toutefois, comme nous l'avons mentionné plus haut, l'implication de l'IRA irlandaise au début des années 90 dans l'organisation d'un vaste trafic de médicaments vétérinaires contrefaits entre l'Irlande du Nord et la Floride a été clairement établie.

iv. Les différente modalités de fonctionnement des organisations criminelles

Un certain nombre de constatations ressortent de ces observations :

- Une fragmentation de la criminalité se produit du fait d'une meilleure accessibilité à des activités illicites. La « démocratisation » des techniques d'impression, de production et de distribution a clairement favorisé une telle évolution.

- Les organisations criminelles fonctionnent souvent sur une logique de « trous structuraux » en cherchant à maximiser les failles systémiques dans la « supply chain » ou à une échelle plus globale (zones franches, paradis fiscaux, serveurs hébergés sur des zones « protégées », etc.).

- À grande échelle, ces organisations se caractérisent par une organisation en réseau hybride, où des acteurs licites peuvent coopérer avec des acteurs illicites voire s'impliquer directement dans de tels trafics criminels.

- Sous l'angle du temps, il est important de distinguer entre organisations susceptibles de créer un risque majeur sur une durée assez courte, et qui requiert un démantèlement aussi rapide que possible, et organisations hybrides de grande envergure dont la suppression totale peut prendre des années.

- Il n'existe pas, à notre connaissance, d'organisations criminelles transnationales d'envergure et pérennes qui combineraient des trafics sur Internet et des trafics dans le monde « réel ».

- Paradoxalement, les réseaux sur Internet paraissent présenter une organisation souvent plus structurée et cohérente que des organisations impliquées dans la contrefaçon de médicaments dans le monde « réel », plus complexes à observer.

- Les médicaments contrefaits distribués ne se limitent plus à des médicaments de « confort » mais concernent aussi des traitements lourds pour le diabète ou le cancer.

III. La stratégie du crime organisé transnational

Le trafic de faux médicaments est devenu extrêmement attractif du fait, qu'à la différence de la drogue, il offre un ratio « faible prise de risque / rendement remarquable ». Cette criminalité intéresse de plus en plus les délinquants parce qu'elle est perçue comme étant d'avenir par le crime organisé transnational. Elle permet en effet une mise à profit dynamique de la mondialisation, de l'intensité de ses flux[10], de leur nécessaire rapidité qui interdit dans la pratique les contrôles systématiques et approfondis des conteneurs devenus l'outil par excellence du trafic transcontinental.

Le trafic de faux médicaments est en passe de devenir la criminalité phare du 21ème siècle, et les grands criminels le comprennent de plus en plus. C'est ainsi que nous avons vu le principal cartel mexicain de la cocaïne se reconvertir dans le trafic de faux médicaments. C'est une manière aussi pour ce dernier de prendre en compte la saturation du marché américain de la cocaïne et de la demande accrue de médicaments par une population vieillissante.

A. Une criminalité opportuniste

La réactivité et l'adaptabilité du crime organisé face aux oppor-

tunités nouvelles de l'actualité mérite d'être reconnue comme on a pu le constater dans le cas du virus Ebola (pour lequel il n'existait en réalité aucun traitement efficace !) et de la grippe aviaire. Les réseaux criminels sont capables de s'adapter à la survenue de la moindre épidémie en proposant un faux médicament pour la traiter dans les jours suivant son apparition. On le constate à nouveau avec le Fentanyl[11] qui a causé l'an dernier plus de 60 000 morts parmi les toxicomanes américains[12]. À cette occasion, le crime organisé chinois s'est immédiatement lancé dans la fabrication et le trafic de faux précurseurs dudit médicament.

B. Le développement de la corruption

Le crime organisé met à profit la corruption qui sévit dans beaucoup de pays en développement pour faciliter et étendre ses activités. Corruption des responsables officiels nationaux de la pharmacie, responsables des douanes, de la police[13] et de la magistrature. Cette corruption peut dans certains cas monter jusqu'au niveau gouvernemental. Ce qui s'est passé récemment par exemple au Bénin et au Sénégal[14] interpelle[15] du fait de la grâce rapide de condamnés sévèrement condamnés pour un trafic important de faux médicaments.

Par ailleurs, dans certains États africains, les organisateurs du marché de rue sont soupçonnés de mettre à profit la campagne de l'élection présidentielle pour obtenir, en contrepartie de leur contribution en faveur de certains candidats, des assurances de pouvoir continuer impunément leurs activités.

Une autre pratique observée, notamment dans le Caucase, consiste dans « l'achat de la route ». Le crime organisé « achète », en quelque sorte, 1 000 Km de douaniers policiers, juges et procureurs dans le Caucase pour une durée déterminée. En contrepartie, il est convenu que les véhicules de tel ou tel transporteurs ne soient pas contrôlés sur la route et aux frontières.

C. La faculté d'adapter les trafics selon le degré de gravité de la répression

Le crime organisé est capable de faire preuve d'un grand sens tactique lorsqu'il doit faire face à une aggravation de la répression. Ainsi, dans le cas de l'aggravation de la répression en Chine (adoption de la peine de mort contre les trafiquants de médicaments) et dans le contexte des affaires de faux vaccins survenus à grande échelle localement[16], on a vu un certain nombre de grands trafiquants migrer au Cambodge pour gérer depuis ce pays leurs activités criminelles. Ils en ont profité de surcroît pour créer des alliances avec les Yakusas japonais. Le problème a pris une telle ampleur et atteint une telle sophistication au Cambodge que cela a donné lieu à un roman policier à succès dénommé « Toxic Phnom Penh » (auteur : Mathias Bernardi, éditions du Masque 2015).

D. La participation de vrais voyous et de délinquants en col blancs ou plutôt en « blouses blanches »

L'occasion fait le larron dit-on. On a vu des acteurs de l'industrie pharmaceutique en Asie créer des canaux de diversions. Ces gens n'avaient à priori aucun lien avec les réseaux mafieux mais avaient accès à des ingrédients qu'ils ont détournés. À partir de là, ils ont créé les filières appropriées d'écoulement, atteignant parfois des hauts niveaux d'activité criminelle et de profits.

Il ne faut pas nécessairement confondre les organisations criminelles impliquées dans la contrefaçon de médicaments avec des organisations criminelles traditionnelles, mais il convient de repérer aussi les graves dérapages des acteurs économiques licites en particulier liés au secteur de la santé. En effet, évaluer les signaux faibles de telles structures à risques est essentiel. Cela implique par exemple davantage d'audits de la « supply chain » des médicaments sur la zone occidentale.

IV. L'action internationale contre le trafic de faux médicaments

A. L'OMS

L'Organisation mondiale de la santé (OMS) est très préoccupée par l'évolution du phénomène des faux médicaments, même si l'action répressive n'est pas à proprement parler de son ressort. En mai 2018, l'Assemblée générale de l'OMS a décidé que la priorité devait être accordée à l'action contre les faux médicaments et les sous- standards, et non plus contre les seuls médicaments contrefaits. En effet, 3 domaines peuvent être considérés[17] :

- Les faux médicaments (fausse représentation, identité, source, historique).
- Les médicaments contrefaits

(utilisation d'une marque sans autorisation).

- Les médicaments non autorisés (sous-standards, contrebande, absence d'AMM), qui relèvent du droit de la propriété intellectuelle.

Traditionnellement, la focalisation a été longtemps sur les seuls médicaments contrefaits et le corolaire était des dispositions répressives très peu sévères (amendes et faibles peines de prison). Or, s'il est évident que les fausses cravates Hermès ne tuent pas, les faux médicaments de leur côté peuvent être mortels. Il importe donc de valoriser l'action effective contre les faux médicaments et non les seuls médicaments contrefaits. L'action pour vaincre les résistances microbiennes doit également être promue. Désormais, l'OMS recommande l'adoption de dispositions appropriées dans les législations nationales et des échelles de peines adaptées à la gravité de ce type de crimes. Il s'agit de supprimer pour les criminels l'avantage qu'ils auraient de switcher du trafic de stupéfiants au trafic de faux médicaments nettement moins réprimé.

B. L'ONU / L'ONUDC

L'Organisation des Nations unies (ONU) a décidé de lancer un programme de lutte contre les faux médicaments et a mis en charge l'Office des Nations unies contre la drogue et le crime (ONUDC) de développer l'action dans ce domaine. L'ONUDC au terme de 5 années d'action a mis au point, en 2019, un guide pour aider les États à améliorer leurs législations[18].

C. Le Conseil de l'Europe

Le Conseil de l'Europe a été à l'origine en 2010 de l'adoption de la première Convention internationale dans ce domaine. Cette dernière dénommée MEDICRIME[19] a été ratifiée par 15 pays et signée par 27.

D. INTERPOL / L'OMD / EUROPOL

L'Organisation internationale de police criminelle (INTERPOL) déclenche chaque année une opération d'envergure mondiale de démembrement des sites internet qui vendent des faux médicaments[20]. En 2018, l'opération PANGEA XI, organisée par INTERPOL et l'Organisation mondiale des douanes (OMD), a conduit à la saisie de 500 tonnes de faux médicaments grâce à la mobilisation des polices de 116 pays. En France, ce sont plus de 466 000 produits de santé illicites et une tonne de produits en vrac qui ont été saisis.

Réalisée du 9 au 16 octobre 2018, l'opération a débouché sur plus de 850 arrestations et a permis de fermer 3 671 sites Internet et pages sur les réseaux sociaux.

L'OMD a développé par ailleurs au cours de la décennie une action d'envergure de lutte contre le trafic de faux médicaments en coopération avec l'IRACM. Au cours de 5 campagnes d'interception de conteneurs menées en commun avec l'RACM qui finançait et organisait la formation des douaniers concernés, dans les ports africains, 860 millions de médicaments ont été saisis[21].

EUROPOL est un organe européen de coordination de l'action des services européens de répression dans les cas d'activités criminelles se déroulant dans plusieurs États européens ou à la fois dans des États européens et dans des États extérieurs. C'est le cas des affaires de faux médicaments et de ce point de vue l'apport d'Europol est précieux[22]. Récemment, l'organisation a décidé d'accorder une priorité aux formes de délinquances qui mettent en cause la santé, et elle a développé des actions pour lutter contre le trafic de produits Bio et de pesticides illégaux.

E. L'IRACM

De son côté, L'IRACM[23] qui est le seul organisme entièrement dédié à la lutte contre les faux médicaments développe depuis 2010 une action considérable dans les domaines suivants.

i. Des actions politiques : sensibilisation des gouvernements

De très nombreuses actions ont été entreprises depuis 2016 pour promouvoir la prise de conscience des gouvernements et initier les premières actions politiques communes au niveau régional. C'est ainsi qu'en 2018, l'IRACM a organisé la première rencontre des ministres concernés des 5 États du Mékong (Cambodge, Laos Myanmar Thaïlande, Vietnam).

ii. Des initiatives de dynamiques régionales

L'IRACM a entrepris un travail important de maillage au niveau régional des responsables nationaux en charge, que ce soit pour l'Afrique francophone avec le processus mené de 2016 à 2019 avec l'Institut International de Droit Pénal de Syracuse[24]. Cela a contribué à la réussite du processus d'élaboration de la première loi modèle mentionnée plus loin. La même entreprise s'est développée avec 5 États d'Asie du Sud Est[25]. De plus, L'IRACM a contribué à Pékin en 2017, à aider les procureurs chinois et africains à se rencontrer pour la première fois et à initier

le développement de l'entraide judiciaire entre eux pour lutter efficacement contre le trafic de conteneurs.

iii. La mise en oeuvre d'outils en droit international

l'IRACM promeut la ratification et l'application de la Convention Médicrime et de la Convention des Nations unies contre le crime organisé transnational (UNTOC) Convention ONU dite de Palerme[26].

iv. L'amélioration des législations nationales

L'IRACM élabore et diffuse des lois modèles dédiées à la lutte contre les faux médicaments sous tous les aspects qui doivent être pris en compte. Il aide les États à s'en inspirer pour moderniser leur propre loi et en rendre l'application effective. Actuellement, 7 États africains (Bénin, Burkina Faso, Côte d'Ivoire, Guinée, Mali, République centrafricaine et Tchad) ont engagé, sur cette base, un processus de modernisation de leurs textes. Dans ce contexte, certains du même groupe et d'autres États (Cameroun, République Centrafricaine, République du Congo, Gabon, Guinée Equatoriale et Tchad) ont spontanément lancé dans le cadre de l'Organisation de Coordination pour la lutte contre les Endémies en Afrique Centrale (OCEAC), un processus pour créer un référentiel fixant les infractions à prévoir pour les États et les échelles de peines à définir.

v. La formation des douaniers et des policiers

L'IRACM a organisé la formation de près de 5000 agents de terrain et mis à leur disposition des guides pratiques réalisés avec un financement de l'Union européenne. Un premier guide européen de soutien technique a même été réalisé pour les magistrats en 2015 et des e-learning sophistiqués ont été élaborés par améliorer encore davantage les performances des services répressifs.

vi. Des actions de prévention

L'IRACM alerte l'opinion publique afin de conscientiser les citoyens, et amener les consommateurs-patients à être vigilants dans leurs choix, que ce soit via Internet ou via les marchés des pays en développement où les médicaments sont vendus sur les étals à moindre coût.

V. Les améliorations nécessaires pour mieux lutter contre le trafic de faux médicaments

A. Mieux cerner les stratégies du crime organisé transnational

Les conclusions du rapport IRACM - PRZYSWA de 2013 sur le crime organisé et les faux médicaments restent valables. Trop souvent, le crime organisé donne le sentiment d'avoir toujours un coup d'avance et il est très difficile d'avoir prise sur ses activités criminelles à l'échelle notamment de l'Afrique et de l'Asie. Cela contribue à développer le sentiment d'invulnérabilité des voyous, et devient une donnée essentielle à prendre en considération pour inverser les tendances. Il importe donc d'identifier les logiques des stratégies criminelles les plus significatives.

- Sur un plan théorique, la connaissance organisationnelle des réseaux criminels est très insuffisante et la criminologie traditionnelle a été trop rigide jusqu'à présent pour réfléchir à un niveau d'échelle globale.

- La mobilisation de chercheurs de nombreuses disciplines (géographie, sciences économiques, urbanisme, logistique, etc.) est ainsi trop négligée dans les approches criminologiques. Par ailleurs, il serait important de favoriser l'émergence de lanceurs d'alerte et d'experts réellement indépendants dans les analyses criminologiques pour la crédibilité du débat public.

- En matière de renseignement, il est important d'insister sur la nécessité d'une plus grande centralisation des informations à améliorer sous l'angle qualitatif tant le risque criminel apparaît volatil et variable. Il serait, par exemple, pertinent de développer des techniques de renseignements nouvelles pour mieux évaluer le profil psychosociologique des contrefacteurs, ou encore des techniques cartographiques en temps réel qui incluraient une dynamique spatiale des risques. Les sources d'information mériteraient aussi d'être affinées sur certaines régions (Asie ou Afrique notamment).

B. Stimuler l'engagement des États

Pour avancer réellement, une action considérable doit être développée au niveau des États qui souvent restent peu ou pas mobilisés.

Pour une majorité d'entre eux, ce combat n'est pas une priori-

té, tant ils ne semblent pas conscients des enjeux. Trop souvent, de surcroît, la corruption continue de ralentir l'action. Il est constaté : l'absence de volonté politique et de stratégie, des législations désuètes et inappliquées qu'il faudrait moderniser d'urgence, des peines prévues très faibles et peu prononcées. Tel est encore trop souvent l'état des lieux. Beaucoup de législations nationales dépassées ne traitent que de la contrefaçon et de la propriété intellectuelle sans prendre en compte la gravité de la menace des faux médicaments contre la santé.

C. Former juges et procureurs et booster une entraide judiciaire balbutiante

Dans beaucoup de pays habitués à traiter plutôt des affaires locales de peu d'ampleur, les magistrats sont incapables de faire face à la technicité de nouveaux domaines comme le trafic de faux médicaments. De plus, alors qu'il est déterminant, les institutions judiciaires nationales souvent sont incapables de prendre en compte l'aspect international qui nécessitent de remonter les filières, de localiser et geler les avoirs criminels, de poursuivre effectivement les auteurs, où qu'ils se trouvent.

Par nature les activités criminelles en cause s'étendent dans pratiquement toutes les affaires sur plusieurs pays et impliquent un recours quasi systématique à l'entraide judiciaire internationale. Or, cela se révèle généralement trop complexe et hors de portée pour des magistrats non formés à l'international.

D. Aider des services répressifs désarmés

Les services des douanes et de police rencontrent des difficultés considérables pour contrôler le trafic sur Internet et la sortie et l'entrée des conteneurs sur leurs territoires nationaux.

Il existe des problèmes de moyens (inadaptation des moyens, fouille des conteneurs irréalisables), des problèmes de méthodologie, des interférences avec les priorités des gouvernements (taxes à l'importation à percevoir).

E. Prévenir les usagers de médicaments

Sur Internet, il faut favoriser l'émergence de normes pour que les consommateurs puissent clairement repérer les sites licites. Des initiatives proactives qui associeraient les patients-clients sur Internet seraient à cet égard pertinentes.

F. Renforcer la motivation de l'industrie pharmaceutique mondiale

Les compagnies pharmaceutiques développent une action importante pour détecter et combattre les fraudes dont leurs produits sont victimes dans le monde. Mais la prise de conscience d'un point de vue collectif et stratégique est lente. La motivation est encore faible pour mettre en place une véritable stratégie commune.

Conclusion

Aujourd'hui, en 2019, les faux médicaments représentent plus que jamais une triple menace : menace accrue pour l'industrie pharmaceutique, menace contre la santé publique à grande échelle, menace contre l'État de droit.

Une stratégie efficace implique une approche holistique couvrant : la connaissance du phénomène, les dispositifs législatifs et leur mise en oeuvre, le soutien opérationnel aux services de police et de douane, les actions de prévention.

Il est manifeste que les contrefacteurs profitent des nouveaux dispositifs d'achat de médicaments - virtuels ou réels - et bénéficient d'un contexte complexe et évolutif. Le binôme crime organisé et contrefaçon de médicaments se joue des failles du système mondial.

C'est la raison pour laquelle les services répressifs, les laboratoires pharmaceutiques et les autorités gouvernementales doivent développer des stratégies à la hauteur pour contrecarrer efficacement le trafic de médicaments.

Notes :

1 Voir : https://www.afrique7.com/societe/21093-plusieurs-tonnes-de-produits-pharmaceutiques-illicites-saisis-au-burkina-fa so.html

2 Voir : https://www.who.int/medicines/p ublications/drugalerts/drug_alert-2-2019/en/

3 Voir : https://www.who.int/antimicrobial-resistance/interagency-coordination-group/IACG_final_report_EN.pdf?ua=1

4 Voir : http://www.iracm.com/veterinaires/mobile/

5 Voir : http://www.iracm.com/2013/09/lira cm-presente-un-rapport-detude-inedit-cont refacon-de-medicaments-et-organisations-cri minelles/

6 Voir : https://newsinfo.inquirer net/108089 9/fake-rabies-vaccine-gets-80-china-execs-in-tro uble

7 Voir : https://www.iracm.com/obser vatoire-thematique/falsification-sur-inte rnet/

8 Voir : https://www.securingindust ry.com/pharmaceuticals/burglars-take-almost-1m-of-meds-from-italian-warehouse/s40/a7688/#.Wx-M7i_pNAZ

9 Voir : https://ansm.sante.fr/S-informer/Points-d-information-Points-d-informa tion/Vol-d-Herceptin-en-Italie-l-EMA-pre cise-que-deux-autres-medicaments-sont-concernes-Alimta-et-Remicade-Point-d-In formation-Actualise-le-23-04-2014

10 Voir : https://euipo.europa.eu/ohim porta l/en/web/observatory/trade-in-fakes-in-small-

parcels?TSPD_101_R0=637b3290412c33d47e0a713081a13b52l780000000000000002f533a35cffff000000000000000000000000000005c34d03f00af95e185

11 Voir : https://teles-relay.com/le-fen_tanyl-est-partout-les-ventes-china-white-sepanouissent-sur-craigslist-l-a-l-a-taco-2/

12 Voir : https://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm60986 9.htm

13 Voir : https://www.guineenews.org/disparition-dune-cargaison-de-faux-medicaments-lordre-des-pharmaciens-appelle-a-la-reclusion-de-medicrime/

14 Voir : https://www.pressafrik.com/Faux-medicaments-Quand-Macky-avoue-implicitement-qu-il-n-a-pas-accorde-de-grace-presidentielle-a-Amadou-Woury-Diallo_a200525.html

15 Voir : http://www.rfi.fr/afriqu e/20190521-senegal-colere-pharmaciens-grace-trafic-faux-medicaments

16 Voir : https://www.manilatimes.net/chi_na-readies-stiff-fines-for-fake-drugs-vaccines/544641/

17 Voir : http://www.who.int/fr/news-ro_om/fact-sheets/detail/substandard-and-falsified-medical-products

18 Voir : https://www.unodc.org/document_s/treaties/publications/19-00741_Guide_Falsified_Medical_Products_ebook.pdf

19 Voir : https://www.coe.int/fr/web/m_edicrime/the-medicrime-convention

20 Voir : https://www.interpol.int/Crime-areas/Pharmaceutical-crime/Operations/Operation-Pangea

21 Voir : http://www.iracm.com/wp-content/uploads/2014/10/Dossier-dePresse-IRACM-sept14_3.p df

22 Voir : https://www.europol.europa.eu/newsroom/news/more-€165-million-of-trafficked-medicines-seized-in-operation-mismed-2

23 Voir : www.iracm.com / info@iracm.com

24 Voir : http://www.siracusainstitute.o_rg/app/fr/

25 Voir : https://www.iracm.com/2018/11/conference-regionale-sur-la-lutte-contre-les-medicaments-falsifies-et-sous-standards-phnom-penh-5-6-novembre-2018/

26 Voir : https://www.iracm.com/e-learning/

OUVRAGES RÉCENTS

CORRUPTION ET DROIT PÉNAL

SOUS LA DIRECTION DE JEAN-PAUL CÉRÉ ET CARLOS EDUARDO JAPIASSU

ÉDITEUR : L'HARMATTAN

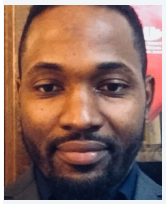
Présentation de l'éditeur

Le thème de la corruption a traversé le temps. L'intérêt du droit pénal est cependant renouvelé par les nombreuses affaires médiatisées qui gangrènent la vie politique et le monde des affaires dans de nombreux pays. L'arsenal législatif interne cherche à s'adapter sous l'effet des multiples textes qui ont vu le jour à l'échelle internationale et régionale. Une nette tendance à l'harmonisation des législations criminelles anti-corruption est perceptible. Cet ouvrage permet de saisir la diversité du phénomène dans sa dimension criminologique et juridique.

Jean-Paul Céré est Maître de Conférences à l'Université de Pau et des Pays de l'Adour (France). Président de l'Association Française de Droit Pénal et Président du Comité International des Pénalistes Francophones.

Carlos Eduardo Japiassu est Professeur de Droit Pénal à l'UERJ/UFRJ (Brésil). Directeur du Programme de Master et Doctorat de l'Université Estacio de Sa, Secrétaire Général de l'Association Internationale de Droit Pénal et Vice-Président du Comité International des Pénalistes Francophones.

LE SORT DE LA RELATION D'AFFAIRES APRÈS UNE DÉCLARATION DE SOUPÇON



MAMADOU DIALLO

DOCTEUR EN DROIT, CONSULTANT EN SÉCURITÉ FINANCIÈRE

La lutte contre le blanchiment de capitaux et le financement du terrorisme (LCB-FT) requiert des établissements financiers, en cas de soupçon sur la licéité des opérations ou lorsque l'identification[1] des parties prenantes à l'opération n'est pas satisfaisante et dans bien d'autres cas[2], à effectuer une déclaration de soupçon (DS). Il s'agit d'une obligation règlementaire strictement encadrée[3] qui commande à l'établissement financier concerné, sans en faire une obligation systématique[4], la rupture de la relation d'affaires lorsqu'au moins l'une de ces conditions précitées fait défaut. Cette rupture se matérialise par la clôture juridique des comptes[5] détenus par le client ayant fait l'objet de la déclaration.

Rappelons néanmoins que si la règle en la matière est la liberté[6] quant au choix à donner à l'issue de la relation d'affaires, l'extrême prudence et la diligence bancaire poussent certains établissements de crédit à rompre systématiquement le lien contractuel. Toutefois, certains évènements peuvent retarder voire carrément ajourner la cessation de la relation entre les parties et ce, nonobstant l'existence d'une déclaration de soupçon. L'enjeu est pour l'établissement financier, dans ce cas de figure, de trancher sans se faire sanctionner par le régulateur puisque, de toute manière, toute poursuite du lien contractuel peut, dans certains cas, donner lieu à des sanctions[7]. À l'inverse, la rupture de la relation nonobstant l'émission d'une déclaration de soupçon peut conduire vers le prononcé de sanctions. Dans le silence des textes, il apparaît nécessaire tout à la fois pour les établissements financiers que pour les clients de clarifier les règles qui encadrent la situation post déclarative dans un contexte de forte hausse des déclarations de soupçon. En tout état de cause, après l'émission d'une déclaration de soupçon[8], la rupture de la relation d'affaires doit rester la règle (I) ; *a contrario*, sa poursuite ne doit être envisagée que de manière résiduelle (II).

I. La cessation de la relation d'affaires : issue logique de la déclaration de soupçon

Même si la cessation de la relation d'affaires obéit au régime de la rupture de droit commun propre aux contrats bancaires (A), elle se heurte néanmoins au dispositif relatif au droit au compte (B).

A. Le cadre général : la rupture de droit commun

L'émission d'une déclaration de soupçon entraîne en règle générale la rupture pure et simple de la relation d'affaires. Il s'agit d'une « obligation légale »[9], même si la décision de rompre ou non la relation d'affaires, après avoir effectué une déclaration de soupçon, « appartient à l'organisme financier et relève de sa seule responsabilité[10]». Le fait de mettre un terme à la relation d'affaires n'est pas non plus susceptible de constituer un manquement aux dispositions du Code monétaire et financier (CMF) relatives à la LCB-FT, la seule réserve étant bien évidemment « de ne pas se rendre coupable d'un abus de droit, ou de ne pas procéder à une clôture brutale[11] ».

Par ailleurs, la confidentialité entourant la déclaration interdit

à l'établissement financier de motiver sa décision[12] de mettre un terme à la relation d'affaires, au risque de transgresser l'obligation de confidentialité[13] qui encadre la déclaration de soupçon.

Il doit cependant observer un délai de prévenance[14] qui en pratique est de deux mois sauf s'il existe des circonstances[15] obligeant l'établissement financier à y déroger. Dans ces conditions, les juges considèrent que l'inobservation par la banque d'un délai de préavis n'est pas illégitime[16]. La rupture de la relation d'affaires peut être envisagée aussi bien lorsque le client est une personne physique que morale. Dans le même ordre d'idées, la cessation de la relation d'affaires pourrait également être envisagée même lorsque le client à un statut mixte, c'est-à-dire lorsqu'il détient un compte personnel et professionnel ou encore lorsqu'il s'agit d'un compte personnel auquel est assorti un compte joint. Dans tous les cas, rien ne s'oppose à ce que la banque clôture l'ensemble des comptes du client puisque, de toute manière, les textes[17] font référence à la « relation d'affaires[18] ».

L'existence d'un prêt n'est pas non plus dans l'absolu un obstacle à la cessation de la relation d'affaires dès lors que le banquier peut, de son propre chef, procéder à la clôture de l'ensemble des comptes du client et ne conserver que le remboursement des échéances. Il demeure néanmoins, dans ces conditions, problématique de poursuivre, même de façon résiduelle, une relation d'affaires en dépit de la perte de confiance.

Dans le même ordre d'idées, la clôture des livrets d'épargne consécutivement à une déclaration de soupçon est envisageable. Pour autant elle n'est pas sans conséquence pour le client notamment sur la fiscalité et les intérêts afférents à leur détention. Elle est susceptible notamment d'entraîner une perte d'antériorité et par ricochet, des avantages[19] patrimoniaux qui en résultent. De toute évidence, le banquier déclarant de bonne foi est couvert par une immunité de poursuites contre toute action en responsabilité qui émanerait de son client et qui porterait sur les conséquences de cette déclaration.

B. La cessation de la relation d'affaires et le droit au compte : une rupture dérogatoire

Au chevet du régime général de la cessation post-déclarative, se trouve le dispositif relatif au droit au compte (DAC)[20] qui, en raison de son caractère dérogatoire[21], interroge sur les conditions et modalités de rupture de la relation d'affaires. Rappelons que même si la relation bancaire repose sur de l'*intuitu personae*, un établissement financier peut se voir imposer au nom du droit à toute personne de disposer d'un compte, l'ouverture d'un compte bancaire. À l'inverse, il est interdit sous peine de sanctions d'ouvrir un compte et d'entretenir une relation d'affaires avec toute personne suspectée d'avoir blanchi de l'argent et/ou de financer le terrorisme.

Ainsi, sous l'empire de l'ancienne législation[22], l'établissement financier pouvait se retrouver dans cette « situation ubuesque[23] ». Pour cause, en cas de suspicion de blanchiment, il devait effectuer une déclaration de soupçon et procédait à la clôture du compte du client. Ce même établissement pouvait se voir demander, sur injonction de la Banque de France « l'ouverture d'un compte pour ce même client sans pouvoir y opposer son refus[24] ». Le risque encouru dans ces circonstances tombait sous le coup de sanction de la Commission bancaire, organe collégial dirigé par le gouverneur de la Banque de France. Depuis la transposition de 3e directive anti-blanchiment par l'ordonnance du 30 janvier 2009, le législateur a pris le soin de concilier le droit au compte à la clôture de compte suite à une déclaration de soupçon. C'est l'article L561-22, V du CMF qui apporte une exonération de responsabilité à l'égard de l'établissement financier auteur d'une ouverture de compte pour le compte d'une personne bénéficiant de ce dispositif.

Même si cette protection est à saluer, il reste qu'elle n'offre pas une protection suffisante à l'établissement financier puisque l'exonération de responsabilité ne concerne pas les cas de financement du terrorisme. Concrètement, si l'on s'en tient au raisonnement du régulateur, un établissement financier, qui soupçonne un individu de financer le terrorisme et qui procède à une déclaration de soupçon, à la clôture de ce compte, peut, en tout cas en théorie, se faire enjoindre d'ouvrir de nouveau un compte pour ce client et courir le risque de se faire sanctionner pour le chef de participation à une opération de financement du terrorisme.

Par ailleurs, rappelons également que si le compte est ouvert suite à une intervention de la Banque de France, il ne peut être clos à l'initiative de l'établissement de crédit qu'à la suite d'une notification écrite et motivée adressée à la Banque de France. Dans ce cas, l'article

L312-1 du CMF prévoit l'observation d'un préavis de 2 mois minimum.

On peut relever au passage l'asymétrie que l'on pourrait qualifier de « normale » entre les conditions d'ouverture classique d'un compte de dépôt et celle d'un autre compte ouvert par le biais du droit au compte d'une part, d'autre part, la subordination au même régime en matière de délai de préavis lors de leur clôture. En d'autres termes, le délai de préavis pour la clôture d'un compte de dépôt classique est en moyenne de 2 mois, le même régime est appliqué au droit au compte. Pour autant, il ne devrait pas en être ainsi. Puisqu'il est évident que ce délai reste « insuffisant, puisqu'identique à la règle générale applicable à toutes les conventions de compte de dépôt[25] ».

A contrario, on peut légitimement s'interroger sur les motivations de créer un régime dérogatoire pour le droit au compte et lui appliquer les règles du droit commun. « Il pourrait paraître opportun de rendre plus difficile la clôture des comptes de dépôt ouverts à l'aide de la procédure du droit au compte[26] ». La seule difficulté serait pour l'établissement financier, dans ce cas, de ne pas maintenir au-delà du délai légal un client dont il a tout intérêt de se séparer. Soulignons que suite à cette clôture du compte bancaire, « le banquier devra, après liquidation des opérations en cours, remettre à son client, ou à la personne dont ce même client lui communique les coordonnées bancaires, le solde créditeur du compte[27] ». La cessation de la relation d'affaires bien qu'acquise en matière de droit au compte n'est pas nécessairement la seule issue en cas de déclaration de soupçon.

II. La continuation de la relation d'affaires

L'établissement financier peut seulement dans des cas résiduels opter pour la poursuite de la relation d'affaires postérieurement à une déclaration de soupçon. Plusieurs situations peuvent être envisagées : l'existence d'une contrainte judiciaire ou administrative (A), de même, l'instrumentalisation du compte du client (B) ou encore la survenance d'éléments nouveaux entraînant la levée de doute (C).

A. L'existence d'une contrainte judiciaire et administrative

L'unité d'investigation administrative destinataire des déclarations de soupçon ou encore l'autorité judiciaire peuvent demander de différer la clôture des comptes ayant fait l'objet de déclaration. Deux situations peuvent se présenter : lorsqu'une procédure de saisie des avoirs est envisagée ou est en cours et lorsque des investigations supplémentaires s'imposent.

En effet, dans le cadre d'une saisie attribution, l'article L162-1 du Code des procédures civiles d'exécution rend indisponible dans un délai de quinze jours ouvrables les sommes objet de la saisie. Il en résulte que durant cette période, les sommes portées au crédit du compte du client sont figées pour les besoins de la saisie. Ce qui signifie in fine que, nonobstant une déclaration de soupçon, il n'est pas possible de clôturer le compte et rompre la relation d'affaires tant que la procédure de saisie n'est pas close.

De même, lorsque l'exploitation des éléments contenus dans la déclaration de soupçon demeure, compte tenu de la spécificité du cas, probante mais insuffisante pour poursuivre les investigations, ou lorsque les éléments sont jugés précoces et que la collecte de nouveaux éléments pourrait consolider l'ensemble des soupçons à l'égard de ce client, l'établissement financier doit, sous peine de sanctions[28], surseoir à la rupture de la relation d'affaires malgré l'existence d'une déclaration de soupçon. D'ailleurs, l'Autorité de contrôle prudentiel et de résolution (ACPR) et Tracfin recommandent fortement dans ces conditions la continuation de la relation d'affaires. Cette situation se trouve justifiée par le fait que « la rupture de la relation d'affaires ne peut se substituer au respect de l'obligation de vigilance par les établissements financiers[29] ». *A contrario*, sa poursuite n'est pas antinomique au respect de l'obligation de vigilance puisqu'elle permet de mener des investigations à terme sur l'ensemble des opérations jugées atypiques[30]. C'est la raison pour laquelle en cas de cessation de la relation, « la responsabilité de l'organisme reste engagée tant que les vérifications n'ont pas été achevées »[31]. La Commission des sanctions de l'ACPR s'est prononcée, à cet égard, s'agissant d'un examen renforcé ou d'un défaut de déclaration de soupçon ; elle a infligé à un établissement financier une sanction pécuniaire d'un million d'euros accompagnée d'un blâme[32]. La Commission a estimé en l'espèce que « les opérations atypiques auraient dû donner lieu à un examen approfondi permettant d'en comprendre la justification économique[33] ». Elle a ajouté que « la clôture de ce compte peu avant la fin de la vérification ne peut permettre de régulariser un défaut

d'examen approfondi d'opérations atypiques qui y ont été enregistrées[34] ». La Commission a conclu que les griefs faits à l'encontre de cet établissement financier étaient bien fondés.

B. L'instrumentalisation du compte du client

En pratique, lorsque le banquier détecte un agissement frauduleux constitutif d'un d'abus de faiblesse[35], il doit procéder à une déclaration de soupçon. Bien évidemment, celle-ci n'entraîne et ne doit pas conduire à la rupture de la relation d'affaires puisque le fait incriminé n'émane pas du client, mais d'un tiers[36]. Si cette solution semble acquise dans la pratique, elle soulève néanmoins quelques difficultés notamment d'ordre juridique[37]. En effet, il convient de se demander quel comportement doit adopter le banquier face à un cas d'abus de faiblesse afin que son action ou son abstention n'engendre des sanctions : doit-il déclarer sous le fondement de l'article L 561-15 du CMF ou doit-il en référer directement au procureur de la République au nom de l'obligation de vigilance générale qui pèse sur lui ?

À la première question, il doit bien évidemment porter à la connaissance de Tracfin de l'existence de tout acte constitutif d'un abus de faiblesse. Cependant, le fondement juridique de la déclaration reste discutable en ce sens que lorsqu'on interprète strictement l'article L561-15 du CMF, on se rend compte que la déclaration susvisée ne concerne que le produit d'une infraction. Or, dans le cas de l'abus de faiblesse, il ne s'agit pas d'un produit[38], mais d'un acte matériel constitutif de l'infraction à savoir l'utilisation frauduleuse des sommes.

À la seconde question, le banquier peut signaler au procureur de la République, en vertu de son obligation de vigilance générale, les anomalies détectées sur le compte de ses clients. Là encore, sa responsabilité ne peut être engagée que pour les anomalies apparentes. Or, l'abus de faiblesse découle, d'une part, des anomalies dites intellectuelles et d'autre part, leur détection se trouve limitée par le principe de non-ingérence qui commande au banquier de ne pas s'immiscer dans la gestion des affaires de ses clients. Par une interprétation stricte de l'article L561-15 du CMF, la déclaration de soupçon à Tracfin pour abus de faiblesse reste critiquable. Les anomalies intellectuelles restent subordonnées à une appréciation *in concreto*. Il en résulte que la mise en jeu de la responsabilité du banquier est systématiquement engagée en cas d'anomalies apparentes, ce qui n'est pas le cas en présence d'anomalies intellectuelles dont l'abus de faiblesse fait partie.

En tout état de cause, la détection d'un cas d'abus de faiblesse donne lieu à la transmission d'une déclaration de soupçon. Celle-ci n'entraîne pas la rupture de la relation d'affaires et n'exonère pas le banquier de porter à la connaissance du procureur de la République de l'existence des faits délictuels à la condition que ces derniers relèvent d'une anomalie dite matérielle.

C. La survenance d'éléments nouveaux entraînant la levée du doute

La déclaration de soupçon, quel que soit son degré d'objectivité, n'est pas infaillible[39] et, à ce titre, sa mise en oeuvre n'est pas irréversible. Pour preuve, la survenance d'éléments nouveaux qu'ils soient factuels ou qualitatifs entraînant la levée des soupçons rend impertinente la déclaration initiale. C'est le cas lorsque l'objet du soupçon porte sur une transaction dont les justificatifs jugés probants et conformes ont été obtenus postérieurement[40]. Il en est de même lorsqu'une personne ou entité est soupçonnée à tort de financer des opérations terroristes qui, après enquête, se sont révélées non fondées ; ou encore par le biais de l'homonymie, un client se retrouve à tord fiché comme appartenant à une « liste noire[41] ».

Dans le même ordre d'idées, dans le processus d'actualisation des données relatives à la connaissance du client, la disparition de l'événement déclencheur entre la déclaration de soupçon et la clôture du compte rend théoriquement caduque la cessation de la relation d'affaires. Précisons néanmoins que la survenance d'un ou plusieurs éléments nouveaux entrainant la levée du doute, doit intervenir avant la fin du délai de clôture du compte. *A contrario*, leur prise en compte reste certes indifférente du point de vue de l'établissement financier puisque le compte est déjà clos et la relation d'affaires rompue. Néanmoins, on peut limiter la casse en transmettant à Tracfin ces éléments nouveaux afin de lever le doute.

Au total, la survenance d'une déclaration de soupçon bouleverse fondamentalement la relation d'affaires. Si la plupart du temps le soupçon l'ayant conduit est légitime, il n'en demeure pas moins que la transmission d'une déclaration n'est et ne doit pas systématiquement être synonyme de rupture de la relation

d'affaires. Un compromis devrait être trouvé quant à la nécessité de préserver le système financier contre l'infiltration des flux financiers d'origine illicites et le respect des droits des personnes physiques et morales à disposer d'un compte et d'en jouir des attributs au sein de l'économie officielle

Notes :

1 L. 561-5 du CMF.

2 Lorsque l'établissement financier soupçonne ou a de bonnes raisons de soupçonner que les fonds proviennent d'une infraction passible d'une peine privative de liberté supérieure à un an ou qu'elle participe au financement du terrorisme, ou encore à la fraude fiscale lorsqu'au moins figure l'un des 16 critères définis par le décret n° 2009-874 du 16 juillet 2009.

3 Cette déclaration détaillée dans les articles L. 561 -15 à L. 561-22 du CMF n'exonère pas l'établissement financier de mettre un terme à la relation d'affaires sauf indication contraire des autorités tutélaires.

4 La déclaration de soupçon n'est pas systématique hormis dans 3 cas de figure. C'est le cas lorsque l'opération dont l'identité du donneur d'ordre reste douteuse malgré les mesures de vigilance effectuées ; ou lorsque la somme ou l'opération dont l'établissement financier sait, soupçonne ou a de bonnes raisons de soupçonner qu'elles proviennent d'une fraude fiscale lorsqu'il y a présence d'au moins un des 16 critères prévu par le décret du 16 juillet 2009 ou quand il dispose de toute information de nature à infirmer, conforter ou modifier des éléments contenus dans la déclaration préalablement envoyée.

5 L.312-1, IV du CMF.

6 MICHAUD Patrick, Tracfin, blanchiment et fraude fiscale : les déclarations de soupçon : de nouvelles obligations pour les juristes et fiscalistes, La Semaine Juridique Notariale et Immobilière, n° 46, 13 Novembre 2009, 1307.

7 ACPR, n° 2016-07, Société générale, 19 juill. 2017 ; ACPR, n° 2016-06, BNP PARIBAS, 30 mai 2017.

8 La forte implication des organismes financiers dans la lutte contre le blanchiment et le financement du terrorisme en 2016 et 2017 s'est traduite par une hausse importante du nombre de déclarations de soupçon reçues à Tracfin en 2 ans (+59 % entre 2015 et 2017).

9 MICHAUD Patrick, Tracfin, blanchiment et fraude fiscale : les déclarations de soupçon : De nouvelles obligations pour les juristes et fiscalistes, op.cit.

10 Lignes directrices conjointes de l'Autorité de contrôle prudentiel et de résolution (ACPR) et de Tracfin sur les obligations de déclaration et d'information à Tracfin, 02/2018.

11 BONHOMME Régine, Dépôts et comptes en banques, Répertoire de droit commercial, 10/2017.

12 L.312-1, IV du CMF que la décision de résiliation est motivée sauf lorsque cette motivation contrevient aux objectifs de sécurité nationale ou de maintien de l'ordre public.

13 L. 561-19 du CMF. La déclaration de soupçon est confidentielle. Sous réserve des dispositions de l'article 44 de la loi n° 78-17 du 6 janvier 1978, il est interdit, sous peine des sanctions prévues à l'article L. 574-1, aux dirigeants et préposés d'organismes financiers, aux personnes mentionnées à l'article L. 561-2, […], de porter à la connaissance du propriétaire des sommes ou de l'auteur de l'une des opérations mentionnées à l'article L. 561-15 ou à des tiers, autres que les autorités de contrôle, ordres professionnels et instances représentatives nationales visées à l'article L. 561-36, l'existence et le contenu d'une déclaration faite auprès du service mentionné à l'article L. 561-23 et de donner des informations sur les suites qui ont été réservées à cette déclaration.

14 Cass. Com. 26 janvier 2010, n° 09-65.086.

15 C'est le cas lorsque le client refuse de fournir des explications sur des dépôts de fonds de sorte à susciter les soupçons de l'établissement financier.

16 CA Amiens, ch., économique, 12 oct. 2004, BNP Paribas c. Naaijer : Juris-Data n° 2004-282028, Com. Patrice COUDERT, La Semaine Juridique Entreprise et Affaires n° 22, 1er Juin 2006, 1850. Voir Cass. com., 14 févr. 2006, n° 04-16.464 : JurisData n° 2006-032234.

17 L 561-8 alinéa 1 du code monétaire et financier.

18 L'ordonnance n° 2009-104 du 30 janvier 2009 modifiée par l'ordonnance n° 2016-1635 du 1er décembre 2016 substitue à la notion classique en droit français de relation contractuelle que l'on trouvait à l'article L563-1 ancien à celle de relation d'affaires. L'article L. 561-2-1 du Code monétaire et financier en donne la définition.

19 Il en est ainsi des avantages liés à la rémunération pour les PEL anciens et ceux liés à la fiscalité pour les PEA.

20 Le droit au compte a été consacré par la loi n° 84-46 du 24 janvier 1984 relative à l'activité et au contrôle des établissements de crédit (art. 58). La loi no 98-657 du 29 juillet 1998 relative à la lutte contre les exclusions, a garanti le droit au compte bancaire pour tous, prévu par l'article L312-1 du CMF.

21 Les conditions d'ouverture et de clôture sont strictement encadrées. Par exemple pour la clôture, 6 cas exhaustifs sont prévus par l'article L 312-1. IV du Code monétaire et financier.

22 Directive 2005/60/CE du Parlement européen et du Conseil du 26 octobre 2005 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme.

23 CUTAJAR Chantal, Droit du blanchiment : une ordonnance nécessaire, mais à parfaire, Recueil Dalloz, 03/2009, n° 12, p. 821.

24 CA Paris pôle 1 chambre 1, 26 août 2011 (RG 11/15269) : LEDB (L'ESSENTIEL droit bancaire) oct. 2011, p. 3, n° 134.

25 STOUFFLET Jean, Compte bancaire. Généralités. Compte de dépôt : JCl. Banque - Crédit - Bourse, fasc. 200, 2013, n° 79 et s. - P. Bouteiller, Compte de dépôt. Clôture: JCl. Commercial, fasc. 354, 2014.

26 LASSERRE-CAPDEVILLE Jérôme, L'encadrement juridique de la clôture du compte en banque et de ses conséquences, La Semaine Juridique Entreprise et Affaires, n° 23, Juin 2015, 1268.

27 Ibid.

28 ACPR, 30 juin 2017, n° 2016-09, Caisse régionale de Crédit agricole mutuel Atlantique Vendée ; Blâme et sanction pécuniaire de 2 millions d'euros.

29 Lignes directrices conjointes de l'ACPR et de Tracfin sur les obligations de déclaration et d'informations à Tracfin, 02/2018, p. 64.

30 « Le blanchiment d'argent n'est pas une opération instantanée, ni isolée, elle est le plus souvent processuelle et nécessite une observation dans le temps afin de redessiner le processus et démêler le bon grain de l'ivraie » Mamadou DIALLO, Les mutations de l'anti-blanchiment à l'aune de la profession bancaire et des libertés individuelles, Thèse de doctorat : Droit, Reims, 2017.

31 Lignes directrices conjointes de l'ACPR et de Tracfin sur les obligations de déclaration et d'informations à Tracfin, op.cit. p. 64.

32 ACPR, Commission des sanctions, procédure n° 2012/08 du 2/12/2013, p. 11- Banque Chaâbi du Maroc.

33 Ibid.

34 Ibid.

35 Article 223-15-2 du Code pénal.

36 De façon non exhaustive c'est la famille, les amis, un employé, un mandataire…

37 LASSERRE CAPDEVILLE Jérôme, La détection du délit d'abus de faiblesse par le banquier, AJ pénal 2018, n° 5, p. 223.

38 Dans le cas de l'abus de faiblesse, les fonds détenus sur leurs livres ne résultent ni d'un crime, ni d'un délit, mais de l'utilisation frauduleuse qui en est faite a posteriori.

39 Fabrice DEFFERRARD écrit à ce sujet que « le soupçon est empreint de subjectivité et résulte d'une opinion défavorable que l'on a d'une personne ou d'une situation ». Fabrice DEFFERRARD, la suspicion légitime, Thèse de Doctorat, Versailles-Saint Quentin en Yvelines, 1998. Dans le même sens, il qualifie le soupçon comme « le résultat d'une confrontation inconciliable, effectuée *in concreto*, entre l'opération en cause et les pratiques ordinaires du client ». Fabrice DEFFERRARD, les métamorphoses de la législation française anti-blanchiment, Gazette du Palais, n° 297, p. 7-15.

40 Il arrive souvent en pratique que le chargé de clientèle soit interrogé par les équipes dédiées à la Conformité et pour diverses raisons celui-ci ne soit pas en mesure de recueillir les justificatifs auprès du client afin de lever le doute. Cependant, postérieurement à la déclaration, il transmet lesdits justificatifs à la Conformité disculpant de la sorte le client. Il s'en suit que si la clôture du compte n'est pas intervenue mais est en cours, le client doit être rétabli dans ses droits.

41 Les établissements financiers disposent de listes noires contenant des noms de personnes et d'entités faisant l'objet de sanctions ou soupçonnées d'être liées au crime organisé et/ou au financement du terrorisme.

OUVRAGES RÉCENTS

DROIT ET PRATIQUE DES SAISIES ET CONFISCATIONS PÉNALES

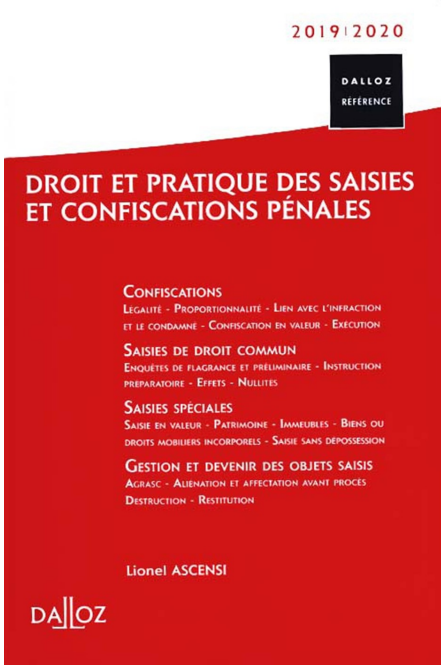
AUTEUR : LIONEL ASCENSI

ÉDITEUR : DALLOZ

Présentation de l'éditeur

Si les saisies et confiscations sont anciennes dans le dispositif pénal français, elles ont connu depuis dix ans une extension majeure de leurs conditions de mise en oeuvre, que ce soient les peines complémentaires de confiscation, dont le champ d'application a été étendu, ou les procédures de saisie, passées d'un rôle probatoire à une fonction patrimoniale. Ces évolutions, législatives puis prétoriennes, ont été accompagnées par la création d'une institution nouvelle : l'Agence de gestion et de recouvrement des avoirs saisis et confisqués, l'Agrasc.

Pensées pour lutter contre la délinquance et la criminalité dans leurs aspects patrimoniaux, les saisies et confiscations pénales obéissent à des règles dont l'application soulève des difficultés sans cesse renouvelées pour l'ensemble de la chaîne pénale, policiers, gendarmes, magistrats du parquet et du siège. En effet, comment identifier le propriétaire économique réel d'un bien immobilier, comment saisir des actifs financiers dématérialisés, comment confis-



quer un bien indivis ou commun ? La jurisprudence y répond par touches successives, en tenant compte d'un cadre conventionnel international et européen à la fois offensif et protecteur des droits fondamentaux.

L'ouvrage présente l'ensemble du dispositif législatif, dernièrement revu par 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, et jurisprudentiel encadrant les saisies et confiscations pénales. Il offre une analyse très fine de la jurisprudence de la chambre criminelle de la Cour de cassation, de la Cour européenne des droits de l'homme et du Conseil constitutionnel. Il examine également les actes spécifiques à chaque procédure et les voies de recours qui s'y attachent.

Le livre s'adresse autant aux magistrats du siège notamment aux juges d'instruction - et membres du ministère public, greffiers, enquêteurs, qu'aux avocats, huissiers, notaires ou responsables juridiques d'établissements financiers.

Docteur en droit, Lionel Ascensi est magistrat et actuellement conseiller référendaire à la chambre criminelle de la Cour de cassation. Il est par ailleurs maître de conférences associé à l'Université d'Angers, où il est membre du Centre Jean Bodin - Recherche juridique et politique (UPRES EA 4337).

Inscription 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

ACTUALITÉS EN MATIÈRE DE CYBERPREUVE

MYRIAM QUÉMÉNER

AVOCAT GÉNÉRAL PRÈS LA COUR D'APPEL DE PARIS, DOCTEUR EN DROIT

L'accès à la preuve numérique, c'est-à-dire l'ensemble des traces éventuellement laissées sur Internet par toute victime ou auteur présumé d'un crime ou d'un délit : adresses IP, mails, échanges WhatsApp, Snapchat, comptes Facebook ou Instagram[1], est désormais au coeur d'enjeux à la fois techniques et juridiques.

La recherche de la preuve numérique dans le cadre des enquêtes pénales est devenue fondamentale, pas spécifiquement définie, et correspond à des indices dématérialisés. Elle présente des caractéristiques qui la rendent fragile, volatile, complexe à localiser. La preuve numérique dans un cadre pénal peut être cernée notamment par le biais des données dématérialisées qui sont de nature diverse puisqu'elles peuvent concerner soit le trafic, les connexions ou le contenu des échanges numériques[2].

Le domaine de la preuve numérique ne concerne pas seulement la cybercriminalité – qui correspond aux infractions visant les systèmes de traitement automatisé de données – mais aussi les infractions classiques comme l'escroquerie, le blanchiment ou l'extorsion prenant le numérique comme vecteur de passage à l'acte.

Au regard du principe de la liberté de la preuve en matière pénale posé par l'article 427 du Code de procédure pénale, la preuve numérique est parfaitement admise par les tribunaux et répond à des impératifs de loyauté, de proportionnalité comme tout mode de preuve classique et doit être débattue contradictoirement lors du procès.

Les cadres juridiques de l'accès à la preuve numérique concernent tout d'abord à des procédures classiques comme les réquisitions, les interceptions de communications, les perquisitions et saisies, l'expertise.

Face à la complexité induite par le numérique, le législateur a mis en place plus récemment des procédures comme l'enquête sous pseudonyme, la captation de données à distance, la sonorisation, la géolocalisation, l'IMSI Catcher. La loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice a notamment apporté des modifications relatives aux procédures destinées au recueil de la preuve numérique[3].

On constate cependant des limites au recueil de la preuve numérique, en raison d'obstacles techniques comme l'anonymisation des données, le chiffrement, l'envoi des données dans le cloud et le darkweb. Le numérique éprouve clairement l'efficacité du système probatoire dans sa globalité[4]. De plus, l'accès aux données est contraint par des obstacles juridiques liés en particulier à sa dimension mondialisée[5].

La recherche de la preuve numérique est au centre de réflexions au niveau du Conseil de l'Europe et de la Commission européenne et elle se confronte aussi à des évolutions technologiques comme par exemple la blockchain qui pourrait offrir prochainement des perspectives probatoires.

I. Les travaux du Conseil de l'Europe

Il faut tout d'abord rappeler que la Convention de Budapest[6] est le seul traité international contraignant en matière de cybercriminalité et les preuves électroniques qui fournit, à ses 63 États parties et aux 8 autres États qui l'ont signée ou ont été invités à y adhérer, un cadre pour les infractions contre et au moyen d'ordinateurs. Il définit les procédures permettant aux autorités de justice pénale d'obtenir des preuves électroniques en rapport avec toute infraction et sous réserve des garanties de l'État de droit. Enfin, ce texte présente les instruments de coopération internationale en matière de cybercriminalité et de preuves électroniques.

Cependant, la Convention ne traite que partiellement la question de l'accès aux preuves électroniques dans le cyberespace et notamment le « cloud computing ». C'est pourquoi les travaux du Comité de la Convention sur la cybercriminalité pour l'adoption d'un second protocole additionnel à la convention sur la cybercriminalité ont débuté en septembre 2017[7] et devraient se conclure en décembre 2019. Les négociations poursuivent la réalisation de plusieurs objectifs dont une entraide judiciaire plus efficace et l'instauration d'une coopération directe entre autorités nationales et fournisseurs de services. Par ailleurs, la collecte de preuves numériques se situant à l'intersection de plusieurs branches du droit, le droit pénal doit composer, notamment, avec les règles en matière de protection des données – élément qui n'échappe pas aux négociations actuellement menées.

Le Conseil de l'Europe a aussi, élaboré un guide[8] sur la preuve électronique à l'intention des services d'enquête, des procureurs et des juges dont l'objectif est de « fournir un soutien et des conseils pour l'identification et le traitement de la preuve électronique en utilisant des méthodes qui garantiront que l'authenticité de la preuve sera maintenue tout au long du processus ».

II. Les travaux européens

De plus, l'Union européenne devrait disposer dans le futur d'un instrument spécifiquement dédié à la collecte transfrontière de preuves numériques[9]. Un projet de règlement « E-evidence » prévoit un corps de règles contenues dans un règlement et, d'autre part, un cadre établi par une directive établissant des règles harmonisées concernant la désignation de représentant légaux aux fins de collecte de preuves en matière pénale[10].

Ces instruments vont permettre la collecte des preuves numériques grâce à une coopération directe entre autorités judiciaires d'un État membre de l'Union et un fournisseur de services qui se situe dans un autre État membre. Ainsi, une autorité judiciaire d'un État membre pourra enjoindre à un acteur privé, tel un fournisseur de services de produire ou de conserver des données, quelle que soit la localisation de ces données. L'application du règlement futur requiert une situation transfrontière, laquelle existe lorsque le fournisseur de services est établi ou représenté dans un autre État membre que celui où l'enquête pénale est menée.

Le futur règlement trouvera également à s'appliquer si le fournisseur de services n'est pas établi au sein de l'Union (comme les GAFAM) mais y propose ses services. Toutes les données informatiques peuvent faire l'objet d'une injonction de produire pour autant qu'elles soient stockées. Ces données devront servir de preuves dans le cadre d'enquêtes judiciaires ou de procédures pénales concrètes. Les injonctions ne pourront être émises dans un but de prévention ; dès lors, l'infraction pénale devra avoir été déjà commise, mais peu importe que le(s) auteur(s) soi(en)t connu(s) ou inconnu(s). De ce fait, l'ouverture d'une enquête pour une infraction particulière se pose comme condition préalable à l'application du règlement. Enfin, le règlement innove par rapport à tous les autres instruments en ce qu'il introduit de très courts délais pour l'exécution de l'injonction de production et prévoit des sanctions applicables aux fournisseurs de services qui ne respecteraient pas leurs obligations.

III. Preuve numérique et blockchain

Au-delà du droit, il est aussi pertinent de s'intéresser aux technologies qui seraient à même de sécuriser des transactions et donc d'offrir des améliorations quant à

la fiabilité de la preuve numérique. Tel est le cas de la blockchain qui semblerait ouvrir des perspectives pouvant permettre de démocratiser le concept de preuve numérique[11]. Selon la définition de Blockchain France (https ://blockchainfrance.net), la blockchain est une « technologie de stockage et de transmission d'informations, transparente, sécurisée et fonctionnant sans organe de contrôle ».

En matière pénale, la preuve étant libre, il apparaît envisageable de considérer que la blockchain peut constituer un élément de preuve numérique de par son caractère infalsifiable, en offrant une date certaine, en évitant le recours au tiers de confiance. D'une manière générale, la blockchain présente de nombreux avantages en matière de preuve comme la transparence, la sécurité, la rapidité, la dimension internationale, la confidentialité. La preuve peut en effet être vérifiée à tout moment, étant inscrite simultanément sur les différents noeuds du réseau. Cependant, dans la mesure où cette technologie numérique, n'est pas encore arrivée à maturité, il semble préférable de la compléter par d'autres indices numériques ou non plus classiques.

En Chine, le tribunal de Hangzhou spécialisé en matière de questions liées à internet a confirmé le 20 juin 2018 que les données électroniques insérées dans une liste d'enregistrements blockchain peuvent tenir lieu de preuve dans un contentieux judiciaire. La décision se fonde notamment sur la crédibilité des moyens techniques d'obtention des preuves, et sur l'intégrité de la preuve blockchain[12]. L'utilisation d'une plate-forme de liste d'enregistrements blockchain - ayant la qualité de tiers, fiable et exempte de conflit d'intérêts - a permis d'apporter la preuve légale de l'atteinte à la propriété intellectuelle[13]. Cette méthode pourrait progressivement s'intégrer dans les mécanismes probatoires actuels tels que le constat d'huissier mais une reconnaissance légale plus affirmée permettrait de sécuriser davantage les procédures pénales.

Notes :

1 https://www.lemonde.fr/societe/article/2018/04/14/la-guerre-discrete-de-la-preuve-numerique_5285412_3224.html

2 H. Matsopoulou, « Les nouveaux moyens de preuve au service de la criminalité organisée – A propos de la loi n° 2016-731 du 3 juin 2016 », JCP G 2016, n° 707, p. 1222 et s.

3 M Quéméner, « La preuve numérique dans un cadre pénal », Fascicule jurisclasseur communication, n° 1105.

4 G.Giudicelli-Delage, « Les transformations de l'administration de la preuve pénale, perspectives comparées : Allemagne, Belgique, Canada, Espagne, États-Unis, France, Italie, Portugal, Royaume-Uni », Archives de politique criminelle, vol. 26, n° 1, 2004, pp. 139-188.

5 M. Mosse « La preuve à l'ère numérique, un enjeu pour l'Europe « https ://business.lesechos.fr/directions-juridiques/droit-des-affaires/brevets-et-marques/030430605583-la-preuve-a-l-ere-numerique-un-enjeu-pour-l-europe-311589.php ou sur le site du Club des juristes ¤ www.leclubdesjuristes.com

6 https://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/185

7 Recommandation autorisant la participation aux négociations sur un deuxième protocole additionnel à la Convention sur la cybercriminalité du Conseil de l'Europe (STE n° 185).

8 Le guide est disponible sur le site de la Communauté Octopus du Conseil de l'Europe, après inscription.

9 Recommandation autorisant la participation aux négociations sur un deuxième protocole additionnel à la convention sur la cybercriminalité du Conseil de l'Europe (STE n° 185).

10 Proposition de règlement e-evidence. Le 7 décembre 2018, le Conseil de l'UE a adopté son orientation générale concernant la proposition de règlement, modifiant le texte initialement proposé par la Commission européenne sur plusieurs points. La version consolidée est disponible sur https://data.consilium.europa.eu/doc/document/ST-15292-2018-INIT/en/pdf (uniquement disponible en anglais). Le 17 mai 2019, un supplément comprenant les annexes au règlement a été publié, disponible sur https://data.consilium.europa.eu/doc/document/ST-9365-2019-INIT/en/pdf (uniquement disponible en anglais

11 S. Canas, Blockchain et preuve : le point de vue du magistrat : Dalloz IP/IT, févr. 2019, p. 82.

12 JCl. Banque-Crédit-Bourse, fasc. 179, Blockchain, par D. Legeais.

13 www.xinhuanet.com/2018-06/28/c_1123051280.htm