LA REVUE DU
GRASCO

www.grasco.eu
www.larevuedugrasco.eu

N°26— Mai 2019

Parution trimestrielle
Gratuite
ISSN 2272-981X

EDITORIAL

CHANTAL CUTAJAR

DIRECTRICE DU GRASCO

La lutte contre la criminalité économique et financière

Dans un référé du 12 décembre 2018 relatif aux « moyens consacrés à la lutte contre la délinquance économique et financière » adressé à la Garde des sceaux, ministre de la Justice, Nicole Belloubet, et au ministre de l'Intérieur, Christophe Castaner, le Premier président de la Cour des comptes constate que la lutte contre cette forme de criminalité constitue une priorité affichée de politique pénale tout en pointant une organisation et des moyens déficients.

Parmi les cinq recommandations formulées, seule la création d'une instance régulière de concertation sur les moyens consacrés en Île-de-France semble avoir retenu l'attention des deux ministres.

Il est clair cependant que l'efficacité de la lutte contre la délinquance économique et financière dépend de la manière dont il est répondu aux enjeux stratégiques, d'organisation et de ressources humaines, parfaitement mis en évidence par la Cour des comptes.

Quels sont les constats ?

La délinquance économique progresse de manière significative. On assiste ainsi à une professionnalisation des réseaux de blanchiment en lien avec la criminalité organisée et à une sophistication des procédés recourant aux nouvelles technologies au fur et à mesure de leur apparition. Le nombre d'enquêtes nécessitant des investigations à l'échelle internationale augmente.

Quelles sont les solutions préconisées ?

Pour lutter efficacement contre cette « délinquance qui préoccupe légitimement nos concitoyens », le Premier président, à travers ses recommandations, préconise de professionnaliser, de spécialiser et de stabiliser dans leurs fonctions, l'ensemble des acteurs de la chaîne pénale en matière d'investigations fi-

SOMMAIRE

ÉDITO 1

INTERVIEW :

CHRISTIANE FÉRAL-SCHUHL, PRÉSIDENTE DU CONSEIL NATIONAL DES BARREAUX 5

DOCTRINE JURIDIQUE :

LA COUR D'ASSISES SANS JURÉS À LA LUMIÈRE DE LA DERNIÈRE LÉGISLATION (LOI DU 23 MARS 2019), PAR JEAN PRADEL 6

DOCTRINE SCIENCES CRIMINELLES :

LA CRYPTO-CRIMINALITÉ, DÉFI DE L'ÉCONOMIE 2.0 PAR FLORIAN MANET 8

LES ENJEUX DE LA DÉLINQUANCE FISCALE GLOBALISÉE, PAR ÉRIC VERNIER 19

JURISPRUDENCE :

ESCROQUERIE COMMISE AU MOYEN DE FAUSSES FACTURES : SOUS QUELLE(S) QUALIFICATIONS(S) POURSUIVRE, PAR DOROTHÉE GOETZ 28

COMPLIANCE/CONFORMITÉ :

L'ÉVALUATION DE L'INTÉGRITÉ DES TIERS EN MATIÈRE D'ANTICORRUPTION EN ENTREPRISE, PAR CHARLES DUCHAINE 30

REGARDONS AILLEURS :

LA RESPONSABILITÉ DES PERSONNES MORALES OU LE "TROU DANS LA RAQUETTE" DE LA LUTTE CONTRE LE CRIME ORGANISÉ EN RUSSIE PAR BENJAMIN DANLOS 37

nancières. Il préconise à cette fin de créer des filières de recrutement d'officiers et de commissaires adaptées aux missions d'investigation spécialisée, notamment en matière économique et financière (Recommandation n° 1) ; de mettre en place un suivi régulier des effectifs des unités d'enquête économique et financière dans les services de sécurité publique et mettre au point des formations spécifiques à leur intention (Recommandation n° 2) ; d'assurer un suivi des magistrats spécialisés en matière économique et financière, portant sur l'évolution de leurs effectifs, les processus d'affectation et de mobilité, et l'offre de formation continue (Recommandation n° 3) et de poursuivre dans les deux ministères, le développement du recours à des compétences externes en matière économique et financière, notamment en diversifiant les voies de recrutement (Recommandation n° 4).

En ce qui concerne la formation des magistrats, si l'offre de formation continue en matière économique et financière est assez complète, la Cour des comptes constate que le recrutement initial des magistrats ne tient pas compte de la spécificité des affaires économiques et financières ; que les voies de recrutement sur titre qui pourraient permettre de sélectionner des juristes expérimentés dans cette matière ne sont pas utilisées ; qu'enfin, la formation initiale d'une durée de 31 mois assurée par l'École nationale de la magistrature « est construite sur un concept de magistrat « généraliste », assumé par l'École et qui exclut toute spécialisation à l'exception de la préparation au premier poste dans les dernières semaines de la scolarité.

C'est à une véritable révolution culturelle que la Cour des comptes appelle visant à mettre face à des délinquants de plus en plus spécialisés et performants, des policiers, des gendarmes et des magistrats spécialisés à ces techniques d'enquêtes spécifiques que sont les investigations financières. C'est à cette mission que contribue le Collège européen des investigations financières et de l'analyse financière criminelle (CEIFAC) à Strasbourg.

On ne perçoit malheureusement pas, à la lecture des réponses au référé, des ministres de l'Intérieur et de la Justice, une réelle prise de conscience de ces enjeux.

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

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

CHRISTIANE FÉRAL—SCHUHL,

PRÉSIDENTE DU CONSEIL NATIONAL DES BARREAUX

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

L.R.D.G. : Qu'est-ce que le Conseil national des barreaux (CNB) et comment est-il composé ?

Le Conseil national des barreaux est l'institution représentative des 68 000 avocats français. Il est composé de 80 avocats élus par la profession pour trois ans, parmi lesquels le président est nommé. Nous avons aussi deux vice-présidents de droit : le bâtonnier de Paris et le président de la conférence des bâtonniers. Ces deux organismes, aux côtés du CNB, permettent d'avoir une représentation unie et influente de la profession d'avocat.

L.R.D.G. : Quelles sont les missions du CNB et comment les exerce-t-il ?

Nous représentons aussi la profession d'avocat en France et à l'international, auprès du gouvernement, des décideurs politiques. Nous rencontrons très régulièrement les députés et les sénateurs, nous faisons des propositions d'amendements.

Nous accompagnons aussi les avocats dans leur exercice quotidien en développant et proposant de nombreux outils : des plateformes en ligne qui permettent de dématérialiser des procédures, des accès sécurisés pour échanger avec les juridictions, des adresses email et un cloud sécurisé ou encore des formations et événements pour actualiser leur connaissance du droit.

Nous règlementons enfin la profession grâce au Règlement interne national (RIN) que nous modifions deux à trois fois par an pour l'adapter notamment aux nouveaux usages.

L.R.D.G. : Quels sont les objectifs prioritaires du CNB ?

Pour mon mandat, j'ai fixé trois objectifs prioritaires : accompagner la profession dans les évolutions de la société, promouvoir l'égalité des chances et développer les outils numériques. Pour atteindre ces objectifs je travaille avant tout à l'unité de la profession : le barreau de Paris, la Conférence des bâtonniers et le CNB doivent s'unir pour faire front commun. C'est l'unité qui nous permet aussi d'être plus influents.

L.R.D.G. : Quelle place tient le numérique dans la profession d'avocat ?

Je suis très attentive à ce sujet car je crois que c'est là que se niche le futur de l'avocat augmenté. Le numérique doit permettre aux avocats de répondre aux mutations de la société et de leur métier. Nous avons lancé un vaste plan d'investissement numérique qui doit permettre de placer l'avocat au coeur de la société numérique en le dotant d'outils fiables et novateurs.

L.R.D.G. : Quel impact ont les legaltech sur la profession d'avocat ?

Elles sont une formidable opportunité d'innover dans notre secteur lorsqu'elles s'accompagnent de toutes les garanties pour les

justiciables. Ces garanties, seuls les avocats peuvent les apporter. Nous avons d'ailleurs lancé, au CNB, la première legaltech d'Europe : le site de consultation juridique en ligne avocat.fr.. À ce jour, plus de 11 000 avocats sont référencés et ils répondent à 40 000 demandes chaque année, un chiffre en hausse constante. Nous sommes bien évidemment favorables à l'innovation dans le secteur, mais nous souhaitons que cela se fasse dans le respect du périmètre du droit : l'innovation ne peut être un prétexte pour empiéter sur la loi.

L.R.D.G. : Quelles actions mènent le CNB pour lutter contre le blanchiment d'argent auquel la profession d'avocat est exposée ?

La profession d'avocat a depuis longtemps réagit et mis en place des garde-fous, notamment par le biais des CARPA (Caisse autonome des règlements pécuniaires des avocats). Je ne peux pas vous laisser dire que notre profession serait particulièrement exposée aux risques de blanchiment. Nous sommes au contraire très en pointe sur ce sujet.

Le CNB a notamment renforcé le groupe de travail dédié à cette problématique. Ce groupe de travail représente la profession au sein des instances en charge de coordonner au niveau national et européen la lutte contre le blanchiment d'argent et le financement du terrorisme (COLB, TRACFIN).

Nous avons par ailleurs publié un guide pratique « lutte contre le blanchiment et le financement du terrorisme » pour sensibiliser les avocats aux implications concrètes dans leur exercice professionnel des impératifs liés à la lutte anti-blanchiment y compris pour les activités nouvelles (mandataire en transactions immobilières, mandataire sportif, mandataire d'artistes et d'auteurs, fiducie, activités commerciales connexes et accessoires…).

L.R.D.G. : En quoi consistent les États généraux de l'avenir de la profession d'avocat organisés par le CNB ?

C'est une démarche inédite : nous élaborons de manière collaborative les propositions qui dessineront la profession d'avocat de demain.

Nous avons d'abord lancé une première consultation en ligne pour définir, avec les avocats, quels sont les sujets prioritaires.

Ces sujets sont aujourd'hui arrêtés et ont été répartis dans des groupes de travail qui vont formuler des propositions concrètes.

Ces propositions seront soumises à une seconde consultation et nous clôturerons la démarche globale lors d'un événement les 25 et 26 juin.

OUVRAGES RÉCENTS

LES PARADIS FISCAUX

AUTEUR : PIERRE-ALEXIS BLEVIN

ÉDITEUR : QUE SAIS-JE ?

Présentation de l'éditeur

Apparus à la fin du XIXe siècle, les paradis fiscaux se sont développés avec la mondialisation. Un phénomène aux visages variés et dont la diversité rend difficile leur identification. Centres financiers offshore, zones franches, micro-États, provinces autonomes, États fédérés… les paradis fiscaux sont le fruit d'une histoire, d'une géographie ou d'un système politique très dissemblables d'un territoire à l'autre. .Il n'existe pas de paradis fiscal type mais de multiples mo-

dèles s'adaptant constamment et proposant des régimes fiscaux incitatifs. Mêlant à la fois secret bancaire, fiscalité et droit des sociétés, les paradis fiscaux permettent la constitution de montages juridiques complexes propices à différentes formes d'évasions fiscales avantageuses. Pierre-Alexis Blevin définit le concept de « paradis fiscal », éclaire ses enjeux géopolitiques et identifie les instruments juridiques qui en résultent. Il conclut avec un panorama complet des principaux dispositifs de lutte contre l'évasion fiscale internationale.

LA COUR D'ASSISES SANS JURÉS À LA LUMIÈRE DE LA DERNIÈRE LÉGISLATION (LOI DU 23 MARS 2019)

JEAN PRADEL

PROFESSEUR ÉMÉRITE DE L'UNIVERSITÉ DE POITIERS, MEMBRE TITULAIRE DE L'ACADÉMIE INTERNATIONALE DE DROIT COMPARÉ

Le recul du jury criminel en France est évident et se manifeste depuis longtemps. Déjà au XIXème siècle, les magistrats, notamment les juges d'instruction, correctionnalisaient les « petits » crimes dans un souci de plus grande célérité de la justice, voire pour réduire le coût de la justice. Au cours du XXème siècle, le législateur se mit à créer des cours d'assises sans jurés, notamment en matière d'actes terroristes et de trafic international de drogues.

Aujourd'hui, nos cours d'assises sont submergées d'affaires et des accusés attendent parfois jusqu'à deux ans de comparaître devant la juridiction criminelle, la chambre de l'instruction devant même en certains cas ordonner la remise en liberté avant le début du procès. C'est ainsi que la conférence des présidents de cours d'appel a émis la proposition d'une suppression de la cour d'assises avec jurés pour un certain nombre de crimes. L'affaire a fait grand bruit. Pourtant, le gouvernement, courant 2018, intégra l'idée dans le projet de loi de programmation 2019-2022 et de réforme de la justice. Le vote de la loi en général et de cette adjonction en particulier se fait avec difficulté. Mais aujourd'hui, à la suite du vote définitif par le Parlement et du recours devant le Conseil constitutionnel vidé par décision du 21 mars 2019, la loi est promulguée le 23 mars 2019.

I. Quels sont les traits essentiels de cette nouvelle cour criminelle qui est traitée à l'article 63 de la loi de 2019 ?

Les personnes majeures accusées d'un crime puni de 15 à 20 ans de réclusion criminelle, non en situation de récidive, sont jugées en premier ressort par la cour criminelle départementale, celle-ci connaissant en même temps des délits connexes ; toutefois, la cour n'est pas compétente s'il existe un ou plusieurs coaccusés ne réalisant pas ces conditions. Cette juridiction départementale siège au même lieu que la cour d'assises et est composée d'un président et de quatre assesseurs, choisis par le premier président de la cour d'appel parmi les magistrats du siège de ladite cour ; deux des assesseurs peuvent être des magistrats exerçant à titre temporaire ou des magistrats honoraires.

Ces personnes auront été mises en accusation par le juge d'instruction devant le tribunal criminel. Le délai de comparution devant la juridiction de jugement est de six mois (éventuellement prolongé de six mois) et non d'un an, s'agissant de « petits » crimes et par dérogation au droit commun en matière criminelle (art. 181 al. 8 CPP).

La cour criminelle départementale applique le droit commun des assises à l'exception des dispositions relatives au jury. Ainsi les pouvoirs du président des assises seront exercés par le président de la cour criminelle comme par exemple le fameux

pouvoir discrétionnaire. Toutefois quelques particularités par rapport à la cour d'assises doivent être signalées : pour l'application des articles 359, 360 et 362 CPP (sur la culpabilité) les décisions sont prises à la majorité ; l'article 347 selon lequel après clôture des débats d'assises le dossier est remis au greffier ne s'applique pas en sorte que la cour criminelle délibère en étant en possession de l'entier dossier ; si la cour constate que les faits constituent un crime passible de 30 ans de réclusion criminelle ou plus, elle se déclare incompétente et renvoie le cas devant la cour d'assises.

Enfin l'appel des décisions de la juridiction criminelle départementale est porté devant la cour d'assises en sa formation d'appel (9 jurés).

Ces dispositions sont applicables à titre expérimental à compter de la date fixée par un arrêté du garde des sceaux pour une durée de trois ans, pour le jugement des personnes mises en accusation au plus tard deux ans après cette date. L'expérience se fera dans au moins deux départements et au plus dix déterminés par un arrêté du garde des Sceaux. Six mois au moins avant le terme de l'expérimentation, le gouvernement adressera au Parlement un rapport d'évaluation. De plus, pour l'application de la réforme, les personnes déjà mises en accusation devant la cour d'assises peuvent être renvoyées devant la cour criminelle avec leur accord recueilli en présence de leur avocat, sur décision du premier président de la cour d'appel. Quant aux personnes déjà mises en accusation devant la cour criminelle avant le 1er janvier 2021 et non encore jugées au 1er janvier 2022, elles sont de plein droit mises en accusation devant la cour d'assises.

II. Quel jugement porter sur la réforme ?

Il est toujours difficile de juger une institution quand elle n'a pas commencé à fonctionner.

On notera tout de même la grande prudence du législateur qui ne vise que les crimes passibles de 20 ans de réclusion criminelle au maximum, ce qui inclut en fait les viols sans circonstances aggravantes, les violences avec de telles circonstances (comme les coups mortels) et les vols avec de telles circonstances. Dès lors, on peut penser que le rôle des assises va baisser de 40 à 50 %.

Prudence encore en ce que la réforme est votée « à titre expérimental ». Il s'agit d'une loi à l'essai, cette pratique à laquelle le législateur fait appel quand il hésite sur le bien-fondé de ses choix. On l'a vu en 1975 pour l'interruption volontaire de grossesse par exemple.

Prudence enfin, puisque la réforme ne concerne que les majeurs et encore non récidivistes, et seulement en première instance. De la sorte, si appel il y a, c'est le peuple qui aura le dernier mot. Curieusement, en common law, le jury n'existe qu'en première instance car en appel, la culpabilité est appréciée par une cour composée de trois juges professionnels.

Cela rappelé, la réforme paraît bien-fondée, non pas du tout en ce qu'elle réduit l'impact de l'avocat, non pas tellement en ce qu'elle exclut des jurés plus imprévisibles que des juges, mais surtout en ce qu'elle devrait accélérer le cours de la justice criminelle : il est en effet scandaleux que des accusés, en détention et toujours présumés innocents, attendent des mois, voire des années de comparaître en jugement, au mépris des exigences du principe de procès équitable, d'une justice rendue dans un délai raisonnable.

Faut-il ajouter que le jury est en recul à l'étranger, notamment en Europe continentale, surtout en Suisse, en Italie, en Espagne, et même dans les pays de common law du fait du choix offert à l'accusé entre être jugé par un juge seul ou par un juge avec jurés, le choix se portant presque toujours sur la première formule.

Le Conseil constitutionnel n'a pas invalidé la réforme pour la raison qu'il n'a pas été saisi à ce titre. N'oublions pas que chez nous – contrairement à ce qui existe aux USA et au Canada par exemple – le jury n'est pas une institution garantie par la Constitution.

Dès maintenant, on peut prévoir que la pratique de la correctionnalisation va régresser puisqu'elle avait été imaginée essentiellement pour ne pas saisir la cour d'assises de « petits » crimes. On peut ainsi imaginer que le stock d'affaires en cours va régresser. Et il est fort possible que à l'issue du délai de trois ans, le législateur pérennise cette nouveauté.

LA CRYPTO-CRIMINALITÉ, DÉFI DE L'ÉCONOMIE 2.0

FLORIAN MANET

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

Bitcoin, Ethereum, Ripple, Dash, Dogecoin, Peercoin, Namecoin,.. la litanie des crypto-devises semble infinie tant cet or 2.0 attire toujours plus d'investisseurs en quête de placements à fort rendement ou de financements innovants. D'ailleurs, cette nouvelle économie semble très florissante comme en témoigne, par exemple, la presse israélienne qui évalue à plus de 10 000 salariés employés par la crypto-industrie à RAMAT GAN, la *city* israélienne.

Au-delà des clichés ou des effets de mode, cette révolution technologique suscite incontestablement intérêt, fascination mais aussi de nombreuses inquiétudes liées à ces promesses de progrès. Considérée comme une alternative formidable aux systèmes bancaires ou comme un vecteur d'unification d'une économie-monde en émergence, elle inspire, par ailleurs, d'autres applications concrètes qui sécurisent des transactions financières ou de données quelles qu'elles soient en apportant traçabilité et immutabilité. À ce titre, ces avancées répondent précisément, aussi, à des besoins partagés par des organisations criminelles de dimension internationale, entreprenantes et, surtout, à l'écoute de toutes nouvelles opportunités. Elles sont, alors, exploitées voire dévoyées par des opérateurs illicites, qui y ont très vite perçu les innombrables avantages pour leur prospérité. Simultanément, la mobilisation des services répressifs peut se trouver, alors, freinée par des difficultés à appréhender clairement la technologie digitale qui sous-tend la crypto-industrie : la *blockchain* ou chaîne de blocs.

De prime abord, pour les enquêteurs et, *in fine*, pour les magistrats, la *blockchain* est associée à ces cohortes toujours plus nombreuses d'investisseurs floués, ruinés, déboussolés, honteux d'avoir cru à un mirage. Un mirage dans lequel a été, subrepticement, englouti leur patrimoine, fruit de tant d'années de labeur, l'espoir d'une vie meilleure et, parfois, leur santé mentale comme physique. Mus par un appât du gain irrésistible et insatiable, des entrepreneurs malveillants ont, en effet, méthodiquement mis sur pied un double dispositif d'hameçonnage d'investisseurs et de « siphonnage » de leur patrimoine. Ainsi, une délinquance astucieuse cible, par exemple, le « cambriolage en ligne » du patrimoine financier de particuliers. Elle exploite, ainsi, les immenses potentialités offertes par l'ingénierie financière internationale tributaire des vecteurs numériques. Après les faux ordres de virement, émerge, désormais, le phénomène des escroqueries aux faux placements depuis fin 2017. Le mode opératoire employé est rodé et difficilement détectable. Ce qui en rend complexe l'identification de l'escroquerie et les actes d'investigation.

Cette première manifestation apparente de cette révolution digitale abuse, en réalité, du concept de la *blockchain*. Elle ne doit pas pour autant masquer d'autres applications criminelles fondées sur une exploitation concrète de la crypto-industrie. Vecteur de blanchiment de fonds illicites ou de diffusion de contenus, monnaie d'échange lors de rançonnement.... Tels sont, désormais, les

autres visages d'une activité criminelle contemporaine croissante.

Au final, l'enjeu majeur posé par cette crypto-criminalité en émergence réside dans la souveraineté de la *data* personnelle ainsi que dans la confiance en l'économie numérique par les populations dans un contexte d'un marché international libéralisé. Ce « cambriolage en ligne » symbolise, à lui seul, les menaces criminelles de demain affectant l'économie 2.0 et appelle, à la fois, une prise de conscience des autorités comme un effort collectif de formation à cet univers globalisé et digitalisé qui s'impose comme le cadre de vie incontournable de nos sociétés.

I. L'environnement digital d'une économie-monde 2.0 : la *blockchain*

Avant de décrire les mécanismes particuliers de dévoiement des outils financiers digitaux, il convient de définir, préalablement, les notions essentielles qui jalonnent l'industrie des crypto-actifs. En creux, se dessineront les enjeux propres à ces nouvelles pratiques criminelles.

A. Un projet politique : créer une monnaie électronique indépendante de l'État

L'émergence des devises virtuelles tire ses racines à la fois du mouvement pour le logiciel libre[1] ainsi que de la communauté « cypherpunk[2] ». Depuis les années 1980, ses membres[3] développent un projet de société dans lequel les autorités publiques se trouvent contournées. Ainsi, par exemple, en matière financière, elle encourage le recours aux technologies de chiffrement pour créer une monnaie électronique. Libre, hors de tout contrôle de l'État et de ses banques centrales, elle favorise l'anonymat des transactions. Ainsi, en 1984, Friedrich Hayek affirme que « *je ne crois pas au retour d'une monnaie saine tant que nous n'aurons pas retiré la monnaie des mains de l'État ; nous ne pouvons pas le faire violemment ; tout ce que nous pouvons faire, c'est, par quelque moyen indirect et rusé, introduire quelque chose qu'il ne peut pas stopper* ».

Les progrès technologiques accompagnent et affinent une conceptualisation progressive d'un projet politique visant à restaurer la confiance dans les transactions financières. Il s'agit de créer *ex nihilo* « *une monnaie de l'internet sur la base d'un internet de la monnaie* ». S'appuyant sur un réseau numérique décentralisé, des jetons ou *token* sont envisagés comme des unités de paiement électronique. L'article fondateur de Satoshi Nakamoto[4] publié en 2008 décrit précisément le fonctionnement d'un protocole permettant la production d'un registre infalsifiable utilisant le réseau informatique pair à pair[5] -la *blockchain*- comme couche technologique d'une nouvelle crypto-monnaie, le *bitcoin*. Cette *blockchain* correspond à l'équivalent d'un grand livre comptable infalsifiable, accessible à tous, consultable et vérifiable. Ceci rend inutile l'existence d'un tiers de confiance, généralement obligatoire dans les cessions de titres ou de valeurs. Ces réalisations révolutionnaires s'inscrivent, il est vrai, dans le contexte de la crise financière de 2008 et de celle des *subprimes* où la question de la confiance dans le système bancaire et monétaire était centrale.

B. Une révolution informatique disruptive

La *blockchain* prend place dans la lignée des révolutions informatiques tels l'ordinateur individuel, à partir de 1975, ou encore l'internet grand public en 1993.

Au coeur du protocole de la *blockchain,* la valorisation du *bitcoin* ou d'un autre quelconque crypto-actif est adossée à un triple consensus relatif aux règles, à l'histoire et au fait que cet actif a lui-même de la valeur.

Les règles sont imposées par le protocole informatique sous-jacent à la *blockchain.* En effet, les transactions entre internautes sont regroupées par « blocs » horodatés. Une fois le bloc validé, la transaction est rendue publique à l'ensemble des détenteurs du registre et, potentiellement, à tous les utilisateurs qui pourront l'ajouter à leur chaîne de blocs. Ainsi, selon *Blockchain France*[6] « une *blockchain* est une base de données numérique infalsifiable sur laquelle sont inscrits tous les échanges effectués entre ses utilisateurs depuis sa création ».

Ce dispositif apporte la traçabilité et l'authenticité des transactions dont l'historique et la chronologie des opérations sont certifiés par cet horodatage et par une signature électronique. Celle-ci repose sur une cryptographie asymétrique composée d'une paire de clés[7], l'une privée, l'autre publique. Par ailleurs, ces blocs sont clairement identifiables par un *hash*, telle une empreinte digitale résultant du « hachage[8] » du bloc précédent, c'est-à-dire par un processus de compression.

Ces registres de données ou chaînes de blocs nécessitent une validation[9] effectuée par certains internautes dénommés « mineurs » au sein d'un réseau

décentralisé. En contrepartie d'une rémunération[10] au bénéfice du mineur ou d'un pool de mineurs, cette opération actualise régulièrement cette chaîne de blocs au sein des « noeuds » du réseau représentés par les détenteurs du registre. Chaque noeud est, alors, connecté à plusieurs pairs, formant un réseau de pairs, maillant, en définitive, l'ensemble du globe. Cette architecture maillée repose sur un dispositif décentralisé de validation, protecteur de toute action malveillante. La validation est opérée par de nombreux utilisateurs à travers le réseau, en l'absence de toute autorité centrale.

Au total, il s'agit d'un processus décentralisé de surveillance collective dans lequel les internautes mineurs vérifient les transactions et assurent, par eux-mêmes, la sécurité de leur propre réseau en utilisant un matériel informatique dédié et crypté.

C. La crypto-monnaie est-elle ... une monnaie ?

Appelés crypto-monnaies ou crypto-devises, ces crypto-actifs sont nés au début des années 2010, dans le sillage même du développement, à l'échelle mondiale, de communautés dites « virtuelles », rassemblant des internautes au moyen d'outils d'interaction numérique (*chat*, forum, etc.). Il s'agissait alors de poursuivre ce travail d'unification et d'échange universel en abattant les cloisons physiques du monde réel. Cette monnaie d'échange commune devait, alors, accélérer le processus mondial de globalisation.

Toutes les *blockchains* des crypto-actifs constituent, de près ou de loin, des avatars du *bitcoin*. Cette crypto-industrie est florissante comme le démontre le site *coinmarketcap.com* qui recense plus de 2000 actifs alternatifs, s'en créant plus d'une dizaine par semaine. Ces avoirs sont stockés dans des coffres-forts électroniques appelés « *wallet* » accessibles en ligne, sur ordinateur, ou hors-ligne sur des supports physiques tels des clés USB spécifiques ou bien encore sur un simple morceau de papier[11].

Souvent désignés, par abus de langage, sous le terme de « monnaies virtuelles » ou « crypto-monnaies », ces actifs sont définis par le Code monétaire et financier (art. L561-2, 7° bis) : « *tout instrument contenant sous forme numérique des unités de valeur non monétaire pouvant être conservées ou être transférées dans le but d'acquérir un bien ou un service, mais ne représentant pas de créance sur l'émetteur* ».Dés lors, ils ne sauraient être considérés juridiquement comme des monnaies ni comme des moyens de paiement[12].

Ces actifs s'apprécient sur un marché partialement non réglementé ou non régulé par une autorité de contrôle[13]. En conséquence, le cours de ces actifs témoigne d'une extrême volatilité et il est régulièrement observé d'importantes fluctuations. Il ne bénéficie, donc, pas d'un cours légal contrairement aux monnaies émises par la Banque de France. Ainsi, le cours du *bitcoin* a explosé au cours de l'année 2017 atteignant les 20 000 dollars en décembre 2017 avant de plonger à 6 800 dollars en juin 2018. Il est évalué à 3 901 dollars le 8 mars 2019. De même, la capitalisation des *bitcoins* a connu un pic historique en décembre 2017 atteignant la barre des 320 milliards de dollars avant de s'évaluer à 120 milliards en juin 2018. Elle est évaluée à 68 milliards de dollar le 8 mars 2019. Non adossés à des contre-valeurs solides, ils sont le jeu ou l'otage de mouvements d'opinion amplifiés par les moyens numériques sur l'ensemble de la toile mondiale. Ainsi, des bulles artificielles fondées sur des rumeurs ou des opérations d'obfuscation exercent des incidences affectant le cours de ces actifs.

Dans ces conditions de forte instabilité de valeur, ces placements en crypto-actifs n'offrent aux investisseurs aucune garantie ni protection du capital-risque. Ces opérations financières sont irréversibles dans leurs effets.

D. Pause ou fin de la *token mania* ?

Ces crypto-actifs représentent des placements évolutifs, agiles et flexibles à l'image d'un marché financier globalisé en perpétuelle évolution. Ils assurent deux fonctions à la disposition des investisseurs et des besoins de financement de l'économie. Instrument de spéculation avant tout, ils constituent, par ailleurs, un moyen alternatif de levée de fonds offert aux entrepreneurs.

Ainsi, l'*Initial Coin Offering* ou ICO ou émission de jeton constitue un outil révolutionnaire de levée de fonds pour des entrepreneurs pressés et audacieux. Considérable, le phénomène est évalué à plus de 10 % des levées de fonds en 2017. À mi-chemin entre la collecte de fonds et le financement participatif, il offre aux *start-up* les conditions favorables à leur développement, apportant rapidité et flexibilité. Le financement se fait par échange de crypto-actifs contre des jetons

ou *tokens*. Ces *tokens* propres au projet financé correspondent à des jetons inscrits sur la *blockchain*. En retour, l'investisseur bénéficie de droit porté à des propriétés ou encore des droits d'usage liés au développement futur des produits.

En juillet 2017, une start-up américano-suisse – Tezos a levé 232 millions de dollars dans un ICO tandis qu'une start-up israélienne proposant une plateforme décentralisée d'échange de crypto-monnaie, Bancor, a rassemblé en seulement trois heures 153 millions de dollars ! En septembre 2017, Domraider, première entreprise française à pratiquer une ICO, a émis sa crypto-monnaie, le DRT[14], et a recueilli 56 millions d'euros afin de créer une plateforme décentralisée dédiée aux enchères en temps réel sur la *blockchain*. Cette ruée vers l'or 2.0 semble marquer le pas aprés une véritable « *token mania* ». Selon le cabinet *Autonomous Research*, les montants des ICO ont chuté de plus de 90 % depuis le pic de janvier 2018.

Hors du système bancaire, ces applications témoignent de la recherche de désintermédiation dans les organisations sociales comme dans les transactions financières. Ainsi, en Estonie, pays avant-gardiste, 99 % des prestations (vote, création d'entreprises ou ouverture de compte..) se font en ligne. L'identification d'un citoyen se fait au moyen d'une signature électronique stockée sur un*e blockchain.* D'autres perspectives élargissent le périmètre d'application au secteur de l'assurance, du notariat et d'autres activités où la conservation de la preuve est fondamentale.

II. Le dévoiement d'une architecture de la confiance par la criminalité organisée

Transnationale par construction, dépourvue d'autorité validatrice et de contrôle, la *blockchain* affiche de multiples capacités susceptibles d'être dévoyées, dans leur usage, par des organisations criminelles en quête d'outils digitaux de transferts ou de collecte d'avoirs criminels comme de diffusion de contenus illicites. Au final, la *blockchain* crée un réseau automatique qui inspire de la confiance aux personnes qui ne peuvent ... se faire confiance. À ce titre, ce réseau mondial facilite la désintermédiation et l'irréversibilité recherchée pour sécuriser des transactions illicites entre acteurs potentiellement animés par des intérêts conflictuels. L'implication d'un tiers de confiance anonymisé et dilué par de très nombreux mineurs à travers le monde, ne se connaissant pas à l'avance, rend cette architecture particulièrement rassurante.

Cette exploitation criminelle des possibilités de la *blockchain* possède encore de nombreuses zones d'ombre et mériterait des études complémentaires. Toutefois, il convient d'évoquer certains aspects principaux afin de mieux appréhender cette réalité de l'économie 2.0.

A. La *blockchain*, argument commercial exploité par des escrocs internationaux : le faux *trading* et les fausses ICO

Des organisations criminelles spécialisées dans l'escroquerie exploitent de manière méthodique l'attrait qu'exercent les possibilités des *blockchains* au travers des promesses de très forts rendements. Deux mécanismes sont généralement mis en oeuvre : le *faux-trading* aux produits complexes et les *exit scam* pour les ICO. Dans chacun de ces deux cas, aucun *bitcoin* ou *Ethereum* ou *token* de start-up n'est réellement généré ou attribué. L'escroquerie se fonde sur ce prétexte technologique associé à des promesses de rendements exceptionnels. C'est une illusion... dramatique !

i. L'approche de la clientèle est effectuée par un dispositif réfléchi et offensif au travers d'internet

Avant de détailler le mode opératoire, il convient de rappeler le fondement propre à toutes escroqueries : la manoeuvre d'emprise psychologique. Méthodiquement, une approche ciblée de la clientèle vise à créer de la proximité et de l'empathie, à agir sur le développement d'un sentiment anti-système et à valoriser les talents personnels de l'interlocuteur. L'épargnant est pédagogiquement instruit de la nature et de l'intérêt d'un placement fiable à fort rendement quitte à prendre des libertés avec la réalité : « *Nous sommes* [ici, le commercial donne le nom de l'entreprise pour laquelle il appelle], *nous sommes régulés par* [ici, le commercial donne le nom d'une banque nationale d'un pays industrialisé], *qui nous régule et contrôle les institutions financières en activité, par exemple* [ici, le commercial donne le nom d'institutions financières connues et établies][15] ». Rassuré, il est, alors, fait appel à la bonne foi et au bon sens du client comme le confirme notre source : « *Notre objectif est de donner un accès et un soutien à de nombreux investisseurs grâce*

à cette formidable capitalisation alternative, qui se trouve hors du système élitiste et intrusif dans nos portefeuilles. Je vais juste vous rappeler les files d'attentes devant les banques de Chypre au mois de mars 2013 lorsque la banque centrale européenne avait empêché les clients de retirer leurs fonds. Ce n'est pas arrivé très loin de nous. Vous en convenez, n'est-ce pas ? ». Ainsi, les prestataires s'informent sur l'état d'esprit de l'investisseur potentiel, sur ses préoccupations au travers d'un tutoiement et d'échanges d'emblée très directs. Mis en confiance, il se laisse séduire par un discours de bon sens comme celui présenté par un grand site promouvant une académie de *trading* : « *trader sur le FOREX, c'est simplement ce que fait le banquier avec votre salaire tous les mois. Les banquiers font d'énorme profit avec votre ARGENT. Alors pourquoi ne pas le faire vous même sans intermédiaire* »[16].

En outre, le site regorge de biographies flatteuses des dirigeants ou encore de courts films sur les membres fondateurs ou sur la start-up, ainsi que d'un « livre blanc » expliquant la technologie et le *business plan* pour les ICO. Le développement d'une relation de dépendance voire d'une addiction aux produits de *trading* est facilité par de multiples offres commerciales plus séduisantes les unes que les autres. Outre les taux et les politiques commerciales, les interlocuteurs proposent une formation en ligne assurée par les « meilleurs *traders* du monde » avec des *live* ou encore la mise à disposition d'outils de *trading* comme des applications dédiées.

ii. Une escroquerie astucieuse fondée sur une architecture criminelle complexe et sectorisée

Les investigations permettent de mettre en lumière une architecture criminelle complexe et sectorisée, distinguant trois types d'acteurs indépendants mais réunis autour d'un projet commun, l'appât du gain : les fournisseurs de moyens, ici les producteurs de *leads*[17], puis les délinquants proprement dits, ici les dirigeants de centres d'appels, et enfin les blanchisseurs.

a) L'hameçonnage par les producteurs de *leads*

La première étape est la constitution d'un vivier de victimes. Les fournisseurs de moyens aux escrocs obtiennent des *leads* par le truchement de vrais faux sites internet, créés *ex-nihilo,* proposant des placements financiers à très fort rendement. Ces *leads* sont des fichiers clients constitués de fait par la consultation de ces sites par de potentiels clients au travers des « *landing pages*[18] » ainsi que les encarts publicitaires sur différents supports offerts par l'internet. Cela s'appuie sur les fondamentaux du marketing d'affiliation. Cette branche de la publicité en ligne consiste en la création d'un site internet principal conduisant l'internaute vers un deuxième site de ventes en échange d'une commission ou de participation aux bénéfices. Ce site principal a pour fonction essentielle d'hameçonner, c'est-à-dire d'attirer une clientèle captive par le biais de toutes sortes d'encarts publicitaires dédiés à des biens ou services les plus divers (biens de consommation, vêtements, livres, rencontres en ligne…). Les concepteurs ont recours aux meilleurs techniques de marketing pour augmenter en permanence le meilleur référencement sur les moteurs de recherches. Cette industrie du marketing d'affiliation crée un environnement de nouvelles trompeuses autour de produits d'appel. Ainsi, un investisseur de bonne foi cherchant, par exemple, les mots « options binaires » sur Google trouve nombre de sites internet créés, chantant les éloges de tels placements. Un ancien employé de ce secteur avait décrit au *Times of Israël*[19] le travail des annonceurs en affiliation : *"Généralement, ils cultivent des liens sur toute la Toile en utilisant quelque chose qu'on appelle un entonnoir. Un entonnoir est une vidéo grossière sur un site plus grossier encore, et le sujet est habituellement un ancien trader de Wall Street qui a découvert une information secrète, ou qui possède un algorithme de dingue qu'il veut faire connaître au public. Il y a toujours urgence à le faire, une offre limitée dans le temps et, bien sûr, tout est faux – de la vidéo elle-même jusqu'aux avis ».* Cette manoeuvre initiale d'hameçonnage est une phase essentielle du processus criminel et témoigne du haut degré de professionnalisme et d'organisation des structures impliquées.

Ensuite, la fiabilisation des centaines de *leads* obtenus quotidiennement sur ces sites est assurée par une équipe de vérificateurs en France ou en Israël. Ceux-ci s'assurent de l'existence réelle des identités collectées et de la véracité des coordonnées[20]. Enfin, une troisième équipe réalise des fiches clients fiabilisées et certifiées qui sont, ensuite, vendus à des centres d'appel. Le producteur de *lead* est rémunéré à la fiche client[21] en fonction du degré de confiance accordée au directeur de centre

d'appel ou par un pourcentage accordé sur le montant de l'escroquerie.

Cette phase d'hameçonnage génère un vivier regroupant de potentielles victimes qui est, ensuite, vendu à des dirigeants de centres d'appels dans une logique purement commerciale.

b) Le démarchage des centres d'appel

La deuxième étape réside dans le démarchage des clients victimes et la souscription de contrats bidon. Des centres d'appel[22], répartis principalement en Israël pour les victimes francophones, démarchent avec une grande force de conviction des clients identifiés dans les *leads* dans le but de leur faire souscrire des contrats de placement de leur patrimoine. Il est constaté :

- Une philosophie d'uberisation et de viralisation du trading

Le salarié du centre d'appel est l'interlocuteur exclusif du client, réuni par une relation professionnelle de confiance. Le processus de souscription est graduel. Un premier placement d'une somme comprise entre 1 000 et 5 000 euros démontre à l'investisseur le sérieux et la rentabilité de l'opération au vu des gains affichés. Puis, s'ensuivent des placements de plus en plus importants ainsi que le recrutement d'autres membres de la famille et de l'entourage du client victime. Cette première rentabilité positive entretient la confiance et suscite une adhésion virale des membres de la famille ou de son milieu professionnel. Les escrocs affichent un haut degré de maîtrise des techniques du *marketing* de réseau (*multi level marketing* -MLM) : plus l'investisseur convainc ses proches d'adhérer à ces contrats de placement, plus il est susceptible d'en tirer des avantages (rémunération en crypto-actifs, attribution de *token*, abonnement gratuit à des formations de *trading* ...).

- Des scénarios rodés de perte progressive de contrôle du patrimoine investi

Enfin, le capital immobilisé sur des périodes de plusieurs mois échappent progressivement à la main de son propriétaire qui ne dispose, alors, d'aucun interlocuteur accessible. Un scénario établi à l'avance évoque, par exemple, des difficultés administratives fictives ou des spéculations ponctuellement défavorables. L'engagement de nouveaux fonds est proposé comme l'unique solution pour débloquer cette situation. Les services d'un pseudo avocat, attaché à cette officine criminelle, sont fortement conseillés moyennant une forte contrepartie financière. Les épisodes s'enchaînent jusqu'à ce que l'investisseur admette qu'il a bien été victime d'une escroquerie et que ses propres fonds ont bel et bien définitivement disparu.

Ruiné financièrement en ayant emporté avec lui ses proches et son réseau amical et professionnel, la victime est aussi psychologiquement détruit. Comment admettre *à posteriori* que l'on a été abusé par un mirage financier de cette nature sur des périodes de plusieurs mois ? Comment concevoir que nombre de projets d'avenir sont irrémédiablement évanouis ? Ce fléau affecte l'ensemble des catégories socio-professionnelles, du modeste épargnant retraité au directeur d'entreprises, de l'agriculteur au professeur d'économie, des salariés aux dirigeants.

c) Le blanchiment du produit de l'escroquerie

Le blanchiment du produit de l'escroquerie est facilité par un système bancaire parallèle.

Les capitaux ainsi récoltés transitent sur des comptes de sociétés factices établies en France comme à l'étranger puis sont rapidement pulvérisés sur différents comptes rendant impossible la traçabilité des flux. Une chambre de compensation occulte permet au directeur du *call center* de reconstituer le patrimoine escroqué et/ou d'investir à l'étranger.

L'agilité criminelle offre des perspectives infinies d'escroqueries. En effet, les produits de placement au coeur de ces escroqueries évoluent au gré des respirations du marché et de l'inventivité sans borne des organisations criminelles. Après les diamants, les Forex, émergent d'autres crypto-actifs voire des supports autour du vin, cet or rouge, voire même, actuellement, les vaches laitières. L'imagination est débordante comme en témoigne le boom des ICO frauduleuses pour plus du quart tel qu'évalué dans un article récent du MIT[23]. Le cas de *Bitconnect* est révélateur d'un système d'escroquerie type pyramide de Ponzi fondée sur un attrait irrésistible pour les crypto-actifs, une campagne de communication animée par des influenceurs et un système de parrainage et d'affiliation. Ainsi, le 28 décembre 2017, un BCC, symbole boursier de *BitConnect*, s'échange contre 477 dollars et la capitalisation boursière s'envole à 3 milliards de dollars. Mais, le 17 janvier tout s'effondre : le site ferme brutalement ses portes et des milliers d'investisseurs perdent leurs avoirs. La pyramide s'est effondrée d'elle-même quand des investisseurs trop nombreux ont réclamé leur dû en même temps alors que le cours des

crypto-actifs était à la baisse.

Au total, les crypto-actifs constituent une aubaine pour les industries, notamment *high-tech* ou les *start-up* en favorisant et élargissant les rentrées d'argent. De fait, tout est mis en oeuvre pour encourager les investisseurs à acheter et à vendre des crypto-devises sur leur « marché », qui, pour une bonne proportion d'entre eux, ne recouvrent aucune réalité concrète.

B. Instrument d'acquisition et de transfert de fonds illicites, de blanchiment de capitaux et de financement du terrorisme[24]

Certaines monnaies virtuelles sont convertibles entre elles ou avec des monnaies fiduciaires (euros, dollars, roubles…) via des plates-formes de change *crypto to fiat* telles que Kraken, Bitfinex, Bitstamp ou *crypto-to-crypto* telles que Poloniex, Shapeshift, Changelly… À la croisée des chemins entre le système financier de change de monnaies fiduciaires et celui propre aux crypto-actifs, ces plates-formes ne sont ni régulées ni même harmonisées au plan international. De fait, elles ouvrent des perspectives insoupçonnées aux organisations criminelles qui voient levés nombre d'obstacles ou de fragilités propres à leurs opérations financières. D'autant plus que la *blockchain* offre une rapidité d'exécution des transactions quelque soit le montant par rapport aux réseaux interbancaires.

i. Des plates-formes de change, tiers de confiance pour des opérateurs criminels

Même si la majorité des plates-formes de change de crypto-actifs s'efforcent de se conformer aux exigences de confiance et de suivi des transactions, certaines se montrent réceptives aux besoins d'anonymat fortement réclamés par des acteurs illicites.

Ainsi, l'opération *Avaricious*[25] menée par les autorités américaines a ciblé un Russe, cerveau du site BTC-e, l'une des plus dynamiques plates-formes de change entre crypto-actifs et monnaies fiduciaires. Arrêté en Grèce en juillet 2017, il lui est reproché d'opérer sur un site de change facilitant des transactions fruits de *ramsomware*[26], d'usurpation d'identité ou de trafics de produits illicites. Ce site permet des transactions anonymes, exigeant seulement un *username,* un mot de passe et une adresse *mel*. Plus grave encore, il délivrerait des conseils pour dissimuler ces flux.

ii. Cyber money mules ou passeur de fonds illicites

À l'image des mules en matière de trafics de produits stupéfiants, les organisations criminelles recherchent des agents financiers dont ils emploient leur compte bancaire pour transférer de l'argent sale. Ciblant des chômeurs ou des personnes en situation de précarité, elles proposent de véritables offres d'emploi faisant miroiter d'importantes commissions, pour une faible charge de travail et une exigence de formation préalable réduite.

Ceux-ci reçoivent, alors, des capitaux illicites sur leurs propres comptes bancaires. Une fois les fonds retirés, ils les envoient à l'étranger soit par la poste (lettre/colis) soit via un service de transfert d'argent type Western Union ou, encore, désormais, via une plate-forme de change en crypto-actifs. En contrepartie de leurs services, les « passeurs » perçoivent une commission.

Dans ce cadre particulier, la *blockchai*n contribue à la phase du placement des opérations de blanchiment d'avoirs criminels grâce à l'anonymisation et à la traçabilité des transactions.

iii. Transfert de fonds à l'échelle mondiale

Les crypto-actifs constituent des instruments a*d hoc* facilitant le transfert de fonds d'un pays à un autre par des opérations de compensation tout en compliquant la détection des flux illicites. L'opération *Tulipan blanca*[27] conduite, en avril 2018, par la Garde civile espagnole avec le soutien d'Europol, de la police finnoise et du *Homeland Security Investigations* américain illustre les modes opératoires employés par des organisations criminelles exploitant les mérites de la *blockchain*.

Conscient des fragilités présentées par des dispositifs de placement de fonds illicites sur de multiples comptes bancaires, cette organisation criminelle espagnole, spécialisée dans le trafic de produits stupéfiants avec les cartels colombiens, convertit ses avoirs en crypto-actifs via une plate forme de change basée en Finlande. Ainsi, le jour même, pour éviter toute fluctuation des cours, les trafiquants colombiens prennent possession du montant exact de la transaction illicite en accédant aux *wallets* constitués par les espagnols lors de l'achat de *bitcoins* et stockés sur la *blockchain*. La transmission de la clé privée débloque, alors, les fonds qui peuvent être intégrés dans le système financier légal ou employés comme tels en *bitcoins*[28] ou convertis encore en d'autres crypto-actifs encore plus intraçables[29] via des plates-formes *crypto to crypto*.

C. Diffusion de contenus illicites d'infos cryptées

Certes, la fonction première du *bitcoin* ou d'autres crypto-actifs est

bien la transmission d'informations de nature financière débouchant sur la création d'actifs. Néanmoins, ce support permet, malgré lui, la diffusion d'autres contenus numériques non liés aux transactions. Ces perspectives de détournement de la finalité de cette invention méritent véritablement d'être appréhendées même si la maturité technologique des *blockchain* n'est pas pleine et entière.

De telles possibilités ont été mises en exergue, en mars 2018, par des travaux de recherche[30] menées par l'Université allemande d'Aix-la-Chapelle. Chargés de l'analyse des données non financières insérées au sein de la *blockchain* du *Bitcoin Cash*, quatre scientifiques ont découvert des liens conduisant vers des sites pédopornographiques. 274 liens ont été identifiés au cours de leur étude dont 142 menant au *darkweb*. Au final, ils estiment que 1.4 % des transactions consignées possèdent des contenus non-financiers soit 118.5 Mo. Au delà de tels contenus répréhensibles, d'autres données sont susceptibles d'être diffusées par ce protocole : données à caractère personnel, politique ou terroriste, violations de la propriété intellectuelle, virus informatiques, divulgation de secrets industriels ou d'État…

Même si les capacités de stockage s'avèrent pour l'heure très réduite, cette découverte pose de nombreuses questions juridiques liées, par exemple, à la responsabilité des mineurs validant les blocs et, donc, favorisant la diffusion de ces données à travers ce réseau visible par tous. De plus, comment identifier l'auteur de l'insertion de données illicites alors que le protocole se fonde sur une anonymisation des transactions ? Comment qualifier pénalement ceux qui valident ces transactions condamnables ? Et ceux qui les consultent ? Comment supprimer préventivement, voire définitivement, de tels contenus alors qu'ils sont réputés être immutables par construction ?

Pour mieux appréhender ces perspectives d'avenir, il convient de comprendre précisément les mécanismes d'insertion de données non financières au sein de la *blockchain*. Cela est rendu numériquement possible soit par de courts messages via l'encodage de données arbitraires soit par des fichiers complets, codés comme des transactions classiques. Pour ce faire, distinguons[31] les méthodes d'insertion de données des services d'insertion de contenus.

L'insertion de données est permise soit par la fonction dénommée *OP_RETURN* soit par *Coinbase.* La fonction *OP_RETURN* tolère l'adjonction de quelques bits (80 octets maximum) d'informations non-transactionnelles dans chaque bloc. Conformément au protocole, ce contenu est validé et les noeuds téléchargent systématiquement ces informations. Par ailleurs, *Coinbase*[32] est un portefeuille de devises numériques en ligne et une plateforme d'échanges permettant d'acheter, de vendre et de stocker des crypto-actifs. Le script d'entré (*input script*) d'une longueur maximale de 100 bits contient des informations sur la position du bloc considéré dans la *blockchain*. En déclarant une longueur supérieure, il est alors possible d'intégrer des données supplémentaires dans l'intervalle ainsi créé.

D'autre part, la *blockchain* dispose de quatre services d'insertion de contenus identifiés. Ainsi, CryptoGraffiti est un service en ligne permettant d'encoder des messages texte cachés sur la *blockchain* du *Bitcoin* en utilisant une interface en ligne. Il offre une capacité de stockage de 60 KiB. Satoshi Uploader peut contenir des archives et des documents en format pdf. P2SH[33] Injectors autorise l'insertion de contenu via des *input script* P2SH. Il conserve les échanges entre mineurs comme les *chats* entre clients de *bitcoin*, des forums ou encore des e-mails. Enfin, Apertus est un service qui fragmente le contenu des transactions en ayant recours à un nombre arbitraire de script P2PKH[34] pour stocker des images.

L'étude menée par cette université d'Aix-la-Chapelle décrit la part prise par chacun de ces services en matière d'insertion de contenu dans la *blockchain*. Le volume total est estimé à 16.12 MiB. Il apparaît alors que P2SH injectors insère plus de la moitié du volume de données non financières devant Apertus et Satoshi Uploader (20%).

Toutefois, en l'état actuel des avancées technologiques, il convient de nuancer l'intérêt de la technologie *blockchain* en matière de diffusion de contenus par des organisations criminelles. En effet, par construction, la *blockchain* apporte sécurité des transactions, traçabilité, immutabilité et accessibilité à tous des données. Or, les malfaiteurs recherchent, avant tout, une couche d'anonymat rendant illisible et très difficilement interprétable les transactions, ce que proposent les *Privacy Coins* tels que Monero, Dash, Zcash… ou encore des applications disponibles sur le *darkweb*. Par ailleurs, les capacités de diffusion sont réduites en taille, ce qui militent pour le faible intérêt porté à cette fonctionnalité, et le

coût d'une transaction, le « *fee* », est fonction de la taille.

D. Les cyberattaques sur les failles du système

i. Le *cryptojacking*, le cyberbraquage

La *blockchain* s'avère un dispositif résilient aux attaques de tout type (réseau, applicative, déni de service…). Néanmoins, les cyberattaques n'épargnent guère l'architecture *blockchain* qui a déjà démontré des vulnérabilités sur les interfaces comme les plates-formes de change. L'enjeu principal de l'atteinte à un système automatisé de traitement de données s'illustre concrètement par la collecte des clés privées qui commandent l'accès aux *wallets*, les portefeuilles numériques, préalable indispensable à tous transferts vers d'autres comptes. Dès février 2014, 850 000 *bitcoins,* soit l'équivalent de 660 millions de dollars au cours du 10 décembre 2016, ont disparu de la plate-forme japonaise MtGox, l'une des plus dynamiques au monde. Selon, l'agence Reuters[35], plus du tiers de ces interfaces de l'écosystème *blockchain* ont ainsi été hackés. Ainsi, l'application *theDAO*[36]a été victime du vol massif d'*ether* pour un montant avoisinant les 50 millions de dollars soit 5 % des actifs délivrés le 17 juin 2016. Le pirate est, en effet, parvenu à sceller un *smart contract*[37]avec *theDAO* pour la fourniture d'un service quelconque.

Le *cryptojacking* consiste à l'installation d'un script, un *webminer*, sur le navigateur à l'insu du propriétaire d'un ordinateur qui permet de miner des crypto-actifs au bénéfice d'un pool de minage qui regroupe tous les autres deutilisateurs du script. Pour ce faire, il suffit de l'intégrer dans une page web et, dès qu'un internaute s'y connecte, le code puise dans les ressources de la machine pour exécuter le fameux calcul de preuve cryptographique. Ainsi, *CoinHive Javascript* permet de miner des *moneros*, *CoinHive* récupérant une commission de 30 % à chaque *monero* créé. Ce dispositif de *web miner* permet aux propriétaires des sites internet de gagner de l'argent en utilisant les navigateurs internet des visiteurs, souvent à leur insu. D'autres applications illicites s'ouvrent pour les sites de streaming illégaux ou, encore, dans le cadre de cyberattaques. Ce phénomène récent de *cryptojacking* s'annonce comme une menace majeure qui est susceptible d'infecter, par exemple, les SCADA[38] au coeur des systèmes d'automatisation industrielle.

ii. Le crypto-actif, monnaie d'échange dans les *ramsomware*

En complément, il convient aussi d'évoquer les crypto-actifs comme moyens de paiement le plus usité dans le cadre des *ransomware* (*Cerber, Cryptolocker, CTB-Locker…*) et autres opérations de rançonnement de victimes, d'extorsion ou de chantage. Le volume de ces cyberattaques est difficilement évalué mais son impact socio-économique devient majeur : en 2017 les pertes globales ont été chiffré[39] à plus de 5 billions de dollars. La tendance actuelle désigne les crypto-actifs comme vecteur de paiement des rançons comme pour *NotPeyta* au printemps 2017. Le libre accès aux données personnelles ou celles de l'organisation est rendu possible contre le paiement d'une rançon en crypto-actifs.

En conclusion, la *blockchain* s'impose, dorénavant, comme un réseau de consensus crypto-économique, source de confiance, d'autonomie organisationnelle et de pérennité économique. Ainsi, les crypto-actifs qu'elle génère constituent à la fois des unités de compte, des réserves de valeurs et des moyens d'échange d'informations qu'elles soient financières ou de tout autre nature. De nouvelles applications dérivées de la *blockchain* sont mises au point quotidiennement qui modifient assurément notre vie de consommateur, de salarié ou même de citoyen. Cette invention disruptive affecte, aussi, le fonctionnement même de l'appareil d'État et de sa sûreté.

Comme toute innovation positive pour l'humanité, la *blockchain* peut être naturellement détournée dans son usage par des organisations criminelles en recherche permanente de solutions rapides, anonymes, résilientes et sécurisées. Cette architecture autonome et transnationale répond parfaitement à ces besoins d'autant plus qu'elles bénéficient encore d'un temps d'avance.

Par construction, cette solution maillée d'échanges numériques constitue à la fois un vecteur et un théâtre d'opération criminelle.

En recourant à cette technologie agile, les organisations criminelles internationales peuvent, ainsi, davantage, dissimuler leurs opérations financières de placement ou de compensation d'avoirs illicites. Ce processus sécurisé accélère les transactions transnationales en même temps qu'il génère de la confiance entre opérateurs criminels et facilite l'insertion de cet argent sale dans l'économie réelle. Par ailleurs, la *blockchain* est l'un des acteurs du cyberespace, objet de convoitise et

source de cyber-conflictualité entre organisations criminelles. Au coeur de ces menaces émergent les enjeux fondamentaux de la protection des données personnelles et de la définition de l'identité des acteurs dans le cadre d'une architecture publique et anonyme, fondée sur des processus traçables et immutables. Dans ce contexte, il s'agit moins de promouvoir un droit à l'oubli qu'un droit à contrôler ce qu'il advient de la donnée intégrée dans cette chaîne de blocs.

En conséquence, la technologie *blockchain* s'inscrit durablement dans les enjeux de sécurité et d'ordre public socio-économique. Elle commande, de fait, le développement rapide de stratégies judiciaires face aux mésusages de ces chaînes, s'intégrant, naturellement, dans les mécanismes de coopération policière internationale et de l'entraide judiciaire internationale. Cela implique un investissement majeur en matière de formation des personnels à qui il faut inculquer de nouveaux réflexes pour appréhender cette dimension technologique dans la lutte contre la criminalité organisée transnationale. Cela suppose aussi le développement de capacités adaptées d'investigations dans une logique partenariale, associant les services régaliens (sécurité, autorités de régulation, opérateurs financiers et bancaires,...) et les acteurs de la *blockchain*.

Notes :

1. Lancé dans les années 1980 par le programmeur américain Richard STALLMAN (1953-) avec la fondation pour le logiciel libre ou FSF (FreeSoftware Foundation). Il se rend célèbre par la création d'un système d'exploitation libre appelé GNU ou GNU's Not Unix (« GNU n'est pas UNIX »).
2. Cyberpunk, association de cyber et de punk, est un genre de science fiction dystopique dépeignant une société imaginaire basée sur les technologies de l'information très avancées de telle façon qu'elle empêche ses membres d'atteindre le bonheur.
3. À l'image de Julien Assange, fondateur de wikileaks, de Tim C.May, ingénieur chez Intel auteur d'un Manifeste crypto-anarchiste publiée en 1992, de Wei Dai, créateur de B-monnaie, d'Adam Back, créateur du hashcash qui valide des transactions par des hash cryptographiques appelés preuve de travail (Proof of work), de Phil Zimmerman, créateur du logiciel de chiffrement PGP (pretty good privacy) ou encore de Nick Szabo, créateur du Bit gold.
4. Derrière ce pseudonyme se cache probablement le collectif des fondateurs du Bitcoin et de la première blockchain.
5. Dans un tel réseau, chaque internaute peut être serveur ou receveur d'un autre.
6. Cité par le Rapport de l'office parlementaire d'évaluation des choix technologiques sur les enjeux technologiques des blockchains (chaîne de bloc) enregistré le 20 juin 2018 à l'Assemblée nationale et au Sénat. Disponible sur : http://www2.assemblee-nationale.fr/documents/notice/15/rap-off/i1092/(index)/rapports
7. Cette clé privée est, en fait, une suite aléatoire de chiffres qui permet de signer une transaction et de la chiffrer. Elle permet, alors, à son émetteur de prouver sa propriété.
8. Le hachage permet de convertir n'importe quel ensemble de données numériques en un hash, soit une courte suite binaire obtenue à la suite d'un calcul itératif et aléatoire. Ces très grands nombres de calculs complexes nécessitent des équipements informatiques de plus en plus puissants. On assiste, de fait, à une concentration des mineurs au sein de véritables usines de calculs appelées ferme de minage pour optimiser les rendements et, donc, la rémunération des acteurs.
9. La validation est une compétition cryptographique qui suppose la réussite d'un opérateur appelé « mineur » à une épreuve cryptographique ou preuve de travail (proof of work) baptisée « minage » (en référence à la découverte de l'or). La création de blocs provoque, alors, l'émission de nouveaux bitcoins qui récompensent le mineur. À titre d'exemple, la validation d'un bloc sur Ethereum nécessite 15 secondes tandis que celle d'un bitcoin 10 minutes.
10. Environ 215 satoshi/ Byte selon le cours d'août 2017 par exemple (1 satoshi= 10-8 bitcoin).
11. Comme des Paper Wallet délivré via bitaddress.org par exemple.
12. Récemment le GAFI a officiellement désigné les crypto-monnaies comme étant des « virtual asset » défini comme: A virtual asset is a digital representation of value that can be digitally traded, or transferred, and used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets which are already covered elsewhere in the FATF Recommendations.
13. Le Luxembourg régule plusieurs échangeurs depuis avril 2016, notamment BITSTAMP qui est reconnu en tant qu'établissement de paiement régulé au niveau européen.
14. Ou DomRaider Token échangeable avec d'autres crypto-actifs en qualité de moyens de paiement.
15. Cité par le Times of Israël consulté le 27/01/2018. Accessible sur https://fr.timesofisrael.com/c-que-lese-escrocs-aux-bitcoins-vous-diront-au-telephone-pour-vous-tromper/
16. Site Imarkets IML consulté le 30/11/2018 sur le lien suivant http://imltradingsuccess.com/imlts/imarketslive-presentation-france-avis/
17. Le lead est un fichier client comportant des informations comme nom, prénom, téléphone, adresse mel, ...
18. Redirection vers sites miroirs.
19. Voir Times of Israël, consulté le 30/12/2018, disponible sur https://fr.timesofisrael.com/des-ex-vendeurs-en-options-binaires-se-tournent-vers-les-crypto-devises/
20. Par des recherches en source ouverte, contre-appel, etc.
21. Entre 15 et 50 euros la fiche client.
22. Utilisant des cartes téléphoniques prépayées dépaysant l'appel téléphonique et à durée limitée en fonction de la tournure que prend la relation client.
23. C.Catalini, J.Boslego et K.Zhang, « Technological opportunity, bubbles and innovation : the dynamics of initial coin offerings », MIT working papers.
24. Cf TRACFIN (Traitement du Renseignement et d'Actions contre les Circuits Financiers Clandestins) – rapport annuel « Tendances et analyse des risques de blanchiment de capitaux et de financement du terrorisme en 2017-2018.
25. Cité par « Virtual currencies money laundering typologies », publié le 31/12/2017 par l'agence Europol. Non classifié.
26. Ce site est suspecté d'avoir blanchi plus de 100 000 bitcoins volés à la plus importante plate-forme d'échange en crypto-actifs, Mt.gox, en 2014. Cf https://www.fincen.gov/news/news-releases/fincen-fines-btc-e-virtual-currency-exchange-110-million-facilitating-ransomware
27. https://www.google.com/search?client=ubuntu&channel=fs&q=Tulipan+blanca&ie=utf-8&oe=utf-8

28. Cette possibilité ouvre les perspectives d'hybridation entre les services traditionnels de paiement en monnaie fiduciaire et en crypto-actifs. Les cartes dites « BTC2plastic » permettent des paiements de transactions courantes en monnaie fiduciaire adossée à un portefeuille en crypto-actifs. Elles sont commercialisées par des sociétés spécialisées et s'appuient sur des établissements de paiement ou de monnaies virtuelles pour assurer les flux de paiement et contraintes réglementaires. Ce risque de blanchiment du quotidien a été dénoncé par Tracfin dans le rapport « Tendances et analyses des risques 2016 », p58-59.

29. Comme monero, zcash, dash ou pivx qui ont cours, notamment, sur le darkweb.

30. Cf. Matzutt et Hiller « A quantitative analysis of the impact of arbitrary blockchain content on bitcoin », Financial Cryptography and Data Security International Conference , 2018, http://fc18.ifca.ai/preproceedings/6.pdf?utm_source=JeromeVosgienFR&utm_medium=SophosFranceLink

31. Pour une recension récente des méthodes d' insertion de données arbitraires dans la blockchain du bitcoin, A.Sward, I.Vecna et F.Stonedahl, « Data Insertion in Bitcoin's Blockchain », 2018, dans le Ledger Journal, https://ledgerjournal.org/ojs/index.php/ledger/article/view/101/93

32. Fondée en juin 2012 par Brian Amstrong et Fred Ehrsam. Ils lancent en même temps des services d'achat et de vente de bitcoin sur internet par virement bancaire. En août 2018, CoinBase compte plus de 20 millions d'utilisateurs.

33. P2SH:Pay to Script Hash c'est à dire le recours à un script plutôt qu'à une clé dans le cadre d'un paiement par de multiples signatures (P2MS : pay to multi signature).

34. P2PKH : pay to public-key hash.

35. Gertrude Chavez-Dreyfuss, « Cyber Threat Grows for Bitcoin Exchanges », Reuters, 29 août 2016.

36. Ou Decentralized Autonomous Organization. Ce projet développé en 2016 par la start-up blockchain Slock.it est une organisation décentralisée dont les règles de gouvernance sont automatisées et inscrites de façon immuable et transparente dans une blockchain. Ouverte à tous, dans une transparence totale, s'appuyant sur aucune juridiction ou entité, les transactions sont uniquement soumises à un code. Pour fonctionner elle a recours à des smarts contracts. Stéphan Tual cocréateur du projet TheDAO décrit : « c'est une forme d'organisation incorruptible qui appartient aux personnes qui ont aidé à la créer et à la financer, et dont les règles sont publiques. Il n'y a donc pas besoin de faire confiance à qui que ce soit, car tout est dans le code, auditable par chacun ». Cité dans: https://blockchainfrance.net/2016/05/12/qu-est-ce-qu-une-dao/ consulté le 12/12/2018.

37. Un smart contract est un programme autonome qui exécute automatiquement un contrat dès lors que les conditions définies à l'avance sont remplies. Il peut s'agir de dépôt de proposition, de vote, de paiement ou de nomination.

38. Cision, Radiflow reveals first documented cryptocurrency malware attack on a SCADA network, https://www.prnewswire.com/news-releases/radiflow-reveals-first-documented-cryptocurrency-malware-attack-on-a-scada-network-300595714.htm, 2018.

39. Morgan, S., Global ransomware damage costs predicted to hit $11.5 billion by 2019, https://cybersecurityventures.com/ransomware-damage-report-2017-part-2/ , 2017.

OUVRAGES RÉCENTS

BLOCKCHAIN ET CRYPTOMONNAIES

AUTEUR : PRIMAVERA DE FILIPPI

ÉDITEUR : QUE SAIS-JE ?

Présentation de l'éditeur

« La blockchain ? Une révolution équivalente à l'invention d'Internet ! C'est du moins ce qu'on en dit parfois. Mais quelles sont les répercussions réelles de cette technologie sur nos modes de vie ?

Si Bitcoin nous permet d'échanger de la valeur de façon décentralisée et sécurisée, les nouvelles applications de la blockchain s'étendent sur des champs bien plus larges. Certaines de ces applications permettent de certifier et d'authentifier des documents, sans qu'il y ait besoin de recourir

aux services d'un notaire. D'autres permettent d'automatiser des transactions, ou même de se coordonner sans passer par une quelconque autorité de confiance. Telle est la promesse de la blockchain : désintermédier en passant d'un système fondé sur la confiance à un système fondé sur la preuve.

Primavera De Filippi décrit le fonctionnement de la blockchain, dont elle est l'une des meilleures spécialistes mondiales. Donnant un aperçu des applications en cours de développement, elle n'examine rien de moins que les implications politiques et sociales de cette nouvelle technologie qui n'a pas fini de faire parler d'elle. »

LES ENJEUX DE LA DÉLINQUANCE FISCALE GLOBALISÉE

ÉRIC VERNIER

MAÎTRE DE CONFÉRENCES HABILITÉ À DIRIGER DES RECHERCHES – ULCO, DIRECTEUR DE LA CHAIRE COMMERCE, ECHANGES & RISQUES INTERNATIONAUX – ISCID-CO, CHERCHEUR ASSOCIÉ – IRIS

La fraude fiscale et les paradis fiscaux représentent les deux visages obscurs d'un même champ social, économique, juridique, scientifique, mais aussi polémique : la fiscalité. Plus vieux que la monnaie, l'impôt a toujours suscité le débat : trop élevé pour les uns, ceux qui le payent, insuffisamment levé pour les autres, ceux qui le perçoivent. L'État quel que soit son régime a joué sur ce levier pour développer le pays, inciter tel ou tel comportement social et économique, attirer les grâces de certains, en punir d'autres…

Dans une pièce de théâtre de 2008, *Le diable rouge*, Antoine Rault fait dire à Mazarin s'adressant à Colbert : « *Il y a quantité de gens qui sont entre les deux, ni pauvres ni riches, rêvant d'être riches et redoutant d'être pauvres. C'est ceux-là que nous devons taxer, toujours plus. Plus tu leur prends, plus ils travaillent pour compenser… C'est un réservoir inépuisable.* » Oeuvre de fiction, ces paroles ne manquent pourtant pas de résonner étrangement aujourd'hui avec notamment la « révolte » des Gilets jaunes d'une part, la transformation de l'impôt sur la fortune en impôt sur la fortune immobilière d'autre part.

Parallèlement aux stratégies des gouvernements successifs pour équilibrer les comptes publics et en partie redistribuer les richesses, les contribuables et les entreprises ont en permanence essayé de contourner l'impôt, ou tout du moins de le réduire, par des moyens plus ou moins légaux. Du retraité isolé à la multinationale aidée d'une armada de fiscalistes internationaux, nombreux sont ceux qui recherchent l'économie d'impôt, parfois à tout prix et quel qu'en soit le risque encouru. Certains justifient ce comportement en arguant d'un matraquage fiscal qui les amène à compenser l'excès par la fraude. D'autres restent dans les limites de la loi, en équilibre entre optimisation et évasion fiscales. Sans vouloir stigmatiser les petits arrangements de quelques artisans ou commerçants, les « omissions » des particuliers employant une femme de ménage ou un jardinier non déclaré, les jeunes journalistes pigeant discrètement, il convient de rappeler les enjeux de la fraude fiscale en la reliant aux territoires opaques protégeant les pires opérations criminelles.

Ces fameux paradis fiscaux ne sont pas une création récente. Le concept est né voici déjà 4 000 ans lorsque les commerçants grecs envoyaient des émissaires dans les ports les plus taxés pour convenir entre vendeurs et acheteurs d'un point de rendez-vous pour transborder la marchandise sans avoir à payer les taxes portuaires existantes. On comprend ici tout le sens du terme « *offshore* ». Mais c'est à la fin du 19ème siècle que la version moderne apparaît, notamment avec l'État du New Jersey aux États-Unis qui propose le plafonnement de l'impôt sur les sociétés pour les entreprises qui y enregistrent leur siège social. Dans les années 1920, le phénomène prend de l'ampleur et s'étend aux Bahamas, à la Suisse ou encore au Luxembourg.

Il est nécessaire afin de comprendre ce phénomène, de rappeler quelques définitions et concepts. Car tant en ce qui concerne la fraude fiscale que les paradis fiscaux, de quoi parle-t-on exactement ? Nous pourrons alors mesurer pleinement les conséquences délétères, parfois terribles pour nos sociétés, de l'existence de ces territoires et de ces pratiques. Heureusement, des mesures ont été mises en place avec une véritable accélération ces dernières années, mais elles s'avèrent encore souvent insuffisantes.

I. Fraude fiscale et paradis fiscaux, de quoi parle-t-on ?

Lorsque le sujet de la fraude fiscale est abordé, il convient nécessairement de préciser au préalable le sens des différents termes de ce champ sémantique. En effet, plusieurs expressions sont employées, parfois à tort. Nous pouvons retenir trois notions principales complétées par deux autres plus marginales : fraude, évasion, optimisation, exil et expatriation.

A. De la fraude à l'optimisation

En ce qui concerne **la fraude fiscale**, aucun doute ne peut planer sur ce qu'elle représente. Le fraudeur essaie de diminuer l'impôt par des pratiques illégales que tout juriste pourra circonscrire. La fraude recouvre notamment tous les actes visant à dissimuler des revenus ou des éléments de patrimoine taxés, quels qu'ils soient. La présence de l'élément intentionnel différencie la fraude de l'évasion.

L'évasion fiscale présente un caractère plus complexe, car elle se situe entre la fraude et l'optimisation. Dans la pratique, c'est donc le juge ou l'exégète qui aura un rôle central dans la qualification des faits. S'il est démontré que ces derniers relèvent d'un abus de droit, une sanction pourra être prononcée. En revanche, s'il est estimé que le contribuable a oeuvré en toute bonne foi en usant dans des conditions normales d'incitations et de prérogatives fiscales prévues par la loi, nous nous retrouvons dans le cadre de l'optimisation fiscale, totalement légale.

L'optimisation procède en effet d'une recherche de réduction des coûts fiscaux en utilisant les niches fiscales ou les montages permettant d'amoindrir les taxes, en respectant l'ensemble des règles et sans en abuser, ni les détourner. La difficulté provient bien de la qualification et de cette notion d'abus. Une expression est alors apparue pour décrire les pratiques jugées non pas illégales mais amorales ou immorales, en tout état de cause considérées comme contraires à l'éthique : la planification fiscale agressive. La confusion est donc de mise, et pas seulement dans l'esprit des béotiens. Le scandale mondial des *Paradise Papers*, sur lequel nous reviendrons, a mis au jour cette pratique décriée engendrant quelques velléités gouvernementales à y mettre fin et à taxer par exemple les fameux GAFAM (Google, Apple, Facebook, Amazon, Microsoft). Mais nous en sommes encore loin.

À ces trois niveaux nous ajouterons **l'exil et l'expatriation**. L'exil fiscal consiste à quitter le pays uniquement pour des raisons fiscales mais sans abandonner son activité sur le territoire d'origine. L'expatriation fiscale amène à plier bagages et à s'installer dans un pays où l'impôt paraît plus doux et y exercer son métier. Le second est donc plus radical et souvent plus réel. L'exil est en effet souvent simulé avec parfois juste les enfants inscrits dans les écoles du pays d'adoption pour justifier de sa résidence. Évidemment, le choix du pays d'accueil n'est pas aléatoire et porte essentiellement sur ce que l'on nomme des paradis fiscaux.

B. La douceur des paradis fiscaux

Nous le disions en introduction, le paradis fiscal n'est pas une nouveauté. Depuis des millénaires, l'être humain cherche à payer moins d'impôt qu'il n'y est obligé, *a fortiori* l'entreprise qui y voit la possibilité d'améliorer sa rentabilité par le levier fiscal. Dans les années 1880, c'est l'État du New Jersey qui le premier, aux États-Unis, propose le plafonnement de l'impôt sur les sociétés pour les entreprises qui y installent leur siège social. Une quarantaine d'années plus tard, le phénomène s'étend au monde entier avec des territoires tels que la Suisse ou le Luxembourg et à d'autres cibles comme les riches (oserais-je dire ultra-riches ?) particuliers qui souhaitaient alléger l'impôt pesant sur leur patrimoine. Les Britanniques inventent alors le concept de résidence fictive, l'entreprise oeuvrant en dehors du lieu où elle est fiscalement enregistrée. Les Suisses créent le secret bancaire

et les sociétés écrans, suite à la célèbre affaire Albertin[1]. Après la Seconde Guerre mondiale, certains petits États oubliés par le Plan Marshall se spécialisent dans les pavillons de complaisance et le secret bancaire. Les euromarchés et les pétrodollars accentuent la tendance dans les années 1960. La première moitié du 20ème siècle a vu ainsi l'apparition d'entreprises dont le siège se situe dans un pays, qui produisent dans un autre, ouvrent leurs comptes bancaires ailleurs, une filiale de commercialisation un peu plus loin et qui payent leurs impôts encore ailleurs.

C. La religion financière et ses trois paradis

Aujourd'hui, les paradis fiscaux sont à leur apogée et n'ont jamais abrité autant d'avoirs cachés, d'argent sale et de produits du *shadow banking*. Ils attirent aussi bien les multinationales qui minimisent ainsi leur impôt, les États à la recherche de discrétion pour certaines transactions comme les commissions sur les ventes d'armes, les dirigeants politiques cherchant à cacher l'argent de la spoliation et la corruption, les particuliers aisés et les criminels dans les opérations de blanchiment. En fait, le paradis fiscal n'est pas que fiscal mais aussi bancaire et judiciaire. C'est un paradis fiscal *stricto-sensu* lorsque l'impôt est faible voire nul. Rappelons cependant que ces avantages n'existent le plus souvent que pour les non-résidents, les résidents payant souvent un impôt élevé qui compense les largesses précitées. C'est un paradis bancaire lorsque l'opacité sur les comptes est totale ou quasiment. C'est un paradis judiciaire et réglementaire car la coopération internationale en la matière est inexistante ou faible.

Ces territoires sont désormais au coeur du système. Ce n'est pas un épiphénomène comme il l'était communément admis. Le sous-titre de la seconde édition de mon ouvrage sur les paradis fiscaux rappelle cette réalité : « Quand l'exception devient la règle[2]». Les scandales successifs ont démontré les faits. Les montages de sociétés écrans révélés dans les *Panama Papers* concernaient aussi bien de riches citoyens français ou américains que des barons de la drogue colombiens. Les *Paradise Papers* impliquaient les multinationales et les milliardaires du sport ou du show-business ; les *Football Leaks*, le monde du foot ; l'affaire du cabinet Seti en Bretagne, les artisans et commerçants ; la carte parabancaire AirBnB, les bailleurs saisonniers. Et lorsque l'on s'intéresse aux questions de blanchiment et de financement du terrorisme, les mêmes territoires apparaissent à nouveau dans les circuits.

Ainsi, les conséquences sur la société sont évidemment nombreuses et importantes, tant sur le plan économique que politique et social.

II. Les conséquences économiques, politiques et sociales

L'existence des paradis fiscaux et de la fraude met en péril les équilibres économiques et leur éradication permettrait de résoudre en grande partie les difficultés budgétaires des États.

A. Une perte sèche pour les États

La conséquence la plus proche de nous émane de la fraude fiscale des Français, estimée selon les études entre 80 et 100 milliards d'euros par an. Au niveau européen, nous oscillons entre 500 et 1 000 milliards d'euros. Une étude britannique très récente évalue l'évasion fiscale en Europe à 825 milliards d'euros dont 120 uniquement pour la France[3]. Évidemment ce manque à gagner pour l'État plombe les comptes et pourrait s'il était récupéré, régler tous les problèmes budgétaires du pays. Or, les soubresauts actuels sont nés de ces difficultés avec la sensation que d'un côté certains, les plus aisés, échappent à l'impôt par la fraude et les cadeaux du gouvernement, réduisant ainsi l'assiette fiscale et que de l'autre côté, la classe moyenne paie pour tout le monde au point de ne plus pouvoir s'en sortir.

Les chiffres concernant le monde sont impressionnants. Si Zucman évoque aujourd'hui 8 000 milliards de dollars cachés dans les paradis fiscaux[4], il n'intègre que les avoirs strictement financiers. Il faut donc y rajouter yachts, or, oeuvres d'art, bijoux... Certaines études et mes propres recoupements évoqueraient plutôt 15 à 30 000 milliards de dollars.

Ainsi chaque scandale, chaque révélation a conduit les Français vers soit la radicalisation idéologique, soit le rejet de la classe politique. Le consentement à l'impôt se réduit peu à peu face

à ce qui est considéré comme une contribution inéquitable de chacun avec d'un côté ceux qui paient, en général les classes moyennes salariées, de l'autre ceux qui échappent à l'impôt, les multinationales et les plus riches. Mais ce n'est peut-être pas là le pire des maux. Il faut se déplacer vers le continent africain pour mesurer toutes les conséquences de ces délits.

B. Un continent sacrifié

L'Afrique peut être présentée comme un cas d'école en matière de corrélation entre les délits financiers et les difficultés des États. Plusieurs études théoriques et empiriques ont montré que lorsque l'Afrique reçoit 100 € d'aides internationales, il y a parallèlement entre 200 et 1 000 € provenant de la corruption, des détournements, de l'optimisation et de la fraude fiscales qui sont discrètement exfiltrés vers les paradis fiscaux. Ils seront ensuite investis dans des projets immobiliers ou fonciers. Ces mauvaises habitudes dégradent évidemment l'économie régionale, rendant inutile toute velléité d'aider au développement du continent. Ce phénomène se retrouve dans de nombreux autres pays du globe. Les fameux biens mal acquis (BMA) proviennent très souvent du fruit de ces pratiques : spoliation de la population, détournements, corruption, crimes, commissions occultes.

L'Uneca, la commission économique pour l'Afrique aux Nations Unies, estime que l'évasion fiscale africaine représente 30 à 60 milliards de dollars et atterrit essentiellement au Panama, aux Îles vierges britanniques et aux Seychelles. C'est évidemment des chiffres à minima car quand on recoupe les différentes études, on aboutit à des montants plus élevés. Par exemple, la fraude et l'évasion fiscales au Ghana correspondent à 50 % de son budget annuel. Le Togo, l'un des pays africains les plus affectés par les flux financiers illégaux, voit s'échapper plus des 3/4 de son PIB. Les multinationales à la recherche permanente de maximisation de leurs profits engrangent 11 milliards de dollars supplémentaires grâce à l'évasion fiscale, mais aussi 38 milliards de dollars par les rescrits fiscaux (*tax ruling*) négociés avec les dirigeants des pays où elles sont implantées, moyennant souvent de généreux bakchichs ou par le chantage à l'implantation. Sans ces accords comment expliquer qu'une entreprise comme AREVA produise 30 % de son uranium au Niger et que ces approvisionnements ne représentent que 7 % du total de ses paiements. De même en Angola, un écart de 100 millions de dollars est mesuré entre les revenus du pétrole déclarés et les revenus réels.

Ce pillage des multinationales par l'évasion fiscale correspond à 65 % des sommes échappant au contrôle et donc à l'impôt en Afrique. Les activités criminelles (drogue, trafic d'armes, traite humaine...) et la corruption des fonctionnaires forment respectivement les 30 % et 5 % restant. Bien loin de la question de l'enfer fiscal décrié en Europe de l'Ouest et censé expliquer la fuite de capitaux et les petits arrangements, ce manque à gagner met en péril durablement cette région du monde, hypothéquant profondément et dangereusement l'espoir d'un développement humain, éducatif, social et sanitaire satisfaisant. Avant même de penser aux robinets de l'aide internationale, il est nécessaire et urgent de colmater les brèches par lesquelles l'argent s'échappe pour rejoindre les paradis fiscaux.

Phénomène que nous commençons à observer aujourd'hui dans les pays industrialisés, l'assiette fiscale s'avère extrêmement réduite dans les pays en voie de développement et ce depuis très longtemps. La quadrature devient alors complexe à résoudre avec des pauvres de plus en plus pauvres et non imposables, des classes moyennes qui se paupérisent, se réduisent et fraudent parfois le fisc face à l'alourdissement exagéré de leur contribution et des riches de plus en plus riches mais qui très souvent parviennent à éviter la taxation par les différents circuits et montages déjà évoqués. Les pays se retrouvent ainsi exsangues car incapables de lever un impôt suffisant auprès d'une frange contributive de plus en plus étroite. Les crises budgétaires accompagnent les crises sociales ayant pour conséquence des risques de soulèvement populaire violent. À une échelle plus globale, les impacts délétères des paradis fiscaux peuvent être surprenants.

C. Argent sale et aggravation des cataclysmes mondiaux

Pour rester sur des considérations modernes et actuelles, les

dysfonctionnements financiers mondiaux sont liés aux problématiques environnementales. Le quotidien *Reporterre* le titrait le 15 novembre 2017 : « L'évasion fiscale est une des causes du changement climatique » car l'évasion fiscale c'est autant d'argent qui ne peut être prélevé par les États et investi dans la lutte contre le réchauffement climatique. Pire, « *l'évasion fiscale est indispensable pour l'industrie fossile : les montants investis sont tellement importants que le modèle n'est rentable que par un recours massif aux subventions publiques, couplé à des mécanismes visant à échapper à l'impôt.* » Le même média, le 13 septembre 2018, indiquait que « *l'opacité financière entrave la capacité d'analyser la manière dont les flux financiers affectent les activités économiques sur le terrain et leurs impacts environnementaux.* » Ainsi, la plupart des capitaux investis dans des opérations suspectes liées à la déforestation sauvage ou à la pêche illicite par exemple, proviennent de comptes offshores.

Les effets de la fraude fiscale sont nombreux et la liste ne peut être exhaustive car bien trop longue. Mais face à cet impact terrible sur les nations et donc les populations, quelles sont les mesures mises en place ?

III. Les mesures de lutte et de régulation

Face à ces dérives et à leurs conséquences délétères, les États ont décidé de réagir peu à peu. Il y eut les premières mesures contre le blanchiment international au début des années 1990. Les textes n'ont cessé depuis de se durcir, en intégrant tout d'abord la lutte contre le financement du terrorisme après les attentats du 11 septembre 2001, puis la lutte contre le blanchiment de fraude fiscale au milieu des années 2000 avec un renforcement à la suite de la crise financière de 2007 et le souhait des États de renflouer leurs caisses. En Europe, c'est aujourd'hui six directives anti-blanchiment qui se sont succédées avec la dernière datant du 23 octobre 2018 et devant être transposée avant le 3 décem bre 2020. En France, l'affaire Cahuzac a marqué les esprits et les ministres successifs du quinquennat de François Hollande ont musclé les dispositifs anti-fraude fiscale, notamment avec la loi sur la transparence, la lutte contre la corruption et la modernisation de la vie économique, dite loi Sapin 2. Le 23 octobre 2018, une nouvelle loi pour lutter contre la fraude était votée.

A. Des mesures nombreuses

En restant sur le cas de la France, on s'aperçoit que la fraude fiscale représente autant que l'impôt sur le revenu des personnes physiques et feu l'impôt sur la fortune réunis et autant que la masse salariale de l'État. Les redressements sont passés de 12 à 18 milliards d'euros entre les années 2006 et 2012 pour ensuite se stabiliser autour de 20 milliards d'euros. Les sommes réellement recouvrées par l'administration représentent à peu près la moitié de ces montants, soit 10 milliards d'euros environ pour une perte d'une centaine de milliards d'euros par an. Le STDR[5] ou « cellule de dégrisement », mis en place en 2013 a recueilli en quatre ans, depuis sa création jusqu'à sa suppression le 31 décembre 2017, plus de 40 milliards d'euros en traitant 50 000 dossiers. Dans 9 cas sur 10, les avoirs se trouvaient en Suisse et provenaient à 70 % d'héritages. À travers le monde, différents projets ont vu le jour durant ces dix dernières années.

i. La loi FATCA

La loi FATCA[6] promulguée en 2010 aux États-Unis et dont l'accord a été signé avec la France le 14 novembre 2013, est entrée en vigueur le 1er juillet 2014. Elle prévoit que les établissements financiers étrangers ont une obligation d'information sur leurs clients imposables aux États-Unis sous peine d'un prélèvement obligatoire de 30 % à la source sur les revenus américains de ces établissements. Il semble que la soumission de l'ensemble des banques à FATCA soit partagée et les établissements, surtout suisses, vont même jusqu'à parfois faire du zèle. La puissance économique et politique des États-Unis explique cette attitude, qui s'avère très différente quand le client est ressortissant par exemple d'un pays en voie de développement.

ii. L'échange automatique d'informations

« L'échange automatique de renseignements relatifs aux comptes financiers en matière fiscale » s'est étendu parallèlement en Europe et au sein de l'OCDE à partir de l'année 2014. Il entraîne la communication automatique et systématique à

intervalles réguliers, de blocs de renseignements relatifs à diverses catégories de revenus (dividendes, intérêts…) par le pays de la source du revenu au pays de résidence du contribuable. Fin 2018, 84 juridictions ont effectivement échangé des informations dans le cadre de cette nouvelle procédure. En revanche, les États-Unis, qui ont obligé le monde entier à appliquer la loi FATCA, ont refusé de signer cet accord. Malheureusement, certains contribuables contournent déjà la mesure en achetant des nationalités de complaisance comme celle de Maltes.

iii. Le registre des bénéficiaires effectifs

Depuis le 1er août 2017, un nouveau registre, le registre des bénéficiaires effectifs, a été instauré. Le bénéficiaire effectif est défini comme la personne physique qui possède ou contrôle, directement ou indirectement, la société déclarante. En aucun cas il ne peut s'agir d'une personne morale. Le registre est déposé au greffe du tribunal de commerce et indique les personnes soit qui détiennent, directement ou pas, plus de 25 % du capital ou des droits de vote de la société ; soit qui exercent, par tout autre moyen, un pouvoir de contrôle sur les organes de gestion, d'administration ou de direction ou sur l'assemblée générale (donc qui peut nommer ou révoquer la majorité des membres des organes d'administration, de direction ou de surveillance). En cas de défaut de déclaration ou en cas de dépôt d'un document comportant des informations inexactes ou incomplètes, les sanctions sont significatives et peuvent aller jusqu'à 6 mois de prison avec des peines complémentaires pour les personnes physiques comme l'interdiction de gérer et la fermeture ou l'exclusion des marchés publics pour les personnes morales.

iv. Le projet BEPS (Base Erosion and Profit shifting)

Selon l'OCDE, l'érosion de la base d'imposition et le transfert de bénéfices (BEPS) « fait référence aux stratégies de planification fiscale qui exploitent les failles et les différences entre les règles fiscales nationales et internationales en vue de transférer artificiellement des bénéfices dans des pays ou territoires où l'entreprise n'exerce guère d'activité réelle, mais où ils sont faiblement taxés, ce qui aboutit à une charge fiscale faible voire nulle pour l'entreprise. Bien que certains dispositifs soient illégaux, la plupart ne le sont pas. Cela nuit à l'équité et à l'intégrité des systèmes fiscaux dans la mesure où les entreprises qui opèrent dans plusieurs pays peuvent utiliser les stratégies d'érosion de la base d'imposition et de transfert de bénéfices pour obtenir un avantage concurrentiel par rapport aux entreprises qui opèrent à un niveau national. En outre, les différentes affaires liées aux pratiques d'optimisations peuvent créer un sentiment d'injustice chez les contribuables et affaiblir le principe du consentement à l'impôt. » Cette mesure, lancée en 2012 par le G20, vise à amoindrir les effets des montages astucieux sur les prix de transfert visant à réduire les bases imposables par exemple. C'est en fait une réponse à la planification fiscale agressive des multinationales que l'on pourrait traduire par « optimisation excessive et délétère ».

v. Le *reporting* pays par pays

Les grandes entreprises dont le chiffre d'affaires dépasse 750 millions d'euros et possédant une filiale dans un des pays de l'Union européenne, doivent révéler le détail de leurs activités pays par pays, même en dehors de l'Union européenne. La déclaration doit indiquer de manière agrégée par pays :

- le montant du chiffre d'affaires intra et hors groupe ;
- le bénéfice avant impôts ;
- les impôts sur les bénéfices ;
- le capital social ;
- les bénéfices non distribués ;
- le nombre d'employés ;
- les actifs corporels hors trésorerie.

L'entreprise doit également indiquer la liste de toutes les entités constitutives de son groupe par juridiction fiscale. Le défaut de déclaration peut entraîner une amende de 100 000 euros (article 1729 F du CGI). Les omissions ou inexactitudes relevées dans la déclaration entraînent une amende de 15 euros par omission ou inexactitude avec un seuil de 60 euros et un plafond de 10 000 euros (article 1729 B 2° du CGI). Pour le moment, aucun consensus n'a été trouvé entre les pays de l'Union européenne, retardant la mise

en place du *reporting*. Cependant, la directive européenne DAC6 du 5 juin 2018 relative à l'échange obligatoire d'informations sur les montages fiscaux transfrontaliers à caractère « dommageable » impose aux intermédiaires (banques, experts -comptables, conseillers fiscaux...) ou aux contribuables particuliers ou professionnels de déclarer les montages fiscaux transfrontaliers à l'administration fiscale et instaure l'échange automatique de ces informations entre les États membres. Ces montages fiscaux dits dommageables peuvent notamment reposer sur l'extériorisation artificielle de pertes pour réduire le montant imposable, l'utilisation de régimes fiscaux spéciaux avantageux ou encore des arrangements avec des pays tiers qui ne respectent pas les normes internationales de bonne gouvernance.

vi. La loi contre la fraude fiscale et le crochetage du verrou de Bercy

En France, la loi contre la fraude du 23 octobre 2018[7] a prévu la mise en place d'un service spécialisé à Bercy, dit de police fiscale mais qui existe déjà sous une forme proche, alourdit les sanctions et renforce la possibilité de rendre publics les noms des fraudeurs, le fameux « *name and shame* ». Elle prévoit également une procédure de plaider-coupable et étend à la fraude fiscale la convention judiciaire d'intérêt public (CJIP), qui permet à une entreprise de payer une amende afin d'éviter des poursuites, sans reconnaissance de culpabilité.

Le plus emblématique, le verrou de Bercy, qui empêchait un magistrat de s'autosaisir d'une affaire fiscale (seul le ministère des Finances peut décider de poursuivre) a été affaibli mais n'a pas été totalement levé. Il persiste pour les affaires les moins graves, inférieures à 100 000 euros. C'est une belle avancée. Malheureusement, cette victoire des ONG et de quelques parlementaires est ternie par deux autres mesures : celle de la repentance et celle du secret des affaires. La loi du 10 août 2018 pour un État au service d'une société de confiance a en effet mis en place un droit général à l'erreur au bénéfice notamment des entreprises dans l'établissement de leurs déclarations administratives ou l'application d'une règle. Avec la possibilité pour les entreprises qui ont fraudé de se faire régulariser et la loi sur le secret des affaires, muselant notamment les journalistes et les lanceurs d'alerte, les entreprises en faute pourront continuer à frauder le fisc et à négocier avec l'État si nécessaire.

Toute la difficulté d'application de textes pourtant judicieux et souvent suffisants, apparaît nettement lorsqu'il s'agit de lutte contre la délinquance en col blanc.

B. Une effectivité des mesures toute relative

Les lois et règlements ont beau satisfaire les autorités, les politiques et la plupart des juristes, le travail sur le terrain montre malheureusement que l'effectivité des mesures demeure toute relative. Je me retrouve souvent en opposition avec les exégètes de la doctrine, car nous voyons bien depuis une dizaine d'années que le législateur durcit les textes et les sanctions prévues. Pourtant, de manière empirique, nous nous apercevons qu'il n'y a jamais eu autant de fraude fiscale dans le monde ; qu'il n'y a jamais eu autant d'argent sale, délictueux comme criminel, dans les paradis fiscaux ; qu'il n'y a jamais eu autant de critiques envers les politiques fiscales et aussi peu de consentement à l'impôt.

i. Des textes qui manquent d'efficacité

La multitude et la multiplication des lois et autres règlements ne peuvent faire oublier que les sanctions prévues sont souvent dérisoires par rapport aux gains tirés de la fraude et des montages délictueux. La sanction n'est parfois même pas prévue. Prenons l'exemple des recommandations du GAFI en matière de lutte contre le blanchiment de capitaux avec un organisme qui n'a aucun pouvoir de sanction et qui n'en suggère aucune par rapport à ses analyses. Même lorsque les amendes paraissent énormes, elles s'avèrent faibles par rapport aux gains émanant de la fraude -comme lorsque HSBC préféra payer 1,9 milliard de dollars en 2012 pour éviter d'être poursuivie pour complicité de blanchiment aux États-Unis, on peut imaginer ce qu'elle a pu tirer comme bénéfices de son laxisme. Même les criminels intègrent ce risque pénal et financier.

Pour la fraude fiscale, il n'y a en France pour ainsi dire aucune peine de prison ferme prononcée. Le sort réservé au Japon à Carlos Ghosn a d'ailleurs ému toute la classe politique et les milieux d'affaires français. Des sanctions dissuasives permettraient peut-être un changement

de comportement.

ii. Des textes peu respectés

Pour qu'une loi ait une quelconque effectivité, il faut qu'elle soit votée, qu'elle fasse l'objet d'un décret d'application, qu'elle soit appliquée, que son application soit contrôlée, que des sanctions soient prévues en cas de manquement, que ces sanctions soient prononcées le cas échéant. Ces différentes phases se retrouvent dans à peu près tous les pays du monde. Quant aux textes internationaux, c'est encore plus aléatoire car il est nécessaire de signer, de ratifier, de transposer, avant d'entamer la démarche précédemment évoquée. L'attitude des États-Unis illustre parfaitement cette complexité et ces difficultés, car ce pays refuse très souvent de signer les accords internationaux, les rendant ainsi quasiment inutiles. Comme nous l'avons vu auparavant, la loi FATCA impose au monde de déclarer les comptes bancaires des ressortissants américains, mais la réciproque n'existe pas, faute de signature du texte sur l'échange automatique d'informations par les États-Unis.

De même, si l'association *Tax Justice Network* place la Suisse en tête de son classement des paradis fiscaux, c'est à cause de sa politique à géométrie variable : coopération avec les pays occidentaux qui deviennent de plus en plus rigoureux, mais hésitation à échanger des données automatiquement avec les pays émergents, beaucoup plus laxistes. C'est ce que l'ONG nomme l'approche « zèbre » : de l'argent blanc, propre pour les pays riches ; de l'argent noir, sale pour les pays en voie de développement. L'effet s'est d'ailleurs immédiatement mesuré, puisque selon Zucman[8], 8 % du patrimoine financier mondial est détenu dans les paradis fiscaux, soit près de 8 000 milliards d'euros contre 6 500 il y a 3 ans. Or cette progression concerne essentiellement les pays émergents, la tendance s'inversant pour les pays riches.

iii. Des intérêts personnels

Certains gouvernements comme certains gouvernants n'ont pas vraiment envie, ni intérêt de changer les choses. La City de Londres qui représente 10 à 13 % du PIB de la Grande-Bretagne ne gagnerait pas forcément à une intensification de la lutte contre les paradis fiscaux. Ces derniers sont en effet très proches du pays (territoires d'outre-mer, anciennes colonies, membres du Commonwealth) et servent de lessiveuse avant d'envoyer les capitaux sales blanchis vers Londres. De même, les potentats de certains pays profitent de l'opacité des mêmes territoires pour y cacher les fruits des détournements et de la corruption qui pourront être lavés dans les mêmes conditions pour être ensuite investis dans les pays les plus riches. Enfin, pour des raisons géostratégiques, le statu quo prévaut souvent, pour ne pas froisser un territoire ami ou pour s'attirer les sympathies d'un pays puissant.

Ces situations et comportements ont pour résultat des moyens de contrôle réduits et des définitions juridiques restrictives : de moins en moins de fonctionnaires sont chargés des contrôles, quel que soit le ministère, et la définition des paradis fiscaux est généralement tellement encadrée que les listes noires demeurent quasiment vides.

Conclusion

En définitive, la fraude fiscale et les paradis fiscaux concernent tout le monde : les multinationales, les milliardaires, les contribuables aisés, les criminels. Des mesures sont mises en place mais il semble que l'attention soit plutôt portée à ne pas gêner les affaires et les échanges internationaux. Si l'information circule de plus en plus avec notamment la mise au jour des plus grands scandales mondiaux, c'est plus du fait de journalistes que d'autorités publiques. Le procès UBS en est l'illustration criante : si le jugement prévoit une amende de 4,5 milliards d'euros, ce sont des lanceurs d'alerte internes (Stéphanie Gibaud et Nicolas Forissier) et un média (Le Monde) qui ont déclenché l'affaire. Et si UBS avait accepté la négociation avec le gouvernement français, il n'y aurait pas eu de procès.

Aujourd'hui, la réponse à la problématique de la fraude fiscale semble se focaliser sur une baisse des impôts. Or, le *dumping* fiscal est loin d'être la panacée, car même les pays les moins fiscalisés subissent le détournement des règles pour éviter les faibles taxations. Il est ainsi nécessaire de rappeler qu'il n'existe aucun lien démontré entre taux d'imposition et évasion fiscale. C'est en fait la perception des institutions gouvernementales (de leur volonté et de leur efficacité) qui explique le niveau de fraude, c'est

la « peur du gendarme » qui freine la fraude. Pour trouver des solutions satisfaisantes, peut-être est-il nécessaire d'organiser une sorte de COP financière et fiscale à l'image des réunions internationales récurrentes pour l'environnement.

Pour aller plus loin, lire :

E. Vernier, *Fraude fiscale et paradis fiscaux : Quand l'exception devient la règle*, Dunod, 2018, 2ème éd.

E. Vernier, *Techniques de blanchiment et moyens de lutte*, Dunod, 2017, 4ème éd.

Notes :

1. L'affaire Albertin éclata en France en 1932 et mit en danger de nombreuses banques suisses. Le secret bancaire fut alors renforcé et protégé par le droit pénal suisse. Il fut dès lors interdit à tout employé de banque, et à la banque elle-même, de divulguer l'identité des propriétaires de comptes dans ses livres à quelque autorité que ce soit, en particulier la justice, qu'elle fut nationale ou étrangère, sous peine d'importantes sanctions pécuniaires et d'emprisonnement.
2. Fraude fiscale et paradis fiscaux. Quand l'exception devient la règle, Dunod, 2018, 2e éd.
3. Richard Murphy, The European Tax Gap, January 2019.
4. Who Owns the Wealth in Tax Havens ? Macro Evidence and Implications for Global Inequality, 27 décembre 2017.
5. Service de traitement des déclarations rectificatives.
6. Foreign Account Tax Compliance Act ou loi sur l'acquittement des obligations fiscales relatives aux comptes à l'étranger.
7. Loi n° 2018-898 du 23 octobre 2018 relative à la lutte contre la fraude.
8. Who Owns the Wealth in Tax Havens ? Macro Evidence and Implications for Global Inequality, 27 décembre 2017.

OUVRAGES RÉCENTS

JUGES EN CORSE

SOUS LA DIRECTION : DE JEAN-MICHEL VERNE

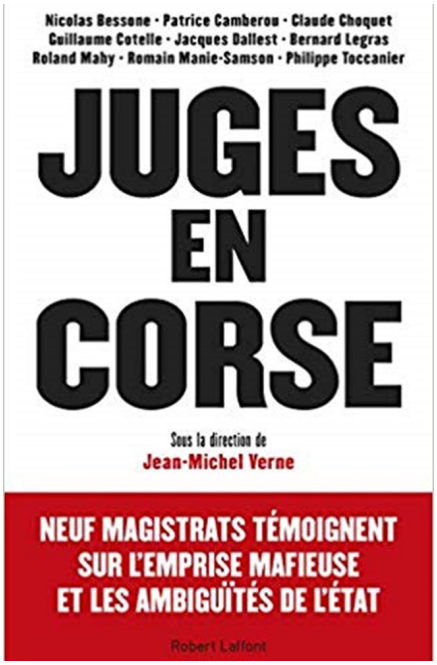
ÉDITEUR : ROBERT LAFFONT

Présentation de l'éditeur

Pour la première fois, neuf magistrats racontent leur tumultueux passage en Corse, entre emprise mafieuse et ambiguïtés de l'État.

" Il ne faut pas rester trop longtemps en Corse. Il faut agir dans la légalité, se garder de certaines fréquentations et, surtout, se tenir éloigné de certaines opérations "barbouzardes"." Ces mots, prononcés par le magistrat Jacques Dallest, révèlent toute la complexité du travail de la justice sur l'île.

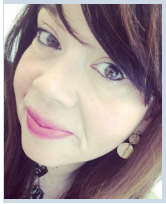
Pressions, menaces, poids des clans et des réseaux, moeurs locales, grand banditisme omniprésent, attentats, coups tordus... Le fonctionnement de la justice insulaire reste très particulier, au moment même où le nationalisme a pris le pouvoir.



Trois juges et six procureurs qui ont exercé dans l'île jusqu'à aujourd'hui témoignent de leurs difficultés à traiter les affaires. Un enjeu majeur, alors que la Corse pourrait plonger irrémédiablement dans un engrenage dangereux.

Chacun évoque ses dossiers les plus sensibles. Tous s'expriment avec la volonté de normaliser la vie insulaire et de permettre à l'île de Beauté de poursuivre son développement dans le respect des lois de la République.

ESCROQUERIE
COMMISE AU MOYEN DE FAUSSES FACTURES : SOUS QUELLE(S) QUALIFICATION(S) POURSUIVRE ?



DOROTHÉE GOETZ

DOCTEUR EN SCIENCES CRIMINELLES, ASSISTANTE SPÉCIALISÉE AU PARQUET DU TRIBUNAL DE GRANDE INSTANCE DE STRASBOURG

Dans son arrêt de principe (Crim. 16 janvier 2019, n°18-81.566), la Cour de cassation s'explique sur les liens pouvant exister entre les infractions d'escroquerie et de faux dans le cas précis (et classique) d'une escroquerie commise au moyen de fausses factures. Cet arrêt est important, car il donne la clé permettant pour démêler les liens pouvant exister entre les qualifications à retenir. Cette clé est le principe *ne bis in idem*.

Les faits de l'arrêt rapporté rappellent les liens étroits pouvant exister entre deux infractions pourtant distinctes : le faux et l'escroquerie. Le faux peut en effet être un moyen utilisé pour commettre une escroquerie. Dans ce cas, un même fait est susceptible de recevoir deux qualifications pénales différentes. Quelle(s) qualification(s) faut-il alors retenir : escroquerie et faux ou seulement l'une d'elles ? La Cour de cassation résout cette question en s'appuyant, dans cet arrêt, sur le principe *ne bis in idem*. Elle énonce en effet que ce principe ne peut s'appliquer que lorsque les faits poursuivis procèdent de manière indissociable d'une action unique caractérisée par une seule intention coupable.

Par le passé, la Cour de cassation a déjà considéré qu'il y avait, dans ce cas, deux infractions distinctes en concours réel[1]. La doctrine justifiait ce choix au motif que les deux infractions – le faux et l'escroquerie – étaient commisses successivement et non séparées par un jugement de condamnation, étant précisé qu'elles ne protègent pas les mêmes valeurs sociales. En effet, l'infraction de faux protège la confiance publique, alors que le délit d'escroquerie est une atteinte à la propriété d'autrui.

L'arrêt commenté vient toutefois relancer ce débat du choix de la qualification à retenir sous l'angle du principe *ne bis in idem*. En l'espèce, un individu était déclaré coupable par le tribunal correctionnel des chefs de faux et escroquerie. Il reconnaissait avoir lui-même confectionné de fausses factures de sous-traitance dans le but d'obtenir une remise indue de TVA. Après avoir relevé que par jugement, devenu définitif, du 24 janvier 2014, le prévenu, poursuivi sous la prévention de faux et usage, avait été déclaré coupable pour les fausses factures et leur usage, les juges du premier degré avaient fait droit à l'exception relative à l'extinction de l'action publique par l'effet de la chose jugée sur les faits de faux et ont rejeté celle formulée aux mêmes fins sur les faits qualifiés d'escroquerie, l'usage de faux dans cette précédente décision visant à masquer des sorties d'argent en espèces par le prévenu. Le ministère public et l'État français, alors partie civile, avaient interjeté appel contre le jugement.

Les juges du second degré avaient quant à eux, constaté l'extinction de l'action publique sur les faits d'escroquerie par l'effet de la chose jugée et déclaré irrecevable la constitution de partie civile de l'État français. Ils expliquaient ce choix en se fondant notamment sur la jurisprudence de la Cour européenne

des droits de l'homme (CEDH) qui a érigé l'interdiction de poursuivre ou de juger une personne pour une seconde infraction qui a pour origine des faits identiques ou qui sont en substance les mêmes que ceux ayant donné lieu à la première procédure[2]. Si, ainsi énoncé, le principe *ne bis in idem* semble simple, sa mise en oeuvre peut s'avérer particulièrement délicate. En effet, cet adage est « susceptible de trois sens : pas de nouvelles poursuites pour les mêmes faits, mais aussi pas de nouvelles poursuites sur de nouvelles qualifications pénales pour les mêmes faits et, enfin, après poursuites pénales, pas de nouvelles poursuites administratives »[3]. En l'espèce, les juges du fond considéraient que les manoeuvres frauduleuses visées par l'escroquerie procédaient des faits d'émission des fausses factures de sous-traitance déjà sanctionnés par le biais de l'incrimination de faux. En d'autres termes, et selon la formule consacrée, ils considéraient qu'ils étaient en présence d'une action unique caractérisée par une seule intention coupable. Pour cette raison, ils faisaient droit à l'exception soulevée relative à l'extinction de l'action publique par effet de la chose jugée.

Le procureur général et l'État français formaient un pourvoi en cassation.

Dans son arrêt de principe, la chambre criminelle entend leurs arguments. La haute juridiction fonde sa solution sur le principe *ne bis in idem* et les articles 6 et 593 du Code de procédure pénale. Selon ce dernier article, tout jugement ou arrêt doit comporter les motifs propres à justifier la décision et l'insuffisance ou la contradiction des motifs équivaut à leur absence. Mais surtout, la maxime latine visée ne peut s'appliquer que lorsque les faits poursuivis procèdent de manière indissociable d'une action unique caractérisée par une seule intention coupable. Or, en l'espèce, la Cour de cassation considère que l'usage des fausses factures auprès de l'administration fiscale pour obtenir une remise indue de TVA, élément matériel des manoeuvres caractérisant le délit d'escroquerie, constitue un nouveau fait d'usage au préjudice de l'État français, distinct de la production de ces mêmes factures par le prévenu au préjudice de la société qu'il gérait. Elle en conclue donc que la cour d'appel, en constatant l'extinction de l'action publique par l'effet de la chose jugée, a violé le principe *ne bis in idem*.

Cette solution s'inspire de deux arguments avancés par les requérants. En effet, le parquet général et l'État français remarquaient opportunément que l'utilisation des fausses factures au titre des manoeuvres frauduleuses n'était pas relative à un faux mais à un usage de faux, non visé par les poursuites. En outre, ils relevaient qu'il ne peut y avoir identité d'intention coupable entre des faits de faux, déjà poursuivis, et des manoeuvres, révélatrices d'une escroquerie. En effet, le prévenu ne se contentait pas, en l'espèce, de falsifier des pièces comptables : il se livrait en outre à des manoeuvres, réalisées par le dépôt de déclarations inexactes, pour déterminer l'administration à procéder à une remise indue.

La réceptivité de la chambre criminelle à ces arguments nous semble justifiée. La haute juridiction tire toutes les conséquences de la jurisprudence déjà rendue en la matière. Ainsi, s'ils ont à de nombreuses reprises déjà refusé le cumul de certains délits, notamment le blanchiment et le recel[4], le blanchiment et l'abus de biens sociaux[5], ou plus récemment en matière de violences[6], la jurisprudence la plus récente témoigne d'une vision pragmatique et ouverte du principe *ne bis in idem*[7].

C'est résolument dans cette veine jurisprudentielle que s'inscrit l'arrêt rapporté.

Notes :

1 Crim. 25 mai 1992, n° 91-82.934, Bull. crim. n° 207 ; 31 oct. 2000, n° 00-81.394, Dr. pén. 2001. Comm. 31, obs. M. Véron.

2 R. Parizot, Le principe ne bis in idem dans la jurisprudence de la Cour européenne des droits de l'homme, AJ pénal 2015. 173 ; N. Catelan, Constitution vs CESDH vs UE : ne bis in idem et la répression des opérations d'initié, RSC 2016. 467 ; Le principe ne bis in idem : entre harmonisation et dissonance européennes, AJ pénal 2013. 270.

3 J. Pradel, Manuel de procédure pénale, 14e éd., Cujas, 2008.

4 AJ pénal 2017. 35; obs. J. Gallois.

5 D. 2016. 2572.

6 Crim. 24 janv. 2018, n° 16-83.045, Dalloz actualité, 15 févr. 2018, obs. S. Fucini ; D. 2018. 241 ; AJ pénal 2018. 196, obs. E. Clément ; RSC 2018. 412, obs. Y. Mayaud.

7 Crim. 6 déc. 2017, n° 16-81.857, Dalloz actualité, 20 déc. 2017, obs. W. Azoulay ; D. 2018. 2259, obs. G. Roujou de Boubée, T. Garé, C. Ginestet, S. Mirabail et E. Tricoire ; Cons. const. 23 nov. 2018, n° 2018-745 QPC, Dalloz actualité, 7 déc. 2018, obs. J. Gallois ; D. 2018. 2237, et les obs. ; 3 mai 2018, n° 17-83.225, Dalloz actualité, 17 mai 2018, obs. W. Azoulay ; D. 2018. 2259, obs. G. Roujou de Boubée, T. Garé, C. Ginestet, S. Mirabail et E. Tricoire ; AJ pénal 2018. 377, obs. M. H-Evans.

L'ÉVALUATION DE L'INTÉGRITÉ DES TIERS EN MATIÈRE D'ANTICORRUPTION EN ENTREPRISE

CHARLES DUCHAINE

DIRECTEUR DE L'AGENCE FRANÇAISE ANTICORRUPTION (AFA)

Le développement de relations d'affaires dynamiques avec les différents partenaires de l'entreprise constitue une condition essentielle de sa croissance. Néanmoins, si ces partenaires sont impliqués, directement ou indirectement, parfois sans le savoir, dans des faits de corruption, ils peuvent constituer pour l'entreprise, un risque de nature juridique, commerciale, financière ou réputationnelle. Il est donc primordial, pour chaque entreprise, de mettre en oeuvre des mesures d'évaluation de l'intégrité de ses tiers afin de ne pas entraver les conditions de sa croissance.

L'évaluation de l'intégrité des tiers (ou *due diligences* selon le terme anglo-saxon) consiste à collecter des informations et des documents concernant ces tiers afin d'identifier ou d'actualiser les risques de conformité, notamment en matière de prévention de la corruption, induits par la relation contractuelle nouée avec chacun d'eux. Le dispositif d'évaluation de l'intégrité des tiers fait partie d'un programme de conformité anticorruption efficace tel que défini par les standards nationaux et internationaux.

Le dispositif d'évaluation de l'intégrité des tiers est au coeur de tout programme efficace de prévention et de détection de la corruption. Il est l'un des huit piliers du dispositif de l'article 17 de la loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, dite « loi Sapin II ».

Au-delà de l'obligation de conformité prévue par la loi, l'évaluation de l'intégrité des tiers procède, pour toutes les entreprises, quels que soient leur taille ou le nombre de leurs effectifs, de l'engagement de l'instance dirigeante et contribue à sécuriser la chaîne contractuelle et à diffuser l'anticorruption dans l'économie. L'élaboration et l'utilisation pertinente de l'évaluation de l'intégrité des tiers en fait, en outre, un outil efficace de maîtrise des risques de corruption.

I. L'évaluation de l'intégrité des tiers contribue à sécuriser la chaîne contractuelle et à diffuser la culture de l'anticorruption

A. L'évaluation de l'intégrité des tiers procède de l'engagement de l'instance dirigeante et s'articule avec les autres composantes du programme anticorruption

La loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, prévoit que « les présidents, les directeurs généraux et les gérants d'une société employant au moins cinq cent salariés, (...) et dont le chiffre d'affaires ou le chiffre d'affaires consolidé est supé-

rieur à 100 millions d'euros » sont tenus de mettre en place un programme de prévention et de détection de la corruption en adoptant les mesures et procédures énumérées au II de l'article 17 de la même loi.

Parmi ces mesures figure l'obligation d'adopter « des procédures d'évaluation de la situation des clients, fournisseurs de premier rang et intermédiaires au regard de la cartographie des risques ».

Si l'article 17 de la loi liste les mesures et procédures anticorruption à mettre en place au sein des entreprises, il n'en précise ni le contenu ni la portée. Les recommandations de l'Agence française anticorruption (AFA) publiées au Journal officiel du 22 décembre 2017 ont précisé le contenu de ces mesures et procédures anticorruption à l'attention des personnes visées par loi et, au-delà, à l'attention de toutes celles souhaitant se prémunir efficacement contre le risque de corruption et ses conséquences.

La mise en place, par une entreprise, d'un dispositif anticorruption comprenant une procédure d'évaluation de l'intégrité des tiers procède donc, soit d'une obligation légale soit d'une démarche volontaire, mais repose dans tous les cas sur l'engagement fort et sans équivoque des instances dirigeantes.

Seule la conscience de la responsabilité que fait peser sur eux un fait de corruption impliquant l'entreprise partenaire permet aux dirigeants de mesurer les risques portés par une relation tierce et peut les déterminer à adopter les mesures adéquates pour s'en prémunir.

Par ailleurs, l'évaluation de l'intégrité des tiers ne peut être envisagée indépendamment des autres composantes du dispositif anticorruption mais s'inscrit au contraire en cohérence avec ces dernières.

L'évaluation de l'intégrité des tiers s'appuie ainsi sur les risques identifiés par la cartographie des risques. La cartographie permet par exemple d'identifier les secteurs d'activité, les types de partenaires ou les zones géographiques appelant une vigilance renforcée. La part que représente une relation tierce dans l'activité de l'entreprise, l'impact réputationnel, financier, stratégique que comporte l'engagement ou la poursuite de cette relation, sont autant de critères à prendre en compte. Ils s'intègrent dans la cartographie des risques de corruption afin de déterminer le degré d'investigation nécessaire à appliquer à un tiers, et les mesures de remédiation à adopter pour réduire l'exposition au risque de corruption. De même, le référentiel des tiers complète l'identification des risques issus de la cartographie des processus.

L'évaluation de l'intégrité des tiers s'articule également avec l'ensemble des autres composantes du dispositif anticorruption. La formation des collaborateurs - prioritairement ceux qui sont au contact des tiers les plus à risque - à la mise en oeuvre des procédures adoptées par l'organisation en termes d'évaluation des tiers et à l'identification des risques, voire à l'utilisation des applications informatiques, sera déterminante de l'efficacité du dispositif.

En troisième lieu, les diligences à mettre en oeuvre en fonction du tiers considéré s'inscrivent dans les procédures du code de conduite, sous le contrôle des autorités managériales. L'intégration des éléments pertinents au code de conduite et l'utilisation de celui-ci par les collaborateurs, contribue à faire connaître la politique anticorruption de l'organisation auprès de ses partenaires, et à diffuser auprès d'eux le référentiel anticorruption de l'entreprise, contribuant ainsi à sa communication.

Enfin, l'évaluation des tiers s'articule avec le contrôle interne et notamment le contrôle comptable. Le suivi périodique de la relation contractuelle avec les partenaires peut en particulier s'appuyer sur les mesures du contrôle interne déployées à l'occasion de l'exécution d'un contrat. De même, l'audit et le contrôle interne peuvent concourir à faire évoluer le dispositif d'évaluation des tiers pour le rendre plus efficace.

B. Au-delà des effets positifs tirés par l'entreprise qui y a recours, l'évaluation des tiers permet de sécuriser la chaîne contractuelle et de diffuser l'anticorruption

Le mécanisme d'évaluation de

l'intégrité des tiers permet de sécuriser la relation contractuelle. De plus, chaque partenaire évaluant lui-même ses propres partenaires, il met finalement en place un mécanisme de contrôle mutuel qui sécurise la relation contractuelle « de bout en bout ».

Par conséquent, l'impact des mécanismes d'évaluation de l'intégrité des tiers s'étend bien au-delà du champ défini à l'article 17 de la loi du 9 décembre 2016. En particulier, la mise en place de dispositifs d'évaluation de l'intégrité des tiers par les plus grands groupes favorise le « ruissellement » de l'anticorruption vers les entreprises de taille intermédiaire (ETI) et les petites et moyennes entreprises (PME) qui n'atteignent pas les seuils fixés par la loi.

Si les plus petites entreprises ne sont pas légalement tenues de mettre en place un tel dispositif, elles sont toutefois progressivement concernées par la diffusion des standards anticorruption. Elles ont par ailleurs un intérêt évident à démontrer à leurs partenaires, leur conformité aux standards de lutte contre la corruption afin de favoriser leur positionnement sur le marché et leur attractivité. Ce positionnement favorisera, en outre, leur accès aux financements externes, liée à la solidité de leur gestion et à leur image de marque.

L'évaluation de l'intégrité des tiers obligeant les entreprises à gérer soigneusement leurs relations d'affaires, l'existence d'un programme anticorruption efficace accroît leurs chances d'être retenues au sein d'un groupement momentané en vue de répondre à des appels d'offres et leur permet de se positionner avantageusement à l'export. Les partenaires commerciaux qui disposent d'un programme de prévention de la corruption bénéficient donc d'un avantage comparatif sur ceux qui n'en sont pas dotés.

Cette diffusion du standard anticorruption s'étend d'ailleurs à l'échelle internationale. Les sociétés-mères françaises sont en effet également tenues d'étendre leur programme anticorruption à leurs filiales étrangères et d'en vérifier la mise en oeuvre efficace. Elles imposent également leur questionnaire d'intégrité à leurs clients et fournisseurs étrangers.

Enfin, les bailleurs de fonds, qu'il s'agisse de banques publiques ou privées, ou d'investisseurs en capital, intègrent de plus en plus de critères de conformité anticorruption dans la sélection de leurs clients ou de leurs cibles d'investissement.

L'évaluation de l'intégrité des tiers contribue ainsi à diffuser la conformité anticorruption à l'ensemble du tissu économique, à l'échelle nationale et internationale. Si elle peut conduire à exclure de nombreuses opportunités de marché les entreprises qui ne se conforment pas à ces exigences, elle peut aussi devenir pour elles un véritable atout compétitif.

En définitive, si la procédure d'évaluation de l'intégrité des tiers peut apparaître contraignante de prime abord, elle se révèle rapidement comme un atout pour sécuriser l'activité des entreprises. Cela explique qu'un nombre croissant d'acteurs économiques perçoivent l'intérêt d'une politique anticorruption intégrée, reposant sur une fonction conformité bien identifiée.

II. L'élaboration et l'utilisation pertinente de l'évaluation de l'intégrité des tiers en fait un outil efficace de maîtrise des risques de corruption

A. L'évaluation de l'intégrité des tiers vise à mesurer l'opportunité et le risque en matière de corruption que peut impliquer une relation

En principe, l'évaluation de l'intégrité d'un tiers est effectuée avant que la relation ne soit formellement nouée. Afin d'être efficace, le « stock » des partenaires avec lesquels une entreprise est déjà engagée, est évidemment concerné par ce dispositif et devra faire l'objet d'une évaluation.

Aussi les entreprises ont elles d'abord un important travail de recensement des tiers avec lesquels elles entretiennent ou envisagent d'entretenir une relation d'affaire.

Selon les recommandations de l'AFA publiées au Journal officiel du 22 décembre 2017, cette évaluation doit concerner l'intégralité des tiers à tous les niveaux de l'organisation, étant entendu qu'il s'agit avant tout de les cartographier et d'adapter ensuite l'évaluation de chacun selon son profil de risque.

L'objectif est de mettre en place un processus continu qui repose davantage sur la prévention du risque de corruption que sur sa gestion ex post.

Conçue comme un système de responsabilisation, l'évaluation exhaustive de l'intégrité des tiers offre à l'instance dirigeante la capacité de démontrer les choix opérés pour toute relation tierce et de justifier les mesures adoptées. L'évaluation complète de l'intégrité des tiers renforce la sécurité juridique de toutes les opérations effectuées par l'entreprise.

À ce titre, la mise en place d'une base de données informatisée recensant les tiers de l'entreprise peut constituer un moyen pertinent pour faciliter la gestion du dispositif compte tenu de l'important volume de relations tierces de certaines entreprises. Elle constituera aussi une première démarche de classement des tiers, selon leur nature, leur statut, leur taille, la nature de la relation contractuelle, l'implantation géographique, les montants en jeu, ou d'autres critères jugés pertinents pour la société.

Point de vigilance : L'articulation avec le règlement général sur la protection des données (RGPD) au regard des conditions de stockage et d'archivage des données.

Le RGPD définit les conditions dans lesquelles le traitement des données à caractère personnel est autorisé : les données doivent ainsi être collectées de manière loyale et licite, pour des finalités déterminées, explicites et légitimes.

L'article 17 de la loi du 9 décembre 2016 et les recommandations prises par l'AFA en application de l'article 3,2° sous-tendent l'intérêt légitime des entreprises à apprécier le niveau de risque de corruption. Les données doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs ; elles doivent être exactes, complètes et mises à jour si nécessaire. Enfin, elles doivent être conservées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont recherchées et traitées.

Un guide conjoint élaboré par la CNIL et l'AFA précisera prochainement l'articulation entre ces dispositifs.

Un premier niveau d'évaluation est effectué par le responsable opérationnel de la relation tierce qui collecte les principales informations concernant l'identité du tiers, son expertise, éventuellement le risque pays etc…

Cette évaluation s'appuie sur la consultation de listes internes à l'organisation, telles que des annexes de pays à risques ou interdits selon ses critères. Elle donne également lieu à la recherche d'informations en « sources ouvertes » c'est-à-dire les informations publiques.

À cet effet, il est particulièrement opportun d'établir une première grille d'évaluation à adresser aux partenaires et éventuellement de préciser les éléments complémentaires auxquels devront s'attacher les responsables opérationnels. La première source de l'évaluation d'un tiers est en effet le tiers lui-même. La réponse faite par un partenaire au formulaire d'information et d'évaluation de la conformité qui lui aura été adressé permettra d'apprécier son degré de coopération. Le responsable opérationnel émettra un premier avis sur le niveau de risque et sur l'opportunité de nouer la relation contractuelle envisagée.

Point de vigilance : Les personnes politiquement exposées et les bénéficiaires effectifs.

Les obligations de vigilance relatives aux personnes qualifiées par la réglementation européenne de « politiquement exposées » ont été introduites, en France, à l'article L.561-10 2° du Code monétaire et financier. Cette liste, qui concernait initialement les fonctions politiques, juridictionnelles ou administratives a été étendue par la quatrième directive anti-blanchiment (UE) 2015/849 du 20 mai 2015 aux personnes qui exercent de telles fonctions en France et aux dirigeants de partis politiques.

L'élargissement des obligations de vigilance aux PPE nationales résulte de l'ordonnance n° 2016-1635 du 1er décembre 2016, qui a transposé la quatrième directive pour celles de ses dispositions qui présentent en droit français un caractère législatif.

La qualification de personne politiquement exposée (PPE) n'emporte pas en elle-même de suspicion de corruption, de blanchiment ou de financement du terrorisme. Ainsi, comme le souligne le considérant 33 de la quatrième directive, « *les exigences concernant les personnes*

politiquement exposées ont un caractère préventif et non pénal et ne devraient pas être interprétées comme stigmatisant les personnes politiquement exposées comme étant impliquées dans des activités criminelles. Refuser une relation d'affaires avec une personne au seul motif qu'elle est une personne politiquement exposée est contraire à la lettre et à l'esprit de la présente directive et des recommandations révisées du GAFI. ».

Par ailleurs, l'évaluation de l'intégrité des tiers ne peut pas tenir lieu en tant que telle de vérification des bénéficiaires effectifs imposée par la législation. De même, l'évaluation de l'intégrité des tiers, qui s'étend à l'intégralité de ces derniers, ne peut se limiter à la vérification des bénéficiaires effectifs.

L'évaluation du tiers repose notamment sur sa propre prise en compte de la conformité anticorruption dans ses processus, laquelle variera suivant que ce tiers est ou non astreint à la mise en place d'un programme de conformité anticorruption. Cette évaluation s'attachera également à examiner les modalités de rémunération du tiers, son actionnariat, les modalités et les flux de paiement.

Le contenu d'un contrat et ses modalités d'exécution apportent d'importantes informations sur les risques induits par la relation. La vérification lors de l'évaluation de l'existence d'une réelle contrepartie ou de la proportionnalité de la rétribution au service effectivement rendu constituent des points de vigilance importants.

Cette vérification peut notamment être faite par comparaison du contrat avec d'autres contrats de même type, établis dans le même pays.

Le moment de l'intervention de la tierce partie doit également être vérifié pour s'assurer de l'intérêt réel de cette intervention.

Suivant le niveau d'information requis et le résultat des premières évaluations, il peut aussi s'avérer nécessaire d'avoir recours à des bases de données payantes, offrant un degré d'information supérieur. En outre, au regard du niveau d'investigation requis et de la charge que l'évaluation des tiers fait peser sur l'entreprise, il peut être opportun d'avoir recours à des fournisseurs de solutions externes.

Point de vigilance : Le choix d'un prestataire extérieur - les fournisseurs de solution.

Il existe deux grandes catégories de fournisseurs : les éditeurs de logiciels et les fournisseurs d'enquêtes de notoriété. Les premiers fournissent un outil d'évaluation permettant d'effectuer une première analyse des partenaires au sein de l'organisation. Les seconds sont généralement des cabinets d'avocats ou de consultants spécialisés en investigations.

Il est recommandé aux entreprises d'être particulièrement vigilantes dans le choix de leur prestataire auquel elles donneront ainsi accès à la connaissance de leurs partenaires et de leur activité. La manipulation et le stockage de ces informations d'importance stratégique doivent pouvoir être pleinement sécurisés.

Avant de recourir à un prestataire extérieur, les entreprises peuvent se renseigner auprès du service de l'information stratégique et de la sécurité économique de la Direction générale des entreprises

(https://www.entreprises.gouv.fr/information-strategique-sisse/creation-du-service-information-strategique-et-securite-economiques).

Dans les cas les plus sensibles, le responsable de la conformité anticorruption accompagne le niveau opérationnel en apportant son expertise.

En principe, l'évaluation de l'intégrité des tiers est effectuée par le niveau opérationnel qui collecte les informations et documents utiles à l'évaluation des tiers avec lesquels il est ou est appelé à être en relation et émet une première appréciation.

Cette appréciation vaut décision dans les cas considérés comme peu risqués. Dans ce cadre, le responsable de la conformité anticorruption apporte son expertise et ses conseils au niveau opérationnel. Il intervient en soutien du niveau opérationnel et accompagne celui-ci dans l'appréciation des cas les plus risqués.

Les manquements identifiés dans le cadre des contrôles de premier niveau sont analysés par le responsable de la conformité qui définit les mesures correctives à mettre en oeuvre.

Si la taille ou l'organisation d'une entreprise ne permet pas de confier au niveau opérationnel le soin d'évaluer l'intégrité des tiers, cette compétence peut-être intégralement confiée au responsable de la conformité anticorruption. Dans ce cas, il convient de veiller

à attribuer à ce responsable les moyens de s'acquitter de cette tâche.

Le responsable de la conformité élabore et met en oeuvre un plan de contrôle de deuxième niveau couvrant l'ensemble du dispositif de prévention et de détection de la corruption.

Ces premières évaluations donnent lieu à un classement des tiers par degré et par profil de risque. La relation peut être approuvée sans réserves, ou reportée dans l'attente d'investigations complémentaires. Lorsque la cotation du niveau de risque est élevée, l'instance dirigeante peut décider de mettre un terme à la relation ou de ne pas l'engager.

Lorsque des cas risqués sont identifiés, seule l'instance dirigeante est légitime à décider de la suite à donner. En pleine connaissance des risques induits par cette relation à un tiers, elle choisit en opportunité d'endosser ou non le risque de cette relation et de prendre, le cas échéant, les mesures appropriées pour le réduire.

Point de vigilance :

Afin de répondre au besoin de traçabilité des évaluations, il est impératif d'être en mesure de documenter la méthodologie retenue pour effectuer l'évaluation de l'intégrité des tiers, les différentes étapes du processus de décision, ainsi que les mesures de remédiation adoptées.

B. Les acteurs économiques ont intérêt à se saisir de l'évaluation de l'intégrité des tiers pour sécuriser au mieux leur activité

L'évaluation de l'intégrité des tiers vise à structurer une gestion différenciée et maîtrisée des relations contractuelles avec ses tiers. Il ne s'agit pas, en effet, de s'interdire radicalement et dans tous les cas où un risque est identifié, une relation avec un tiers, mais d'ajuster les mesures de remédiation en gérant activement la relation contractuelle.

Plusieurs niveaux de mesures de remédiation peuvent être définis en fonction du risque identifié. Il s'agit en premier lieu d'affirmer l'attachement de l'entreprise au respect des règles éthiques en communiquant au partenaire son code de conduite, par exemple. L'entreprise peut également solliciter de son partenaire qu'il s'engage par écrit à lutter contre la corruption et à vérifier, notamment, l'ensemble de ses sous-traitants.

Dans les cas les plus sensibles, l'entreprise peut demander à son partenaire d'assurer lui-même la vérification de la conformité de ses propres partenaires aux standards de lutte contre la corruption. Ce « monitoring » peut se matérialiser par l'organisation de formations anticorruption auprès de ses partenaires. Certains types de contrats peuvent également contenir une clause d'audit, définissant les conditions d'exercice auprès de ses partenaires d'un audit de conformité anticorruption.

Dans tous les cas de figure, la relation avec le tiers fait l'objet d'un suivi spécifique afin de prévenir et de détecter les faits de corruption.

L'entreprise doit avoir une visibilité complète sur les paiements ordonnés ou reçus afin de s'assurer que la rémunération et les modalités de paiement sont conformes aux dispositions contractuelles. Lorsque ce n'est pas le cas, et notamment que des modalités anormales de paiement sont exigées, les services financiers alertent le responsable de la conformité.

Il est enfin fortement recommandé de procéder à des réévaluations périodiques de ses partenaires, notamment lorsque le risque de corruption est élevé ou lorsqu'un changement significatif est intervenu au sein de l'entreprise ou chez un partenaire, telle qu'une nouvelle acquisition ou une fusion. Dans ces cas, une nouvelle phase d'évaluation s'impose.

Point de vigilance :

Les investissements en capital constituent à cet égard un enjeu stratégique tant pour les acteurs industriels ou de service qui procèdent à des opérations de croissance externe, que pour les acteurs ayant pour activité le conseil ou l'investissement en capital dont c'est le coeur de métier.

Contrairement à d'autres droits, le droit français n'impose pas la réalisation d'un audit préalablement à une opération de fusion-acquisition. Cependant, si les acquéreurs réalisent en général un audit financier, il est plus rare qu'ils diligentent un audit plus approfondi.

Or, la mise en cause pour corruption ou l'inexistence ou l'insuffisante robustesse du dispositif de conformité anticorruption de la société ciblée n'est pas sans conséquence pour la société qui l'acquiert, l'absorbe ou fusionne avec elle. Elle peut notamment se traduire par des coûts financiers susceptibles de

se révéler significatifs postérieurement à l'opération.

Il est donc de l'intérêt de l'acquéreur, quelles que soient ses caractéristiques, de conduire des vérifications anticorruption consistant à prendre la mesure des risques associés à l'implication éventuelle de la cible dans une affaire de corruption d'une part, à évaluer la qualité de son dispositif de prévention et de détection des atteintes à la probité et les insuffisances auxquelles il conviendra de remédier après l'opération, d'autre part.

Notes :

1 Formulaire de contact : https://www.entreprises.gouv.fr/dge/ecrire-a-la-dge.

OUVRAGES RÉCENTS

DÉFIS N°9 DE L'INSTITUT NATIONAL DES HAUTES ÉTUDES DE LA SÉCURITÉ ET DE LA JUSTICE (INHESJ)

LA REVUE DU DÉPARTEMENT INTELLIGENCE ET SÉCURITÉ ÉCONOMIQUES

Cette neuvième édition de DéfiS explore un sujet en pleine structuration au sein de l'État et des entreprises : la compliance. Plus de 40 contributeurs, experts, acteurs des politiques publiques et du secteur privé, apportent leurs éclairages. Ce numéro repose la question de la définition de l'intelligence économique au sein de l'État et des pratiques en entreprise à travers un entretien croisé avec Thomas COURBE (Direction générale des entreprises – DGE), Alain JUILLET et Philippe CLERC.

La rubrique « Enjeux » est consacrée à la relation police-population, actuellement au coeur des préoccupations.

Pour consulter la revue, le lien est le suivant : https://inhesj.fr/sites/default/files/inhesj_files/publications/pdf/DefiS_9_compliance_decembre_2018.pdf

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

REGARDONS AILLEURS

LA RESPONSABILITÉ PÉNALE DES PERSONNES MORALES OU LE « TROU DANS LA RAQUETTE » DE LA LUTTE CONTRE LE CRIME ORGANISÉ EN RUSSIE

BENJAMIN DANLOS

MAGISTRAT DE LIAISON FRANÇAIS EN RUSSIE

Les propos tenus dans le présent article n'expriment que l'opinion de leur auteur. Ce dernier remercie Kristina DROZHZHA et Marianne CESTARI (respectivement assistante du magistrat de liaison et stagiaire au sein du service) pour les recherches effectuées en amont de la rédaction de ce texte.

La menace que représente le crime organisé en Russie est connue depuis plusieurs décennies et constitue un sujet politique et sociétal important, étudié tant au niveau national que par les observateurs internationaux[1]. La lutte contre ce phénomène est, comme en Europe, présentée comme une priorité des organes d'enquête et de poursuite. Dans le cadre de sa stratégie pour contrer les activités illégales des nombreux groupes criminels sévissant sur son territoire ou au préjudice de ses ressortissants, la Russie peut compter sur une législation moderne et des services aux moyens matériels et humains conséquents. Ces atouts lui ont permis d'obtenir des succès non négligeables dans ce domaine. Pourtant, un outil qui a démontré sa grande efficacité à l'étranger manque toujours à son arsenal juridique : il s'agit de la responsabilité pénale des personnes morales, toujours inexistante en droit positif.

L'argumentaire en faveur de l'institution d'un tel mécanisme n'est plus à faire. En effet, la faculté de poursuivre les personnes morales impliquées dans la commission d'infractions, isolément ou aux côtés des personnes physiques ayant participé aux actes en cause, offre un potentiel accru d'efficacité des poursuites et décuple le caractère dissuasif de la prévention et de la répression pénale, en offrant notamment une gamme plus large de peines (tant en ce qui concerne la nature des mesures qu'au regard des quantums encourus). À cet égard, le caractère exemplaire des amendes parfois prononcées par les tribunaux, plus seulement outre-Atlantique[2], suffit à convaincre de l'intérêt de cette institution. En effet, dans les situations observées, l'imposition de sanctions similaires aux personnes physiques n'aurait été ni possible légalement, ni appropriée au vu des patrimoines des intéressés, souvent bien plus limités que ceux des entités juridiques derrière lesquelles ils opèrent.

Dans le cas du crime organisé russe, l'engagement de la responsabilité pénale des personnes morales offrirait des avantages supplémentaires pour contourner certaines difficultés auxquelles sont particulièrement confrontées les forces de l'ordre.

D'une part, la mise en cause des personnes physiques se heurte souvent en Russie à la stratégie des auteurs d'infractions, qui consiste à se réfugier à l'étranger, de préférence dans des pays où l'extradition est impossible (soit en raison d'une double nationalité, soit en l'absence de convention le prévoyant entre la Fédération et l'État requis). Lorsque leur remise aux autorités requérantes ne se trouve pas empêchée en raison

d'un obstacle juridique incontournable, ils tentent d'entraver néanmoins son exécution par tous les moyens, par exemple en invoquant le prétendu caractère politique des poursuites engagées, y compris dans des dossiers où la réalité des infractions commises est pourtant étayée par un dossier solide, ou encore en faisant valoir la jurisprudence de la Cour européenne des droits de l'homme relative aux conditions de détention en Russie. Cette démarche peut s'avérer fructueuse, la fluidité des procédures d'extradition pouvant parfois paraître perfectible. Dans ces situations, il existe pourtant des personnes morales dont la poursuite par les autorités russes pourrait s'avérer pertinente en termes de réponse pénale et efficace dans la lutte contre le groupe criminel organisé concerné.

D'autre part, les autorités russes sont confrontées depuis plusieurs années à un développement important de la « criminalité des personnes juridiques », c'est-à-dire de la commission d'infractions dans l'intérêt ou au moyen d'une personne morale. Ce phénomène est particulièrement notable dans le cadre du blanchiment de l'argent issu de l'activité des groupes criminels organisés et du phénomène de fraudes fiscales massives désigné sous le terme « d'offshorisation ». Dans un article du 26 janvier 2015, Alexandre Ivanovitch Bastrykine, président du Comité d'enquête de la Fédération de Russie, alertait ainsi sur la menace que cette tendance représentait pour la sécurité économique de l'État et pour les intérêts des acteurs privés agissant de bonne foi, ce qui pesait significativement sur le caractère attractif du pays pour les investisseurs. Il observait que ces infractions favorisaient une hausse du niveau général de la criminalité, en facilitant des phénomènes tels que la corruption, les atteintes illégales à l'environnement, le financement du terrorisme et le crime organisé[3]. Il appelait en conséquence à l'adoption d'une loi instituant dans la législation russe une responsabilité pénale des personnes morales.

Il y a donc lieu de constater que les arguments en faveur de la mise en oeuvre d'un tel mécanisme ne sont nullement méconnus au sein de la Fédération. Au contraire, depuis le milieu des années 90, le débat juridique et politique est resté relativement vif entre les partisans et les adversaires d'une telle réforme[4]. Trois projets de lois ont même été soumis au législateur afin de combler cette lacune du droit russe. En effet, dès 1994, lors de la rédaction du nouveau Code pénal, le projet initial prévoyait d'instaurer la responsabilité pénale des personnes morales au sein de la partie générale du texte. De même, en 2011, le Comité d'enquête de la Fédération de Russie (déjà présidé par A. I. Bastrykine) était l'auteur, dès sa première année d'activité, d'un projet de loi relatif à l'institution d'une responsabilité pénale des « personnes juridiques ». Enfin, en 2015, Olga Fedorovna Kovitidi, membre du Conseil de la Fédération et Alexandre Alexandrovitch Remezkov, député de la Douma d'État, proposaient au président de cette assemblée l'adoption d'une loi fédérale « relative à l'amendement de plusieurs actes législatifs de la Fédération de Russie en lien avec l'introduction d'une responsabilité pénale des personnes morales ». L'examen de ce texte a été définitivement abandonné le 23 juillet 2018.

Les auteurs et promoteurs de ces projets rappellent qu'un certain nombre de normes internationales tendent vers l'adoption d'un tel mécanisme. Par exemple, la Convention des Nations Unies contre la criminalité transnationale organisée du 15 novembre 2000, ratifiée par la Fédération de Russie le 26 mai 2004, prévoit en son article 10.1 que « *Chaque État Partie adopte les mesures nécessaires, conformément à ses principes juridiques, pour établir la responsabilité des personnes morales qui participent à des infractions graves impliquant un groupe criminel organisé et qui commettent les infractions établies conformément aux articles 5, 6, 8 et 23 de la présente Convention* ». De même, des dispositions similaires figurent aux articles 26 de la Convention des Nations Unies contre la corruption du 31 octobre 2003 (ratifiée par la Russie le 9 mai 2006) et 18 de la Convention pénale sur la corruption, adoptée dans le cadre du Conseil de l'Europe le 27 janvier 1999 (et ratifiée le 4 octobre 2006 par les autorités russes).

Certains font néanmoins observer que ces normes internationales sont déjà satisfaites en droit russe[5]. De fait, celles-ci sont rédigées dans des termes relativement larges, permettant d'admettre que la responsabilité des personnes morales soit mise en oeuvre par des voies autres que pénales. Ainsi, l'article 10.2 de la Convention des Nations Unies contre la criminalité transnationale organisée dispose : « *Sous réserve des principes juridiques de l'État Partie, la responsabilité des personnes morales*

peut être pénale, civile ou administrative ». Or, en Fédération de Russie, les personnes dites « juridiques » peuvent déjà voir leur responsabilité engagée au civil ainsi que pour toute une gamme d'infractions administratives (« административные правонарушение »)[6]. Le nombre de celles qui leur sont applicables s'est en effet considérablement accru au cours de la période récente. Ce phénomène a par exemple permis au Parquet général de la Fédération d'intensifier l'efficacité de sa politique relative à la lutte contre la corruption[7].

Reste que ces types de responsabilité ne sont pas aussi efficaces pour lutter contre les phénomènes visés par ces textes. En particulier, plusieurs auteurs dénoncent les limites de la responsabilité pour les infractions administratives ; ils rappellent que les moyens d'investigation ne sont pas aussi étendus dans ce domaine que dans le cadre de la procédure pénale, que la prescription de l'action publique les concernant est rapidement acquise, que l'entraide pénale internationale ne peut être mise en oeuvre dans le cadre de leur poursuite et que les peines complémentaires applicables aux personnes morales dans le cadre administratif sont lacunaires[8].

D'autres leur répondent que certaines dispositions législatives ont durci la répression de certaines infractions administratives, notamment lorsque l'auteur est une personne juridique, ce qui a permis de les rendre plus redoutables encore que certaines infractions pénales. En effet, le financement du terrorisme (article 15.27.1 du Code des infractions administratives de la Fédération de Russie) ou, dans certaines circonstances, la violation des dispositions légales applicables à l'ouverture d'un compte bancaire et d'une lettre de crédit auprès d'un établissement de crédit (article 15.39 du même Code) sont réprimés par une peine d'amende pouvant aller jusqu'à 60 millions de roubles lorsqu'ils sont commis par une « personne juridique », soit bien au-delà des 5 millions de roubles prévus au maximum pour les personnes physiques dans le Code pénal[9]. De plus, la prescription des infractions administratives est parfois étendue jusqu'à 6 ans (en matière de lutte contre le terrorisme et la corruption – article 4.5 du même Code). Force est néanmoins de constater que ces textes spéciaux sont très limités par leur nombre et par leur champ d'application.

En réalité, au-delà de ce débat sur le caractère efficace ou non de la répression des infractions administratives, les projets de loi visant à instaurer une responsabilité pénale des personnes morales semblent butter systématiquement sur deux arguments fondamentaux, tirés de la théorie du droit pénal général. Le premier consiste à faire valoir qu'un tel mécanisme heurterait les règles relatives à l'intentionnalité de l'infraction. Cette objection revient d'une certaine manière à paraphraser l'aphorisme classique prêté à Léon Duguit, en faisant valoir que si l'on ne peut pas « dîner avec une personne morale », celle-ci ne peut pas non plus avoir l'intention de commettre un délit ; pour reprendre la réponse faite par Jean-Claude Soyer, il serait dès lors injuste de lui faire « payer l'addition » correctionnelle... Le second insiste sur le principe de la responsabilité individuelle, pour critiquer le fait de retenir la culpabilité d'une entité juridique pour des actes commis en réalité par une personne physique agissant en son nom, en tant que dirigeant de droit ou de fait.

Ces arguments[10] révèlent chez les juristes et chez le législateur russe une approche de la théorie juridique qui peut être qualifiée de puriste. Certains pourraient objecter que les principes sur lesquels ils se fondent ne sont nullement propres au système de droit de la Fédération, mais sont également en vigueur dans l'ensemble des pays qui ont instauré une forme de responsabilité pénale des personnes morales dans leur législation. Les mécanismes utilisés pour y rendre cette institution compatible avec les règles fondamentales de l'intentionnalité de l'infraction et de l'individualité de la culpabilité, bien que parfaitement connus et analysés en Fédération de Russie, n'ont néanmoins pas suffit, pour le moment, à convaincre suffisamment de membres des pouvoirs législatif et exécutif pour se manifester par une réforme du droit positif. Ce débat reste néanmoins très actuel et la recherche d'efficacité accrue de la lutte contre le crime organisé pourrait lui permettre de revenir prochainement à l'ordre du jour législatif.

Notes :

1 V., not., Gilles Favarel-Garrigues, « Concurrence et confusion des discours sur le crime organisé en Russie », Cultures & conflits, L'Harmattan, 2001, pp. 2-23. <hal-01016942> ; et Dmitri Nikolaevitch Tishkin, « Государственная политика по борьбе с организованной преступностью в России: оценка эффективности », Философия права, 2016 N°5 (78), pp. 76-61.

2 V., par ex., sur la condamnation récente en France d'UBS, en premier ressort, à une amende de 3.7 milliards d'euros pour des faits de démar-

chage bancaire illégal et blanchiment aggravé de fraude fiscale, AFP, « Fraude fiscale: UBS condamnée à la plus lourde peine prononcée en France », 20 février 2019, 19h50, FRA.

3 Alexandre Ivanovicth Bastrykine, « К вопросу о введении в России уголовной ответственности юридических лиц », https://sledcom.ru/blog/bastrikin/item/888481 .

4 V., not., Boris Vladimirovitch Voljenkine, « Уголовная ответственность юридических лиц », Серия "Современные стандарты в уголовном праве и уголовном процессе", СПб, 1998 40 с. ; N.N. Smirnov, « Уголовная ответственность юридических лиц: дискуссия – за и против », Юристъ - Правоведъ, 2007, https://cyberleninka.ru/article/n/ugolovnaya-otvetstvennost-yuridicheskih-lits-diskussiya-za-i-protiv ; Tatiana Fedorovna Miniazeva et Anna Valerievna Serebrennikova, « Уголовная ответственность юридических лиц в России и Германии: к постановке проблемы », Lex Rossica, N°2 (123), fév. 2017, pp. 147-154.

5 V., par ex., Tatiana Fedorovna Miniazeva et Anna Valerievna Serebrennikova, « Уголовная ответственность юридических лиц в России и Германии: к постановке проблемы », précité, p. 149.

6 V. P.N. Smoliakov, « Ответственность юридических лиц », КонсультантПлюс 2019, www.consultant.ru.

7 V., à cet égard, l'interview accordée par Iouri Tchaïka, Procureur général de la Fédération, à l'agence d'information interfax, le 8 décembre 2016, https://genproc.gov.ru/genprokuror/interview/document-1145087/.

8 V., par ex., A. I. Bastrykine, « К вопросу о введении в России уголовной ответственности юридических лиц », précité.

9 Argument soulevé dans l'avis du gouvernement N° 3723п-П4 en date du 15 juin 2015, relatif au projet de loi de O. F. Kovitidi et A. A. Remezkov précité.

10 D'autres arguments moins souvent relayés consistent à invoquer le risque que l'engagement de la responsabilité pénale des personnes morales conduise au licenciement d'employés innocents (du fait des sanctions imposées aux entreprises), ou la rupture d'égalité due à l'immunité pénale accordée aux personnes morales de droit public. Enfin, certains craignent que la poursuite des entités juridiques pour des crimes ou des délits constitue un nouveau facteur de déstabilisation pour les entreprises russes. V. par ex, Tatiana Fedorovna Miniazeva et Anna Valerievna Serebrennikova, « Уголовная ответственность юридических лиц в России и Германии: к постановке проблемы », précité, p. 150.

OUVRAGES RÉCENTS

LA CHAMBRE DES COUPABLES

LA JUSTICE FACE AUX DJIHADISTES FRANÇAIS

AUTEUR : MATHIEU DELAHOUSSE

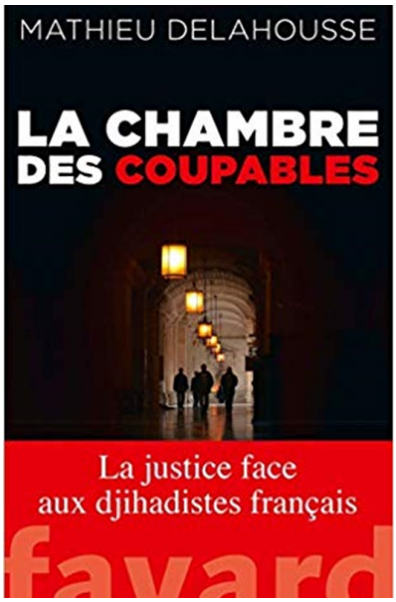
ÉDITEUR : FAYARD

Présentation de l'éditeur

Ils sont à peine majeurs et se sont rêvés djihadistes. Ils sont en prison et déjà sur le point d'en sortir. Ils ont voulu combattre la France. Elle doit à la fois les punir, s'en protéger et les réintégrer.

Celle-ci a 19 ans et a tenté de « monter à Paris » pour aller « tuer des gens » et faire « pire qu'au Bataclan ». Celui-là a quitté sa famille pour la Syrie, d'où il est revenu, plein de haine, décidé à frapper son propre pays. Ceux-là s'aimaient en France, mais s'imaginaient un avenir meilleur au cœur de l'État Islamique. Leur point commun est d'avoir entrepris le pire, et d'avoir échoué.

Revenus vivants, sans gloire ni martyre, tous sont poursuivis pour association de malfaiteurs

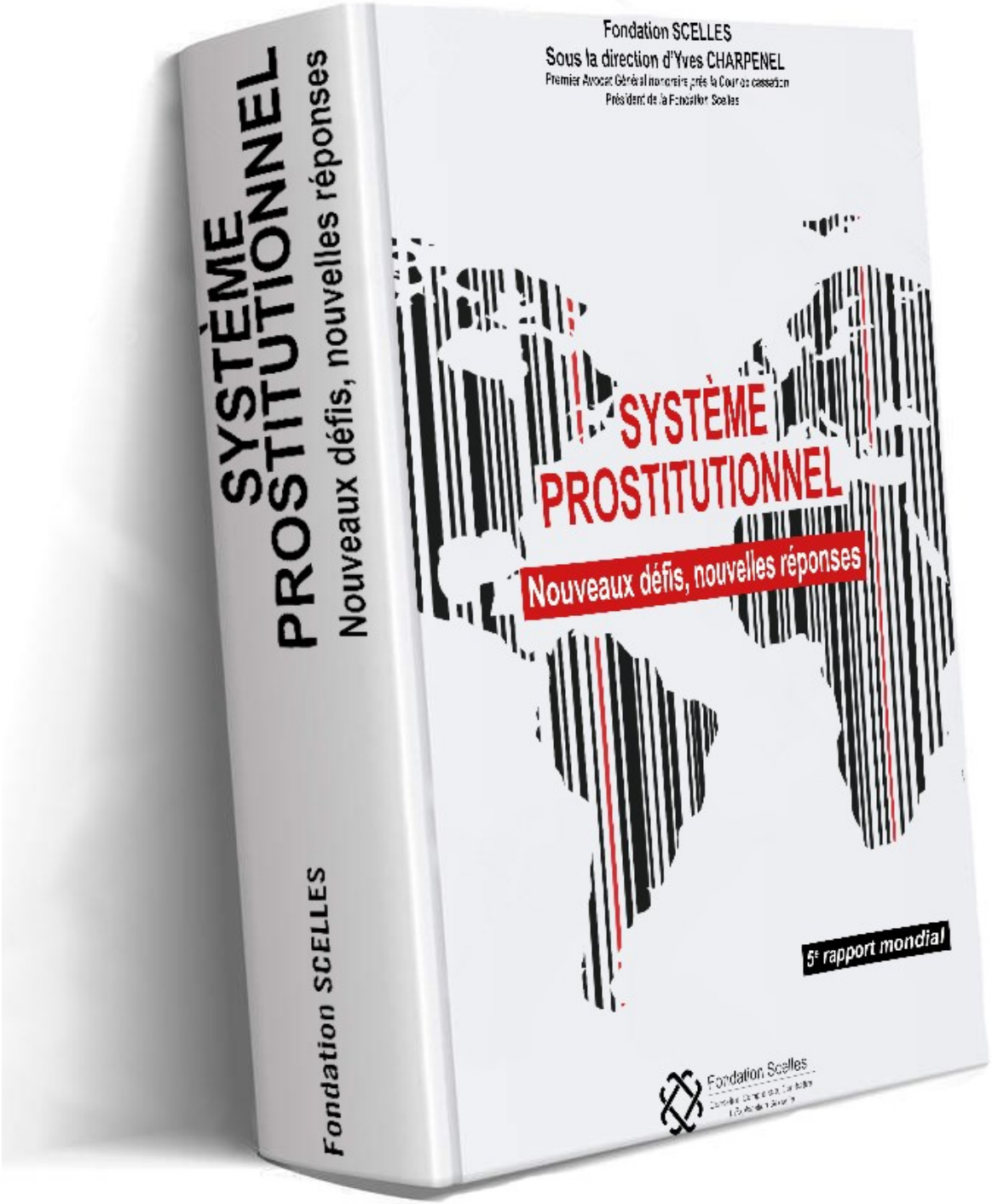


terroristes. Ils posent à la justice l'énigme de leur parcours, du mépris de soi à la détestation des autres, de l'illusion d'une vie meilleure à l'appel du mal radical.

La justice découvre en eux à la fois des enfants et des ennemis de la société française.

En nous emmenant au cœur des audiences, Mathieu Delahousse élève chaque enquête au rang d'un récit véritable. Il ne nous épargne aucune des questions auxquelles le juge devra répondre en quelques heures. Il nous fait participer à cette justice rendue en notre nom et pour notre avenir.

Mathieu Delahousse est grand reporter spécialiste des affaires judiciaires. Il a déjà publié plusieurs ouvrages, notamment La chambre des innocents (Flammarion, 2017), consacré aux victimes d'erreurs judiciaires.



La Fondation Scelles publie son 5e Rapport mondial sur l'exploitation sexuelle. Depuis 2012, année après année, ce « tour du monde » a pour objectif de détecter et d'anticiper les évolutions. Qu'observons-nous aujourd'hui ?

Jamais les facteurs de vulnérabilités n'ont été aussi nombreux et les exploitations des êtres humains aussi intenses, alors même que les relations femmes/hommes sont au cœur des débats. Dans le contexte de la crise migratoire et de la libération de la parole engendrée par le mouvement #MeToo dans différentes parties du monde, que pouvons-nous dire de l'exploitation sexuelle aujourd'hui ? Quelles nouvelles tendances ont émergé ? Quelles réponses nos sociétés apportent-elles ?

Le rapport est disponible sur le site de la Fondation Scelles : www.fondationscelles.org