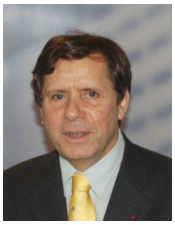
LA REVUE DU GRASCO

www.grasco.eu
www.larevuedugrasco.eu

N°30— juillet 2020

Parution trimestrielle
Gratuite
ISSN 2272-981X



EDITORIAL

FRANÇOIS FALLETTI

ANCIEN PROCUREUR GÉNÉRAL DE PARIS, MEMBRE DU COMITÉ SCIENTIFIQUE DE LA REVUE DU GRASCO

« Oh, Temps, suspends ton vol ! » Une bonne partie de l'Humanité aurait sans doute boudé ces derniers mois la supplique du poète et appelé les heures propices à reprendre rapidement leur cours.

Indifférentes à tout romantisme, les organisations criminelles n'ont pour leur part guère ralenti leur inlassable course au profit. Elles se sont vite adaptées au nouveau contexte mondial, s'employant à immiscer leurs tentacules dans les moindres failles d'un univers déstabilisé. Or, ces vulnérabilités furent nombreuses.

Aux pénuries de masques répondirent rapidement des offres, parfois fictives, de matériels impropres ou issues de vols ou de braquages commis en bande, parfois bien loin des lieux de revente. Des invitations en forme de collectes au bénéfice des soignants ont été lancées pour abuser des personnes désireuses de marquer leur solidarité.

L'invitation à un recours massif au télétravail fut un temps béni pour les auteurs de fraudes sur internet, qu'il s'agisse d'escroquerie aux présidents, de rançongiciels, d'attaques de sites privés ou publics.

Certes, la raréfaction des transports et les limitations de circulation découlant des divers confinements ont un temps compliqué certains approvisionnements, notamment en produits stupéfiants, provoquant la hausse de leur prix. Elles ont aussi exigé une adaptation des modes d'acheminement, par exemple par un report des go fast vers des semi-remorques transportant des denrées alimentaires ou des produits sanitaires. Comme pour les activités licites, ces circonstances si particulières auront sans doute favorisé sur la durée un recours à des modes de distribution appuyés sur les réseaux cryptés, marquant le développement de « drive « et de livraisons « uberisées » à domicile, tout en stimulant la tendance à la cannabiculture de proximité. Au demeurant, le trafic de rue des stupéfiants, un temps fortement contracté, n'a jamais cessé et est vite remonté en puissance, alors que le retour vers des conditions normales a vite vu réapparaitre, avec des règlements de comptes sanglants, les cambriolages et braquages que ne favorisaient guère des artères désertées.

Cette formidable capacité d'adaptation, fondée sur l'observation que la nature a horreur du vide, n'est pas une nouveauté. On l'a relevée au cours de toutes les guerres et périodes troublées qui ont d'ailleurs permis à certaines organisations criminelles de traverser les plus grandes secousses de l'Histoire, voire de se renforcer au cours de ces périodes.

SOMMAIRE

ÉDITO 1

INTERVIEW :

MARYVONNE LE BRIGNONEN, DIRECTEUR DE TRACFIN 4

DOCTRINE JURIDIQUE

QUEL CADRE LÉGAL POUR LUTTER EFFICACEMENT CONTRE LA CONTREFAÇON CRIMINELLE ? PAR MARION BRIATTA 12

DOCTRINE SCIENCES CRIMINELLES

LA TRANSPARENCE FISCALE : DIX ANS D'AVANCÉES ? PAR MATHILDE SABOURET 19

LES ENTREPRISES ACTRICES DE L'ANTICORRUPTION PAR NATHALIE KALESKI 26

LA POURSUITE DES CYBERCRIMINELS EN 2020 PAR JACQUES MARTINON 34

DU CÔTÉ DES PRATICIENS

ÉLÉMENTS STATISTIQUES SUR LA TRAITE DES ÊTRES HUMAINS EN FRANCE PAR AMANDINE SOURD 44

REGARDONS AILLEURS

LA POLITIQUE CRIMINELLE AU SÉNÉGAL À L'AUNE DE LA LUTTE CONTRE LA CYBERCRIMINALITÉ PAR THIERNO AMADOU NDIOGOU 53

CRIMINOGÉNÉITÉ DU FOOTBALL PROFESSIONNEL : CONSIDÉRATIONS À L'AUNE DES AFFAIRES SECOUANT LA BELGIQUE PAR MICHAËL DANTINNE 59

Reste alors à mesurer comment les institutions publiques et les structures privées peuvent se prémunir d'abus susceptibles de saper encore un peu plus la confiance des citoyens dans les mécanismes d'une économie déjà fortement ébranlée par la crise sanitaire.

Les différentes rubriques de cette nouvelle livraison de la Revue du Grasco y aideront largement, avec l'avantage que la vision défendue par leurs auteurs replace la conjoncture récente dans une perspective inscrite dans la durée. Consacrées à certains aspects de la cybercriminalité, de l'exploitation et des trafics de personnes, de la contrefaçon, des fraudes dans le monde sportif, ces contributions apportent à n'en pas douter des éléments de réflexion précieux à l'heure de la quête d'un univers marqué par de nombreuses vulnérabilités. Les développements relatifs à la lutte contre le blanchiment et à la transparence fiscale sont à cet égard particulièrement utiles, tant il demeure évident que l'argent constitue la finalité commune des diverses formes de criminalité organisée. C'est donc plus que jamais à ce nerf de la guerre qu'il convient de s'attaquer, sans pour cela négliger d'autres entrées dans les phénomènes criminels qui emportent indissolublement leur lot de violences. Pour en rester à l'approche financière, on ne saurait nier l'importance d'adaptations récentes apportées à nos dispositifs. Certaines d'entre elles ont été soulignées par la circulaire prise le 2 juin 2020 par le ministre de la Justice à propos de la lutte contre la corruption internationale. Ce document met à juste titre en évidence les profondes évolutions qu'à connu la Justice pour s'adapter à un contexte fort spécifique avec l'institution du parquet national financier (PNF), de l'Agence française anticorruption (AFA), du plaider-coupable et de la convention judiciaire d'intérêt public (CJIP). La finalisation de l'affaire Airbus fin janvier 2020, après une dizaine d'autres CJIP en quelques années, illustre l'ampleur du chemin parcouru en terme d'efficacité et de coopération internationale.

La prochaine entrée en fonctionnement du parquet européen au terme d'une gestation de près d'un quart de siècle devrait également représenter une étape significative porteuse d'enjeux essentiels.

On sait également combien la procédure pénale a été modifiée, notamment par l'attribution à des agents de l'administration fiscale de prérogatives judiciaires lourdes, quitte à bousculer certains des principes traditionnels du Droit français.

Ces adaptations citées ici parmi d'autres, pour conséquentes qu'elles soient, sont-elles suffisantes ? À l'évidence, la route demeure encore longue pour donner pleine efficacité à notre dispositif. Dans un univers en constante évolution, l'une des clés de la réussite réside certainement dans une capacité d'adaptation et d'innovation qui impliquent l'appui de moyens à la hauteur des grandes fraudes de dimension internationale. L'effort doit se poursuivre en ce sens.

Pour autant, cette indispensable impulsion au niveau central ne doit pas faire oublier la nécessité d'ajuster de façon globale les capacités de traitement de la Police et de la Justice. La lutte contre la criminalité organisée locale et régionale souffre d'une insuffisance chronique de moyens depuis des décennies, encore accentuée par la défection d'enquêteurs rebutés par des mécanismes procéduraux que l'on a fortement alourdis au fil des ans. Ces durées ne vont évidemment pas se réduire à la suite de la longue grève des avocats en début d'année immédiatement suivie du confinement du printemps. Comment se satisfaire des délais, comptés en années, pris par nombre de procédures, et peut-on imaginer combien de cas sont laissés de côté faute de capacité d'investigation dans un délai raisonnable ? C'est un autre chiffre noir qui explique à lui seul bien des dérives violentes dans certains territoires de la République que l'on peine à reconquérir ! L'enjeu est pourtant ici majeur si l'on veut vraiment emporter le combat contre les dérives maffieuses dont souffrent des quartiers entiers que certains cherchent à placer en coupe réglée en faisant refluer la police républicaine, quand ils ne se sentent pas suffisamment puissants pour venir régler leurs comptes au coeur de nos villes.

La centralisation parisienne des structures policières et judiciaires ne doit pas faire oublier l'importance des actions sur des réseaux locaux acteurs majeurs d'une dynamique économie souterraine. Le thème d'une excessive centralisation a été vigoureusement mis en évidence à propos des structures de soins. Il ne faudrait pas que la Justice s'inscrive, mutatis-mutandis, à contre courant alors que l'on mesure la difficulté de recruter et maintenir en Île-de-France les divers personnels, depuis les enquêteurs jusqu'aux agents pénitentiaires, qu'implique un jacobinisme judiciaire croissant. Entre autres mesures, le cadre des juridictions interrégionales spécialisées dans la lutte contre la criminalité organisée (JIRS) apparu en 2004, conciliant profondeur territoriale et proximité relative des phénomènes criminels, mériterait d'être actualisé et renforcé dans une stratégie d'ensemble favorisant le développement des capacités et initiatives locales ainsi que des diverses spécialisations. C'est à ce prix que notre dispositif pourra se hausser à la hauteur des enjeux.

COMITÉ SCIENTIFIQUE DE LA REVUE 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.

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

MARYVONNE LE BRIGNONEN,

DIRECTEUR DU SERVICE TRAITEMENT DU RENSEIGNEMENT ET ACTION CONTRE LES CIRCUITS FINANCIERS CLANDESTINS (TRACFIN)

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

L.R.D.G. : Quelle place a Tracfin dans le monde du renseignement français ?

Créé le 9 mai 1990[1], le service « Traitement du renseignement et action contre les circuits financiers clandestins » (Tracfin) participe à la protection de l'économie nationale et à la lutte contre les circuits financiers clandestins, le blanchiment de capitaux et le financement du terrorisme. Tracfin est à la fois la cellule de renseignement financier française (CRF) au sens des standards du Groupe d'action financière (GAFI) et un service de renseignement du premier cercle, placé sous la tutelle du ministre de l'Action et des Comptes publics et spécialisé en renseignement financier.

Les missions du Service ont évolué au fil du temps. D'abord dédié à la seule lutte contre le blanchiment de capitaux en 1990, Tracfin a vu son champ de compétence s'élargir à la lutte contre le financement du terrorisme en 2001 et les fraudes aux finances publiques (fraude fiscale en 2009 et fraude sociale en 2012).

Comme Service de renseignement, Tracfin est membre du Conseil National du Renseignement (CNR) depuis 2008 et coopère étroitement avec les autres services du premier cercle de la communauté française du renseignement[2] dont l'action est coordonnée par le Coordonnateur du renseignement et de lutte contre le terrorisme. En la matière, dans le cadre fixé par le Code de sécurité intérieure et sur la base des informations reçues, Tracfin a vocation à recueillir et traiter des renseignements relatifs notamment à la défense et la promotion des intérêts fondamentaux de la Nation, la prévention de toute forme d'ingérence étrangère, la défense des intérêts économiques, industriels et scientifiques majeurs de la France, la prévention du terrorisme, la prévention de la criminalité et de la délinquance organisées et la prévention de la prolifération des armes de destruction massive.

Tracfin reçoit des informations par 3 canaux : les déclarations de soupçon des professionnels assujettis au dispositif de lutte contre le blanchiment de capitaux, le financement du terrorisme (LCB/FT) ; les informations transmises par les différents organismes publics ou chargés d'une mission de service public ; les informations transmises par les cellules de renseignement financier (CRF) étrangères.

Les informations financières obtenues par Tracfin sont donc continues, fiables et objectives. Leur transversalité dans tous les

domaines du renseignement et l'expertise de Tracfin sont désormais reconnues au sein de la communauté du renseignement. Cette dynamique est le fruit d'une adaptation constante de l'organisation du service pour répondre aux impératifs de ses missions prioritaires et aux attentes de ses partenaires. Dans le cadre de l'adaptation permanente de Tracfin aux évolutions de ses missions, une cellule dédiée au renseignement fiscal a été créée fin 2019, permettant ainsi d'établir des synergies, un traitement rapide du renseignement et son orientation optimale.

L.R.D.G. : Tracfin a fêté ses 30 ans en février 2020. Comment s'explique l'accroissement soutenu de l'activité de votre Service ces dernières années ?

La pertinence et la qualité du renseignement financier est au coeur de l'efficience du dispositif de lutte contre le blanchiment de capitaux et le financement du terrorisme. Tracfin a adapté son organisation interne pour développer ses relations avec les professionnels assujettis au dispositif de lutte contre le blanchiment de capitaux, le financement du terrorisme (LCB/FT), mieux suivre l'activité déclarative et assurer auprès d'eux des retours réguliers sur les pratiques déclaratives et les points perfectibles. La pédagogie est la clé de voûte du système et Tracfin s'y emploie au travers de réunions bilatérales, des lignes directrices communes avec les autorités de contrôle et de publications (lettres d'information aux professionnels, rapport d'activité, rapport Tendances et analyses des risques BC/FT[3]).

Tracfin réalise un important travail sur les typologies pouvant être dégagées. Elles ont vocation à être partagées avec les services conformité des grands acteurs financiers français, améliorant d'autant leur capacité de détection. Ces derniers sont notamment conviés à des réunions dédiées afin de leur transmettre le retour d'expérience nécessaire à la bonne calibration de leurs capteurs.

Ces capteurs deviennent au fil des années de plus en plus efficaces. L'année 2019 a constitué une nouvelle année de forte progression de l'activité de Tracfin. Le service a reçu 99 527 informations en 2019 soit une progression de 25 % par rapport à 2018. En 2019, le service a réalisé 14 082 enquêtes, celles-ci ont débouché sur l'externalisation de 3 738 notes à l'autorité judiciaire et aux autres partenaires du service, soit une hausse de 34 % de notes diffusées en 1 an.

En 10 ans, le nombre de déclarations de soupçon reçues a été multiplié par 5 et le nombre de notes externalisées a été multiplié par 4. Sur cette même période, le nombre d'agents a été multiplié par 2,5. L'accroissement de l'activité de Tracfin s'explique aussi par le dynamisme du service et sa capacité d'adaptation pour répondre aux attentes de ses partenaires.

Entre 2015 et 2019, le nombre de notes administratives (sans infraction pénale caractérisée) a été multiplié par 10 en matière de financement du terrorisme et a doublé à destination des administrations responsables de la lutte contre les fraudes. Cette nette progression du nombre de transmissions spontanées s'explique notamment par la volonté de Tracfin de mieux exploiter et valoriser le volume croissant de renseignement financier dont elle est récipiendaire. Tracfin diversifie le partage de ses informations au profit de multiples destinataires, incluant des services de renseignement et des acteurs de lutte contre la fraude. En 2019, 39,6 % des notes disséminées par Tracfin l'ont été à destination des services de renseignement.

L.R.D.G. : Quels sont, selon vous, les principaux apports de la 5ème directive (UE) 2018/843 du Parlement européen et du Conseil du 30 mai 2018 modifiant la directive (UE) 2015/849 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme ?

La 5ème directive européenne de lutte contre le blanchiment des capitaux et le financement du terrorisme (LCB/FT) a été transposée en France par l'ordonnance n°2020-115, ainsi que par les décrets n°2020-118 et n°2020 -119 du 12 février 2020. Les principaux apports de ces textes résident notamment dans les évolutions relatives au périmètre des professionnels assujettis et aux missions et prérogatives de Tracfin.

Le périmètre des professionnels assujettis à la LCB/FT a évolué pour intégrer de nouvelles professions et modifier les obligations de professions déjà assujetties. Le champ des professions assujetties citées à l'article L561-2 du Code monétaire et financier (CMF) s'est étendu et inclut désormais deux nouvelles professions : les Caisses des règlements pécuniaires des avocats (CARPA) et les Greffiers des tribunaux de commerce (GTC). Les CARPA pouvaient déjà, depuis 2016, recevoir des demandes d'informations de la part de Tracfin. Ce dispositif,

très utile dans la conduite des investigations menées par le Service, est renforcé avec l'accord de la profession des avocats. Leur contrôle en matière LCB/FT a été confié à la commission de contrôle des CARPA.

L'assujettissement des GTC est, quant à lui, l'aboutissement d'un partenariat déjà bien établi : concernée par l'article L561-27 du CMF au titre des personnes chargées d'une mission de service public, la profession pouvait déjà adresser à Tracfin toute information nécessaire à l'accomplissement de sa mission. Leur rôle dans la transparence de la vie économique (tenue du Registre du commerce et des sociétés et du Registre des bénéficiaires effectifs) permettra à Tracfin de bénéficier d'informations essentielles sur des sociétés impliquées dans des schémas de fraude, de blanchiment ou tout autre infraction liée aux prérogatives du Service. Leur contrôle est assuré par le Conseil national des GTC.

D'autre part, le périmètre d'assujettissement de certaines professions a évolué : certaines succursales d'entités du secteur financier ainsi que les activités de conseil fiscal proposées par les professionnels du droit sont désormais incluses dans le champ des assujettis. En revanche, les professionnels des secteurs de l'art et de la location immobilière ne sont désormais assujettis aux obligations de LCB/FT que pour les transactions d'un montant égal ou supérieur à 10 000 € tandis que les syndics de copropriété sortent de l'assujettissement au dispositif LCB/FT.

Parallèlement, les missions et prérogatives de Tracfin évoluent. Les principales modifications du Code monétaire et financier concernant les missions et pouvoirs de Tracfin s'inscrivent dans l'optique :

– d'améliorer les capacités d'investigation du Service en lui permettant de mener des investigations sur des personnes mentionnées dans les communications systématiques d'informations (COSI prévues à l'article L. 561-15-1 du CMF) au même titre que sur les personnes mentionnées dans les déclarations de soupçon ou les informations reçues d'administrations ou de cellules de renseignement financier étrangères ;

– de renforcer les liens et les échanges d'informations entre Tracfin et ses partenaires. D'une part, le CMF prévoit désormais expressément la possibilité pour les services spécialisés du renseignement dit du « premier cercle » et les services de renseignement dits du « second cercle », d'adresser des informations à Tracfin (art L561-27 du CMF). D'autre part, il renforce les capacités de Tracfin à échanger avec les cellules de renseignement financier étrangères en précisant les conditions dans lesquelles ces dernières peuvent disséminer les informations transmises par le Service ;

– de consacrer juridiquement des pratiques du Service relatives à la protection et la confidentialité des informations : confidentialité du droit d'opposition (L561-24 du CMF) et protection des sources dans le cas des transmissions administratives effectuées par Tracfin (L561-30-1du CMF).

L.R.D.G. : Quelles sont les relations qu'entretient Tracfin avec l'Autorité de contrôle prudentiel et de résolution (ACPR) et l'Autorité des marchés financiers (AMF), qui concourent également à la lutte contre le blanchiment de capitaux et le financement du terrorisme ?

Tracfin entretient une coopération à deux niveaux avec l'ACPR et l'AMF : en amont, une coopération de nature institutionnelle donne lieu à des travaux réglementaires conjoints et à la diffusion de bonnes pratiques à destination des professions assujetties à la LCB/FT relevant de leur supervision respective ; celle-ci se répercute en aval sur une coopération de nature opérationnelle reposant sur des échanges d'informations réguliers prévus par l'article L561-28 du CMF.

Certaines des professions supervisées par l'ACPR et l'AMF sont également assujetties, au titre de l'article L561-2 du CMF, à la LCB/FT et donc tenues à l'envoi de déclarations de soupçon à Tracfin. Une coopération de nature institutionnelle entre Tracfin et l'ACPR d'une part, et Tracfin et l'AMF d'autre part, est donc indispensable pour élaborer des orientations communes et aiguiller au mieux sur les sujets relevant de la LCB/FT, les professions relevant de la supervision de l'ACPR ou de l'AMF.

Une coopération règlementaire est également instituée. Tracfin et l'ACPR publient des lignes directrices conjointes relatives aux obligations de déclaration et d'information à Tracfin, dont la dernière version a été actualisée en novembre 2018. Ce document explicite les dispositions du Code monétaire et financier relatives aux obligations des professionnels

assujettis supervisés par l'ACPR[4].

Les échanges entre les deux administrations se sont également renforcés par la présence de Tracfin aux réunions de la Commission consultative LCB/FT organisée par l'ACPR et par des discussions permanentes relatives à la rédaction des textes législatifs et réglementaires, notamment à l'occasion de la transposition des directives européennes anti-blanchiment.

En novembre 2019, l'AMF a publié ses nouvelles lignes directrices présentant les obligations s'imposant aux professionnels assujettis à la LCB/FT et placés sous sa supervision[5]. Bien que n'étant pas publiées conjointement par Tracfin et l'AMF, ces lignes directrices ont fait l'objet d'échanges fournis entre les deux Services.

Enfin, des actions communes de sensibilisation des professionnels assujettis sont menées. L'ACPR et Tracfin co-organisent des réunions annuelles réunissant les principaux établissements de crédit et de paiement de la place financière française, ainsi que leurs organisations professionnelles. Ces évènements permettent de présenter un bilan de l'activité déclarative des professionnels, de préciser les attentes du Service, d'aborder des sujets d'intérêts communs relatifs aux obligations de LCB/FT et de répondre aux interrogations des professionnels déclarants.

En outre, Tracfin est à l'initiative, depuis 2017, de réunions de place spécifiquement dédiées à la lutte contre le financement du terrorisme. Organisées conjointement avec l'ACPR, ces instances de dialogue réunissent également les principaux établissements de crédit, de paiement et de monnaie électronique. À la demande des participants, la fréquence de ces échanges s'accroît avec la mise en place d'un Comité dédié à la lutte contre le financement du terrorisme, dont la première réunion a eu lieu en décembre 2019.

Par ailleurs, Tracfin intervient lors de rencontres organisées par l'AMF à destination des professionnels assujettis placés sous sa supervision afin de leur rappeler leurs obligations de déclaration et de leur exposer des exemples de typologies de blanchiment observées par le Service.

Les actions de sensibilisation et l'élaboration de bonnes pratiques à destination des professions assujetties à la LCB/FT se matérialisent, en bout de chaîne, par des échanges d'informations de nature opérationnelle entre Tracfin et l'ACPR et Tracfin et l'AMF.

Sur le plan juridique, ces relations sont codifiées par le Code monétaire et financier qui prévoit, à l'article L561-28, l'échange mutuel de toute information entre Tracfin et ces autorités pouvant être utile à l'accomplissement de leurs missions respectives. Sur le fondement de cet article, Tracfin reçoit, en leur provenance, des informations résultant de contrôles sur place. En retour, Tracfin leur signale des éléments rendant compte du niveau et de la qualité des déclarations de soupçon (DS) traitées et de la réactivité des déclarants aux droits de communication adressés par le Service. Sur la base de ces signalements, elles sont à même de déclencher des contrôles et, le cas échéant, de sanctionner les établissements concernés.

Les professions assujetties supervisées par l'ACPR représentent la part la plus importante des DS reçues par Tracfin. L'enjeu principal de la relation entre Tracfin et l'ACPR consiste donc à définir le degré d'exigence mis en oeuvre par les établissements relevant de la supervision de l'ACPR afin d'optimiser la quantité et la qualité des DS (intérêt, pertinence, montant) traitées par Tracfin. L'objectif de ce travail conjoint est de préciser au maximum les critères justifiant l'envoi d'une déclaration de soupçon par les établissements financiers en recherchant le juste équilibre entre, d'une part, le respect des règles de conformité et d'autre part, l'envoi de déclarations pertinentes présentant un soupçon étayé et caractérisé.

Par ailleurs, un officier de liaison, détaché par l'ACPR, est également présent à Tracfin. Rattaché au Département de l'Analyse, du renseignement et de l'information (DARI), il coordonne les travaux conjoints entre les deux administrations et renforce la fluidité des échanges.

Les professions supervisées par l'AMF représentent un volume de déclarations de soupçon plus restreint que celui des établissements financiers. L'activité de Tracfin est donc plus réduite sur ces métiers que sur les métiers de banque commerciale et de financement supervisés par l'ACPR. Néanmoins, Tracfin et l'AMF coopèrent sur diverses typologies, en particulier sur des cas d'escroqueries aux faux investissements (options binaires, cryptoactifs) pour participer à l'identification de sites internet frauduleux susceptibles d'être inscrits à la « liste noire » de l'AMF. Les échanges sur ces sujets sont facilités par la désignation de

référents dans chacune des deux administrations et une convention de coopération signée en 2012.

En outre, l'AMF est en charge, depuis la loi n° 2019-489 relative à la croissance et à la transformation des entreprises du 22 mai 2019 (dite loi PACTE), de l'enregistrement ou, le cas échéant, de l'agrément, des prestataires de services en actifs numériques (PSAN) exerçant au moins une des dix activités listées à l'article L54-10-2 du CMF. Parmi ces activités figurent la conservation d'actifs numériques pour le compte de tiers, l'achat-vente d'actifs numériques contre une monnaie ayant cours légal ou l'échange d'actifs numériques contre d'autres actifs numériques. Les relations entre Tracfin et l'AMF sont donc naturellement amenées à se renforcer sur ce sujet.

L.R.D.G. : Quels sont les axes de priorité de Tracfin parmi les principaux risques de blanchiment de capitaux, de fraudes et de financement de terrorisme constatés ? Quelles stratégies développe Tracfin pour lutter contre ces risques, notamment dans le partenariat public-privé ?

Les efforts du Service portent donc aussi bien sur le maintien de ses capacités de lutte contre le blanchiment de capitaux issus d'activités illicites (criminalité organisée, atteintes à la probité, délinquance économique, financière ou astucieuse, infractions à la législation sur les stupéfiants), le financement du terrorisme, les atteintes aux intérêts fondamentaux de la Nation et la lutte contre les fraudes fiscale et sociale.

En 2019 et 2020, le Service a adapté son activité pour appréhender plus activement les typologies de blanchiment associées à l'usage de produits et services financiers numériques. La cybercriminalité ne constitue pas nécessairement un nouveau type de criminalité mais recycle des formes traditionnelles de criminalité (vol, fraude, escroquerie) pour les recomposer en ligne. Dès lors, resserrée autour de son caractère financier, la notion de cybercriminalité financière peut être considérée, au sens large, comme l'ensemble des activités financières illicites réalisées au moyen d'une atteinte à un STAD ou ayant pour vecteur un STAD.

Les cybercriminels exploitent, pour cela, les failles contenues dans l'émergence, favorisée par la libéralisation des services financiers, d'un écosystème d'acteurs que l'on peut regrouper dans la catégorie des *Fintech*, voire des *Big Tech* lorsqu'il s'agit des produits et services financiers proposés par les géants du web américains ou chinois. Ces derniers exercent essentiellement en France en tant que prestataires de services de paiement (EP), de monnaie électronique (EME) ou sur actifs numériques (PSAN) depuis un État tiers de l'Espace économique européen grâce au passeport européen et au régime de la libre prestation de services.

Dévoyés à des fins frauduleuses, ces nouveaux acteurs du paiement brouillent la traçabilité des flux et réduisent les capacités d'analyse des établissements de crédit sur les transactions de leurs clients. Privilégiant par nature les relations à distance et favorisant l'usage d'identités falsifiées ou usurpées, ils ne disposent pas de la même culture de conformité que les établissements de crédit et posent des difficultés de contrôle aux superviseurs nationaux, du fait du passeport européen.

Pour renforcer ses moyens d'action, Tracfin s'est doté, en 2018, d'une division d'enquête composée d'agents spécialisés en cybercriminalité financière. Cette équipe a développé des compétences pour retracer les transactions financières effectuées sur la *blockchain* et identifier les flux financiers résultant d'opérations délictueuses commises sur le *clear, deep* comme sur le *dark web*. Leur action repose sur une étroite coopération avec les services d'enquêtes spécialisés (douane, police, gendarmerie) et les homologues de Tracfin à l'étranger.

En outre, le renforcement du renseignement fiscal constitue, depuis le début de l'année 2020, un nouvel axe de travail de Tracfin. La lutte contre les fraudes fiscales et sociales constitue une priorité nationale, expressément identifiée dans la nouvelle stratégie nationale du renseignement. Elle vise notamment à renforcer les capacités de lutte contre l'évasion fiscale dont l'ampleur porte préjudice à la société et aux intérêts fondamentaux de la Nation. Tracfin joue un rôle de détection important grâce, en particulier, à la coopération internationale permettant d'identifier des comptes ou avoirs détenus à l'étranger et aux compétences de ses agents issus pour partie de l'administration fiscale.

Au sein du ministère de l'Action et des Comptes publics, une « Task-force renseignement fiscal », composée d'agents de la direction générale des Finances publiques (DGFiP), de la Direction nationale du renseignement et des enquêtes douanières (DNRED) et de Tracfin, a été créée fin 2019, afin de mutualiser et coordonner de l'information pour

des dossiers communs en vue de leur judiciarisation. Ces dossiers portent sur les thématiques suivantes : e-commerce, carrousel de TVA, avoirs détenus à l'étranger et avoirs transférés depuis et vers l'étranger. À cette fin, Tracfin a créé une cellule dédiée au renseignement fiscal fin 2019.

Pour mener à bien ces missions, la nature de l'activité de Tracfin suppose un partenariat public-privé de qualité afin d'assurer la réception d'informations exploitables et pertinentes en provenance du secteur privé financier comme non-financier. Dans le cadre de leurs enquêtes, et pour reconstituer l'ensemble des transactions d'une personne physique ou morale, les agents de Tracfin sont amenés à exercer des droits de communication auprès des différentes personnes assujetties, conformément aux dispositions de l'article L561-25 du CMF. Le Service peut également émettre des appels à vigilance afin de leur signaler des personnes ou opérations présentant un risque important de BC/FT.

En retour, Tracfin s'est employé à renforcer son organisation pour mieux dialoguer avec les professions assujetties. Depuis 2015, chaque groupe bancaire ou chaque profession assujettie dispose d'un référent au sein du Service, qui est son point de contact privilégié. Le référent sensibilise les professionnels des secteurs financiers et non-financiers à leurs obligations en termes de LCB/FT, les assiste dans leurs démarches, suit leur activité déclarative et leur assure un retour régulier. Un bilan d'activité par groupe bancaire, ainsi qu'avec les principaux ordres professionnels des professions non-bancaires, est réalisé chaque année. Il en résulte une amélioration quantitative et qualitative du flux déclaratif pour la plupart des professions assujetties.

Tracfin diffuse, en outre, de nombreux supports d'informations afin d'aiguiller au mieux les professionnels assujettis dans leurs propres classifications des risques et processus de conformité. Chaque année, le Service publie deux rapports : un rapport d'activité qui fait un bilan de l'activité déclarative des professionnels assujettis au dispositif de LCB/FT et qui présente des cas typologiques marquants mettant en relief l'action de déclarants et un rapport d'analyse des risques qui s'adresse aux déclarants comme aux autorités compétentes et au grand public. Des éléments de contexte et de nombreux cas typologiques sur les risques identifiés y sont décrits. La diffusion d'éléments d'information auprès des déclarants se fait également par le biais de lignes directrices détaillées édictées conjointement par Tracfin et les autorités concernées, ainsi que par des lettres d'informations ciblées auprès de certaines catégories de professionnels.

L.R.D.G. : Quelles sont les difficultés particulières de la lutte contre le blanchiment d'argent et le financement du terrorisme dans le secteur de l'art ?

Le secteur du marché de l'art constitue un secteur à risque élevé en matière de blanchiment de capitaux et de financement du terrorisme, compte-tenu de l'opacité de certaines pratiques. En particulier, ce secteur se distingue notamment par une fréquence importante des paiements en espèces[6], des prix de vente extrêmement volatiles et un fort développement des enchères et ventes en ligne, qui facilitent le trafic d'oeuvres d'art et opacifie la traçabilité des biens.

Par ailleurs, la présence à l'international des grandes maisons de vente d'art est de nature à contourner les actions de contrôle et de suivi des oeuvres mises sur le marché, et des flux financiers qui en découlent. Le recours à des sociétés et/ou des comptes *offshores* par certains acheteurs et vendeurs ne permet pas d'assurer une traçabilité des oeuvres vendues et des fonds utilisés.

Enfin, la mobilisation encore très limitée des professionnels au dispositif LCB/FT, notamment des commissaires-priseurs judiciaires et des opérateurs de vente volontaire, qui adressent peu de déclarations de soupçon au regard du dynamisme et des enjeux financiers liés au marché de l'art est soulignée. L'implication des professionnels semble inversement proportionnelle à leur chiffre d'affaires, et donc à leur exposition aux risques de BC/FT, bien qu'une meilleure implication des maisons de ventes soit à noter[7]. Sur le plan qualitatif, les déclarations de soupçon en provenance des professionnels du secteur de l'art sont également perfectibles. Elles ne comportent le plus souvent qu'une analyse succincte du soupçon et sont rarement assorties de pièces-jointes, rendant difficile leur exploitation par Tracfin.

Afin d'atténuer les vulnérabilités du marché de l'art en termes de BC-FT et améliorer la pratique déclarative du secteur, Tracfin a entrepris plusieurs actions de sensibilisation des professionnels assujettis. Tracfin consacre systématiquement une partie de son rapport annuel d'activité aux professionnels de l'art avec

un bilan déclaratif de l'année écoulée. Par ailleurs, le rapport Tendances et analyse des risques LCB/FT 2017-2018 a dédié une partie au secteur de l'art. Enfin, la lettre d'information aux professionnels de Tracfin n°16 de juin 2018 porte sur la lutte contre le blanchiment et le financement du terrorisme dans le secteur de l'art[8].

L.R.D.G. : Le blanchiment d'argent étant par nature international, quelles sont les modalités d'échanges internationaux d'informations ? Des mesures vous semblent-t-elles nécessaires pour améliorer la qualité des échanges ?

L'activité de Tracfin s'inscrit dès l'origine dans un cadre international. Les dispositifs de lutte contre le blanchiment de capitaux et le financement du terrorisme sont nés en 1989 de la décision du G7 de créer le Groupe d'action financière (GAFI), dont le rôle est de définir des normes pour l'organisation de dispositifs nationaux de LCB/FT (les 40 Recommandations du GAFI), et de promouvoir la bonne application de ces normes à travers un système de contrôle entre pairs (les évaluations mutuelles). Une grande partie de ces Recommandations, juridiquement non contraignantes, a été transposée dans les droits nationaux via, en Europe, des directives européennes.

La création, dans chaque pays, d'une Cellule de Renseignement Financier (CRF) - telle que Tracfin en France - est prévue par ce dispositif. Ce cadre normatif s'est progressivement étoffé, élargissant les pouvoirs et le périmètre d'action des CRF. Au plan international, le GAFI a ainsi affiné ses Recommandations, enrichies en 2001 des mesures de lutte contre le financement du terrorisme. À l'échelle européenne, l'Union européenne a publié cinq directives anti-blanchiment en 1991, 2001, 2005, 2015 et 2018.

À l'échelle mondiale, l'échange d'informations entre CRF fonctionne bien ; il repose sur un outil mis à disposition de ses 164 CRF membres par une organisation de CRF dénommée Egmont Group of Financial Intelligence Units (le groupe EGMONT). Il permet de sécuriser et fluidifier les échanges internationaux opérationnels d'informations. Soumis au principe de réciprocité, l'échange veut que le demandeur ne sollicite que des informations qu'il serait lui-même susceptible d'obtenir dans son pays.

La qualité de la coopération demeure toutefois variable selon les pays et leurs capacités d'identification des acteurs et d'accès, sur demande, aux informations détenues par les assujettis et les autorités compétentes.

À ce titre, le développement d'outils permettant d'accéder aux informations sur les comptes bancaires, de registres des bénéficiaires effectifs et la généralisation de la possibilité d'interroger les assujettis sur simple demande d'une CRF apparaissent comme des vecteurs clés de l'amélioration de la coopération internationale.

Les évolutions portées dans l'Union européenne par la 4ème directive bis[9] vont dans ce sens. Elle oblige par exemple chaque État membre à mettre en place des registres ou systèmes permettant l'identification de toute personne physique ou morale détenant des comptes de paiement et des comptes bancaires, les cellules de renseignement financier (et les autorités compétentes) devant pouvoir accéder en temps réel aux données qu'ils contiennent.

Elle prévoit également l'obligation de mettre à disposition, au sein d'un registre accessible aux CRF (et aux autorités compétentes en matière de lutte contre la criminalité financière), les informations permettant l'identification de toute personne physique ou morale détenant des biens immobiliers.

Parmi d'autres, ces avancées européennes sont un gage de progrès pour la LCB/FT.

L.R.D.G. : Cette année, le dispositif français de lutte contre le blanchiment de capitaux et le financement du terrorisme est évaluée par le Groupe d'action financière (GAFI) dans le cadre du quatrième cycle d'évaluations mutuelles. Comment Tracfin s'engage à la préparation de cette évaluation ?

L'une des principales missions du GAFI est d'élaborer des normes – les « Recommandations » - et de promouvoir l'application efficace de mesures législatives et opérationnelles en matière de lutte contre le blanchiment de capitaux, le financement du terrorisme (LBC/FT) et les autres menaces liées pour l'intégrité du système financier international. Il évalue à cet égard les progrès réalisés par ses membres dans la bonne mise en oeuvre des Recommandations.

Cette évaluation est conduite par des experts évaluateurs issus des différentes juridictions et organisations membres du GAFI (et des organismes régionaux de type GAFI) et s'appuie sur une méthodologie produite par l'organisation. Le cycle actuel d'évaluation (2014-2022) se

concentre sur l'analyse de l'efficacité des systèmes nationaux.

Les forces et les faiblesses du dispositif français de LBC/FT seront présentées et analysées dans le rapport d'évaluation mutuelle que le GAFI publiera à l'issue de la Plénière de juin 2021, à la suite d'un rigoureux processus d'évaluation technique et opérationnelle par une équipe d'évaluateurs francophones. Cette évaluation se déroule en deux phases : une évaluation technique sur pièces à partir d'un dossier remis par les autorités françaises entre le mois de décembre 2019 et le premier semestre 2020[10], et une visite sur place destinée à apprécier l'efficacité du dispositif national, initialement prévue à l'été 2020 et repoussée à l'automne 2020 en raison de la pandémie de Covid-19.

Selon la méthodologie du GAFI, l'évaluation et la compréhension des risques de BC/FT par le pays et les différents acteurs, publics ou privés, ainsi que la mise en oeuvre de mesures fondées sur ces risques constituent le socle fondamental d'un système efficace. Ainsi, les autorités françaises réunies au sein du Conseil d'orientation de la lutte anti-blanchiment (COLB), ont élaboré une analyse nationale des risques (ANR), qui a fait l'objet d'une publication en septembre 2019. Le COLB joue un rôle central dans la préparation et la conduite de l'évaluation mutuelle de la France, en assurant le pilotage interministériel de l'exercice et la mobilisation de l'ensemble des acteurs concernés, dont Tracfin.

À cet égard, le COLB a constitué une *task force* responsable de la préparation opérationnelle des différentes étapes de l'évaluation et de la mise en cohérence des réponses préparées. Sous l'égide du Président du COLB et de la Direction générale du Trésor, qui assure le Secrétariat du COLB, elle rassemble les services et administrations concernés au premier chef par cet exercice (notamment ACPR, AMF, DGDDI, DGFiP, ministère de l'Intérieur, DCPJ, DGGN, ministère de la Justice, et bien évidemment Tracfin). Ses membres, qui se réunissent à fréquence hebdomadaire, peuvent également s'appuyer sur un réseau de « référents GAFI » désignés au sein de chaque direction ministérielle.

Tracfin participe ainsi très activement à la préparation de cette évaluation, notamment en contribuant à la rédaction du dossier déjà remis aux évaluateurs qui décrit les bases juridiques encadrant les missions et les pouvoirs du Service, ainsi que le fonctionnement opérationnel de la CRF. Tracfin se prépare désormais à accueillir l'équipe d'évaluation dans ses murs afin de faire la démonstration de son efficacité dans l'exercice quotidien de ses missions au service de la lutte contre toutes les formes de criminalité financière.

Notes :

1 Décret du 9 mai 1990 portant création d'une cellule de coordination chargée du traitement du renseignement et de l'action contre les circuits financiers clandestins.

2 Les services spécialisés de renseignement sont la direction générale de la sécurité extérieure (DGSE), la direction générale de la sécurité intérieure (DGSI), la direction du renseignement militaire (DRM), la direction du renseignement et de la sécurité de la défense (DRSD), la direction nationale du renseignement et des enquêtes douanières (DNRED) et le service de traitement du renseignement et d'action contre les circuits financiers clandestins (TRACFIN).

3 www.economie.gouv.fr/tracfin

4 Les établissements de crédit, les établissements de paiement, les établissements de monnaie électronique, les sociétés de financement, les organismes d'assurance vie et non-vie, les courtiers en assurance, les intermédiaires en opérations de banque et en services de paiement (IOBSP), les entreprises d'investissement et les changeurs manuels.

5 Les sociétés de gestion de portefeuille (SGP), conseillers en investissements financiers (CIF), conseillers en investissements participatifs (CIP), dépositaires centraux et gestionnaires de systèmes de règlement/livraison.

6 décret n°2015-741 du 24 juin 2015. L'interdiction des paiements en espèces au-delà de 1 000 € n'est applicable qu'aux résidents français. Les résidents étrangers, très représentés dans le secteur de l'art, peuvent régler leurs achats en liquide jusqu'à un plafond de 15 000 €.

7 La meilleure implication des maisons de ventes réalisant les transactions les plus importantes permet une diversification des typologies (ex : absence de concordance entre l'adjudicataire et le titulaire du compte émetteur du paiement ; difficulté d'identification du bénéficiaire effectif de la transaction du fait de l'utilisation de comptes/structures offshore ; présentation par des acheteurs étrangers de plusieurs passeports ; tentatives de paiement en espèces au-delà des seuils autorisés ; ordres d'achat passés pour des montants bien supérieurs au cours du bien concerné ; fraudes fiscales).

8 Ce document de 16 pages, disponible en ligne, expose notamment les risques LCB-FT du secteur de l'art, des typologies de blanchiment avec des critères d'alerte, ainsi qu'un point sur la réglementation LCB-FT qui s'impose au secteur.

9 Directive (UE) 2018/843 du Parlement européen et du Conseil du 30 mai 2018 modifiant la directive (UE) 2015/849 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme ainsi que les directives 2009/138/CE et 2013/36/UE. Cette directive a été transposée en France par une ordonnance ainsi que deux décrets d'application publiés le 13 février 2020.

10 Les pays évalués sont appelés à remettre deux documents : tout d'abord une analyse de leur corpus législatif et réglementaire et de leur cadre institutionnel LBC/FT, selon la grille de lecture et les exigences spécifiques définies par les 40 Recommandations du GAFI ; ensuite, un dossier d'auto-évaluation de l'efficacité qui doit souligner la bonne mise en oeuvre de ces Recommandations et à « déterminer dans quelle mesure [le] pays obtient un ensemble de résultats qui sont essentiels à la solidité d'un système LBC/FT. »

QUEL CADRE LÉGAL POUR LUTTER EFFICACEMENT CONTRE LA CONTREFAÇON CRIMINELLE ?

MARION BRIATTA

DOCTEURE EN DROIT - ENSEIGNANTE ET CHERCHEUSE
AFFILIÉE À SCIENCES PO

Effet collatéral de la crise sanitaire mondiale liée au COVID-19, le trafic de contrefaçons connut une recrudescence alarmante ces derniers mois[1]. Les alertes sont venues de toute part et notamment du Conseil de l'Europe qui publia le 8 avril dernier un avis à l'attention des gouvernements les invitant à la plus grande vigilance face à la contrefaçon ou la falsification des médicaments et des produits médicaux[2].

À première vue, la distinction entre la contrefaçon d'un médicament et sa falsification frôle le pléonasme. Sous l'angle du droit de la propriété intellectuelle, il existe pourtant une différence importante entre ces deux concepts. En effet, bien que souvent associée à l'idée de faux produits, la contrefaçon interagit moins avec la notion d'authenticité qu'avec celle de licéité. Une contrefaçon n'est pas nécessairement un faux produit, mais consiste simplement dans un objet fabriqué et commercialisé sans le consentement de celui qui a le droit exclusif de le faire. Ce droit exclusif peut prendre des formes diverses, qu'il s'agisse d'un droit de brevet, d'un droit de marque, de dessin ou modèle ou encore d'un droit d'auteur. Bien que différents, ces droits de propriété intellectuelle tendent tous à conférer à leur titulaire un monopole leur permettant d'exploiter de manière exclusive et pendant une durée limitée, les utilités économiques de leur création immatérielle, pourvu que celle-ci rencontre un public intéressé. Le titulaire d'un brevet de médicament bénéficie par exemple d'un monopole sur le principe actif du médicament lui permettant d'interdire aux tiers la fabrication et le commerce de produits pharmaceutiques incorporant le principe actif breveté pendant une durée de vingt ans. La valorisation des droits de la propriété intellectuelle est conditionnée par cette faculté du titulaire de droit d'exclure autrui de son périmètre réservé et très fréquemment d'en monnayer l'accès. La contrefaçon consiste tout simplement dans le fait de surmonter cette exclusion, elle est un *« acte d'empiétement sur le monopole »* du titulaire d'un droit de propriété intellectuelle[3].

Si aujourd'hui, l'essentiel du contentieux de la contrefaçon oppose avant tout des concurrents cherchant à défendre et à étendre leur monopole sur le marché, on assiste depuis plusieurs années à l'essor d'une contrefaçon d'un nouveau type trahissant une implication croissante d'organisations criminelles. Face à celles-ci les mesures répressives prévues par le droit de la propriété intellectuelle peinent à produire un effet dissuasif et s'avèrent même largement inadaptées, suggérant la nécessité d'une refonte du cadre légal de lutte anti-contrefaçon.

I. La contrefaçon, « l'activité criminelle du XXIe siècle »

Imbriquée au sein d'une délinquance économique complexe, la contrefaçon criminelle est aujourd'hui alimentée par la mondialisation au point d'être souvent présentée comme la face obscure de celle-ci[4]. Elle n'est plus le fait de

quelques individus spécialisés dans la reproduction artisanale de produits de luxe, mais est au contraire devenue une activité de trafic décentralisée, déhiérarchisée et axée sur les biens de grande consommation. Ce trafic prospère à partir d'un réseau horizontal d'intermédiaires divers localisés dans le monde entier et grâce à une implication croissante des organisations criminelles.

Participant d'une véritable économie parallèle, le trafic de contrefaçons obéit à une stratégie de prix fondée sur le contournement systématique des réglementations étatiques liées à la vente de marchandises, qu'il s'agisse des normes sanitaires, fiscales ou encore des lois sur la propriété intellectuelle. L'imitation de produits originaux se présente ainsi comme un moyen et non comme une fin pour les contrefacteurs dont l'objectif consiste avant tout à répondre à une demande croissante de produits à bas prix[5]. L'enjeu central structurant l'activité des organisations criminelles est de répondre à cette demande tout en minimisant les risques de saisie en recourant à de nombreux intermédiaires et à des sociétés écrans. La libéralisation des échanges internationaux et l'optimisation des écarts de réglementation entre chaque État en matière de propriété intellectuelle se présentent à cet égard comme un avantage décisif pour les organisations criminelles qui ont fait de la contrefaçon une source de revenu intégrée au coeur de leur plan de développement[6].

Il en résulte une croissance endémique du trafic de contrefaçons. Bien que son caractère occulte la rende très difficile à mesurer, on estime ainsi que la contrefaçon aurait bénéficié d'une croissance huit fois supérieure à celle du commerce légitime depuis le début des années 1990[7]. Alors que ce trafic ne représentait que 2,5 % du commerce mondial en 2013, il est aujourd'hui évalué à plus de 3,3 % du commerce mondial et représente près de 7 % des importations de l'Union européenne depuis les pays tiers[8]. Certains spécialistes estiment à cet égard que la contrefaçon *« deviendra l'activité criminelle du XXIe siècle »*[9].

II. Un trafic devenu incontrôlable

Devenue la deuxième source de revenus des organisations criminelles après le trafic de stupéfiants, la contrefaçon présente l'intérêt majeur d'être un trafic à la fois extrêmement rentable et peu risqué. Le risque judiciaire s'avère en effet quasiment nul pour des organisations criminelles ayant trouvé dans la contrefaçon une manne financière illimitée dont elles peuvent profiter quasiment sans entrave. Loin d'être une évidence, cette impunité se présente au contraire comme un véritable paradoxe compte tenu des très nombreux dispositifs de lutte anti-contrefaçon développés dans le monde depuis les années 1980.

La réponse des pouvoirs publics à ce phénomène endémique et mondialisé fut en effet conçue dès l'origine comme devant intervenir à une échelle globale. À la suite d'intenses et longues négociations internationales, la conclusion au sein de l'Organisation mondiale du commerce (OMC) de l'Accord sur les Aspects des droits de Propriété Intellectuelle qui touchent au commerce (ADPIC) dans les années 1990 harmonisa les dispositifs répressifs des États signataires en matière de contrefaçon. Devant agir comme un tamis entravant la circulation des marchandises de contrefaçon au sein des marchés mondialisés, les mesures coercitives consacrées par les ADPIC peinèrent cependant à contrer la croissance endémique de la contrefaçon criminelle[10].

La France ne fait pas exception à ce constat d'échec et témoigne, à l'instar de ses partenaires commerciaux, d'une forme d'impuissance face à un trafic illicite devenu incontrôlable. Engagé à partir des années 1990 dans une pénalisation effrénée de la contrefaçon, le législateur français a pourtant multiplié les sanctions à tel point que notre régime répressif en la matière est devenu l'un des plus sévères au monde[11]. Depuis 2004, ce ne sont pas moins de sept lois qui furent votées en la matière, diversifiant, multipliant et aggravant les sanctions de la contrefaçon[12]. Dans ce court laps de temps, les peines maximales encourues par les contrefacteurs sont ainsi passées de deux à sept ans de prison et de 150 000 € à 750 000 € d'amende[13]. Cette pénalisation à outrance de la contrefaçon s'accompagna de l'émergence d'un régime douanier inédit consistant à assimiler la contrefaçon à un trafic international de marchandises de contrebande. À la faveur de l'adoption de règlements douaniers européens[14], les douanes se virent ainsi confier une *« mission de police économique »*[15] consistant à surveiller le flux de marchandises entrant sur le territoire douanier européen afin de protéger les intérêts des titulaires de droits non sans que cela soulève d'ailleurs quelques étonnements des spécialistes du droit douanier[16].

Si les textes ne manquent pas d'ambition, leur mise en oeuvre s'avéra cependant largement aléatoire et sporadique. Au plan pénal,

les juges peinent à identifier la contrefaçon comme étant une atteinte à l'intérêt général et manifestent à l'égard de celle-ci une certaine *« timidité »*[17]. Représentant moins de 10 % du contentieux global des droits de la propriété intellectuelle, le contentieux pénal de la contrefaçon demeure résiduel, les quelques peines prononcées par les juridictions répressives s'avérant souvent dérisoires[18] et se concentrant presque exclusivement en droit des marques[19]. Un décalage étonnant se forma ainsi entre les ambitions politiques du dispositif répressif de la contrefaçon et la marginalité de son contentieux que les titulaires de droits ne semblent d'ailleurs pas enclins à privilégier.

Le dispositif douanier de lutte anti-contrefaçon produit des résultats tout aussi modestes et ce, en raison de deux freins majeurs à l'action des douanes. D'une part, car le contrôle douanier s'exerce sur une partie infime du flux des marchandises entrant sur le territoire douanier européen, les douanes étant donc limitées structurellement dans leur capacité d'interception des contrefaçons. D'autre part, en raison des nouveaux modes de distribution des contrefaçons dont le commerce s'effectue de plus en plus à travers les plateformes de vente en ligne. Internet est même devenu le premier canal de diffusion des marchandises contrefaisantes, les trafiquants ayant très tôt compris l'intérêt d'un tel mode de distribution qui permet d'être directement en contact avec le consommateur, de réduire les intermédiaires et donc de minimiser les risques de contrôle. Distribuées par le biais de petits colis, les contrefaçons deviennent de plus en plus dures à intercepter et à localiser et le trafic prospère allègrement.

III. Des sanctions non dissuasives

Comme nous l'avons évoqué plus haut, la contrefaçon se présente de nos jours comme un trafic mondialisé opérant selon un processus commercial similaire à celui de l'industrie licite. La France est ainsi visée par les trafiquants en raison du marché qu'il abrite, les infractions de contrefaçon commises sur le territoire français étant essentiellement des faits attachés à la commercialisation des marchandises contrefaisantes et non à leur fabrication que l'on sait être réalisée pour l'essentiel en dehors de l'Union européenne[20]. À défaut de pouvoir appréhender le phénomène à sa source, la lutte contre la contrefaçon se structura dès lors autour du consommateur pris en sa qualité de destinataire final de la marchandise contrefaisante. Le consommateur se présente ainsi comme le pivot décisif d'une lutte menée à l'encontre d'un phénomène protéiforme au sein duquel il apparaît comme la seule constante. Dissuader le consommateur d'acheter une contrefaçon est en effet la manière la plus simple de lutter contre un trafic qui peut certes survivre à la perte d'un distributeur, mais non à celle de la demande.

La dissuasion du consommateur de contrefaçons se déploya sur deux niveaux. Elle consista d'une part, à l'informer sur les risques attachés à l'achat de contrefaçon, et procéda d'autre part, d'un recours appuyé à la fonction dissuasive des sanctions pénales et douanières de la contrefaçon. Coïncident par conséquent deux images a priori contradictoires du consommateur. Il est à la fois le *consommateur victime*, trompé quant à la qualité et l'origine de la marchandise et le *consommateur voyou* tirant complaisamment profit de l'aubaine économique que représente la contrefaçon. La fonction dissuasive des peines de la contrefaçon souffre de ce discours ambigu souhaitant réprimer l'avantage retiré par le consommateur d'un trafic dont il est supposé être la première victime. Une étude de l'Union des Fabricants pour la lutte contre la contrefaçon (UNIFAB) menée en 2012 a révélé que si *« la notoriété du risque encouru par le consommateur de* contrefaçon *est certes quasi unanime, celui-ci est essentiellement centré sur le danger santé/sécurité (25 à 40 %), tandis que la sanction n'apparaît pas comme un risque prioritaire (13 %) »*[21]. Une autre étude a pu montrer que les consommateurs français ont tendance à rattacher la contrefaçon *« à la dimension « revanche sur les grands groupes », le consommateur français considérant comme amusant de défier les grands groupes qui commercialisent leurs marques à des prix jugés prohibitifs ».*[22]

Face à cette indifférence notable des consommateurs à l'aggravation des sanctions de la contrefaçon, on peut s'interroger sur le bienfondé d'une telle approche répressive. À plus forte raison que celle-ci ne produit pas plus d'effet dissuasif sur les contrefacteurs criminels. Ce *"paradoxe de la contrefaçon"* poussa même certains spécialistes à se demander si la pénalisation à outrance de la contrefaçon ne conduirait pas finalement à aggraver le phénomène criminel qu'elle entend précisément endiguer[23].

IV. L'*effet boomerang* de la prohibition légale de la contrefaçon

Toute prohibition légale imposée sur des biens de consommation

entrave l'accès à ceux-ci en imposant un risque pénal sur les distributeurs de ces marchandises. Elle crée de ce fait un marché pour les organisations criminelles dont le *corps de métier* consiste justement à assumer ce risque pénal. Pour être efficace, une prohibition doit dès lors être en mesure d'infliger aux acteurs du trafic un risque pénal supérieur au profit qu'ils sont susceptibles de retirer de la vente des marchandises prohibées[24]. À défaut, la prohibition légale est non seulement inefficace, mais risque au surplus d'aggraver la criminalisation du phénomène qu'elle entend endiguer[25]. Cet *effet boomerang* attaché à toute prohibition légale a pu être étudié en matière de lutte contre les stupéfiants[26], et fut identifié dès les négociations ayant entouré l'élaboration des ADPIC à l'occasion de laquelle de nombreux observateurs soulignèrent le caractère potentiellement néfaste d'une pénalisation croissante de la contrefaçon[27].

Parce que la contrefaçon est une activité économique avant d'être un phénomène criminel, le durcissement des sanctions pénales de la contrefaçon peut en effet avoir pour effet pervers d'encourager la criminalisation de celle-ci. La production illicite de marchandises de contrefaçon réclame des investissements conséquents que seules les plus grandes organisations criminelles sont à même de fournir. À mesure que le régime pénal se durcit, le risque pénal pour le contrefacteur augmente. Dès lors, seules les plus grosses organisations criminelles pourront à terme se permettre de courir le risque de commercialiser des marchandises contrefaisantes[28]. Le développement du marché occulte sur lequel sont écoulées les contrefaçons est en outre aggravé par l'inefficacité de la réponse pénale qui peine à produire un effet dissuasif sur les contrefacteurs. En France, on observe en effet une *« timidité »* des juges pénaux qui, compte tenu de la violence quotidienne à laquelle ils ont à faire, peinent à considérer les atteintes aux droits de la propriété intellectuelle comme étant des infractions majeures. Dans son référé sur la politique publique de lutte contre la contrefaçon, la Cour des comptes a ainsi relevé que de *« nombreuses critiques sont émises sur l'insuffisance (…) des condamnations par les milieux professionnels, voire les administrations chargées de l'action répressive »*[29]. Or, et comme nous allons le voir à présent, cette mise en oeuvre insuffisante du dispositif répressif de la contrefaçon procède moins de l'incurie des juridictions répressives ou de l'Administration des Douanes que de la conception baroque et imparfaite du cadre légal de lutte anti-contrefaçon.

V. Un cadre légal à réinventer

En matière de propriété intellectuelle, les législations étrangères et notamment anglo-saxonnes distinguent clairement l'*infringement* désignant la violation des droits de propriété intellectuelle et les cas de *counterfeiting* désignant plus spécifiquement le trafic de marchandises illicites. Bien qu'intéressant tous deux la violation d'un droit de brevet, on perçoit en effet intuitivement que la *« guerre des brevets »*[30] opposant des concurrents comme Apple et Samsung[31]recouvre des enjeux différents de ceux soulevés par un trafic de médicaments contrefaisants pouvant affecter la santé des consommateurs. Le droit français ignore pourtant une telle distinction et aborde ces différents problématiques sous le qualificatif unique de *contrefaçon*, n'hésitant pas à s'en remettre au pouvoir d'appréciation des juges pour départager la contrefaçon criminelle du reste du contentieux de la propriété intellectuelle. Considérant que *« la contrefaçon doit être sanctionnée dès le premier euro. C'est du moins ce que la loi doit afficher »*[32], le législateur français ne transposa d'ailleurs pas le critère de l'*« échelle commerciale »* consacré par les textes internationaux et européens selon lesquels seuls les actes de contrefaçon commis à une échelle commerciale doivent donner lieu à des poursuites pénales[33]. Il n'existe donc pas au plan juridique de critère de distinction effectif entre la fraude commerciale procédant du trafic international de marchandises illicites et la violation de droit réel organisant l'appropriation d'actifs immatériels.

Amalgamant le régime pénal et douanier de la contrefaçon au régime civil des droits de propriété intellectuelle, le droit français de la propriété intellectuelle postule au contraire une équivalence de principe entre la répression de la contrefaçon et la sanction civile des droits de propriété intellectuelle. Des faits aussi différents que le trafic international de contrefaçons dangereuses pour la santé des consommateurs, le téléchargement illégal, la violation d'un contrat de licence de marque, l'atteinte au droit moral de l'auteur, les importations parallèles, le *camrecording* ou encore le transit

de médicaments génériques par le territoire européen furent ainsi indifféremment qualifiés de *contrefaçons* par la seule coïncidence de consommer une atteinte à un droit de propriété intellectuelle. Si en matière civile cette approche unitaire soulève peu de problèmes puisque l'ensemble de ces faits consomme effectivement une atteinte à un droit de propriété intellectuelle, elle s'avère en revanche hautement problématique sur le plan répressif.

D'une part et comme le releva la Commission Lescure à propos du piratage en ligne, elle tend à priver le législateur de la possibilité d'adapter la réponse pénale au comportement qu'il entend réprimer[34]. En effet, si la contrefaçon est définie de manière abstraite et générale comme *la violation d'un droit de propriété intellectuelle*, sa caractérisation devient dès lors indifférente au type d'acte ayant consommé l'atteinte au droit exclusif. D'autre part, cette approche unitaire du contentieux de la propriété intellectuelle impose d'appréhender la répression d'un trafic international à travers le régime civil des droits de propriété intellectuelle qui emprunte la plupart de ses concepts au droit des biens. Or, et comme l'avait souligné le député européen Jacques Toubon à l'occasion de débats parlementaires sur l'impact de la contrefaçon sur le commerce international[35], ce détour par le droit civil peut s'avérer problématique sur le plan opérationnel. Celui-ci est en effet un outil juridique éminemment abstrait difficile à manier dans le cadre d'une répression effective d'un trafic illicite.

Cela s'avère particulièrement saillant au regard du volet douanier du Code de la propriété intellectuelle. On parle à cet égard du *« syndrome du douanier »* qui se voit dans l'impossibilité matérielle et juridique de constater l'atteinte à un droit de propriété intellectuelle[36]. La solution retenue par les règlements douaniers européens fut d'adopter une *« prohibition conditionnelle »* de la contrefaçon[37], le bien-fondé de la retenue douanière devant être confirmé a posteriori par l'autorité judiciaire seule compétente pour apprécier l'existence d'une atteinte à un droit de propriété intellectuelle. Bien que cohérente sur le plan juridique, cette prohibition conditionnelle n'est cependant pas sans soulever quelques problèmes sur le plan opérationnel. Depuis quelques années, les autorités douanières ont d'ailleurs pris l'habitude d'intervenir sur le seul fondement du Code des douanes afin de se libérer des contraintes imposées par le Code de la propriété intellectuelle qui impose notamment le déclanchement d'une action au fond dans les dix jours suivant la retenue des marchandises suspectées de porter atteinte à un droit de propriété intellectuelle[38]. Cette pratique qui a été validée par la Cour de cassation à plusieurs reprises[39], se justifie certes d'un point de vue pratique, mais interroge quant à sa conformité au droit du commerce international qui prohibe explicitement une telle autonomisation du droit douanier[40]. À défaut d'une décision au fond ayant confirmé l'atteinte au droit de propriété intellectuelle, le caractère illicite des marchandises demeure en effet purement hypothétique et leur saisie par les autorités douanières manque par conséquent de fondement légal.

Mais alors, comment fonder l'action des autorités en matière de contrefaçon ? Dans son ouvrage consacré à la contrefaçon criminelle, le criminologue Pierre Delval proposa de développer une approche répressive différente qui serait à la fois complémentaire et autonome du droit de la propriété intellectuelle[41]. Selon lui, il conviendrait d'adopter un dispositif répressif rénové qui n'aurait plus pour objet la contrefaçon entendue comme la violation d'un droit exclusif, mais le *crime-contrefaçon* finançant la criminalité organisée et mettant en péril la sécurité et la santé des consommateurs. Cette idée fait écho à projet de réforme assez ancien. Au siècle dernier, certains avaient en effet suggéré un rapprochement des incriminations de la contrefaçon de celles encadrant la répression de la tromperie commerciale[42].

Sur le plan juridique, une telle réforme impliquerait de revoir substantiellement la *ratio legis* des incriminations de contrefaçon qui ne consisterait plus à réprimer la violation d'un droit de propriété intellectuelle, mais à sanctionner l'altération ou l'imitation frauduleuse d'une *« marque d'autorité »* permettant de tracer l'origine commerciale d'un produit. Démunies face au trafic de contrefaçons, un grand nombre d'entreprises recourent d'ailleurs de plus en plus à des techniques de *« marquage anti-contrefaçon »* leur permettant d'assurer la traçabilité de leurs produits et *in fine,* une meilleure maîtrise de leurs canaux de distribution[43].

Il ne serait dès lors plus question de protéger les droits de propriété intellectuelle, mais tout simplement de garantir la loyauté des échanges commerciaux en identifiant les produits non authentiques et en les extrayant des

circuits marchands. Sur le plan répressif, le consommateur serait alors considéré comme une victime et non plus comme un complice de la contrefaçon. Il ne bénéficierait pas pour autant d'un état d'impunité, mais se verrait simplement opposer des instruments juridiques mieux adaptés à la nature du préjudice causé par son achat.

Le droit répressif aurait quant à lui une finalité tout autre. Il ne tendrait non point à garantir un actif immatériel, mais à protéger le marché sur lequel celui-ci est exploité. La rénovation du dispositif répressif de la contrefaçon permettrait en effet de garantir au consommateur la fiabilité des signes le renseignant sur la qualité des produits qu'il achète. À défaut d'une telle garantie, le consommateur se retrouve exposé à une asymétrie d'information dangereuse, son achat s'opérant sur la base d'une perception incertaine de la qualité du produit. Le risque est alors double. D'une part, le consommateur s'expose à un risque important compte tenu de la dangerosité de certaines contrefaçons. D'autre part, l'asymétrie d'information à laquelle le consommateur est soumis perturbe son choix d'achat et conduit *in fine* à évincer du marché les fabricants de produits de qualité.[44] Protecteur de l'intérêt général, le droit pénal s'intéresserait à cette double menace planant sur l'ordre public économique en confondant le régime répressif de la contrefaçon avec celui des tromperies commerciales. La valeur sociale protégée ne serait dès lors plus *la propriété intellectuelle*, mais la confiance publique et la rhétorique s'en trouverait modifiée : la contrefaçon n'est pas un vol, elle une imposture.

Notes :

1 Washington Examiner, 19 mars 2020, « Counterfeits in the time of pandemic » ; Les Echos, 25 mars 2020, « Coronavirus : des millions de faux médicaments, de masques et de gels contrefaits circulent en Europe » ; National Post, 28 avril 2020, « COVID-19: From counterfeit medical masks to fake treatments, criminals cashing in on pandemic panic ».

2 Conseil de L'Europe, Comité MEDICRIME, Avis sur l'application de la convention MEDICRIME dans le contexte du COVID-19, 8 avril 2020 ; EUROPOL, Communiqué de presse, 17 avril 2020, « Viral marketing: counterfeits in the time of pandemic »; OCDE, EUIPO, Communiqué de Presse, 21 avril 2020, « La crise du Covid-19 met en évidence la nécessité de lutter contre la vente de faux médicaments ».

3 J. FOYER, M. VIVANT, Le droit des brevets, Thémis, 1991, p. 288.

4 Rapport de l'Union des fabricants (UNIFAB), Contrefaçon et criminalité organisée, 2003, p. 12.

5 S. A. STUMPF, P. E. CHAUDHRY, L. PERRETTA, « Fake : Can business stanch the flow of counterfeit products? », Journal of Business Strategy, Vol. 32, n° 2, 2011, p. 9.

6 Stefano BETTI, « Key global enforcement issues on illicit trade in goods », in Peggy E. CHAUDHRY (Ed.), Handbook of Research on Counterfeiting and Illicit Trade, Elgar, 2017, p. 31; Rapport de l'Union des fabricants (UNIFAB), Contrefaçon et terrorisme, 2016, p. 24 ; EUROPOL, "Serious and Organised Crime Threat Assessment (Public Version)", March 2013, p.22.

7 Moisés NAÍM, Illicit : how smugglers, traffickers and copycats are hijacking the global economy, ibid, p. 112.

8 Rapport de l'OCDE et de l'EUIPO, Trends in Trade in Counterfeit and Pirated Goods, 2019.

9 James MOODY, ancien chef de la division de la criminalité organisée et de la drogue du FBI cité dans : Pierre DELVAL, Le marché mondial du faux. Crimes et contrefaçons, CNRS éditions, 2010, p. 87.

10 B. A. SULLIVAN, J. M. WILSON, R. KINGHORN, « Illicit trade in counterfeit products : an examination of the opportunity-risk connection », in Peggy E. CHAUDHRY (Ed.), Handbook of Research on Counterfeiting and Illicit Trade, Elgar, 2017, pp. 19-21 ; P. E. CHAUDHRY, A. S. ZIMMERMAN, The Economics of Counterfeit Trade : Governments, Consumers, Pirates, and Intellectual Property Rights, Springer, 2009, p. 167 ; Miriam BITTON, « Rethinking The Anti-Counterfeiting Trade Agreement's Criminal Copyright Enforcement Measures », The Journal Of Criminal Law & Criminology, Vol. 102, 2012, p. 113.

11 Rapport d'information sur la lutte de l'Union européenne contre la contrefaçon présenté par M. LAFFINEUR à l'Assemblée nationale le 8 juin 2005, p .70, cité dans C. BERNAULT, « La sanction pénale de la contrefaçon » Droit de l'immatériel, 2012, n° 86 ; C. LE GOFFIC, M. WAGNER, « La pénalisation de la contrefaçon », Droit pénal, n° 12, Décembre 2009, étude n° 29.

12 Loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité, dite loi « Perben II » ; Loi n° 2007-1544 du 29 octobre 2007 de lutte contre la contrefaçon ; Loi n° 2006-961 du 1er août 2006 relative au droit d'auteur et aux droits voisins dans la société de l'information ; Loi n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet dite loi « HADOPI 1 » ; Loi n° 2009-1311 du 28 octobre 2009 relative à la protection pénale de la propriété littéraire et artistique sur internet dite loi « HADOPI 2 » ; Loi n°2014-315 du 11 mars 2014 renforçant la lutte contre la contrefaçon, dite loi « Yung » ; Loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale.

13 Article 44 de la Loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale.

14 Règlement (CEE) n° 3842/86 du Conseil du 1er décembre 1986 fixant des mesures en vue d'interdire la mise en libre pratique des marchandises de contrefaçon ; Règlement (CE) n° 3295/94 du Conseil, du 22 décembre 1994, fixant des mesures en vue d'interdire la mise en libre pratique, l'exportation, la réexportation et le placement sous un régime suspensif des marchandises de contrefaçon et des marchandises pirates ; Règlement (UE) n ° 608/2013 du Parlement européen et du Conseil du 12 juin 2013 concernant le contrôle, par les autorités douanières, du respect des droits de propriété intellectuelle.

15 C.-J. BERR, H. TREMEAU, Le droit douanier communautaire et national, Economica, 7e éd., 2006, n° 17, p. 11.

16 Claude-J. BERR, Chronique de Droit douanier, La Semaine Juridique Entreprise et Affaires n° 28, 20 Juillet 1989, 15552.

17 Rapport d'information sur l'évaluation de la loi n° 2007-1544 du 29 octobre 2007 de lutte contre la contrefaçon, L. BÉTEILLE et R. YUNG, 9 février 2011, p. 53.

18 Il ressort d'un rapport du Sénat qu'en 2009, sur les « 1 236 infractions liées à la contrefaçon ayant donné lieu à une condamnation », il y a eu seulement 47 peines d'emprisonnement prononcées, dont seulement 8 d'emprisonnement ferme. Concernant les peines d'amende, celles-ci sont également bien en deçà des 300 000 € prévus par les textes. En 2009, celles-ci atteignaient en effet une moyenne de 870 €. En 2013, le ministère de la justice communiquait des chiffres assez similaires, avec une petite

augmentation de l'amende moyenne prononcée en matière de contrefaçon (1 647€). Voir : Rapport d'information sur l'évaluation de la loi n° 2007-1544 du 29 octobre 2007 de lutte contre la contrefaçon, L. BÉTEILLE et R. YUNG, 9 février 2011, pp. 50 et s.; Notes statistiques de l'Observatoire national de la délinquance et des réponse pénales, La contrefaçon en France - Éléments de mesure et d'analyse du phénomène, Focus n° 6, Juin 2011, p. 28.

19 Notes statistiques de l'Observatoire national de la délinquance et des réponse pénales, La contrefaçon en France- Éléments de mesure et d'analyse du phénomène, Focus n° 6, Juin 2011, p.73.

20 Rapport de la Cour des Comptes du 3 mars 2020, « La lutte contre les contrefaçons », pp. 20 et s.

21 Étude Union des fabricants (UNIFAB) et IFOP, Les français et les dangers de la contrefaçon, Septembre 2012, p. 39.

22 F. KREMER, C. VIOT, A. LE ROUX et I. PONCIN, « Les consommateurs face à la contrefaçon : une comparaison entre Belges et Français », Reflets et perspectives, XLVII, 2008/2.

23 Andreas RAHMATIAN, « Trade Mark Infringement as a Criminal Offence », Modern Law Review, Vol. 67 Issue 4, p. 683 ; Shari Dawn OLENICK, « Draft International Anticounterfeiting Code: Neo-Realism as a Vehicle for Analyzing the Effect of Non-signatories' Perceptions on the Development of an Anticounterfeiting Norm », précit., pp. 834 et s.; Moisés NAÍM, Illicit : how smugglers, traffickers and copycats are hijacking the global economy, op. cit., p. 32; L. HARMS, L'application des DPI au moyen des sanctions pénales : une évaluation, OMPI, ACE/4/3, 7 septembre 2007, n° 176 cité dans C. BERNAULT, « La sanction pénale de la contrefaçon », Droit de l'immatériel, 2012, n° 86.

24 Mark THORNTON, The Economics of Prohibition, University of Utah Press, 1991, pp. 75-76.

25 J. PRIEGER, J. D. KULICK, « Violence in Illicit Markets: Unintended Consequences and the Search for Paradoxical Effects of Enforcement », Pepperdine University,School of Public Policy Working Papers, 2014, Paper 52, p. 2.

26 « both practical experience and economic theory show that enforcement against illegal activity in drug markets may have the unintended consequence of exacerbating violence. Systematic reviews of the empirical literature show that nearly all studies find evidence of an adverse impact of drug law enforcement on levels of violence », Ibid., p. 1.

27 Shari Dawn OLENICK, « Draft International Anticounterfeiting Code: Neo-Realism as a Vehicle for Analyzing the Effect of Non-signatories' Perceptions on the Development of an Anticounterfeiting Norm », précit., pp. 834 et s.

28 La pénalisation de la contrefaçon risquerait ainsi d'« encourager la contrefaçon à une échelle plus importante » car « prendre le risque d'une lourde peine n'est payant que pour des opérations importantes », L. HARMS, L'application des DPI au moyen des sanctions pénales : une évaluation, OMPI, ACE/4/3, 7 septembre 2007, n° 176 cité dans C. BERNAULT, « La sanction pénale de la contrefaçon », Droit de l'immatériel, 2012, n° 86.

29 Référé de la Cour des comptes du 20 mai 2014 sur la politique publique de lutte contre la contrefaçon, p. 3.

30 Qui concernait non seulement des brevets (patents), mais également des dessins et modèles protégés (design patents).

31« Apple contre Samsung : "le procès de l'irrationnalité'' », L'Express, 21 août 2012 ; « Apple contre Samsung, la guerre à coups de brevets », Challenges, 7 décembre 2016 ; « Brevet: Samsung condamné à verser 533 millions de dollars à Apple », Le Figaro, 25 mai 2018.

32 Comme l'expliquait M. Laurent Béteille, le rapporteur du projet de loi. Sénat, 2ème lecture du projet de loi de lutte contre la contrefaçon de 2007, Séance du 19 septembre 2007, compte rendu intégral des débats consultable sur le site du Sénat : http://www.senat.fr/seances/s200709/s20070919/s20070919_mono.html

33 Le considérant 14 de la directive n° 2004/48 du 29 avril 2004 dispose que « les actes perpétrés à l'échelle commerciale sont ceux qui sont perpétrés en vue d'obtenir un avantage économique ou commercial, direct ou indirect, ce qui exclut notamment les actes perpétrés par des consommateurs finaux agissant de bonne foi ». Les États membres conservant tout de même la faculté d'appliquer les mesures en cause de façon plus large, à des actes qui ne seraient pas commis à l'échelle commerciale.

34 Rapport « contribution aux politiques culturelles à l'ère numérique », Pierre LESCURE, T.1, 2013, p. 376.

35 Cité dans Pierre DELVAL, Le marché mondial du faux. Crimes et contrefaçons, op. cit., p. 37.

36 Pierre DELVAL, Le marché mondial du faux. Crimes et contrefaçons, op. cit., pp. 40 et s.

37 Arrêt CJCE, 28 mai 1998, aff. C-3/97, Goodwin et Unstead, pt. 14.

38 Karine DISDIER-MIKUS, « Saisie de marchandises contrefaisantes, lorsque le droit douanier prend le pas sur le droit de la propriété intellectuelle », Dalloz IP/IT, 2018, p.428.

39 Cass. Com., 5 juillet 2017, n° 16-13698, LEPI 9/2017, obs. D. LEFRANC ; PIBD 2017, n°1079, III, p. 654 ; Cass. Com. 7 mars 2018, n°16-24.851, D. 2018. Actu. 560.

40 « Si, dans un délai ne dépassant pas 10 jours ouvrables après que le requérant aura été avisé de la suspension, les autorités douanières n'ont pas été informées qu'une procédure conduisant à une décision au fond a été engagée par une partie autre que le défendeur ou que l'autorité dûment habilitée à cet effet a pris des mesures provisoires prolongeant la suspension de la mise en libre circulation des marchandises, celles-ci seront mises en libre circulation (...) », Article 55 de l'Accord sur les Aspects des Droits de Propriété Intellectuelle qui touchent au commerce (ADPIC).

41 Pierre DELVAL, Le marché mondial du faux. Crimes et contrefaçons, CNRS éditions, 2010, p. 48.

42 Tr. Seine, 7 août 1908, Ann. 1921, I, p. 367 ; Paris, 10 décembre 1930, Ann. 1931, p. 215 ; Cass. Crim. 1er mai 1931, Ann. 1933, p. 127 cités dans Paul ROUBIER, Du droit de la propriété industrielle, 1952, Sirey, Tome 1, p. 392, n° 86, note 1.

43 Jean-Michel LOUBRY, « Lutte contre la contrefaçon. Authentification et traçabilité », Techniques de l'ingénieur, 10 novembre 2011, Réf. TR980 V2, p. 4.

44 George A. AKERLOF, "The market for "lemons": Quality uncertainty and the market mechanism", Uncertainty in economics. Academic Press, 1978, pp. 235-251.

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

LA TRANSPARENCE FISCALE : DIX ANS D'AVANCÉES

MATHILDE SABOURET

CONSEILLÈRE EN POLITIQUE FISCALE, FORUM MONDIAL SUR LA TRANSPARENCE ET L'ÉCHANGE DE RENSEIGNEMENTS À DES FINS FISCALES, ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES (OCDE)

Les opinions exprimées dans cet article le sont à titre personnel et n'engagent que son auteur.

Face à la crise financière, les dirigeants du G20 s'engageaient en 2009 à mettre fin à l'ère du secret bancaire. S'ouvrait ainsi une décennie d'avancées significatives en matière de transparence fiscale, dont les scandales successifs connus sous les noms de « Offshore leaks » (2013), « Luxleaks » (2014), « Swiss leaks » (2015) ou encore « Panama papers » (2016) ont été autant de catalyseurs. La transparence et l'échange de renseignements à des fins fiscales s'avèrent des outils efficaces pour lutter contre l'évasion et la fraude fiscales. En resserrant les mailles du filet, ils permettent de générer des recettes supplémentaires pour l'ensemble des juridictions y ayant recours. Cet article se propose de mettre en lumière les raisons qui ont présidé à l'établissement de standards de transparence fiscale au niveau international, d'expliquer leur mise en oeuvre et d'en apprécier les résultats, sans omettre d'esquisser les défis qu'il reste à relever.

I. Pourquoi la transparence fiscale ?

La transparence fiscale a accompli des progrès considérables au cours de ces dix dernières années. Mais pourquoi n'a-t-elle pas toujours été considérée comme une évidence ? Comment s'est-elle finalement affirmée comme une solution incontournable pour résoudre un problème mondial ?

A. Crise financière et scandales fiscaux

La crise de 2008, dont l'origine est à chercher dans les dérives d'une finance internationale peu et mal régulée, aura coûté des centaines de milliards d'euros d'argent public. Conscients du prix à payer pour sauver un secteur financier défaillant et relancer une économie mondiale en berne, les chefs d'État et de gouvernement du G20, réunis à Londres le 2 avril 2009, décidèrent d'adopter une déclaration intitulée : « Renforcer le système financier »[1], parmi laquelle figurait « l'engagement de prendre des mesures à l'encontre des juridictions non-coopératives, y compris les paradis fiscaux, d'appliquer des sanctions pour protéger nos finances publiques et les systèmes financiers ». En bref, les dirigeants y affirmaient que « l'ère du secret bancaire était révolue ».

L'objet de cet article n'est pas de décrire ce que sont les paradis fiscaux ou les juridictions non-coopératives. Des organisations internationales, gouvernementales, académiques ou non-gouvernementales se sont déjà livrées à des exercices de définition, souvent accompagnés de critères. Cependant, les processus de construction de listes qui ont pu en résulter seront abordés lors du prochain chapitre.

La révélation de plusieurs scandales fiscaux est venue accélérer la dynamique initiée en 2009 par le G20. Les enquêtes menées grâce à des lanceurs

d'alerte et publiées par des consortiums internationaux de journalistes ont pointé du doigt certains abus du secret bancaire. Elles ont mis au jour l'existence de stratégies d'optimisation fiscale - dont certaines légales - fondées sur l'opacité d'entités et de constructions juridiques, à l'instar des trusts. Elles ont dévoilé l'envergure de pratiques fiscales iniques utilisées par des entreprises ou des particuliers. Elles ont ainsi fait naître un fort sentiment d'injustice d'autant plus légitime que les fuites de documents survenaient dans le sillon de la crise financière de 2008 qui avait massivement ponctionné les liquidités publiques. Les « Offshore leaks », « Swiss leaks », « Luxleaks » ou encore « Panama papers » ont affaibli la confiance des citoyens à l'égard de l'équité du système fiscal.

Par ailleurs, la mondialisation des échanges et la mobilité des flux de capitaux ont rendu de plus en plus complexe l'application des lois fiscales nationales. Dans leurs juridictions respectives, les administrations fiscales peuvent contraindre les contribuables, mais aussi les banquiers, ou encore les avocats et les conseillers fiscaux à leur fournir des renseignements. Mais dans un contexte transfrontalier, l'accès à ces renseignements doit reposer sur un accord international et être facilité par l'administration fiscale homologue. Nombreux sont les obstacles qui peuvent entraver l'accès à ces renseignements, tels que le secret bancaire ou le manque de transparence des entités et constructions juridiques qui peuvent être utilisées pour dissimuler leur propriétaire légal ou leur bénéficiaire effectif. Ces obstacles créent, in fine, des possibilités d'évasion et de fraude fiscales, mettant à mal l'intégrité des systèmes fiscaux nationaux et minant la confiance des citoyens.

B. Mise en place d'un standard international et du Forum mondial

Afin de mettre en oeuvre les décisions du G20 sur la fin du secret bancaire, le Forum mondial sur la transparence et l'échange de renseignements à des fins fiscales - appelé ci-après le Forum mondial - a été restructuré, et des normes internationales ont été adoptées.

La création d'un Forum mondial destiné à mettre en oeuvre la norme internationale sur la transparence fiscale et l'échange de renseignements sur demande remonte à 2000. Le Forum mondial n'était alors qu'un club restreint, dont faisait seulement partie des pays membres de l'OCDE et quelques Centres Financiers Internationaux[2] (CFI). En 2009, le Forum mondial prend une nouvelle dimension. Il s'ouvre à l'ensemble des juridictions qui souhaitent mettre en oeuvre la norme internationale. Il inclut dès lors 89 juridictions qui prennent également l'engagement de se soumettre à des évaluations par les pairs. En un peu plus de dix ans, le nombre de membres est passé de 89 à 161, couvrant ainsi l'ensemble des pays de l'OCDE et du G20, les CFI et de plus en plus de pays en développement.

L'échange de renseignements sur demande concerne les situations dans lesquelles les autorités fiscales d'un pays demandent un renseignement à leurs homologues d'un autre pays dans le cadre d'une enquête ou d'un contrôle fiscal. Il peut s'agir, par exemple, de demander des informations sur la propriété d'une entité juridique, sur les états financiers d'une entreprise ou sur les relevés bancaires d'un contribuable.

En 2014, une seconde norme internationale sur l'échange automatique de renseignements financiers voit le jour sous l'impulsion de plusieurs pays européens décidés à placer le développement de cette initiative multilatérale sous l'égide de l'OCDE. Elle s'inspire de la loi américaine FATCA (Foreign Account Tax Compliance Act). Entrée en vigueur en 2010, cette dernière est destinée à collecter les impôts dus par les citoyens et résidents américains qui pensaient pouvoir y échapper en ayant recours à des comptes étrangers. Pour y parvenir, la loi FATCA oblige tous les établissements financiers situés en dehors des États-Unis à déclarer au fisc américain toute information pertinente relative aux comptes financiers détenus par leurs clients américains. En 2014, près de 100 juridictions adoptent la Norme Commune de Déclaration (NCD) dans le cadre du Forum mondial et s'engagent à échanger automatiquement, sans demande préalable, les renseignements sur les comptes financiers de leurs résidents étrangers. Les premiers échanges ont eu lieu en 2017 et 2018, créant un nouveau canal par lequel les autorités fiscales peuvent être alertés d'éventuelles infractions. Ces informations peuvent donner lieu à de nouvelles enquêtes et incitent fortement les contribuables à déclarer leurs avoirs détenus à l'étranger. La probabilité de détection des fraudeurs

fiscaux tentant de cacher leur argent dans un pays tiers a considérablement augmenté grâce à l'échange automatique de renseignements, qui devient un outil efficace de lutte contre l'évasion fiscale.

II. La mise en oeuvre de la transparence fiscale au niveau mondial

L'établissement de normes de transparence et d'échange de renseignements à des fins fiscales ne garantissait pas leur mise en oeuvre effective. Comment cette mise en oeuvre a-t-elle été réalisée ? Pourquoi toutes les juridictions, y compris celles qui permettaient dans leur système juridique une certaine opacité des entités et constructions juridiques ou des comptes bancaires, ont-elles accepté de jouer le jeu ?

A. La pression des pairs

La restructuration du Forum mondial en 2009 le transforme en une organisation ouverte et globale, où tous les membres participent sur un pied d'égalité. Toutes les juridictions qui rejoignent le Forum mondial s'engagent à mettre en oeuvre la norme d'échange de renseignements sur demande et à se soumettre à un examen par les pairs. Pour que la mise en oeuvre de la transparence fiscale soit efficace, il était essentiel qu'un nombre d'acteurs considérable rejoigne l'initiative. Plusieurs éléments permettent d'expliquer ce succès du Forum mondial et de la transparence fiscale.

Tout d'abord, les règles du jeu au niveau international ne pouvaient fonctionner que si les juridictions connues pour leurs pratiques d'opacité acceptaient de remettre en cause leur modèle et de garantir la transparence et l'échange de renseignements avec leurs partenaires. Dès lors, la participation sur un pied d'égalité de tous les membres, indépendamment du volume et de la nature des flux les concernant, a été un élément crucial pour encourager les CFI à rejoindre le Forum mondial.

Les conséquences de la crise financière sur l'état des finances publiques et l'indignation des opinions publiques face aux scandales fiscaux ont également eu un rôle déterminant. La crédibilité des dirigeants qui s'engageaient à lutter efficacement contre l'évasion fiscale pour garantir des recettes et un traitement équitable face à l'impôt était en jeu. Celle des CFI, inquiets de leur survie, l'était aussi.

L'adoption de la NCD en 2014 prévoit les premiers échanges quatre ans plus tard pour l'ensemble des juridictions, sauf pour les pays en développement dépourvus de centres financiers. Tous les pays du G20, de l'Union européenne ainsi que les CFI doivent donc appliquer le dispositif en 2018, qui stipule que les échanges doivent avoir lieu avec chaque partenaire intéressé dès lors que ce dernier respecte les normes de confidentialité et d'utilisation appropriée des données. Cette approche globale et uniformisée des règles du jeu a permis d'empêcher que des contribuables puissent transférer leurs actifs vers d'autres juridictions non engagées dans le but d'éviter le partage de renseignements avec la juridiction de leur résidence fiscale.

La communauté internationale prend conscience de l'importance capitale de la coopération internationale pour la performance des administrations fiscales. Convaincues par les avantages de la transparence fiscale et de l'échange de renseignements, de plus en plus de juridictions décident de rejoindre le Forum mondial.

B. Une mise en oeuvre efficace

Le Forum mondial a défini un processus rigoureux et robuste d'examen par les pairs pour faire respecter les engagements pris par ses membres. L'évaluation est confiée à une équipe composée de deux experts nationaux (n'appartenant pas à l'administration fiscale de la juridiction examinée) et du secrétariat du Forum mondial. La supervision revient quant à elle à un groupe de 30 pairs. Ce processus évalue à la fois le cadre juridique des juridictions et son application.

De chaque examen découle une notation globale de la conformité de la juridiction avec la norme d'échange de renseignements sur demande. Une juridiction peut être jugée conforme, conforme pour l'essentiel, partiellement conforme, ou non conforme. Depuis 2010, 126 juridictions[3] ont été évaluées par le Forum mondial dans le cadre du premier et/ou du second cycle d'examens par les pairs. Un processus similaire a débuté en 2020 afin d'évaluer la mise en oeuvre de la norme d'échange automatique de renseignements par les juridictions s'y étant engagées.

La notation obtenue a une influence sur la réputation de la

juridiction évaluée sur la scène internationale. D'elle peut dépendre des conditions économiques importantes, comme le niveau des investissements étrangers ou le volume des transactions commerciales.

Le G20, l'Union européenne, ainsi que des gouvernements nationaux ont dressé des listes noires de juridictions non-coopératives. Les notations obtenues par les juridictions dans le cadre de leurs examens par le Forum mondial sont prises en compte dans les critères de ces listes.

Une juridiction répertoriée peut subir des conséquences variables et être soumise à diverses mesures défensives (taux de retenue à la source plus élevé, suppression d'avantages fiscaux ou de déductions fiscales, augmentation des contrôles fiscaux, restriction des transactions financières). Par ailleurs, des banques de développement ont intégré les notations du Forum mondial dans leurs politiques d'investissement, impactant négativement le secteur financier et les investissements dans les juridictions notées partiellement ou non conformes. Enfin, les organisations non-gouvernementales et la société civile peuvent s'appuyer sur les notations pour faire avancer leur cause.

III. Des résultats concrets et convaincants

La création de normes internationales de transparence fiscale et leur instauration effective ont eu des résultats impressionnants au cours des dix dernières années. Ces normes ont en effet réduit les pratiques d'évasion fiscale qui avaient pu se développer grâce à l'usage de constructions opaques et à l'existence de juridictions non-coopératives.

A. La fin du secret bancaire

Les problèmes liés au secret bancaire et les recommandations pour y remédier ne sont pas apparus avec la déclaration des dirigeants du G20 de 2009. Dès 1985, le Comité des affaires fiscales de l'OCDE proposait dans un rapport intitulé « Fiscalité et abus du secret bancaire »[4], d'utiliser davantage les données pouvant être obtenues auprès des banques par le biais de l'échange de renseignements et « d'accroître, le cas échéant, les renseignements disponibles au niveau national en assouplissant le secret bancaire vis-à-vis des autorités fiscales ». Par la suite, plusieurs rapports, parfois approuvés sans l'unanimité des membres de l'OCDE, ont également souligné les risques, y compris d'évasion fiscale, que pose l'accès restreint aux données bancaires par les administrations fiscales.

Le secret bancaire assure la confidentialité des affaires financières d'une personne physique ou morale. Il est légitime dans la mesure où il protège le droit à la vie privée du titulaire d'un compte, notamment en empêchant les banques d'en partager les données avec un tiers. Mais il peut alors encourager des contribuables peu scrupuleux à se livrer à des activités illégales si le tiers en question est une administration fiscale ou une agence chargée de la lutte contre le blanchiment de capitaux.

Les examens par les pairs ont apporté des améliorations significatives en la matière. Le rapport des dix ans du Forum mondial[5] établit que, sur 70 juridictions qui avaient un secret bancaire, 67 ont modifié leur législation pour autoriser leur administration à accéder aux renseignements bancaires à des fins d'échange de renseignements.

Le passage à la norme d'échange automatique de renseignements, qui permet aux autorités nationales d'accéder sans demande préalable aux renseignements sur les comptes financiers étrangers de leurs résidents, marque une nouvelle étape décisive. Le souhait du G20 de Londres de 2009 a donc été largement exaucé : la transparence fiscale a mis fin à l'ère du secret bancaire.

B. La transparence des entités légales et des constructions juridiques

La mission principale du Forum mondial, qui a présidé à sa fondation, est de favoriser la transparence fiscale. Outre le secret bancaire, de nombreux mécanismes permettaient en effet d'assurer l'anonymat des propriétaires légaux ou effectifs de certaines entités et constructions juridiques. Il s'agit par exemple de la détention d'actions au porteur, de l'utilisation de prête-noms ou encore de la superposition de sociétés fictives. Plus nombreux sont les mécanismes opaques, généralement utilisés en couches, plus il est difficile d'identifier le véritable propriétaire d'une entité légale ou d'une construction juridique.

En plus de l'accès aux informations bancaires, la mise en oeuvre des recommandations

émises dans le cadre des examens par les pairs a modifié des centaines de dispositions juridiques qui restreignaient jusqu'alors la disponibilité des renseignements sur la propriété légale, les bénéficiaires effectifs et les données comptables des entités et constructions juridiques.

L'un des exemples phares de progrès remarquable en matière de transparence fiscale concerne les actions au porteur. Ces titres négociables confèrent la propriété d'une entité et le statut d'actionnaire aux personnes qui détiennent le certificat d'actions. La propriété d'actions au porteur étant fondée exclusivement sur la possession matérielle de ce certificat, leur transfert peut se faire facilement, de la main à la main. Le suivi de la propriété d'actions au porteur est d'autant plus délicat qu'il n'implique pas d'enregistrement nominatif au registre des actionnaires. Ces instruments présentent donc un risque élevé aux yeux des autorités fiscales et celles luttant contre la criminalité financière. Grâce au Forum mondial, plus de 40 juridictions ont soit aboli les actions au porteur, soit mis en place des dispositions adéquates d'identification de leurs propriétaires[6]. Désormais, 90% des juridictions qui ont fait l'objet d'examens par les pairs interdisent l'émission d'actions au porteur sans l'identification de leurs propriétaires.

Les « Panama papers », publiés en avril 2016, ont montré que différents mécanismes légaux pouvaient être superposés afin de dissimuler le bénéficiaire effectif d'une personne morale, d'une construction juridique ou d'un compte en banque, c'est-à-dire la personne physique qui en détient le contrôle en bout de chaîne. Depuis 2017, le Forum mondial s'efforce d'assurer la disponibilité et l'accessibilité des renseignements sur les bénéficiaires effectifs, afin que les fraudeurs ne soient plus en mesure de cacher leurs actifs en utilisant des entités ou des structures opaques. À cette fin, il a intégré la norme du Groupe d'Action Financière (GAFI) sur les bénéficiaires effectifs dans les normes d'échange de renseignements sur demande et d'échange automatique de renseignements financiers. Les examens par les pairs réalisés par le Forum mondial analysent par conséquent la conformité et l'application des systèmes juridiques concernant la disponibilité et l'accessibilité des informations sur les bénéficiaires effectifs. Dans le cadre du second cycle d'examens par les pairs sur l'échange de renseignements sur demande, le Forum mondial a déjà évalué le respect de la norme sur les bénéficiaires effectifs au sein de 69 juridictions. Pour une majorité d'entre elles, il a émis des recommandations dont la teneur révèle que le cadre juridique et la supervision des bénéficiaires effectifs méritent encore d'être renforcés. Le Forum mondial suit la mise en oeuvre de ces recommandations dans le but de faire progresser les juridictions déficientes.

Enfin, l'assujettissement et le calcul de l'impôt dépendent essentiellement de la disponibilité de données comptables. Une trentaine de membres du Forum mondial présentait des lacunes significatives dans ce domaine. Ces juridictions ont modifié leurs législations et travaillent désormais à leur mise en oeuvre.

C. Échanges accrus et nouvelles recettes

Outre son effet dissuasif sur le recours à l'élaboration de montages opaques ou à la détention de comptes bancaires à l'étranger, l'échange de renseignements a aussi permis le recouvrement de recettes importantes pour les États. Le Forum mondial estime que les programmes de divulgation volontaire et les enquêtes fiscales à l'étranger ont abouti à la collecte de 102 milliards d'euros de recettes supplémentaires (impôts, intérêts et pénalités)[7].

Le passage à l'échange automatique de renseignements a été clé. En 2018, les échanges automatiques sur les comptes financiers détenus à l'étranger représentaient plus de 11 millions de comptes d'un montant de 4 900 milliards d'euros. La transparence et l'échange de renseignements ont remodelé les comportements des contribuables. L'évolution des dépôts et flux d'investissements dans les centres financiers internationaux donne un aperçu de l'envergure du changement : selon une étude de l'OCDE[8], les dépôts bancaires détenus par des non-résidents dans les centres financiers ont diminué de 24% (410 milliards de dollars) entre 2008 et 2019. Cette baisse a d'abord correspondu à l'augmentation des signatures d'instruments d'échange de renseignements par les CFI avant de s'accentuer lors de l'entrée en vigueur de l'échange automatique de renseignements en 2017 et 2018. Bien que d'autres

facteurs aient pu entrer en compte, la transparence fiscale et l'échange de renseignements demeurent les raisons principales d'une telle contraction.

IV. Quels défis pour l'avenir ?

L'accroissement de la transparence des systèmes juridiques, l'élargissement de l'accès aux renseignements et la hausse des échanges d'informations ont produit des résultats remarquables. Ils ont eu des effets dissuasifs certains sur l'évasion fiscale. Ils ont permis le recouvrement de recettes nécessaires au financement des services publics. Toutefois, la vigilance reste de mise pour empêcher l'apparition de nouveaux scandales fiscaux et garantir que l'ensemble des pays, en particulier les pays en développement, puisse bénéficier pleinement de ces progrès.

A. Rester vigilants quant aux risques émergents

L'échange d'informations, au coeur de la coopération internationale en matière fiscale, s'affirme comme l'une des méthodes privilégiées par les États pour lutter avec succès contre l'évasion et la fraude fiscales. Le passage à l'échange automatique de renseignements financiers a été crucial. Il s'agit désormais de rester vigilants afin de pouvoir réagir rapidement aux menaces que présentent de nouveaux risques émergents.

Par les examens qu'il mène, le Forum mondial est responsable de la mise en oeuvre effective de la norme sur l'échange de renseignements sur demande et de la NCD. Ainsi, le second cycle d'examens par les pairs sur l'échange de renseignements sur demande a accordé une attention particulière à la transparence des informations sur les bénéficiaires effectifs. Le Forum mondial accompagne ses membres dans la transposition des recommandations émises et surveille de près leur application afin de garantir la transparence effective de ces informations. Par ailleurs, 2020 marque le début des examens par les pairs sur la norme d'échange automatique de renseignements. Ces examens visent à assurer que l'ensemble des juridictions consacre des ressources suffisantes et appropriées à la mise en oeuvre de cette norme, notamment pour veiller au respect des obligations des institutions financières en charge de transmettre les informations à échanger.

L'OCDE détecte et analyse également les nouveaux risques qui peuvent émerger et mettre en péril les progrès de la transparence fiscale. Par exemple, l'un de ces risques consiste en la modification d'une résidence fiscale par l'obtention d'une autre résidence ou d'une autre nationalité via un investissement, une pratique aussi connue sous le terme de « passeport doré ». Certains de ces schémas d'investissement peuvent s'apparenter à des artifices conçus pour tromper les procédures de diligence des institutions financières dans le cadre de la norme de l'échange automatique de renseignements. Un tel scénario pourrait se produire lorsqu'un individu ne résidant pas réellement ou uniquement dans la juridiction dans laquelle l'investissement a eu lieu est capable de fournir à sa banque les pièces justificatives délivrées dans le cadre de cette résidence ou citoyenneté acquise par investissement. Afin de réduire le recours à ce genre de dispositif potentiellement frauduleux, l'OCDE a publié en octobre 2018 les noms des pays dont les programmes d'obtention de la résidence ou de la nationalité par un investissement présentent des risques élevés de détournement à des fins d'évasion fiscale[9].

B. S'assurer de n'oublier personne

Enfin, les bienfaits de la transparence fiscale ne doivent pas uniquement profiter aux pays développés. La couverture de l'échange de renseignements s'est largement étendue à l'échelle mondiale : les pays en développement représentent désormais plus de la moitié des membres du Forum mondial. Eux aussi doivent pouvoir recueillir les fruits de la coopération internationale en matière fiscale. Il est donc essentiel qu'ils puissent procéder aux réformes nécessaires de leur cadre légal et de leurs pratiques. C'est dans cette perspective que le Forum mondial a élaboré un programme robuste et complet d'assistance technique. Destiné à l'ensemble de ses nouveaux membres et mené en partenariat avec d'autres organisations régionales et internationales, il a pour objectif de favoriser une mise en oeuvre adéquate des normes internationales d'échanges de renseignements. L'application de tels standards porte en elle-même la promesse, rarement déçue, d'alimenter par de nouvelles recettes les finances publiques. De telles ressources sont propices au développement économique et social.

C'est là tout l'intérêt de la transparence fiscale mobilisée comme instrument de lutte contre l'évasion et la fraude fiscales.

Notes :

1. http://www.g20.utoronto.ca/2009/2009communique0402-fr.pdf
2. La définition de centre financier international utilisée est celle du Fonds Monétaire International (2000) : https://www.imf.org/external/np/mae/oshore/2000/eng/back.htm
3. http://www.oecd.org/tax/transparency/exchange-of-information-on-request/ratings/
4. OCDE, Taxation and The Abuse of Bank Secrecy ("the 1985 Report"), International Tax Avoidance and Evasion: Four Related Studies, 1987.
5. OCDE, Rapport du 10ème anniversaire du Forum mondial sur la Transparence et l'Echange de Renseignements à des fins fiscales, 2019, http://www.oecd.org/tax/transparency/rapport-10-ans-forum-mondial.pdf
6. OCDE, Rapport du 10ème anniversaire du Forum mondial sur la Transparence et l'Echange de Renseignements à des fins fiscales, 2019, http://www.oecd.org/tax/transparency/rapport-10-ans-forum-mondial.pdf
7. OCDE, Rapport du 10ème anniversaire du Forum mondial sur la Transparence et l'Echange de Renseignements à des fins fiscales, 2019, http://www.oecd.org/tax/transparency/rapport-10-ans-forum-mondial.pdf
8. O'Reilly, P., K. Parra Ramirez and M. A. Stemmer (2019), "Exchange of Information and Bank Deposits in International Financial Centres", OECD Taxation Working Papers, No. 46, OECD Publishing, Paris, https://doi.org/10.1787/025bfebe-en.
9. https://www.oecd.org/tax/automatic-exchange/crs-implementation-and-assistance/residence-citizenship-by-investment/

OUVRAGES RÉCENTS

LA COLÈRE ET LE COURAGE

PLAIDOYER CONTRE LA CORRUPTION POUR UNE RÉPUBLIQUE ÉTHIQUE

AUTEUR : JEAN-CHRISTOPHE PICARD

ÉDITEUR : ARMAND COLIN

Résumé

Corruption, fraude fiscale, gaspillage de l'argent public… Les affaires continuent !

Avec l'explosion de la dette publique et le creusement des inégalités, le flot ininterrompu des scandales est de plus en plus insupportable. Leur coût est tel que même assumé par l'ensemble des contribuables, l'impact sur chacun est énorme : des impôts et taxes supplémentaires, des prestations sociales diminuées et des services publics de moins bonne qualité. Surtout, la succession des affaires abîme l'indispensable lien de confiance entre élus et électeurs.

Ce passionnant ouvrage ne se contente pas de dresser un état des lieux implacable des failles de notre République. Il évoque les solutions à mettre en oeuvre pour mettre fin aux abus. Président de la République, parlementaires, élus locaux, candidats, militants, citoyens… tous les acteurs de la vie politique ont un rôle à jouer !

Une République plus éthique est à portée de main. La recette qui déclenche tous les grands changements n'a besoin que de deux ingrédients : la colère et le courage. « La colère face aux choses telles qu'elles sont. Et le courage nécessaire pour les changer. »

LES ENTREPRISES ACTRICES DE L'ANTICORRUPTION

NATHALIE KALESKI[1]

DIRIGEANTE FONDATRICE DE IKTINOS, SOCIÉTÉ D'ÉTUDES ET DE CONSEILS EN GOUVERNANCE ET COMPLIANCE, SECRÉTAIRE GÉNÉRALE DE L'ASSOCIATION FRANCE AUDACIEUSE

Longtemps, le principe de régulation de l'activité économique a été limité aux secteurs de la banque, de l'assurance et de la pharmacie. Avec la montée en puissance d'un cadre normatif mondial anticorruption, la régulation s'est étendue à tous les secteurs et affecte toutes les entreprises, internationales ou non, grandes ou petites.

La sévérité accrue des autorités de différents pays, notamment l'augmentation du montant des sanctions civiles et pénales[2], a rendu vitale pour les entreprises l'intégration de la norme anticorruption dans leur stratégie. La norme internationale anticorruption, imposée ou volontaire (norme ISO 37001), est ainsi entrée durablement au coeur des entreprises.

Or, elle modifie leur rôle : pour lutter contre la corruption, les États leur imposent de lourdes exigences de probité, éventuellement au détriment de leurs intérêts immédiats, et en font des agents de la normalisation mondiale. Quoi qu'elles pensent de ce nouveau rôle, les entreprises doivent s'y adapter et concilier deux impératifs : la maximisation des profits d'un côté, le développement de l'intégrité de l'autre. Avec des limites dans les deux cas : la maximisation des profits risque de nuire à la pérennité, le développement de l'intégrité à la création de valeur à court terme.

Ces tensions expliquent le rapport ambivalent des entreprises à la norme anticorruption, d'autant que les dirigeants et salariés des entreprises sont également des citoyens qui, en tant que tels, sont rarement favorables à la corruption.

Seule la puissance publique qui incarne l'intérêt général, au nom duquel est lancée la lutte contre la corruption, peut aider les entreprises à dépasser cette difficulté et à faire en sorte que l'intérêt général et l'intérêt particulier se rejoignent. Et elle doit le faire car, sans leur adhésion à la norme de probité, il ne peut y avoir de lutte efficace contre la corruption.

Il faut donc comprendre l'impact général de la norme anticorruption sur les entreprises, pour mesurer l'ampleur du défi qu'elles doivent relever.

I. Les effets de la norme anticorruption sur les entreprises

La norme implique une modification profonde de l'entreprise : les actions qui semblaient auparavant normales doivent être systématiquement questionnées au regard des règles anticorruption ; il faut parfois désapprendre ce qu'on avait appris. C'est une mutation complète de l'entreprise, qui la bouleverse et affecte toutes ses composantes : pratiques, gouvernance, organisation, stratégie, modèle économique.

A. Les effets sur les pratiques de l'entreprise

Les nouvelles règles anticorruption sont diversement appréciées par les professionnels. Elles soulèvent souvent de fortes critiques : la norme anticorruption est perçue comme une contrainte

imposée de l'extérieur sans prendre en compte les spécificités du métier et risquant même de remettre en cause ce métier lui-même en modifiant la façon de travailler.

Pour ces professionnels critiques, on entre dans un système bureaucratique favorisant la prudence et l'aversion au risque, voire la déresponsabilisation, contraire à l'esprit d'entreprise. On passe d'une culture largement orale à une culture de l'écrit et des formulaires sur lesquels il faut « cocher la case ». On passe son temps à administrer des listes et des registres.

Les entreprises connaissent les processus de normalisation (par exemple ISO) et peuvent y adhérer et l'assimiler. Mais, même dans ce cas, la norme n'est pas toujours mise en place facilement, compte tenu de ce qu'elle implique en termes de conduite du changement et d'acculturation. Ainsi, la norme de probité volontaire (ISO 37001) se montre délicate à mettre en place, en raison même du sujet qu'elle traite : la corruption. L'implémentation - volontaire ou non- d'une norme anticorruption peut susciter des suspicions : le salarié à qui l'on donne un code de conduite peut soupçonner qu'il se passe des choses ou craindre qu'on se méfie de lui. Certaines entreprises disent savoir que 0,1 % seulement de leurs collaborateurs sont des fraudeurs et refusent par conséquent de mettre en place des contraintes qui vont peser sur 99,9 % d'entre eux[3].

Cependant, les dispositifs anticorruption ont aussi de fervents défenseurs car ils mettent en oeuvre des outils de traçabilité qui rendent les actes plus lisibles et plus visibles : la norme anticorruption peut alors être acceptée sans réticence, voire facilitée par la pratique déjà en place du *monitoring* et de l'amélioration des procédures internes. La norme anticorruption renforce la coordination entre les équipes dans ce but.

Mais dans tous les cas, son implémentation est un effort de longue haleine car, au-delà des pratiques, elle touche à la culture de l'entreprise, qui met du temps à changer.

B. Les effets sur l'organisation et la gouvernance de l'entreprise

La norme de probité est non seulement un enjeu opérationnel, mais aussi un enjeu de pouvoir et d'influence qui impacte toute l'organisation de l'entreprise. Dans une organisation décentralisée, elle aura tendance à centraliser certaines fonctions par le biais du contrôle.

L'élaboration des procédures, la mise en place et l'application des nouvelles normes relèvent également de la gouvernance. Ainsi la cartographie des risques, étape transversale sur le risque financier et extrafinancier, relève de la gouvernance, car elle établit une évaluation complète de l'entreprise : elle identifie, définit, évalue et fait remonter les risques afin de les gérer et de poser des priorités.

C'est parce que la prévention de la corruption relève de la gouvernance de l'entreprise que l'Agence française anticorruption (AFA) demande à rencontrer les administrateurs des entreprises qu'elle contrôle. Et de son côté, l'Institut Français des Administrateurs (IFA) rappelle le rôle déterminant du Conseil d'administration dans les différentes phases de maîtrise des risques de fraude et de corruption. La corruption est en effet considérée comme l'échec de la gouvernance, voire comme une faute organisationnelle, selon les termes des juges dans le dossier Total[4].

Or, c'est précisément un nouveau modèle de gouvernance que recommandent les parties prenantes et notamment les investisseurs, nouvelle gouvernance qui impacte la stratégie et le modèle économique de l'entreprise.

C. Les effets sur la stratégie et le modèle économique de l'entreprise

La stratégie même de l'entreprise est touchée : aller ou pas dans tel pays ; conclure ou pas avec tel partenaire ; faire ou pas telle acquisition. Des entreprises sont amenées à modifier leur stratégie de développement international : d'exportatrices, elles deviennent industries locales avec un partenariat dans les pays où auparavant elles exportaient.

La mise en place de la norme anticorruption permet enfin de se différencier et de bénéficier d'un véritable avantage compétitif. Ainsi une étude menée, en Egypte, au Zimbabwe et en Inde souligne que construire une réputation éthique dans de tels environnements doit être considéré comme une opportunité et le coût de la résistance à la corruption, comme un investissement pour bâtir cette réputation[5]. Un comportement éthique est en effet très différenciant, comme le soulignent les professionnels.

L'existence d'un programme anticorruption peut alors être la condition pour répondre aux appels d'offres. Les PME et les petites entreprises non assujetties à 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 " Sapin 2 ", ont ainsi intérêt à se mettre à l'anticorruption, ce qui contribue à les valoriser.

Si la résistance à la corruption a un coût, ce coût peut donc être considéré comme un investissement en réputation, voire comme un avantage compétitif sur certains marchés.

Mais à quelles conditions la norme anticorruption peut-elle s'intégrer au fonctionnement normal de l'entreprise ?

II. Les conditions de réussite de la norme anticorruption

Au vu de la gravité des risques encourus – de sanction, de réputation, voire de disparition –, l'entreprise est consciente de la nécessité d'implémenter la norme anticorruption dans sa structure. Cette norme lui impose un type d'organisation et un mode de travail, indépendamment de l'existence d'actes de corruption. C'est pourquoi elle peut être vécue par l'entreprise comme une intrusion, une contrainte forte qui s'ajoute à celle du coût financier immédiat de cette implémentation.

Pour réussir, la norme anticorruption doit donc être acceptée, et pour cela infuser dans les valeurs de l'entreprise en s'appuyant sur les équipes.

A. Les valeurs de l'entreprise

Les professionnels insistent sur l'importance de l'éthique et des valeurs dans la politique de probité de l'entreprise : il faut donc identifier les risques et s'assurer que les opérationnels vivent la norme anticorruption sans la considérer comme imposée de l'extérieur : cela doit devenir naturel et infuser dans toute l'entreprise, sans diffuser une culture bureaucratique. Il faut en effet éviter le formalisme de la procédure, sous peine de s'encombrer d'un système rigide et déconnecté des réalités de l'entreprise.

Et quelles qu'elles soient, il est essentiel de renforcer les valeurs de l'entreprise par la formation des collaborateurs, en les articulant à la norme anticorruption.

B. La formation des collaborateurs

Du fait de la norme, l'entreprise est confrontée à une véritable mutation. Pour la réussir, les professionnels soulignent que sa mise en place doit s'appuyer sur le management, et notamment miser sur la formation et la motivation des équipes. La clé de la bonne application de la norme anticorruption réside dans son adaptation aux réalités du terrain et dans son appropriation par les professionnels. Sinon, elle risque d'être contournée, d'où l'importance du travail sur les codes de conduite, ainsi que la sensibilisation des équipes. L'article 17 de la loi Sapin 2 prescrit ainsi de former les équipes, au minimum tous les collaborateurs exposés. La formation est un élément essentiel pour infuser la culture de la probité au coeur de l'entreprise et éviter qu'elle ne soit qu'une façade, situation pire qu'une absence de norme anticorruption car elle peut abuser les équipes, et l'entreprise peut à tort se sentir à l'abri.

De nombreux praticiens soulignent également l'importance de la formation en ce qu'elle permet aussi aux équipes de parler de leur propre expérience et des difficultés rencontrées pour traiter les situations « grises » ou les dilemmes. Dans la pratique il est parfois difficile de déterminer où commence et où finit la corruption. Le versement d'une commission indue ou douteuse est clairement de la corruption pour les professionnels, mais leurs avis sont partagés sur la question des cadeaux et invitations : courtoisie et savoir-vivre pour les uns, risque de concussion pour les autres. L'essentiel dans la lutte anticorruption est donc la prévention qui passe par l'information et la sensibilisation, c'est-à-dire la formation afin que les entreprises adhèrent à cette lutte.

III. L'adhésion des entreprises

A. Les apports positifs de la norme anticorruption

Malgré les critiques et les difficultés, la norme anticorruption est en voie d'acceptation, et pas uniquement par crainte des sanctions. Les entreprises s'approprient progressivement cette nouvelle exigence dont elles relèvent les aspects positifs. Elles mettent en place une organisation plus dynamique car la prévention de la corruption est un

processus évolutif permanent qui doit être innovant : les entreprises qui ne peuvent plus gagner des marchés par la corruption les gagnent en innovant et en devenant plus efficaces.

Elles sont ainsi amenées à analyser et documenter chaque prise de décision importante et les raisons qui les ont conduites à cette décision. Cette documentation qui nourrit la réflexion préalable à la prise de décision, améliore la circulation de l'information et aboutit à une meilleure connaissance par l'entreprise de son environnement et de ses risques.

Par exemple, le choix des fournisseurs sera documenté et considéré comme explicable et objectif alors qu'un choix « paresseux » sera souvent lié à du « copinage » sans que ce soit forcément malhonnête.

La cartographie des risques, exercice structuré, permet de connaître mieux les risques pays, au-delà des idées préconçues sur le niveau de corruption de tel ou tel pays.

Les aspects positifs du dispositif d'alerte sont également soulignés. Contrairement à une idée reçue, beaucoup de professionnels trouvent que cette ligne d'alerte a un grand intérêt en ce qu'elle fait remonter les anomalies et les problèmes de management. Dans l'ensemble, selon certains, les alertes ne dépassent guère la centaine par entreprise et par an, et portent en général sur des questions de ressources humaines (discrimination, management etc.). Il peut bien y avoir des réticences de salariés lors de l'installation de ce dispositif qui est vu parfois comme un système de dénonciation pouvant donner lieu à des « règlements de compte » entre collègues, ou encore une façon de contourner les représentants du personnel, mais les retours sont plutôt positifs, notamment dans les entreprises avec des filiales dans des pays où le management est traditionnellement autoritaire[6].

Il existe donc des conditions favorisant une mise en place réussie de la norme anticorruption, malgré les profonds bouleversements induits. Mais elles varient d'une entreprise à l'autre : il n'y a pas de « recette ». Peut-on pour autant définir une entreprise type qui serait naturellement plus réceptive à la norme anticorruption et qui réussirait, par nature, à faire de cette contrainte une opportunité, tant elle l'intègrerait parfaitement ? Un modèle qui garantirait la réussite de sa mise en place, ce qui faciliterait la tâche des professionnels ?

B. Vers une entreprise vertueuse type ?

Les cas connus de corruption et les témoignages de professionnels ne permettent pas de dessiner le portrait robot de l'entreprise vertueuse. Le domaine d'activité de l'entreprise semble avoir peu d'effet par lui-même : s'il existe bien des secteurs à risques, il n'y a pas pour autant de secteur préservé par nature.

Apparaissent toutefois, à travers les témoignages de professionnels, des éléments propices à la mise en place efficace de normes de probité. Sont déterminantes la culture, la gouvernance, l'organisation, la stratégie, la vision du rôle de l'entreprise. La présence d'un actionnariat très impliqué (souvent familial) dans une entreprise (parfois) ancienne et chargée d'histoire, peut également jouer un rôle clé dans la diffusion de la norme anticorruption qui correspondra d'emblée aux valeurs de l'entreprise et de sa gouvernance.

Mais vertueuses ou non, toutes les entreprises rencontrent des difficultés dans l'application de la norme anticorruption que seule peut résoudre la puissance publique qui en est la source.

IV. Une nécessaire action de la puissance publique

Pour mettre en place la norme anticorruption, tout en s'appuyant sur un système de contrôle et de sanction efficace, la puissance publique doit à la fois répondre aux attentes des entreprises qui demandent des améliorations du dispositif anticorruption et s'efforcer de coordonner le système de répression international.

A. L'amélioration du dispositif anticorruption

Les systèmes de contrôle et de sanction varient d'un pays à l'autre : sanctions pénales ou civiles, organes dédiés ou non à la lutte anticorruption, séparant ou non la prévention et la répression. Il n'y a pas de modèle type.

Quelle que soit son efficacité, un dispositif de contrôle et de sanction ne peut, à lui seul, être l'unique instrument de lutte anticorruption. Pour que cette lutte soit efficace, la puissance publique doit appuyer ce dispositif sur la prise de conscience des entreprises elles-mêmes, dans une concertation prenant

en compte leurs demandes d'amélioration du dispositif.

Ces demandes sont nombreuses et fortes, à la hauteur des contraintes engendrées par l'exigence de probité. Elles portent principalement sur la nécessité de régler la question de la multiplication des normes et de leur concurrence, de renforcer la loi n° 68-678 du 26 juillet 1968 relative à la communication de documents et renseignements d'ordre économique, commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères, et de développer un dispositif européen.

i. La réduction de la multiplication et la concurrence des normes

70 % des entreprises européennes[7] considèrent le changement rapide de réglementation comme une difficulté, juste après la pression fiscale (72 %). Aux yeux des professionnels, les nouvelles réglementations se sont multipliées en un court laps de temps (loi Sapin 2, loi sur le Devoir de vigilance, Règlement Général sur la Protection des Données personnelles (RGPD), Déclaration de performance extra financière) suscitant pour les entreprises des difficultés, en raison notamment du manque de ressources humaines et budgétaires[8] pour intégrer ces nouvelles normes.

Outre leur multiplication, les normes peuvent se concurrencer, voire se contrarier dans leur exercice. En France, beaucoup de professionnels ont évoqué le conflit possible dans l'application respective du RGPD du 27 avril 2016 et de la loi Sapin 2 du 9 décembre 2016 sur le traitement des données, par exemple dans le cadre des procédures d'évaluation des tiers prévue par la loi Sapin 2. Il s'agit de procéder à toutes vérifications et enquêtes sur des clients, des partenaires d'affaires, des intermédiaires et des fournisseurs, notamment de collecter et de traiter des données pénales, ce que prohibe l'article 10 du RGPD, sauf exceptions, par exemple si « le traitement est autorisé par le droit de l'Union européenne ou par le droit d'un État membre qui prévoit des garanties appropriées pour les droits et libertés des personnes concernées ». La possibilité ou non d'inclure dans lesdites exceptions les enquêtes sur les tiers fait débat parmi les professionnels. Certains considèrent que la loi Sapin 2 constituerait l'autorisation légale permettant de faire ces enquêtes. D'autres soulignent que le risque d'infraction au RGPD demeure, le texte même de la loi ne précisant pas le type de diligence requis et les recommandations sur ce point de l'Agence française anticorruption (AFA) ne pouvant tenir lieu de réglementation ou de loi. Une position commune de la CNIL (Commission Nationale de l'Informatique et des Libertés) et de l'AFA est attendue[9].

ii. Le renforcement de la loi n° 68-678 du 26 juillet 1968

Les entreprises demandent la mise en place d'un dispositif pour les protéger des actions judiciaires à leur encontre émanant d'autorités étrangères. En France, ce rôle est celui de la loi du 26 juillet 1968, relative à la communication de documents et renseignements d'ordre économique, commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères[10]. Cette loi est souvent désignée comme une loi de blocage alors qu'il s'agit plutôt d'une loi d'aiguillage et de coopération interétatique dans les procédures judiciaires. Elle vise à contrôler la transmission des données entre la France et l'étranger, afin non pas de « bloquer » toute transmission mais de la réaliser via le filtre d'une commission rogatoire internationale. Sa violation expose son auteur à un emprisonnement de six mois et à une amende de 18 000 € (jusqu'à 90 000 € pour les personnes morales).

Cette loi a permis aux entreprises françaises de négocier les conditions du contrôle ou monitoring auxquelles elles étaient soumises dans le cadre des dossiers transigés avec les autorités américaines : recours à des moniteurs en général français et transmission de leurs rapports aux autorités américaines par le biais de l'administration française de sorte que puisse être vérifié le respect de la loi.

Mais des critiques sont portées à son encontre : l'efficacité est questionnée car elle a été très peu appliquée par le juge ; une première fois par la chambre criminelle de la Cour de cassation le 12 décembre 2007 (n° pourvoi : 07-83228) et une seconde fois par la cour d'appel de Nancy le 4 juin 2014 (arrêt n° 14/01547). La Cour suprême américaine a ainsi considéré que la menace de condamnation d'une entreprise française au titre de cette loi était de ce fait peu probable et ne pouvait constituer une excuse légale justifiant le refus de communiquer les pièces demandées par une juridiction américaine. Il faudrait donc qu'elle « fonctionne » beaucoup plus pour mieux protéger les entreprises concernées.

Les entreprises demandent son amélioration. Il a été préconisé dans un premier rapport parlementaire en date du 5 octobre 2016 de revoir sa rédaction pour bien identifier les informations réellement sensibles à ne pas communiquer et d'alourdir les sanctions pour la rendre plus crédible notamment aux yeux des autorités américaines[11]. C'est également ce que propose un second rapport parlementaire en date du 26 juin 2019 en y ajoutant un mécanisme obligatoire d'alerte en amont des pouvoirs publics par l'entreprise concernée[12].

Certains professionnels restent cependant sceptiques et invoquent l'intérêt de se doter d'un dispositif européen anticorruption avec une loi de blocage européenne qui aurait plus de poids qu'une loi nationale.

iii. Le développement d'un dispositif européen

La lutte contre la corruption est mondiale, mais ses règles sont nationales. C'est l'une des difficultés que rencontrent les entreprises : la lutte anticorruption n'est pas harmonisée, même en Europe.

Les entreprises évoluant dans un cadre international ont mis en place des règles pour se conformer à la norme de la loi américaine (le Foreign Corrupt Practices Act 1977 (FCPA)), puis à celles d'autres lois étrangères notamment la loi britannique (l'UK Bribery Act 2010 (UKBA)). Et pour se conformer ultérieurement au dispositif prévu par Sapin 2, elles ont eu à compléter leur système anticorruption avec de nouveaux outils de prévention non obligatoires pour les législations américaine et britannique, ce qui reflète la différence entre ces normes nationales.

À défaut d'une harmonisation à l'échelle planétaire, les entreprises demandent qu'elle se fasse au moins à l'échelle européenne. Au-delà de la seule résolution des différences de règles, l'enjeu consiste à mettre en place une compliance européenne, soucieuse à la fois de promouvoir les entreprises européennes dans le monde et de rendre la norme anticorruption plus efficace et plus crédible.

Premier pas dans cette direction d'une norme anticorruption harmonisée : l'adoption d'une directive européenne de protection des lanceurs d'alerte (Directive UE 2019/1937 du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union).

B. La coordination du système de répression international

Une autre source de difficultés réside dans l'extension extraterritoriale des normes nationales : ainsi la loi française a une portée extraterritoriale comme les lois des autres pays dans ce domaine, créant des risques de multiplication des poursuites judiciaires émanant de différents États, amenant à s'interroger sur la portée à l'international du principe « *non bis in idem* ».

Comment éviter les poursuites d'autorités étrangères sur des affaires déjà jugées en France ou ayant fait l'objet d'un accord judiciaire censé mettre un terme à toute procédure sur le dossier en vertu du principe « *non bis in idem* » ?

Les autorités américaines indiquent que ce principe, présent dans leur droit, n'a pas de valeur contraignante entre États sauf stipulation conventionnelle, et entendent décider de poursuivre ou non en fonction de l'existence de procédures étrangères, au cas par cas, d'où une incertitude qui crée un environnement juridique peu propice au développement international des affaires.

C'est également la position d'autres pays, tels que la France. Le droit pénal français n'admet l'application du principe « *non bis in idem* » aux procédures étrangères que de manière restrictive. La Cour de cassation[13] a rappelé que la règle ne s'applique que dans les relations transnationales européennes. Pour les relations hors Union européenne, elle ne s'applique que lorsque l'action de la justice française se fonde sur la compétence extraterritoriale (cf. art 113-9 Code pénal et 692 Code de procédure pénale). Cependant, en instaurant la loi Sapin 2, les autorités ont eu notamment comme objectif de permettre aux entreprises françaises d'échapper aux poursuites des autorités étrangères.

De leur côté, les autorités américaines ont souligné dans leur déclaration du 9 mai 2018[14], leur souci de ne pas « empiler » les condamnations et de tenir compte de l'existence des poursuites d'autorités étrangères dans le traitement des dossiers. En cela, elles se conforment à leur pratique de longue date qui consiste à tenir compte de la coopération internationale et des montants d'amende payés par les entreprises auprès des différentes autorités dans un

même dossier. Sans qu'elles prennent aucun engagement par avance, elles s'acheminent vers une coordination internationale des poursuites avec parfois un abandon pur et simple des poursuites.

C'est ce mécanisme de coordination internationale que l'on peut relever dans le traitement des dossiers :

– Siemens (2008) : le Department of Justice (DOJ) américain a salué l'aide exceptionnelle des autorités de poursuite allemandes : le montant total de l'amende payée par Siemens s'est élevé à plus de 1,6 milliard $ dont 800 millions $ versés aux États-Unis ;

– SBM Offshore (2014) : le DOJ a abandonné les poursuites compte tenu du montant de la pénalité payée aux Pays-Bas. Et si le dossier a été rouvert en 2016, c'est en raison d'éléments nouveaux qui n'avaient pas été portés à la connaissance du DOJ lors de la première enquête.

Cette coopération s'est également produite dans les dossiers où sont intervenues les autorités de poursuite de différents pays :

– VimpelCom (en 2016 : USA, Pays-Bas)

– Odebrecht/Braskem (en 2016 : USA, Brésil, Suisse)

– Rolls Royce (en 2017 : USA, UK, Brésil)

– Keppel Offshore (en 2017 : Brésil, USA et Singapour ; il y est précisé que si les montants à payer à Singapour ou au Brésil sont réduits, la différence sera versée aux USA)

– Telia (en 2017 : USA, Suède, Pays-Bas)

–Société Générale (en 2018 : USA, France)

– Groupe ING (en 2018 : USA, Pays-Bas : après le paiement par ING de 900 millions $ aux autorités néerlandaises, les autorités américaines ont stoppé les poursuites contre cet établissement, en accord avec leur politique énoncée dans leur déclaration du 9 mai 2018, et comme elles l'avaient déjà fait dans le dossier SBM Offshore en 2014).

Et récemment, en janvier 2020, le parquet national financier (PNF), le Serious Fraud Office (SFO) britannique et le Department of Justice (DOJ) américain sont parvenus à la signature simultanée de trois accords avec le Groupe Airbus. Airbus s'est ainsi engagé à verser au Trésor public une amende de 2 083 137 455 € qui tient compte de celle versée au DOJ (265 953 892 €)[15].

Ainsi, dans cette pratique de coopération internationale, le principe « *non bis in idem* » s'applique du moins pour le calcul de l'amende : l'entreprise poursuivie n'est pas amenée à la payer plusieurs fois pour les mêmes faits. Et cette coopération internationale des autorités judiciaires permet de gagner en efficacité dans les enquêtes sur des dossiers complexes qui touchent à de nombreux territoires. De fait, dans le traitement du dossier Société Générale, première coordination des poursuites entre la France et les États-Unis, le PNF avait salué le bénéfice de cette coopération avec le DOJ. Dans le dossier Airbus, le PNF a évoqué un travail mené « en confiance et en totale coopération avec le SFO, le DOJ et le procureur fédéral du district de Columbia »[16]. Et c'est le système de transaction judiciaire tel que le Deferred Prosecution Agreement (DPA) ou la convention judiciaire d'intérêt public (CJIP)[17], qui permet de donner une solution globale impliquant plusieurs juridictions.

On peut donc considérer que le règlement coordonné des litiges tel que pratiqué par les différentes autorités respecte l'esprit de coordination invoqué par la Convention de l'OCDE du 21 novembre 1997 sur la lutte contre la corruption d'agents publics étrangers dans les transactions commerciales internationales[18] puisque l'on a un système de coopération avec une allocation entre les pays qui se joindront aux procédures. L'exercice de cette coopération internationale respecte par ailleurs le principe de souveraineté de chaque État concerné, ce qui ne serait pas le cas si la saisine d'un juge empêchait toute intervention judiciaire d'un autre pays.

Les craintes des entreprises sont compréhensibles : elles ne sont pas « à l'abri » de poursuites étrangères, même si le juge national est déjà saisi. Mais l'interdiction qui serait faite à un juge (national ou étranger) de se saisir, dès lors qu'un autre le serait déjà, ne permettrait-il pas le développement du « *forum shopping* » ? Une entreprise, craignant d'être poursuivie par une autorité jugée sévère, s'auto-dénoncerait en saisissant le juge d'un pays qui lui semblerait plus conciliant, réduisant ainsi l'efficacité de la répression contre la corruption.

À ces difficultés s'ajoutent celles provenant, outre le manque invoqué des ressources, de la complexité des

mesures à mettre en oeuvre, ce qui expliquerait que les entreprises en France n'ont pas achevé cette mise en oeuvre alors même qu'elles connaissent leurs obligations[19].

Le défi de l'anticorruption n'est donc pas complètement relevé.

Notes :

1 Auteur de l'étude Les Entreprises face au défi de l'anticorruption - décembre 2018 (Institut Friedland – CCI Paris-Idf)

2 De 2008 à 2016 année de promulgation de la loi dite Sapin 2 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, 132 entreprises (américaines, françaises et d'autres pays) poursuivies par les autorités américaines au titre de la corruption transnationale, ont dû payer plus de 9 milliards de dollars (source : fcpablog.com).

3 Étude Les Entreprises face au défi de l'anticorruption par Nathalie KALESKI - décembre 2018- P.14.

4 Arrêt cour d'appel de Paris 26 février 2016 (n°13/09208) : première condamnation française de personnes morales au titre de la corruption transnationale.

5 Harvard Business Review : Being an ethical business in a corrupt environment, 23 Mars 2017, S.Ramkrishna Velamuri, William S. Harvey, et S.Venkataraman.

6 Étude Les Entreprises face au défi de l'anticorruption par Nathalie KALESKI - décembre 2018- P.19.

7 TNS Political & Social: Flash Eubarometer 374, Businesses'Attitudes towards Corruption in the EU, February 2014.

8 Enquête AFJE Ethicorp.org (2019-2020) intitulée « Compliance et anticorruption, où en sont vraiment les entreprises en France ? », réalisée auprès de plus de 7 500 juristes représentant environ 1500 entreprises : les répondants invoquent le manque de ressources humaines (55%) et budgétaires (29,38%).

9 À ce jour, l'AFA et la CNIL n'ont pas encore publié leur position.

10 Cette loi interdit, « sous réserve des traités ou accords internationaux », aux Français et résidents en France, ainsi qu'aux dirigeants et agents d'entreprises (ou autres personnes morales) ayant leur siège ou un établissement en France, de communiquer « à des autorités publiques étrangères, les documents ou les renseignements d'ordre économique, commercial, industriel, financier ou technique dont la communication est de nature à porter atteinte à la souveraineté, à la sécurité, aux intérêts économiques essentiels de la France ou à l'ordre public ».

11 Recommandation du Rapport d'information Pierre Lellouche- Karine Berger, Assemblée Nationale, 5 octobre 2016.

12 Recommandation du Rapport établi par Raphaël Gauvain, Assemblée Nationale, 26 juin 2019.

13 Arrêt ch.crim. du 14 mars 2018 (pourvoi n° 16-82117 : les autorités françaises restent compétentes. Après avoir été relaxé par le tribunal correctionnel en 2013, puis condamné par la cour d'appel en 2016 (elle avait retenu sa compétence et rejeté l'application à ce dossier de la règle non bis in idem), Total est définitivement condamné pour corruption d'agent étranger, 20 ans après les faits -affaire pétrole contre nourriture. Pour cette même affaire, Total avait dû verser un montant de 398 millions $ en 2013 aux États-Unis. Le représentant du DOJ avait alors salué la coopération renforcée entre les deux pays, compte tenu des poursuites engagées contre cette société des deux côtés de l'Atlantique, prémisse d'une collaboration qui se retrouvera dans le dossier Société Générale en 2018 puis dernièrement (2020) dans le dossier Airbus.

14 Deputy Attorney General Rod J. Rosenstein delivers remarks at the American conference Institute's 20th Anniversary New York Conference on the FCPA, May 9, 2018, https://www.justice.gov/opa/speech/

15 Convention judiciaire d'intérêt public (CJIP) du 29 janvier 2020 : convention avec le PNF qui évoque expressément la « coordination avec les sanctions prononcées par les autres autorités de poursuite ». Les accords avec ces dernières prévoient qu'Airbus versera 983 974 311 € aux autorités britanniques et 525 655 000 € aux différentes autorités américaines.

16 Communiqué de presse du procureur de la République financier du 31 janvier 2020.

17 DPA et CJIP : la CJIP ou Convention judiciaire d'intérêt public, instaurée par la loi Sapin 2, est inspirée du dispositif américain Deferred Prosecution Agreement (DPA) ou Accord de poursuite différée, dispositif qui permet à une entreprise mise en cause pour faits de corruption, de conclure un accord avec l'autorité de poursuite.

18 L'article 4 de la Convention OCDE du 21 novembre 1997 appelle à une coopération internationale afin de désigner l'État le mieux à même d'exercer les poursuites.

19 Enquête AFJE Ethicorp.org (2019-2020) intitulée « Compliance et anticorruption, où en sont vraiment les entreprises en France ? » : les entreprises ne sont que partiellement à jour de leurs obligations (58,43%) voire absolument pas (3,62%).

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

LA POURSUITE DES CYBERCRIMINELS EN 2020

JACQUES MARTINON

CHEF DE LA MISSION DE PRÉVENTION ET DE LUTTE CONTRE LA CYBERCRIMINALITÉ À LA DIRECTION DES AFFAIRES CRIMINELLES ET DES GRÂCES (DACG) DU MINISTÈRE DE LA JUSTICE

Les idées exprimées dans l'article n'engagent que son auteur et non la Direction des affaires criminelles et des grâces du ministère de la Justice

La crise sanitaire mondiale de 2020, avec ses mesures de confinement et de distanciation sociale, a certes paralysé la majorité des activités économiques mais aussi l'ensemble des activités nécessitant une interaction physique, y compris les activités criminelles. Les trafics de stupéfiants "traditionnels", hors Darknets et assimilés, ont ainsi connu une chute vertigineuse de leur chiffre d'affaires (de l'ordre de 30 à 40% en France), accélérant une migration technologique de "l'ubérisation" du trafic (usage de réseaux sociaux et livraison à domicile)[1]. À l'instar des entreprises et administrations se tournant vers le télétravail, la cybercriminalité a pu encore une fois démontrer sa résilience lors de cette crise mondiale sans précédant, mais aussi son opportunisme.

Ainsi, l'exploitation des failles de cybersécurité présentes dans des applications populaires de visioconférence comme le logiciel Zoom (utilisé par 200 millions de personnes en mars 2020), l'habillage des campagnes de phishing aux couleurs de la prévention de la COVID-19, l'angle d'attaque des configurations de télétravail insuffisamment sécurisées (*Remote Desktop Protocol* (RDP) mal contrôlé, usage inconstant de Réseaux Privés Virtuels (VPN)), le ciblage des laboratoires de recherche médicale, n'en sont que les exemples les plus marquants. Les pouvoirs publics en France ne sont d'ailleurs pas restés inactifs et une campagne de sensibilisation à ces risques cyber a notamment été portée par l'entité cybermalveillance.gouv.fr au bénéfice des salariés et employeurs[2].

Le cybercriminel est dans la grande majorité des cas un délinquant ayant le souhait d'optimiser sa rentabilité économique[3] et s'adapte en conséquence rapidement aux nombreuses opportunités du monde numérique. L'aspect communautaire est également très important, des spécialistes émergeant afin d'offrir une galaxie de services (*Cybercrime as a Service*) dans le cadre d'un écosystème désormais bien établi.

Toutefois, certains acteurs de la cybercriminalité ont des motivations différentes, soutenus voire armés par des ressources étatiques plus ou moins clandestines, dans le cadre de guerres économiques larvées (cyberespionnage) ou de démonstrations de puissance (cybersabotage) multipliant les pré-positionnements à l'intérieur de systèmes critiques. Comme le relève la Revue stratégique de cyberdéfense élaborée en février 2018, la menace est hybride et le cloisonnement entre cyberdéfense et cybercriminalité s'estompe[4]. Dissimuler une cyber agression en acte de cybercriminalité n'est pas que théorique, comme le démontre l'affaire NotPetya (2017).

Un exemple documenté concerne les agissements supposés de certains services de Corée du Nord comme le Groupe LAZARUS, régulièrement accusés par les USA et leur proches alliés de commettre

des faits de cybercriminalité à l'échelle industrielle dans le domaine spécifique des cryptoactifs (détournements de fond sur des plateformes ou directement au préjudice des portefeuilles des particuliers) ou d'établissements bancaires (jackpotting) afin de financer diverses activités, dont potentiellement leur programme nucléaire. Ces agissements sont de nature à compenser les nombreuses sanctions économiques frappant ce pays comme le souligne un rapport d'experts de l'ONU[5]. La détermination de la justice américaine est notable, avec la mise en place de primes pour toutes informations utiles permettant de lutter contre ces méfaits, et ce jusqu'à 5 millions de dollars[6].

D'autre part, si l'on assiste à une structuration constante des cybercriminels, certaines organisations comme Carbanak[7] ayant constitué de véritable trésor de guerre (près d'un milliard de dollars de bénéfice présumé), il existe également de manière plus résiduelle (mais inexorable) une "cyberisation" de la criminalité organisée[8] dans sa partie logistique (communications chiffrées et techniques d'obfuscation) et financière via les cryptoactifs à la traçabilité délicate (versement initial ou blanchiment postérieur).

Les acteurs judiciaires de lutte contre la cybercriminalité doivent donc adapter rapidement leurs stratégies, méthodes et organisations afin d'améliorer leur efficacité. La France n'a initié véritablement ce mouvement qu'en 2015, dans les suites du rapport de référence sur la cybercriminalité « *Protéger les internautes* » élaboré sous l'égide du procureur général Marc Robert[9]. Des progrès indéniables ont été réalisés, mais la poursuite de ces efforts est essentielle afin de consacrer un véritable levier judiciaire redouté par les cybercriminels et activable dans le champ de la cyberdéfense.

Si toutes les juridictions peuvent connaître de faits de cyberdélinquance[10], il convient de relever que le tribunal judiciaire de Paris bénéficie d'une compétence concurrente nationale en matière de cyberattaques[11]. Les contours d'une politique pénale de lutte contre la cyberdélinquance sont en voie de consolidation en priorisant les tendances les plus préoccupantes touchant la population française ainsi que son tissu économique.

Seront présentées dans un premier temps les caractéristiques principales de la cybercriminalité (I) avant d'aborder les adaptations stratégiques et organisationnelles des acteurs judiciaires, ainsi que les nouvelles relations de ces acteurs avec ceux de la cybersécurité (II).

I. Une cybercriminalité polymorphe et souvent occulte

La typologie de la cybercriminalité demeure un défi intellectuel puisque l'angle traditionnel des qualifications pénales est largement imparfait. Les « cyberattaques » recouvrent en réalité de nombreux « phénomènes cyber » distincts dans leur mode opératoire et leur motivation, tels le cyberespionnage, le cybersabotage, le rançongiciel…

Aujourd'hui, la cybercriminalité reste largement occulte notamment car les outils statistiques traditionnels sont *de facto* inopérants pour apprécier finement les évolutions des phénomènes. À cela s'ajoutent les problématiques classiques du chiffre noir (part des infractions qui ne parviennent pas à la connaissance des autorités judiciaires) et d'une preuve numérique parfois chimérique.

A. Une cybercriminalité polymorphe et évolutive

La cybercriminalité a pour caractéristiques principales d'être non seulement polymorphe mais naturellement très évolutive, bénéficiant du fort dynamisme de l'écosystème numérique (surface d'attaque en pleine expansion, nouvelles logistiques et flux financiers émergeants). Au défi de la classification (i) s'ajoutent la création constante de nouveaux métiers cybercriminels (ii) et des évolutions inquiétantes de phénomènes anciens comme dans le cas des rançongiciels (iii).

i. Une classification traditionnelle mais grossière

Traditionnellement, la cyberdélinquance au sens strict couvre les phénomènes pénaux dont l'objet est l'atteinte à un système de traitement automatisé de données (STAD) réprimées par les articles 323-1 à 323-4 du Code pénal.

Dans la pratique, cette première grande catégorie est subdivisée entre les phénomènes de haute intensité (atteinte aux intérêts fondamentaux de la Nation, dimension internationale, haute technicité, nombre important de victimes avérées ou supposées) et de basse intensité. Dans cette perspective, une échelle de gravité a été mise au point dans le

cadre de la Revue stratégique de cyberdéfense, en miroir de l'échelle de gravité américaine (Cyber Incident Severity Schema (CISS)) des actes cybermalveillants (cf schéma ci-dessous), nécessaire à l'application du droit international en cas d'agression cyber caractérisée de la part d'un État hostile.

La seconde grande catégorie de la cybercriminalité regroupe les phénomènes qui ont pour vecteur principal un réseau de communication électronique ou ont été grandement facilités par son utilisation. Il s'agit de la cyberdélinquance au sens large, incluant de nombreuses cyberescroqueries. Ces infractions mixtes couvrent également la lutte contre les activités illicites sur l'internet sombre (darknets[12]).

Enfin, une autre distinction est parfois faite entre les phénomènes de cyberdélinquance purement réalisés dans le cyberespace et ceux qui nécessitent une interaction coordonnée entre monde virtuel et monde physique. Un phénomène hybride est par exemple la multitude de variantes de jackpotting avec une coordination entre une opération informatique de piratage d'un système bancaire et le retrait physique par des complices (*money mules*) des liquidités présentes dans les distributeurs automatiques de billets (DAB), objets dudit piratage.

ii. Les nouveaux métiers de la cybercriminalité

La cybercriminalité prospère et de nouveaux « métiers spécialisés » fleurissent régulièrement, autour d'un concept de « *Cybercrime as a Service* » (analogie avec les services informatiques traditionnels).

Sans être exhaustif, l'on peut citer les locations/ventes d'infrastructures de type *botnets* (réseau d'ordinateurs ou d'objets connectés[13] « zombies », sous le contrôle d'un serveur dit *Command & Control*), d'accès informatiques à des entités déjà piratées (*Access as a service*), de reventes d'informations personnelles (*login* et mot de passe d'une boîte courriel ou d'un compte client, coordonnées bancaires), de maliciels divers (comme certains rançongiciels, cf infra), des services de *Crypter/Packer* augmentant la furtivité de ces maliciels, de *Money mules* (personne qui transfère de l'argent acquis illégalement pour le compte de tiers) ou encore de *Mixer/Blender*[14] facilitant le blanchiment des cryptoactifs comme le Bitcoin.

Tous ces services constituent autant de briques "prêtes à l'emploi" (*Cybercrime enabler*) qui, une fois habilement combinées, permettent de bâtir, en un temps record et avec un investissement financier abordable, un projet cybercriminel plus ou moins sophistiqué mais très souvent lucratif.

Une affaire médiatisée parmi d'autres est celle de la plateforme Deer.io démantelée en mars 2020 par les autorités de poursuite américaines, suite à l'arrestation de son administrateur présumé, Kirill Victorovich Firsov (28 ans). Selon le dossier déposé par le tribunal fédéral de San Diego (Californie), Deer.io permettait depuis 2013, par l'intermédiaire de 24 000 magasins (*shops),* "la *vente d'une variété de données financières et d'entreprises américaines et internationales piratées et/ou compromises, des informations personnelles identifiables (IPI) et des comptes d'utilisateurs compromis de nombreuses entreprises américaines* »[15].

Les comptes de réseaux sociaux piratés sont ainsi très prisés par les cybercriminels afin de lancer des campagnes de phishing à des montants dérisoires (ex : 267 millions de comptes Facebook piratés pour la somme modique de 600 dollars sur un Darknet[16]).

Les cryptomonnaies sont sources de nombreuses opportunités, en les dérobant aux plateformes d'échanges ou aux particuliers, mais également en détournant la puissance de calcul de terminaux afin de « miner » des cryptomonnaies au bénéfice de l'attaquant (*Cryptojacking*).

Autre tendance forte de la cyber-

Echelle de gravité	Equivalence avec l'échelle CISS USA	Caractérisation de l'impact	Caractérisation comme agression armée au sens de l'article 51 de la Charte des Nations-Unies
Niveau 5 - Situation d'urgence extrême	Level 5 Emergency (Black)	Impact extrême	Probablement possible : à examiner au cas par cas.
Niveau 4 - Crise majeure	Level 4 Severe (Red)	Impact majeur	Probablement impossible : les actions correspondant à ces niveaux pourraient néanmoins constituer d'autres faits internationaux illicites (intervention, violation de la souveraineté, usage de la force, etc.).
Niveau 3 - Crise	Level 3 High (Orange)	Impact fort et étendu	
Niveau 2 - Incident grave	Level 2 Medium (Yellow)	Impact fort et circonscrit	
Niveau 1B - Incident	Level 1 Low (Green)	Impact significatif et circonscrit	
Niveau 1A - Evénement significatif		Impact faible	
Niveau 0 - Evénement	Level 0 Baseline (White)	Impact négligeable	

Schéma national de classement des attaques informatiques

criminalité, le phénomène de jackpotting déjà évoqué qui, depuis sa première démonstration théorique en 2010 par le hacker Barnaby Jack, a déferlé en plusieurs vagues notamment en Asie et en Europe, dans les suites du célèbre groupe Carbanak. Les techniques peuvent varier, soit en attaquant le système central de la banque soit en attaquant directement l'ordinateur du DAB, ce qui nécessite alors de réaliser un accès physique (via un adroit coup de perceuse). Là encore, la crainte d'une généralisation de ce phénomène est réelle avec la mise à disposition pour quelques centaines de dollars de maliciels de ce type (cf figure).

Maliciel de Jackpotting

Plus original, il existe des compagnes de recrutement via des annonces d'emploi pour des administrateurs de Darknets, comme pour Liberty Market : *« Nous cherchons à recueillir un membre, homme ou femme, qui possède une bonne orthographe. Vous devrez être familier avec la gestion ergonomique des pages web. Il faudra que vous puissiez vous connecter au moins une heure et demie, quatre fois par semaine. Vous serez en charge de la correction des postes du forum et responsable de leur bonne lisibilité. Vous devrez aussi corriger des douzaines de posts à chaque connexion. Vous aurez votre propre tableau de bord afin que vous puissiez travailler en toute autonomie. »* (Source : www.ladn.eu).

Dans la même veine, on relèvera un service de type « Tag Telegram », où des personnes sont simplement rémunérées pour réaliser des tags dans des zones urbaines prédéterminées, comprenant des indications techniques pour rejoindre une discussion Telegram d'un dealer. Ce nouveau *job* est une autre illustration de « l'ubérisation » rampante des trafics de stupéfiants, où le consommateur commande directement sa drogue via son *smartphone* et une application de messagerie cryptée, et se fait livrer à domicile H24 7j/7. Plutôt que le terme d'ubérisation, on préférera d'ailleurs le terme de "cyberisation" des logistiques criminelles.

Dès lors, une des conséquences probables pourrait être l'éclatement des logiques des territoires de points de *deals*, avec un déplacement sur la visibilité, furtivité et popularité de leur vecteur numérique de communication. On rappellera aussi les affaires judiciaires ayant mis en cause aux États-Unis et en Europe des sociétés (PhantomSecure, PGP Safe, Ennetcom...) commercialisant des smartphones cryptés spécialement adaptés aux besoins de criminels et autre cartels.

iii. Évolution des rançongiciels en 2019/2020

Cas ukrainien (15$/jour – SMIC mensuel local 140$). Source Trustwave

Selon une étude du Club des Experts de la Sécurité de l'Information et du Numérique (CESIN) de 2020, 25% des cyberattaques à l'encontre des entreprises françaises auraient eu pour conséquence une tentative de rançongiciel[17].

Pour mémoire, ce type de maliciel a pour but de chiffrer les données des systèmes infectés (ainsi que les sauvegardes connectées) afin d'extorquer une rançon payable en cryptoactifs en échange de la clé de déchiffrement. Ainsi, selon une autre étude de la société Proofpoint, 33% des sociétés piégées par un rançongiciel auraient payé la rançon[18].

Depuis 2019, on voit apparaître en France un phénomène connu sous le nom de "chasse aux gros gibiers" (*Big Game Hunting*) avec des rançons dépassant le million d'euros. Ces opérations sont bien plus sophistiquées, effectuées par des équipes mieux préparées et choisissant leur victime avec soin.

De plus, les cybercriminels voient leur méfait facilité d'une part, grâce au rançongiciel en tant que service (*ransomware as a service*) dont le modèle économique rappelle celui de l'affiliation (le paiement des développeurs du rançongiciel se faisant par le versement d'une commission d'environ 30% sur les rançons récoltées auprès des victimes), et d'autre part, avec des pirates qui vendent directement des accès illégitimes de système informatique aux cybercriminels désireux de déployer un rançongiciel (*Access as a service*).

Dernier raffinement en date, les cybercriminels menacent désormais les victimes de révéler des données confidentielles de l'entreprise (*leaks*) pour forcer la main des dirigeants en faveur du paiement de la rançon. Ainsi, des groupes malveillants comme Maze, Sodinokibi ou Doppel ont publié plusieurs échantillons de données afin de prouver leurs dires. Cette technique semble redoutable à l'encontre de sociétés multinationales ou des professions libérales (cabinets d'avocats par exemple).

B. Une cybercriminalité occulte

La lutte contre la cybercriminalité est handicapée par plusieurs facteurs, notamment un nombre important d'infractions qui ne sont pas portées à la connaissance de la justice (i) et une preuve numérique aléatoire (ii).

i. Le chiffre noir de la cybercriminalité

Certains phénomènes cybercriminels de haute intensité, comme le cyberespionnage ou le cybersabotage, sont peu judiciarisés, du fait de leur nature sensibles[19]. La publicité d'une cyberattaque à l'encontre d'une entreprise peut nuire à son image. Le règlement européen pour la protection des données personnelles (RGPD) est un espoir, dès lors que les graves violations de données personnelles conduisent à une obligation de notification dans les 72h à la Commission nationale de l'informatique et des libertés (CNIL)[20]. En effet dans 99% des cyberattaques, des données personnelles comme des courriels sont touchées et la nouvelle règlementation oblige le responsable de traitement (ici l'entreprise victime) à notifier officiellement à la CNIL cette violation de données personnelles, dès lors que cette dernière atteint un certain seuil de gravité. En cas de manquement à cette obligation de notification, le responsable de traitement encourt une amende administrative pouvant atteindre 2% du chiffre d'affaires.

Concernant les particuliers, les raisons du chiffre noir sont diverses, du fait d'un caractère parfois imperceptible de l'infraction ou d'un sentiment erroné de l'inutilité de la plainte, souvent couplé à de faibles préjudices matériels.

Une meilleure sensibilisation semble nécessaire, d'où l'importance du dispositif national d'assistance aux victimes d'actes de cybermalveillance[21], et des mesures facilitant le dépôt de plainte. La future plateforme THESEE (projet porté par le ministère de l'Intérieur) est susceptible d'améliorer la connaissance statistique pour certains phénomènes de cybercriminalité. La loi n° 2019-222 de programmation pour la Justice (LPJ) du 23 mars 2019 insère d'ailleurs de nouvelles dispositions afin d'encadrer la plainte en ligne[22].

ii. Preuve numérique, « going dark »[23] et extraterritorialité

La libéralisation du chiffrement a amélioré sensiblement le niveau de cybersécurité, mais a provoqué de manière collatérale des difficultés propres aux investigations judicaires.

La banalisation des applications

de messageries instantanées chiffrées avec des protocoles particulièrement robustes comme ceux dits *End to end* est un défi actuel (Telegram, WhatsApp, Signal...).

De même, la généralisation du chiffrement de type *full disk* sur les terminaux informatiques, dont les *smartphones*, a rendu délicate l'exploitation forensique. Le Centre technique d'assistance (CTA) au sein de la Direction générale de la sécurité intérieure (DGSI) est d'une aide certaine pour l'autorité judiciaire qui peut le requérir afin de tenter de mettre au clair les données chiffrées présentes dans les terminaux numériques saisis.

Comme déjà évoqué, les architectures réseaux de type TOR (*The Onion Router*) participent évidemment à l'obfuscation des comportements criminels sur les *Darknets*, même si les poursuites judiciaires contre la Main Noire (2018) et du French Deep Web Market (2019) menées en France ont visiblement mis un certain coup d'arrêt à l'écosystème francophone.

Demain, la fusion annoncée entre les applications de messageries et les cryptoactifs ne manque pas d'inquiéter les professionnels[24]. L'annonce du LIBRA par la société Facebook, par son caractère systémique au vu du nombre de ses utilisateurs potentiels, a suscité une forte réaction politique qui devra se concrétiser en régulation efficiente et de mécanismes *AML* (mesures anti-blanchiment) et *KYC* (connaissance de clientèle).

Complétant un tableau déjà bien sombre, s'ajoute la difficulté d'une preuve numérique désormais largement stockée en dehors de nos frontières, du fait de l'essor de l'informatique à distance (*Cloud*), mais une éclaircie semble percer les nuages.

En effet, une révolution est à venir avec le futur règlement européen "E-Evidence", qui redéfinit les règles pour l'accès transfrontalier de la preuve numérique et à amener la négociation au nom de l'UE un accord avec les États-Unis afin de faciliter l'accès croisé aux preuves électroniques aux fins de la coopération judiciaire en matière pénale, doublé d'une directive dite « représentant », cette dernière posant le prérequis juridique de l'applicabilité du droit européen aux entreprises mondiales dirigeant leur activité économique sur le territoire européen[25]. Le sujet est au centre de tensions diplomatiques avec les USA, un indispensable dialogue devant être mené par la Commission européenne avec ces derniers afin de résoudre certains conflits de lois dans lesquels sont pris en étau les entreprises du numériques comme les GAFAM. Des négociations entourant un second protocole additionnel à la Convention de Budapest sur la cybercriminalité (Conseil de l'Europe) sont par ailleurs bien avancées et ce, de manière coordonnée avec les travaux menés à Bruxelles.

Il est d'ailleurs intéressant de noter qu'anticipant ces révolutions dans l'accès transfrontalier à la preuve, la politique interne de certaines sociétés (Google par exemple) s'est modifiée récemment en transférant la gestion de certaines réquisitions judiciaires françaises de leur maison mère basée aux USA à leur filiale de droit irlandais[26], lorsqu'il s'agit de données personnelles de citoyens européens.

II. Une adaptation stratégique et organisationnelle des acteurs judiciaires

Une enquête cyber possède plusieurs spécificités, souvent liées à la preuve numérique. La dissémination des victimes cyber sur le territoire conduit à une certaine rationalisation du traitement judiciaire, tandis que la culture du silo administratif doit laisser la place à des échanges interinstitutionnels du fait de la nature transversale des enjeux numériques.

A. Aperçu de stratégies judiciaires en cybercriminalité

Seuls quelques exemples seront évoqués ici, par volonté de ne pas trop en dévoiler (le lecteur nous en pardonnera mais les cybercriminels sont à l'affût de toutes informations en la matière[27]).

La récupération de la preuve numérique nécessitera souvent d'identifier et localiser les serveurs "Back End", où se situe l'essentiel des éléments, pouvant être dissimulés derrière une multitude de serveurs "Proxy", afin de lancer *in fine* des opérations de perquisition chez le prestataire. Il n'est pas rare que les serveurs en ques-

tions soient à l'étranger, et une fine coopération judiciaire internationale sera primordiale d'autant que les migrations de serveur se font parfois en quelques heures.

Concernant les techniques spéciales d'enquête, le régime de l'enquête sous pseudonyme est particulièrement adapté. Ce régime a d'ailleurs été harmonisé récemment dans le Code de procédure pénale (art 230-46) par souci de cohérence et de généralisation aux infractions punies d'une peine d'emprisonnement commises par la voie des communications électroniques, champ large pouvant concerner l'intégralité de la cybercriminalité[28].

La traçabilité de certains cryptoactifs comme le Bitcoin peut également grandement être facilitée par des logiciels commerciaux tels que Chainalysis à destination des enquêteurs spécialisés. D'autre part, la lutte et le démantèlement de plateformes de blanchiment de cryptoactifs (Crypto Mixing) peut permettre de manière complémentaire d'agréger des connaissances sur les transactions douteuses passées via ces plateformes.

Dans la même idée, concentrer les efforts judiciaires contre les plus grandes plateformes d'échanges illégaux sur les Darknets permet non seulement de dissuader les criminels mais également de parfois récupérer des données précieuses relatives aux trafics antérieurs, ouvrant la voie de procédures incidentes contre les utilisateurs de ces plateformes.

Lors de la phase d'interpellation des suspects, priorité sera donnée au "Live Forensics", c'est-à-dire aux investigations numériques d'urgence sur les supports informatiques découverts, afin de minimiser des difficultés techniques ultérieures comme le chiffrement des données. La préparation d'un scénario d'intervention avec des agents infiltrés comme le pratique souvent le FBI est également de nature à surprendre les cybercriminels et d'atteindre plus facilement leurs terminaux numériques.

Enfin, la recevabilité des preuves obtenues par des services d'enquête étrangers demeure un sujet complexe, et la jurisprudence nous paraît relativement fragile. Ainsi, la cour de cassation a considéré que la création d'un faux site pédophile par les autorités américaines constituait une provocation à l'infraction, et a donc annulé la procédure incidente française (Cass. Crim. 7 février 2007, n°06-87753). Toutefois en 2014, elle a validé un recueil de preuves via un forum créé par le FBI sur la fraude à la carte bancaire (Cass. Crim. 30 avril 2014, n° 13-88162). Assurément les débats juridiques se poursuivront avec la multiplication des techniques dites de "pot de miel" (*Honey Pot*) par certaines autorités étrangères.

B. Adaptations organisationnelles et relations des acteurs judiciaires avec ceux de la cybersécurité

La nouvelle forme de criminalité qu'est la cyberdélinquance a conduit l'organisation judiciaire à un début d'adaptation, non achevée, afin de se mettre en ordre de bataille. Ce combat ne peut se mener seul et nécessite d'une part un décloisonnement des acteurs de la cybersécurité (au sens large) ainsi que des réseaux dépassant les frontière hexagonales.

i. Constats sur l'organisation judiciaire en 2020

Sans pouvoir détailler ici les multiples compétences territoriales de l'autorité judiciaire en matière de cybercriminalité, il est important de retenir le rôle primordial du tribunal judiciaire de Paris bénéficiant depuis la loi n° 2016-731 du 3 juin 2016 d'une compétence concurrente nationale en matière d'atteintes aux STAD et crime de sabotage informatique[29].

Cette réforme a permis de consolider la création en 2015 d'une section originellement nommée « F1 » désormais "J3" au parquet de Paris, dédiée au traitement de certaines affaires de cybercriminalité, notamment les plus complexes. Cette section fait désormais partie de la JUNALCO (Juridiction nationale de lutte contre la criminalité organisée). Les effectifs de cette section sont modestes mais en progression[30]. D'ailleurs, la compétence de la juridiction parisienne en matière de cybercriminalité a vocation à croître, en application de la nouvelle compétence nationale concurrente en matière d'infractions très complexes attribuée par la loi du 23 mars 2019 précitée.

Le constat est plus inquiétant au siège avec l'absence notamment de juge d'instruction véritablement spécialisé, ce qui pourrait évoluer dans les prochains mois. D'autre part, il apparaît également nécessaire de constituer des formations de jugement correctionnel sensibilisées aux enjeux de la

cybercriminalité.

Concernant la politique pénale, plusieurs dépêches de centralisation du traitement de certains phénomènes de cybercriminalité ont été produites par la Mission de lutte contre la cybercriminalité (MLC) de la Direction des affaires criminelles et des grâces (DACG) du ministère de la justice[31], notamment le traitement judiciaire des rançongiciels.

Au-delà, les juridictions interrégionales spécialisées (JIRS) connaissent de plus en plus de contentieux de la cybercriminalité, notamment liée à la criminalité organisée et au phénomène de cyberisation déjà décrit[32].

Enfin, un réseau de magistrats « cyberréférents » dans les tribunaux, cours d'appel et JIRS a été consacré, dans les suites de la première réunion nationale des magistrat cyberréférents, co-organisé en juin 2019 par le parquet de Paris et la DACG. Ces magistrats cyberréférents constituent ainsi le vivier de demain pour lutter contre la cyberdélinquance, et des actions de formation sont régulièrement organisées à leur bénéfice par l'administration centrale sur des thèmes comme les cryptoactifs ou la lutte contre les Darknets illicites.

ii. Densification des liens entre acteurs judiciaires et ceux de la Cybersécurité

De manière globale, les acteurs judiciaires et ceux de la cybersécurité, de l'industrie numérique et de la protection des données personnelles assurée par la CNIL ont naturellement vocation à croiser leur regard et expérience afin de potentialiser leurs efforts respectifs.

L'administration centrale (DACG), via la Mission précitée, contribue aux travaux stratégiques du Centre de coordination des crises cyber (C4) instauré suite à la Revue stratégique de cyberdéfense et piloté par le Secrétariat général à la défense et à la sécurité nationale (SGDSN).

D'autre part, des échanges réguliers se font avec l'industrie numérique, notamment dans le cadre du Groupe de ontact ermanent (GCP). Ce GCP, piloté par la Délégation ministérielle en charge des industries de sécurité et à la lutte contre les cybermenaces (DMISC), a pour objectif d'améliorer le dialogue avec les acteurs privés comme Apple, Google, Twitter, Microsoft, Facebook, et récemment Dropbox, dans un esprit constructif partagé, tant sur les modalités des réquisitions judiciaires que les dispositifs de retrait de contenu toxique (toutefois, la récente loi contre la haine en ligne dite loi AVIA adoptée le 13 mai 2020 par l'Assemblée nationale donne à ce sujet un rôle central de régulateur des réseaux sociaux au Conseil supérieur de l'Audiovisuel (CSA).

Enfin, la DACG fait partie du conseil d'administration du Groupement d'intérêt public ACYMA en charge du site gouvernemental cybermalveillance.gouv.fr qui a su s'imposer en quelques années comme une des références de sensibilisation des particuliers et des entreprises françaises aux menaces cyber. Le dynamisme de cette structure est à saluer.

Afin de sensibiliser des membres éminents de la société civile, il faut également s'enorgueillir de la création en 2018 d'une formation commune « *souveraineté numérique et cybersécurité* » de l'IHEDN (Institut nationale des hautes études de la défense nationale) et de l'INHESJ[33] (Institut national des hautes études de sécurité et de justice) dont le public est constitué de hauts cadres publics et privés.

iii. Des réseaux internationaux indispensables

La coopération internationale est un facteur clé de ce succès, avec l'aide conjointe d'EUROPOL, d'EUROJUST et d'INTERPOL.

La création de l'EC3 (European CyberCrime Center) au sein d'EUROPOL a permis la concentration d'enquêteurs d'élite et d'analystes de talent en cybercriminalité. La possibilité de créer des JCAT (Joint Cybercrime Action Taskforce) pour coordonner des stratégies européennes est un succès.

Concernant EUROJUST, l'investissement dans la lutte contre la cybercriminalité est également une réalité, avec un nombre grandissant d'équipes communes d'enquêtes (ECE) assurant une meilleure planification entre autorités judiciaires et une certaine fluidité procédurale. Le soutien d'EUROJUST au réseau European Judicial Cybercrime Network (EJCN) est également à souligner.

La vénérable institution qu'est INTERPOL a aussi su prendre le tournant de la cybercriminalité, en contribuant fortement à la lutte contre la pédopornographie en ligne, ainsi qu'en établissant

dès 2015 un nouveau Complexe mondial basé à SINGAPOUR orienté notamment sur les défis technologiques.

CONCLUSION

Le levier judiciaire doit encore gagner en maturité mais des progrès sont indéniablement en cours. Les menaces issues du monde numérique ne doivent pas rester sans réponse, d'autant que la surface d'attaque ne cesse de s'étendre, avec des conséquences potentiellement systémiques pour l'économie et des mises en danger de l'intégrité physique de nos citoyens (dysfonctionnement des systèmes informatiques d'un hôpital ou de machines médicales).

Heureusement, nos élites semblent enfin prendre conscience de ces enjeux mais il faudra beaucoup de volonté pour traduire des discours optimistes en réalité opérationnelle. Les autorités publiques des pays d'Europe n'ont pas suffisamment vu venir la vague de la cybercriminalité, et la France ne fait pas figure d'exception. Il est encore temps d'agir, mais la perspective d'un tsunami cyber est un réel danger dans les années à venir.

Notes :

1 Déclaration publique du ministre de l'Intérieur Christophe Castaner, 15 mai 2020.

2 https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/recommandations-securite-informatique-teletravail

3 Le cas des "hacktivistes" comme le collectif Anonymous semble ainsi une exception. Particulièrement difficiles à analyser, ces mouvements peuvent connaître des regains d'activités en réponse à de fortes tensions sociopolitiques, illustrées en juin 2020 par des manifestations antiracistes dénonçant les violences policières aux USA suite au décès tragique de George Floyd.

4 http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf

5 Le rapport du groupe d'experts du comité de sécurité 1718 du Conseil de sécurité des Nations Unies indique que la Corée du Nord génère des revenus importants malgré les sanctions du Conseil de sécurité des Nations Unies en utilisant des cyber activités malveillantes. Fin 2019, ce pays aurait tenté de voler jusqu'à 2 milliards de dollars par des moyens cybercriminels. Ce rapport détaillé et finalisé en mars 2020 est disponible à l'adresse suivante (notamment p52-53 et p65-69 : https://www.undocs.org/fr/S/2020/151

6 https://rewardsforjustice.net/english/about-rfj/north_korea.html

7 Voir le documentaire "tomorrow unlocked, hacker : hunter - Cashing In" : https://www.youtube.com/watch?v=RTalC_nKtVQ

8 Von Lampe, Klaus. (2016). Organized Crime: Analyzing illegal activities, criminal structures, and extra-legal governance. 10.4135/9781506305110.

9 Rapport « Protéger les internautes » du groupe de travail interministériel sur la lutte contre la cybercriminalité, février 2014, consultable à l'adresse suivante : http://www.justice.gouv.fr/include_htm/pub/rap_cybercriminalite.pdf

10 Nous utiliserons indifféremment les expressions « cybercriminalité » et « cyberdélinquance », étant entendu que le terme « cybercriminalité » est le plus usité du fait de son pendant anglo-saxon « cybercrime », alors même que la quasi intégralité des infractions « cyber » sont bien des délits, et non des crimes au sens du droit pénal français.

11 Article 706-72-1 du CPP (créé par la loi n°2016-731 du 3 juin 2016) : « Pour la poursuite, l'instruction et le jugement des infractions entrant dans le champ d'application de l'article 706-72, le procureur de la République, le pôle de l'instruction, le tribunal correctionnel et la cour d'assises de Paris exercent une compétence concurrente à celle qui résulte de l'application des articles 43, 52 et 382. ». Les infractions visées correspondent aux attaques aux systèmes de traitement automatisé de données (STAD) et au cybersabotage.

12 Le plus connu étant le protocole TOR (The Onion Router).

13 Un cas célèbre étant le Botnet issu du maliciel Mirai en 2016, ayant servi à des attaques DDos (Distributed Denial of Service) touchant notamment OVH et Dyn, cette dernière affectant une partie critique d'Internet au niveau de la gestion des services DNS (Domaine Name System). En août 2019, le C3N (gendarmerie nationale) a démantelé avec succès le Botnet Retadup composé de plus 500 000 machines infectées.

14 Le site Bestmixer.io a toutefois était mis sur la touche en 2019 par une action conjointe d'EUROPOL et des enquêteurs financiers néerlandais, avec un chiffre d'affaires estimé à 200 millions d'euros.

15 https://www.justice.gov/usao-sdca/pr/fbi-takes-down-russian-based-hacker-platform-arrests-suspected-russian-site

16 https://www.presse-citron.net/267-millions-comptes-facebook-etaient-vente-600-dollars-dark-web/

17 https://www.cesin.fr/uploads/files/BJ20433%20-%20Barom%C3%A8tre%20du%20CESIN%20vague%205%20-Vdef.pdf

18 https://www.usine-digitale.fr/article/fic-2020-d-apres-proofpoint-33-des-organisations-attaquees-par-ransonware-paient-la-rancon.N923974

19 La doctrine américaine est différente à cet égard, au vu de l'activisme récent du Department of Justice (DoJ) à l'encontre de ressortissants chinois ou russes.

20 Voir le cas d'Airbus en janvier 2019.

21 https://www.cybermalveillance.gouv.fr/

22 Nouvel article 15-3-1 du CPP.

23 Cette expression d'origine militaire fait référence à la perte soudaine des communications de l'adversaire pouvant être analysées, au profit de moyens de communications indétectables.

24 Voir le lancement du réseau TON et la cryptomonnaie GRAM par l'entreprise TELEGRAM, annoncé pour le dernier trimestre 2019, suite à une levée de fonds de 1,7 milliards de dollars.

25 Le règlement européen de protection des données (RGPD) avait posé une première pierre à l'édifice, quoique sur des critères de rattachement distincts.

26 Force est de constater que la quasi-totalité des sociétés californiennes du numériques sont installées en Irlande, potentiellement pour des questions d'optimisation fiscale.

27 Preuve en sont les échanges en procédure pénale détectés sur certains forums de Darknets.

28 Article 230-46 du CPP : « Aux seules fins de constater les crimes et les délits punis d'une peine d'emprisonnement commis par la voie des communications électroniques, et lorsque les nécessités de l'enquête ou de l'instruction le justifient, les officiers ou agents de police judiciaire agissant au cours de l'enquête ou sur commission rogatoire peuvent, [...], procéder sous pseudonyme aux actes suivants sans en être pénalement responsables :

1° Participer à des échanges électroniques, y compris avec les personnes susceptibles d'être les auteurs de ces infractions ;

2° Extraire ou conserver par ce moyen les données sur les personnes susceptibles d'être les auteurs de ces infractions et tout élément de preuve ;

3° Après autorisation du procureur de la République ou du juge d'instruction saisi des faits, acquérir tout contenu, produit, substance, prélèvement ou service, y compris illicite, ou transmettre en réponse à une demande expresse des contenus illicites. »

29 Article 706-72-1 du CPP.

30 Trois magistrats, ainsi qu'un assistant spécialisé et un greffier (juin 2020).

31 Ex : dépêches DACG des 10 mai 2017 et 22 juin 2018 concernant d'une part la mise en oeuvre opérationnelle de la compétence nationale concurrente du parquet de Paris en matière d'atteintes aux systèmes de traitement automatisé de données (STAD) et le traitement judiciaire des "rançongiciels", et d'autre part la centralisation du traitement des "fraudes aux réparations informatiques".

32 Ex : le démantèlement de la Main noire, une plateforme du Darknet, sous la supervision de la JIRS de Lille.

33 La suppression prochaine et malheureuse de l'INHESJ ne devrait pas remettre en question cette formation.

OUVRAGES RÉCENTS

CYBER CRIMES

AUTEURS : PIERRE PENALBA

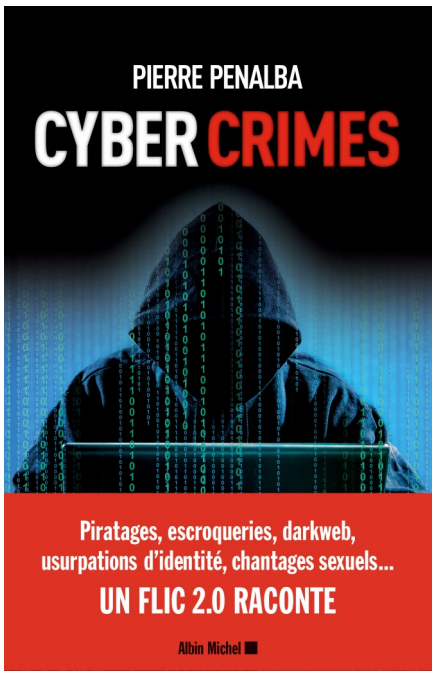
ÉDITEUR : ALBIN MICHEL

Résumé

La cybercriminalité explose.

Piratages de données, escroqueries, réseaux pédophiles... Nous sommes tous concernés, souvent sans le savoir. Ce sont en effet 978 millions de personnes dans le monde qui subissent une cyberattaque chaque année.

Le commandant Pierre Penalba, à la tête du premier groupe de lutte contre la cybercriminalité de la Police nationale, traque quotidiennement les criminels du Net. Dans ce voyage au coeur d'un monde inconnu et pourtant tout proche, il nous dévoile, de l'intérieur, leurs ruses, leurs procédés et le cynisme impressionnant qui



guide leurs méfaits. Escrocs déposant plainte contre leurs victimes, hackers s'emparant de gigantesques fichiers, vidéos intimes provoquant des chantages sexuels, faux documents administratifs, usurpations d'identité, le hasard des enquêtes amène l'auteur à se retrouver au coeur de situations dramatiques ou loufoques.

Il nous livre aussi son expérience et ses conseils pratiques.

Un document captivant sur cette société qui est désormais la nôtre, pour nous éviter d'en devenir les victimes.

Spécialiste du Net, Pierre Penalba est également expert informatique et formateur auprès d'unités de police françaises et étrangères. Il a écrit ce livre avec Abigaelle Penalba

ÉLÉMENTS STATISTIQUES SUR LA TRAITE DES ÊTRES HUMAINS EN FRANCE

AMANDINE SOURD

CHARGÉE D'ÉTUDES À L'OBSERVATOIRE NATIONAL
DE LA DÉLINQUANCE ET DES RÉPONSES PÉNALES (ONDRP)

La mesure de certains phénomènes criminels peut s'avérer complexe. Toutefois, plusieurs sources de données peuvent être mobilisées pour apporter des connaissances sur ces derniers. Communément, les enquêtes de victimation sont considérées comme étant les sources de données les plus fiables pour apprécier l'ampleur réelle de certains crimes ou délits. C'est le cas des violences sexuelles pour lesquelles il est possible d'estimer le nombre de personnes victimes malgré la faible proportion de dépôt de plainte[1].

Néanmoins, ces enquêtes ne sont pas pertinentes pour mesurer tous les types de crimes ou délits. En effet, l'illégalité dans laquelle se trouvent les victimes de certains phénomènes criminels rend ces dernières quasiment invisibles auprès des autorités. C'est notamment le cas des victimes de traite des êtres humains.

Plusieurs estimations du nombre de victimes de traite des êtres humains sont réalisées par les organismes internationaux. Nous pouvons notamment citer celle de l'Office des Nations Unies contre la drogue et le crime (ONUDC) recensant plus de 24 000 victimes détectées par 97 pays en 2016[2] et celle de l'Organisation Internationale du Travail portant à 25 millions le nombre de personnes victimes de travail forcé (incluant l'exploitation sexuelle) dans le monde en 2016[3]. Toutefois, le manque de données statistiques précises sur ce phénomène est un constat partagé par de nombreux organismes internationaux et européens qui enjoignent les pays, dont la France[4], à poursuivre leurs efforts pour mieux mesurer la traite des êtres humains.

Comme évoqué, la mesure de ce phénomène est complexe du fait de l'invisibilité de ces protagonistes[5]. Les autorités peuvent donc avoir des difficultés pour identifier les victimes et les auteurs de traite, notamment en raison du difficile report des faits auprès des autorités pour les victimes[6]. Ces dernières expriment généralement une peur de représailles en cas de dépôt de plainte ou de témoignages contre leurs exploiteurs[7]. De plus, l'implication des États à lutter contre ce phénomène criminel peut également avoir un impact. Ainsi, les chiffres des autorités n'en reflètent qu'une petite partie.

Le premier Plan d'action national de lutte contre la traite des êtres humains (2014-2016)[8] préconisait la mise en place d'outils statistiques permettant de mesurer le phénomène de la traite en France. En réunissant ses partenaires, l'Observation national de la délinquance et des réponses pénales (ONDRP) a réfléchi aux meilleures méthodes possibles pour estimer l'ampleur de ce phénomène. Depuis 2015, deux initiatives sont mises en oeuvre avec la création de deux groupes de travail sur les données statistiques.

Pour analyser les données d'un phénomène criminel peu visible, il faut d'abord commencer par étudier ce qui est visible. C'est pourquoi, un premier groupe de travail a réuni les administrations

susceptibles de transmettre des informations chiffrées sur les victimes ou les auteurs de traite (I.). Un second groupe a été créé rassemblant les associations accompagnant des victimes de traite (II.). En effet, leur connaissance de la problématique et du terrain en font des acteurs essentiels.

Les derniers apports de ces deux initiatives sont disponibles dans les publications suivantes : « La traite et l'exploitation des êtres humains en France : les données administratives » (Grand angle n° 52 octobre 2019), et « La traite des êtres humains en France. Profil des victimes suivies par les associations en 2018 » correspondant aux résultats de la 3ème édition de l'enquête annuelle sur les victimes de traite suivies par les associations[9].

Définir la traite des êtres humains

Plusieurs textes internationaux et européens ont servi de base à la création de l'incrimination de « traite des êtres humains » en France. En particulier, le Protocole additionnel de la Convention des Nations Unies contre la criminalité transnationale organisée visant à prévenir, réprimer, et punir la traite des personnes, en particulier des femmes et des enfants, dit Protocole de Palerme, adopté par l'Assemblée générale de l'Organisation des Nations Unies le 15 novembre 2000 (entrée en vigueur le 25 décembre 2003), qui définit la traite des êtres humains en son article 3 comme étant « *le recrutement, le transport, le transfert, l'hébergement ou l'accueil de personnes, par la menace de recours ou le recours à la force ou à d'autres formes de contrainte, par enlèvement, fraude, tromperie, abus d'autorité ou d'une situation de vulnérabilité, ou par l'offre ou l'acceptation de paiements ou d'avantages pour obtenir le consentement d'une personne ayant autorité sur une autre aux fins d'exploitation. L'exploitation comprend, au minimum, l'exploitation de la prostitution d'autrui ou d'autres formes d'exploitation sexuelle, le travail ou les services forcés, l'esclavage ou les pratiques analogues à l'esclavage, la servitude ou le prélèvement d'organes* ».

La Convention du Conseil de l'Europe sur la lutte contre la traite des êtres humains du 16 mai 2005, dite Convention de Varsovie (entrée en vigueur le 1er février 2008) reprend cette définition précitée et crée, par la même occasion, un groupe d'experts sur la lutte contre la traite des êtres humains (GRETA) chargé de l'évaluation et du suivi des dispositions relatives à la traite dans les pays signataires.

La Directive du Parlement européen et du Conseil du 5 avril 2011 concernant la prévention de la traite des êtres humains et la lutte contre ce phénomène ainsi que la protection des victimes réaffirme l'engagement de l'Europe dans la lutte contre la traite et incite les États membres à faire de la répression des auteurs, de la prévention et de la protection des victimes, des priorités nationales. Par ailleurs, dans cette Directive, l'exploitation de la mendicité et la contrainte à commettre des délits sont citées explicitement comme étant des finalités de la traite des êtres humains.

La loi n° 2013-711 du 5 août 2013 portant diverses dispositions d'adaptation dans le domaine de la justice en application du droit de l'Union européenne et des engagements internationaux de la France a transposé et adapté au droit pénal français la Directive du 5 avril 2011. Le droit pénal français a renforcé ainsi sa législation relative à la lutte contre la traite initiée en 2003. L'article 225-4-1 du Code pénal définit la traite des êtres humains comme suit :

« La traite des êtres humains est le fait de recruter une personne, de la transporter, de la transférer, de l'héberger ou de l'accueillir à des fins d'exploitation dans l'une des circonstances suivantes :

1° Soit avec l'emploi de menace, de contrainte, de violence ou de manoeuvre dolosive visant la victime, sa famille ou une personne en relation habituelle avec la victime ;

2° Soit par un ascendant légitime, naturel ou adoptif de cette personne ou par une personne qui a autorité sur elle ou abuse de l'autorité que lui confèrent ses fonctions ;

3° Soit par abus d'une situation de vulnérabilité due à son âge, à une maladie, à une infirmité, à une déficience physique ou psychique ou à un état de grossesse, apparente ou connue de son auteur ;

4° Soit en échange ou par l'octroi d'une rémunération ou de tout autre avantage ou d'une promesse de rémunération ou d'avantage.

L'exploitation mentionnée au premier alinéa du présent I est le fait de mettre la victime à sa disposition ou à la disposition d'un tiers, même non identifié,

afin soit de permettre la commission contre la victime des infractions de proxénétisme, d'agression ou d'atteintes sexuelles, de réduction en esclavage, de soumission à du travail ou à des services forcés, de réduction en servitude, de prélèvement de l'un de ses organes, d'exploitation de la mendicité, de conditions de travail ou d'hébergement contraires à sa dignité, soit de contraindre la victime à commettre tout crime ou délit. [...]

II. - La traite des êtres humains à l'égard d'un mineur est constituée même si elle n'est commise dans aucune des circonstances prévues aux 1° à 4° du I. » Art. 225-4-1 du CP.

I. Une harmonisation des données des autorités sur la traite et l'exploitation des êtres humains

En France, seules les autorités désignées comme compétentes peuvent identifier « officiellement » une victime de traite. L'instruction du 19 mai 2015 relative aux conditions d'admission au séjour des ressortissants étrangers victimes de la traite des êtres humains ou de proxénétisme émanant du ministère de l'Intérieur rappelle que l'identification de ces victimes relève de la *« compétence exclusive des services de police et des unités de gendarmerie »*. Cette identification permet la mise en place de mesures de protection de la victime, notamment étrangère, et d'une prise en charge adaptée. Depuis 2016, ces prérogatives ont été étendues à l'Inspection générale du travail en application de l'ordonnance n° 2016-413 relative au contrôle de l'application du droit du travail modifiant l'article L.8112-2 du Code du travail.

Depuis 2015, l'ONDRP coordonne un groupe de travail réunissant les services du ministère de l'Intérieur, du ministère de la Justice, de la Direction générale des étrangers en France et de la Direction générale du travail. Ce groupe vise à harmoniser l'ensemble des données officielles sur la traite des êtres humains. L'objectif est de pouvoir dresser un panorama des victimes et auteurs identifiés par les autorités compétentes en France en ayant une lecture commune des données.

A. Une nomenclature commune pour identifier les infractions relevant spécifiquement de traite et celles correspondant à l'une de ses finalités

En France, comme explicité dans l'article 225-4-1 du Code pénal, la traite des êtres humains peut recouvrir différents types d'exploitation. Cependant, ces derniers ne sont pas toujours identifiés par les autorités comme relevant d'une infraction de traite des êtres humains *stricto sensu* mais peuvent être appréhendées sous l'angle d'autres infractions liées à l'une des finalités de la traite spécifiées dans ce même article[10]. Par exemple, elles peuvent correspondre à d'autres infractions prévues par le Code pénal telles que le proxénétisme ou la réduction en esclavage.

C'est pourquoi la Direction des affaires criminelles et des grâces (DACG) du ministère de la Justice a réalisé une nomenclature spécifique permettant d'identifier les natures d'infractions (NATINF)[11] relevant de la traite des êtres humains *stricto sensu* et celles correspondant à l'une des finalités de la traite. Du fait de l'impossibilité d'identifier une forme d'exploitation dans les natures d'infractions spécifiques à la traite, il a été nécessaire d'ajouter à cette nomenclature les infractions relevant des finalités de la traite. Par ailleurs, les natures d'infractions de traite ne sont pas systématiquement utilisées, bien qu'une circulaire datant de 2015 incite les magistrats à recourir de manière accrue aux qualifications de traite des êtres humains[12]. En raison de la mise en place de cette nomenclature par les administrations compétentes, pour évoquer leurs données, nous utilisons l'expression « traite et exploitation des êtres humains » et non celle de « traite des êtres humains ».

Cette classification est, aujourd'hui, commune aux ministères de l'Intérieur et de la Justice permettant ainsi d'harmoniser le décompte des victimes et des auteurs de ces infractions. À cet égard, 135 infractions ont été identifiées et réparties en 9 groupes distincts. Ces derniers ont été rassemblés selon les formes d'exploitation auxquels ils renvoient. Il y a donc deux types de données disponibles : celles sur les infractions de traite des êtres humains (au sens de l'article 225-4-1 du Code pénal) sans distinction possible sur la forme d'exploitation subie et celles ne relevant pas de l'infraction de traite *stricto sensu* mais d'une infraction liée à l'une des finalités de la traite décrites dans l'article 225-4-1 du Code pénal.

Ce travail d'harmonisation de la nomenclature utilisée pour comptabiliser les victimes et les auteurs de traite et d'exploitation des êtres humains permet aujourd'hui d'avoir des données à différents niveaux de la chaîne pénale allant de l'identification de la victime par la police ou la gendarmerie (données issues du Service statistique ministériel de la sécurité intérieure - SSMSI)[13], en passant par les données sur les personnes poursuivies du ministère de la Justice (Sous-direction de la statistique et des études - SDSE), jusqu'à celles sur les auteurs condamnés (DACG).

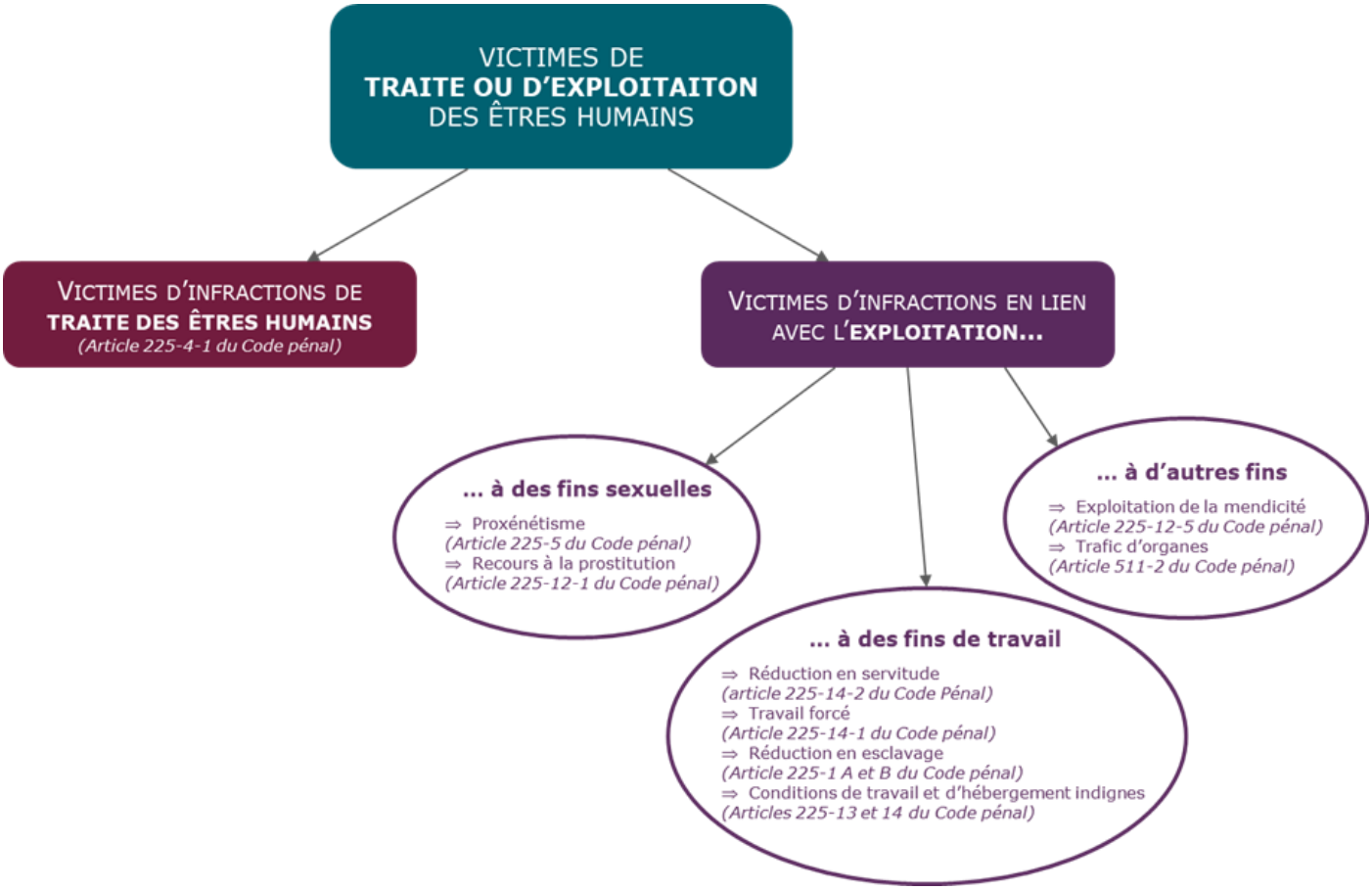
B. Les données sur les victimes et les auteurs de traite ou d'exploitation des êtres humains

Les analyses portant sur les victimes, les personnes poursuivies ou condamnées ont été réalisées en cumulant les données de 2016 et 2017 car les effectifs sont faibles[14].

i. Les victimes de traite ou d'exploitation des êtres humains

Selon la nomenclature établie par la DACG et les données transmises par le SSMSI, 1 593 victimes de traite ou d'exploitation des êtres humains ont été identifiées par la police et la gendarmerie en 2016 et 2017. Parmi elles, 8 % l'ont été pour au moins une infraction de traite des êtres humains (au sens de l'article 225-4-1 du Code pénal) soit 123 victimes. Près des deux tiers des victimes ont été identifiées pour une infraction en lien avec l'exploitation à des fins sexuelles (1 022 victimes, soit 57 % pour proxénétisme et 7 % pour recours à la prostitution de personnes vulnérables). Plus d'un cinquième étaient victimes d'une infraction en lien avec l'exploitation à des fins de travail (327 victimes dont 314 pour des conditions de travail et d'hébergement indignes). De plus, 8 % des victimes ont été identifiées pour une infraction d'exploitation de mendicité (soit 124 victimes). Aucune victime de trafic d'organes n'a été enregistrée par les forces de l'ordre en France en 2016 et 2017.

Concernant le profil des victimes de traite ou d'exploitation des êtres humains, plus des trois quarts sont des femmes (76 %). Cette surreprésentation



Source : ONDRP, représentation du champ concernant les données des administrations sur la traite et l'exploitation des êtres humains

des femmes est commune à toutes les infractions à l'exception des victimes d'infractions en lien avec l'exploitation à des fins de travail pour lesquelles la majorité des victimes sont des hommes (61 %).

Au moment des faits, 70 % des victimes de traite ou d'exploitation des êtres humains sont majeures. La moyenne d'âge des victimes est de 26 ans. Les victimes mineures sont généralement des jeunes filles ; elles représentent 75 % des mineurs identifiés. Les mineurs sont majoritairement victimes d'infractions en lien avec l'exploitation à des fins sexuelles (61 % des mineurs). Près d'un quart des mineurs sont victimes de mendicité forcée ; ils représentent 85 % des victimes de ce type d'infraction et sont âgés en moyenne de 9 ans.

La traite et l'exploitation des êtres humains est un phénomène criminel mondial : 64 nationalités différentes ont été enregistrées par la police et la gendarmerie. Plus de la moitié des victimes sont de nationalité étrangère (59 %). La France, la Roumanie et la Chine sont les trois principaux pays d'origine des victimes, représentant respectivement 41 %, 11 % et 8 % des victimes.

Les nationalités des victimes diffèrent selon les infractions subies. Les victimes d'infractions de traite des êtres humains sont 43 % à avoir la nationalité d'un pays d'Asie, majoritairement la Chine. Près de la moitié des victimes d'infraction à des fins sexuelles ou de travail sont de nationalité française (respectivement 48 % et 43 %). Les victimes d'exploitation de la mendicité sont aussi originaires d'Europe, la plupart étant de nationalité roumaine (53 %).

Les victimes ayant une nationalité d'un pays européen représentent 63 % de l'ensemble des victimes (soit 1 011 victimes). Près des deux tiers de ces victimes sont de nationalité française (65 %) et près de 5 % ont spécifiquement été identifiées comme victimes de traite. La plupart sont victimes d'une infraction en lien avec l'exploitation à des fins sexuelles (70 %) et 16 % d'une infraction en lien avec l'exploitation par le travail.

Les victimes ayant la nationalité d'un pays d'Afrique représentent 15 % de l'ensemble (231 victimes). Les services de police et les unités de gendarmerie ont identifié 14 % de victimes de traite des êtres humains au sens strict dont 45 % sont des ressortissants du Nigéria.

Les forces de l'ordre ont identifié 14 % de victimes ayant la nationalité d'un pays d'Asie (218 victimes). Un cinquième a subi une infraction de traite des êtres humains au sens strict (43 victimes) dont la moitié est de nationalité chinoise. Parmi les victimes d'infractions en lien avec l'exploitation à des fins de travail (27 %) ; celles ayant la nationalité bangladaise sont les plus représentées (32 %).

Parmi les victimes de nationalité d'un pays d'Amériques (77 victimes), 92 % ont été victimes d'une infraction en lien avec l'exploitation à des fins sexuelles, majoritairement de nationalité brésilienne.

ii. Les personnes poursuivies pour traite ou exploitation des êtres humains

Les données fournies par la SDSE du ministère de la Justice portent uniquement sur les personnes ayant fait l'objet de poursuite par les parquets. En 2016 et 2017, 2 446 personnes ont été poursuivies par les procureurs de la République pour traite ou exploitation des êtres humains. Parmi elles, 16 % ont été poursuivies pour au moins une infraction de traite des êtres humains (au sens de l'article 225-4-1 du Code pénal). Les personnes ont été majoritairement poursuivies pour une infraction de proxénétisme (68 %) ou pour une infraction de conditions de travail et d'hébergement indignes (24 %).

Contrairement aux victimes, la plupart des personnes poursuivies pour traite ou exploitation des êtres humains sont des hommes (75 %), majeurs (87 %) et sont généralement jeunes (35 % ont entre 18 et 29 ans). Toutefois, les personnes poursuivies pour une infraction de conditions de travail et d'hébergement contraires à la dignité de la personne sont plus âgées : 37 % ont entre 30 et 44 ans et 23% entre 45 et 59 ans.

Notons que la part des femmes est plus importante parmi les personnes poursuivies pour une infraction de traite des êtres humains au sens strict. Cela s'explique par la spécificité de certains réseaux comme les réseaux de traite nigérians ayant comme finalité l'exploitation sexuelle. En effet, les femmes, appelées les *madams*, occupent une place importante et visible au sein de l'organisation criminelle. Souvent anciennes prostituées, elles de-

viennent à leur tour exploiteur afin de rembourser leur dette plus rapidement[15].

Concernant plus spécifiquement les nationalités des personnes poursuivies, plus de 60 % sont de nationalité étrangère et 37% de nationalité française. Lorsque les personnes sont poursuivies pour une infraction de traite des êtres humains *stricto sensu*, 65% sont de nationalité hors Union européenne et 18% française.

Il est intéressant de relever que les personnes poursuivies pour proxénétisme en 2016 et 2017 sont majoritairement de nationalité française (48%) ou d'un pays hors Union européenne (42%). À l'inverse, les personnes poursuivies pour une infraction de conditions de travail et d'hébergement contraires à la dignité de la personne ont en général une nationalité d'un pays de l'Union européenne (47 %) : 28 % sont françaises et 23 % ont la nationalité d'un pays hors de l'Union européenne.

iii. Les personnes condamnées pour traite ou exploitation des êtres humains

Les données portant sur les condamnations sont extraites du fichier statistique du casier judiciaire national et sont fournies par la DACG. En 2016 et 2017, 1 525 personnes ont été condamnées pour une infraction de traite ou d'exploitation des êtres humains. Parmi elles, 119 ont été condamnées pour au moins une infraction de traite des êtres humains au sens de l'article 225-4-1 du Code pénal (soit 8 %).

Les effectifs sur les condamnations étant petits, les données sur le profil ont été cumulées pour les années 2013 à 2017 représentant 3 755 personnes condamnées. Ces dernières sont principalement des hommes (72 %, soit 2 701 individus). Une différence est à noter lorsque les personnes sont condamnées pour au moins une infraction de traite des êtres humains au sens de l'article 225-4-1 du Code pénal. Comme pour les personnes poursuivies, la part des femmes est plus importante parmi ces dernières. En effet, entre 2013 et 2017, 46 % des personnes condamnées pour traite des êtres humains étaient des femmes (28 % pour celles condamnées pour une infraction de traite ou d'exploitation des êtres humains).

Parmi les personnes condamnées pour traite ou exploitation des êtres humains, 93 nationalités ont été relevées entre 2013 et 2017. La part des personnes condamnées de nationalité française est la plus importante, 39 %. Près d'un cinquième des personnes condamnées pour traite ou exploitation des êtres humains sont de nationalité roumaine (19 %) et 8 % de nationalité chinoise.

Pour les personnes condamnées spécifiquement pour au moins une infraction de traite des êtres humains, la part des personnes condamnées de nationalité française ne représente plus que 6 %. Les personnes condamnées sont principalement nigérianes (36 %). Par ailleurs, près d'un tiers (31 %) sont de nationalité roumaine.

Les données administratives présentées ci-dessus sont le reflet de l'activité des services de police et de gendarmerie ainsi que de celles de la Justice. Elles ne permettent donc pas d'appréhender ce phénomène dans sa globalité. Afin d'apporter une vue plus générale, il s'est avéré nécessaire de se tourner vers ceux qui sont souvent les premiers interlocuteurs des victimes, à savoir les associations.

II. L'enquête annuelle sur les victimes de traite des êtres humains suivies par les associations en France

Depuis 2016, la Mission interministérielle pour la protection des femmes victimes de violences et la lutte contre la traite des êtres humains (MIPROF) et l'ONDRP ont mis en place un groupe de travail réunissant, notamment, les associations membres du Collectif « Ensemble contre la traite des êtres humains ». Ce groupe de travail a abouti à la réalisation d'une enquête annuelle collectant les données sur les victimes de traite des êtres humains suivies par les associations en France. Ce travail permet ainsi d'améliorer la connaissance de ce phénomène, et d'apporter des enseignements sur les profils et les parcours des victimes, qui restent parfois invisibles des autorités.

A. Aspects méthodologiques de l'enquête

Chaque année, cette enquête est réalisée sous la forme d'un questionnaire en ligne, transmis à l'ensemble des associations identifiées comme pouvant potentiellement accompagner des victimes de traite. L'unité de compte correspond aux victimes accompagnées au cours d'une année par chacune des associations. Le suivi a pu commencer lors de l'année d'enquête ou avant.

Le questionnaire comporte un socle commun (nombre de victimes, forme d'exploitation, genre, âge et pays d'origine) et un socle facultatif approfondissant les connaissances sur les profils des victimes, les conditions d'exploitation ou encore les démarches entreprises pour les associations. Pour chaque question, les parts sont calculées à partir du nombre de victimes suivies par les associations répondantes[16].

Pour rappel, en France, seules les autorités compétentes peuvent identifier une victime de traite des êtres humains. Les personnes qui sont suivies par les associations n'ont pas toutes décidé d'engager des démarches auprès de ces autorités. Les personnes comptabilisées comme victimes de traite dans cette partie sont donc celles pour lesquelles les associations estiment, au regard de critères qui leur sont propres, qu'elles sont ou étaient en situation de traite.

B. Les résultats de l'enquête

Pour la troisième édition de cette enquête, 53 associations[17] ont transmis des informations sur 2 918 personnes victimes de traite des êtres humains, que l'accompagnement ait débuté en 2018 ou non. Ce questionnaire a mis en évidence le caractère mondial du phénomène (79 pays d'origine identifiés) ainsi que la forte emprise de l'exploiteur passant par le transfert ou l'hébergement de la victime. Par ailleurs, cette étude a permis à la fois de distinguer des profils selon les formes d'exploitation mais également certaines spécificités selon les régions d'origine des victimes.

Ainsi, pour certains pays ou régions, une seule forme d'exploitation prédomine. C'est notamment le cas du Nigéria où la quasi-totalité des victimes sont exploitées sexuellement. Ces réseaux de criminalité organisée sont bien identifiés par les autorités et les associations. À l'inverse, pour les régions d'Europe de l'Est et du Sud, d'Afrique du Nord, d'Afrique de l'Ouest (hors Nigéria) ou encore d'Asie, les formes d'exploitation sont plus diverses avec notamment une part plus importante de victimes d'exploitation par le travail. Par ailleurs, les victimes de mendicité forcée sont quasiment toutes originaires d'Europe de l'Est et du Sud.

Plus spécifiquement, cinq profils de victimes ressortent des résultats de l'enquête au regard des formes d'exploitation.

i. Les victimes d'exploitation sexuelle

Ces victimes représentent 74% de l'ensemble (soit 2 160 victimes suivies par 49 associations). Cette surreprésentation doit être nuancée pour deux raisons : d'une part, le nombre important de victimes suivies par les associations spécialisées et accompagnant des personnes prostituées et d'autre part, les victimes de cette forme d'exploitation sont plus « visibles » et plus accessibles. Ces dernières sont principalement des femmes (93 %) et 88% sont majeures. La majorité des victimes sont originaires du Nigéria (65% soit 1 404 victimes). Leur vulnérabilité peut être accentuée par la maternité, 25% des femmes ont connu une grossesse au cours de leur exploitation, et par une situation d'addiction détectée par l'association pour 19 % des victimes. Les principaux exploiteurs sont des inconnus (38 %), cependant, 6 % sont le conjoint de la victime (phénomène des *loverboys*[18]).

L'enquête a par ailleurs confirmé l'émergence du phénomène de l'exploitation sexuelle de jeunes filles françaises mineures ou jeunes majeures (7 % des victimes). Ces dernières généralement en rupture familiale et/ou scolaire entrent dans un système d'exploitation dont elles ne peuvent plus sortir.

ii. Les victimes d'exploitation par le travail

L'exploitation par le travail concerne 510 personnes suivies par 30 associations, soit 17 % des victimes en 2018. Deux profils d'exploitation par le travail se distinguent : les victimes d'exploitation domestique (233 victimes – 8 %) et les victimes d'exploitation par le travail hors domestique (277 victimes – 9 %). Ces dernières concernent majoritairement des hommes (74 %) et 77 % sont majeures. Ces victimes d'exploitation sont, pour près de la moitié d'entre elles, originaires d'Asie du Sud-Est, et en particulier du Vietnam (46 %). Plus du tiers sont originaires d'Afrique du Nord et de l'Ouest (36 %). Leur transfert en France a été organisé par l'exploiteur ou le réseau pour 59 % des victimes. Cela diffère des victimes des autres formes d'exploitation pour lesquelles le transfert vers le lieu d'exploitation est quasi toujours organisé par l'exploiteur ou le réseau.

Les victimes d'exploitation domestique sont dans leur quasi-

totalité des femmes (94 %) et 97 % sont majeures. Ces victimes sont plus âgées, 41 % ont 30 ans ou plus. Cependant, 13 % des victimes avaient moins de 18 ans lorsque l'exploitation a débuté. Un peu plus du tiers sont originaires d'Afrique de l'Ouest (34 %), principalement de Côte d'Ivoire et du Sénégal. Contrairement à d'autres formes d'exploitation, les victimes sont généralement sorties de leur situation d'exploitation lors de la prise en charge par l'association (75 %). Lorsque le principal exploiteur est connu de la victime, il s'agit d'une personne de son entourage (27 %), de son employeur (24 %) ou d'un membre de la famille (12 %). La vulnérabilité des victimes peut être plus importante pour les femmes victimes car certaines d'entre elles peuvent vivre une grossesse au cours de leur exploitation (c'est le cas de 11 % des femmes victimes).

iii. Les victimes de contrainte à commettre des délits

En 2018, les victimes de contrainte à commettre des délits représentent 5 % de l'ensemble des victimes dans l'enquête (soit 135 victimes suivies par 5 associations). Ces dernières sont principalement mineures : 96 %. La plupart sont de jeunes garçons (84 %). Ces victimes sont originaires de 7 pays dont 61 % de Roumanie. Pour 96 % d'entre elles, le principal exploiteur fait partie de la famille ou de la belle-famille. Bien que ces réseaux soient familiaux, ils semblent étendus, toutes les victimes faisaient partie d'un réseau de traite exploitant d'autres victimes. L'emprise des exploiteurs sur ces victimes est d'autant plus forte du fait de leur proximité familiale qui implique des conflits de loyauté si ces dernières dénoncent leurs proches[19]. Pour toutes ces victimes, les associations ont détecté une situation d'addiction (alcool, drogue ou médicament). L'une des particularités de la contrainte à commettre des délits est que les personnes exploitées se retrouvent à la fois victimes de traite des êtres humains et auteurs de délits : 15 % des victimes ont été mises en cause dans des faits liés à leur exploitation. Plus de 8 victimes de ce type d'exploitation ayant été mises en cause sur 10 ont été condamnés pour ces faits.

iv. Les victimes de mendicité forcée

En 2018, les victimes de mendicité forcée représentent 3 % de l'ensemble des victimes (soit 73 victimes suivies par 7 associations). La mendicité forcée concerne principalement des femmes, cependant la répartition des victimes selon le genre est moins marquée que pour les autres formes d'exploitation : 58 % sont des femmes et 42 % des hommes. Les victimes sont jeunes : 59 % ont moins de 18 ans. Quasiment toutes sont originaires d'Europe de l'Est et du Sud : 58 % étaient originaires de Roumanie et 36 % de Bulgarie. Comme pour la contrainte à commettre des délits, pour 96 % d'entre elles, l'exploiteur principal fait partie de la famille, la belle-famille ou est le conjoint. Les associations n'ont reporté aucun déplacement à la police ou à la gendarmerie, ni aucune plainte enregistrée. Ces victimes accompagnées par les associations restent donc totalement invisibles pour les autorités.

Notons que seule une partie des victimes de traite est accompagnée par les associations. Ainsi, les victimes recensées dans l'enquête ne peuvent pas être considérées comme un échantillon représentatif de l'ensemble des victimes présentes sur le territoire français. Il est possible que certaines catégories de victimes, notamment selon le type d'exploitation qu'elles subissent, soient davantage détectées et prises en charge par les associations que d'autres. Comme évoqué supra, les activités des associations ayant répondu ont un fort impact sur les résultats et peuvent ainsi entraîner une surreprésentation des victimes de certaines formes d'exploitation.

Conclusion

La traite des êtres humains est un phénomène complexe à mesurer et peut être étudiée à travers différentes sources de données. Les données administratives nous renseignent sur les victimes et auteurs connus par les autorités, cependant les informations disponibles sont assez limitées (sexe, âge et nationalité). La mise en place de l'enquête auprès des associations a permis de mettre en lumière les victimes qui restaient invisibles des autorités. Ces données apportent des éléments de connaissances complémentaires sur ce phénomène criminel en mettant en évidence des spécificités selon les formes d'exploitation, les pays d'origine ou encore les conditions d'exploitation.

Les données issues de ces deux sources, administratives et associatives, ne sont pas comparables mais apportent, toutes deux, des éléments de compréhension sur un phénomène dont les contours sont encore difficiles à délimiter. Par ailleurs, elles sont le reflet des activités à la fois des administrations compétentes pour identifier les victimes et des associations accompagnant des victimes de traite. Les résultats n'ont donc pas vocation à être représentatifs de l'ensemble du phénomène de la traite et de l'exploitation des êtres humains en France.

Pour pallier à cette difficile mesure du phénomène liée à l'invisibilité des protagonistes, plusieurs méthodes ont été mise en oeuvre. Par exemple, l'ONUDC a mis en avant la méthode appelée « Capture, marquage et recapture » pour estimer la part « cachée » de la population des victimes de traite des êtres humains. Cette méthode, développée en biologie, a pour objectif de comparer des listes de population recensée par plusieurs organismes et de recouper les doublons présents dans les différentes séquences afin d'estimer de la taille et les principales caractéristiques de cette population. En sciences sociales, elle a été employée afin d'estimer la population de sans domicile ou encore des prostituées de rue. Cette méthode a été appliquée dans plusieurs pays comme le Royaume-Uni[20] ou les Pays-Bas[21] pour mesurer l'ampleur de la traite des êtres humains et pourrait être intéressante à mettre en place pour la France.

Notes :

1 ONDRP (2019) Victimation 2018 et perception de la sécurité, résultats de l'enquête « Cadre de vie et sécurité » 2019. Institut national des hautes études de la sécurité et de la justice (INHESJ).

2 UNODC. (2018). Global Report on Trafficking in Persons 2018. Vienne: United Nations publication.

3 International Labour Organization & Walk Free Foundation. (2017). Estimations mondiales de l'esclavage moderne: travail forcé et mariage forcé. Genève: Bureau International du travail.

4 Plus spécifiquement pour la France, en 2015, dans son rapport La lutte contre la traite et l'exploitation des êtres humains, la CNCDH a enjoint la France à poursuivre ses efforts en matière statistique et en 2017, le GRETA l'a également fait dans le Rapport concernant la mise en oeuvre de la Convention du Conseil de l'Europe sur la lutte contre la traite des êtres humains par la France.

5 Tyldum, G., & Brunovskis, A. (2005). Describing the Unobserved: Methodological Challenges in Empirical Studies on Human Trafficking. International Migration, 43(1/2), 17-34.

6 Peyroux, O. (2014). Bonnes feuilles : délinquants et victimes - la traite des enfants d'Europe de l'Est en France. Journal du droit des jeunes,1(331), 23-32. ; Simoni, V. (2010). Territoires et enjeux de pouvoir de la traite à des fins d'exploitation sexuelle : le cas de Paris.Hérodote, 1 (136), 134-149.

7 Guinamard, L. sous la direction de Geneviève Colas, Secours Catholique Caritas France (2015). Les nouveaux visages de l'esclavage. Ivry-sur-Seine: Les Éditions de l'Atelier / Éditions Ouvrières.

8 Ministère des droits des femmes, de la ville, de la jeunesse et des sports. (2014). Plan d'action national contre la traite des êtres humains (2014-2016). Paris. La France a adopté son second Plan d'action national le 18 octobre 2019.

9 https://inhesj.fr/ondrp/

10 CNCDH (2015). La lutte contre la traite et l'exploitation des êtres humains. Paris: La documentation française.

11 Créée en 1978 par le Ministère de la Justice, la nomenclature par nature d'infraction ou « codes NATINF » (NATure d'INFraction) sert à qualifier juridiquement les infractions définies dans le Code pénal. Cette nomenclature est mise à jour régulièrement par la Direction des affaires et des grâces (DACG) pour prendre en compte les évolutions législatives. Les codes NATINF sont utilisés depuis 1984 pour les statistiques relatives au casier judiciaire (Le Bouillonnec, J-Y & Quentin, D. (2013). Rapport d'information relatif à la mesure de la statistique des délinquances et de leurs conséquences, Assemblée nationale).

12 Pour plus d'information, consulter : Circulaire du 22 janvier 2015 de politique pénale en matière de lutte contre la traite des êtres humains (NOR JUSD1501974C).

13 Les données du SSMSI sont issues des procédures judiciaires dressées par la police ou la gendarmerie nationales. Dans cet article, elles concernent les personnes physiques victimes d'un crime ou d'un délit, non routier.

14 Langlade, A & Sourd, A. (2019). La traite et l'exploitation des êtres humains en France : les données administratives. Grand Angle. n°52.

15 Lavaud-Legendre, B. (2012). Les femmes soumises à la traite des êtres humains adhèrent-elles à l'exploitation ? Une mauvaise formulation pour un vrai problème. Étude réalisée auprès des femmes nigérianes sexuellement exploitées en France. Archives de politique criminelle, 1(34), 103-121.

16 Toutes les informations sur la méthodologie et les limites de l'étude se trouvent dans la publication Grand Angle n°48 (Simon & Sourd, 2018). Par ailleurs, vous pouvez retrouver l'ensemble des résultats dans la dernière publication sur le sujet « La traite des êtres humains en France. Profil des victimes suivies par les associations en 2018 » (Sourd & Vacher, 2019).

17 Le terme « association » regroupe à la fois des associations et des établissements spécialisés appartenant à certaines de ces associations. Par commodité de lecture, ce terme est utilisé pour désigner ces deux possibilités.

18 Peyroux, O. (2012). Traite des mineurs roumains migrants : processus d'exclusion, types d'exploitation et stratégie d'adaptation. Journal du droit des jeunes. 313(3). 9-16.

19 Lavaud-Legendre, B. & Peyroux, O. (2014). Mineur(e)s nigérian(e)s et originaires des Balkans en situation de traite en France. Regards pluridisciplinaires sur les processus d'asservissement et les échecs de la protection. Revue européenne des migrations internationales 30(1). 105-130.

20 Bales, K., Hesketh, O., & Silverman, B. (2015). Modern slavery in the UK. How many victims? Significance, 16-21.

21 UNODC. (2017). Monitoring Target 16.2 of the United Nations Sustainable Development Goals. A multiple systems estimation of the numbers of presumed human trafficking victims in the Netherlands in 2010-2015 by year, age, gender, form of exploitation and nationality. Research Brief.

LA POLITIQUE CRIMINELLE AU SÉNÉGAL À L'AUNE DE LA LUTTE CONTRE LA CYBERCRIMINALITÉ

THIERNO AMADOU NDIOGOU

DOCTEUR EN DROIT PRIVÉ ET ENSEIGNANT-CHERCHEUR À LA FACULTÉ DES SCIENCES JURIDIQUES ET POLITIQUES DE L'UNIVERSITÉ CHEIKH ANTA DIOP (FSJP-UCAD) DE DAKAR (SÉNÉGAL)

Nul ne peut aujourd'hui contester que le développement de nouvelles formes de criminalité fait bouger les lignes juridiques ; il soumet incontestablement les systèmes juridiques à une forte pression qui impose aux gouvernants d'innover, parfois dangereusement[1]. C'est ainsi qu'on assiste au Sénégal à une démarche globale de modernisation qui est un enjeu de politique criminelle.

La politique criminelle est considérée comme « *science et art, explicative, préventive et répressive* »[2] du phénomène criminel. À cet effet, elle dépasse les champs d'action du droit pénal et de la procédure pénale ; mais elle peut les servir tous[3]. Stratégie juridique et sociale fondée sur des choix de politiques publiques, la politique criminelle permet de répondre avec pragmatisme aux problèmes posés par la prévention et la répression de la criminalité[4], ici la cybercriminalité.

C'est dans cette perspective que le législateur sénégalais a réaménagé sa politique juridique et sociale pour dissiper le malaise du juge pénal[5] et être en phase avec le combat mené par la communauté internationale contre la cybercriminalité[6]. Ce réaménagement issu de la loi n° 2008-11 du 25 janvier 2008 sur la cybercriminalité[7] s'est caractérisé par l'élaboration d'une stratégie de modernisation des instruments de répression et par l'articulation d'une stratégie d'amélioration du processus de répression[8]. Huit ans après[9], le législateur sénégalais a entendu corriger les tares originelles de son dispositif juridique en apportant des améliorations techniques importantes à la législation contre les cyber-délinquants. Ont été adoptées des dispositions relatives aux interceptions de correspondances téléphoniques ou émises par voie électronique. Ainsi, cette nouvelle législation sénégalaise s'articule autour d'une politique d'extension des pouvoirs des investigateurs grâce à une politique d'instrumentalisation des technologies de l'information et de la communication (TIC) à des fins probatoires.

Cette volonté du législateur sénégalais paraît cependant inachevée puisqu'il laisse planer un doute sur la notion de « *cybercriminalité* »[10]. Mais, à l'analyse de l'exposé des motifs de la loi n° 2008-11 susvisée, il semble admettre que la cybercriminalité renvoie aux infractions commises dans les réseaux de télécommunication ou au moyen de ces derniers[11]. Toutefois, une telle conception serait fort réductrice en ce sens qu'elle ne prend pas en compte les infractions commises contre les réseaux de télécommunication et elle n'inclut pas les infractions utilisant ces réseaux pour menacer ou tromper[12]. Il est donc à espérer que le projet de loi sur la cybercriminalité qui sera bientôt adoptée pour abroger et remplacer celle de

2008[13], permettra de trouver des réponses qui fassent autorité et satisfassent les uns et les autres[14].

Dès lors, l'interrogation est donc moins celle de savoir si une stratégie juridique et sociale fondée sur des choix politiques est d'actualité au Sénégal que de s'assurer qu'elle répond de manière adéquate à l'extension de la criminalité sur internet.

Cette question est d'un enjeu pratique. En réalité, internet n'a pas seulement favorisé la perpétration d'actes de criminalité classique, il a également modernisé cette criminalité et donné naissance à de nouvelles infractions. C'est ce qui explique que l'analyse de l'organisation de la réponse méthodique contre la cybercriminalité au Sénégal[15], passe par l'articulation d'un véritable mouvement d'expansion du champ de la politique criminelle.

En réponse à la problématique centrale, il convient de reconnaître une variété d'approches. Elles peuvent traduire des tendances négatives, positives ou mitigées. Cependant, la présente entreprise se propose d'explorer la physionomie de la stratégie juridique et sociale de lutte contre le phénomène de la cybercriminalité. La démarche débute par le constat d'une intensification de la politique criminelle (I). Elle se poursuit par les déficits de cette intensification (II).

I. L'intensification de la politique criminelle face à la lutte contre la cybercriminalité

Cette intensification se traduit en premier lieu par une portée élargie des mesures cyber-préventives (A), et en second lieu par le renforcement des mesures cyber-répressives (B).

A. L'élargissement des mesures cyber-préventives

Au Sénégal, la stratégie de prévention de la criminalité sur internet constitue un vaste sujet qui englobe de nombreux programmes et initiatives. Une grande variété d'infractions constitue la cible de cette prévention et différentes approches ciblent différents facteurs contribuant à la criminalité sur internet. C'est ce qui explique que divers acteurs s'engagent fréquemment dans la prévention de la cybercriminalité. Cela inclut le Gouvernement sénégalais, les organisations non gouvernementales, la société civile, les volontaires, les activistes, le secteur privé et les citoyens. Ces acteurs jouent un rôle clé dans les stratégies et les mesures visant à réduire les risques de criminalité sur internet et leurs effets néfastes potentiels sur les Sénégalais et la société sénégalaise.

Le point 4.3 relatif aux objectifs de la Stratégie Nationale de Cybersécurité du Sénégal (SNC 2022) prévoit que « *la réussite d'un Sénégal numérique s'appuiera sur la confiance des organisations et des particuliers en matière des services en ligne. Le Gouvernement devra alors travailler avec les secteurs public et privé afin d'augmenter la connaissance et la compréhension des cybermenaces auxquelles sont confrontés le Sénégal et les Sénégalais* ». Il convient alors de reconnaître que l'État du Sénégal est dans une logique d'élaborer une stratégie de prévention appropriée qui combine des réponses étatiques[16] et sociétales.

Sur le plan sociétal, la cybercriminalité soulève des questions d'autant plus difficiles à résoudre qu'elle affecte toute une société globalisée. C'est pourquoi, les autorités publiques et les acteurs non étatiques ne cessent d'inviter à une culture de la cybercriminalité et ce, à travers la sensibilisation et la formation. Ces dernières, élargies à plusieurs couches de la population notamment les élèves et les enseignants[17], consistent à informer et à former non seulement sur les risques spécifiques qu'internet présente, mais également sur les moyens de protection qui existent pour s'en prémunir[18].

La sensibilisation peut s'articuler autour de quatre points : l'éducation aux médias, le rôle des parents, le rôle de l'école et la nécessité d'une collaboration entre le public et le privé. Quant à la formation, s'ouvre aux policiers et militaires une École nationale de cybersécurité à vocation régionale (ENVR) en collaboration avec la France, sise dans les locaux de l'École Nationale d'Administration de Dakar. Cette entité intégrera également des « *candidatures civiles* » non sans « *tisser des partenariats avec des entreprises et des universités qui permettront des labellisations académiques telles des masters* »[19]. Quid de la cyberstratégie de répression ?

B. Le renforcement des mesures cyber-répressives

Conscients de la multiplication des infractions impliquant l'utilisation

des TIC et des enjeux de sécurité qui imprègnent ce phénomène, la volonté politique du Sénégal s'inscrit dans une démarche qui transparaît encore dans un renforcement de la cyberstratégie de répression. Sous l'effet d'une pénalisation soutenue, le champ d'application de la lutte contre la cybercriminalité ne cesse de s'étendre. Ce qui justifie que les différentes facettes criminelles de la sphère internet appellent sans cesse de nouvelles réponses du législateur sénégalais. Elles se développent, classiquement, en termes d'extension ou de diversification des incriminations, d'aggravation des peines[20]. Bien que cette pénalisation soit à beaucoup d'égards d'une portée qui dépasse les seuls rapports textuels avec l'internet, elle ne peut que profiter à la lutte menée contre les contenus pédopornographiques ou nocifs pour les mineurs sur internet et à la protection générale de l'information.

Sont également conférés aux autorités d'enquêtes des outils plus adaptés à la recherche et la conservation des preuves. En réalité, au gré des évolutions techniques et scientifiques et à la faveur de l'émergence de nouveaux visages du phénomène criminel, le législateur sénégalais a institué un dispositif probatoire dense en matière pénale[21]. C'est dans cette perspective qu'il a rendu possible les sonorisations des lieux et même la géolocalisation en édictant que les services spéciaux de renseignement peuvent « *recourir à des procédés techniques, intrusifs, de surveillance ou de localisation pour recueillir les renseignements utiles à la neutralisation de la menace* »[22]. Sans aller aussi loin que ses homologues français, belges et allemands qui en ont profité pour instituer le fichier génétique, le dossier judiciaire numérique, les interrogations et auditions par vidéoconférence, le législateur sénégalais a autorisé la surveillance, l'infiltration, la captation de données informatiques, les perquisitions nocturnes et les écoutes téléphoniques dès la phase policière[23].

Constituent encore autant de ripostes les nouvelles obligations des entreprises liées aux déclarations d'incidents. À cet effet, la Commission de Protection des données personnelles[24] intensifie progressivement son contrôle en obligeant les fournisseurs de services de communications électroniques au public à notifier toute violation de données à caractère personnel. De même, l'Agence de l'Informatique de l'État, le Service Technique Central des Chiffres et de la Sécurité des Systèmes d'Information et la Division Spéciale de lutte contre la Cybercriminalité contraignent les opérateurs de télécommunication à déclarer tout incident de sécurité.

Ce faisant, les opérateurs et les fournisseurs d'accès, d'hébergement et de services mettront rapidement à la disposition des enquêteurs les informations utiles à la manifestation de la vérité. Comme c'est déjà le cas en France, la transmission de ces informations sous forme numérique[25] permettra de gagner non seulement du temps dans l'action mais éviter la disparition ou le dépérissement des preuves. Les réquisitions par voie télématique permettent à l'officier de police judiciaire, par exemple, d'accéder directement, par la voie d'un réseau de communication télématique ou informatique, aux informations utiles à la manifestation de la vérité qui sont contenues dans le ou les systèmes informatiques ou traitements de données à caractère personnel administrés par l'organisme ou la personne morale faisant l'objet de la réquisition.

Au demeurant, cette intensification porte cependant atteinte, du point de vue de la sauvegarde de l'ordre public, à la nécessaire protection de certains droits.

II. Les déficits de l'intensification de la politique criminelle face à la lutte contre la cybercriminalité

L'analyse globale de la stratégie juridique et sociale de lutte contre la cybercriminalité conduit au constat de quelques manquements relatifs aux droits numériques, d'une part (A) et aux droits humains, d'autre part (B).

A. Les insuffisances relatives au respect de certains droits numériques

Un diagnostic minutieux de la politique criminelle au Sénégal face à la cybercriminalité permet de constater, non sans regret, des carences relatives à la protection de certains droits numériques tels que la liberté d'expression sur internet et les données à caractère personnel[26].

Au sujet de la liberté d'expression, l'article 431-43 du Code pénal (CP) incrimine « *l'insulte*

commise par le biais d'un système informatique envers une personne en raison de son appartenance à un groupe qui se caractérise par la race, la couleur, l'ascendance, l'origine nationale ou ethnique ou la religion ou envers un groupe de personnes qui se distingue par une de ces caractéristiques ».

En l'absence de définition du mot « *insulte* », cette disposition pourrait être utilisée afin de mettre certaines personnes à l'abri des critiques du public et aurait pour effet d'étouffer la liberté d'expression. Cette disposition pourrait notamment être utilisée pour réprimer les personnes critiques à l'égard de groupes religieux. D'ailleurs, nous avons enregistré au moins deux cas de personnes poursuivies pour injures liées à la religion[27].

Aussi, l'article 431-60 issu de la même réforme, incrimine la fabrication, l'affichage, l'exposition ou la distribution, par un moyen de communication électronique, de *« tous imprimés, tous écrits, dessins, affiches, gravures, peintures, photographies, films ou clichés, matrices ou reproductions photographiques, emblèmes, tous objets ou images contraires aux bonnes moeurs »*. La notion de « *bonnes moeurs* » ne faisant pas l'objet de définition dans la législation répressive sénégalaise, pourrait être utilisée pour restreindre la liberté d'expression et réprimer les personnes en fonction de leur orientation sexuelle ou de leur choix vestimentaire.

Concernant les données personnelles, il importe de souligner que les opérations de collecte[28] ou de traitement[29], attestent une évolution des pratiques dont les avantages sont importants notamment pour les entreprises. Toutefois, ces opérations sont porteuses, en général, de risques d'impacts négatifs sur la vie privée[30] et en particulier, de risques de cybercriminalité. En guise d'illustration, les images et les voix des personnes collectées par les vidéosurveillances installées dans certains immeubles, magasins, institutions sans information des personnes et sans autorisation de la Commission de protection des données personnelles, sont à des fins ignorées par les concernés.

Il en est de même des prospections commerciales des banques et autres[31]même si certaines ont initié le processus de régularisation[32]. L'on pourrait y rajouter les dossiers de recrutement du personnel des structures. Ces dernières collectent en effet une quantité importante d'informations sur les postulants mais il n'y a aucune information sur le traitement qui est fait suite à l'échec de la sélection.

De surcroît, sur le Web, les logs de connexion sont automatiquement collectés lors d'un passage sur internet et l'historique des pages consultés également. Ces informations constituent l'or noir d'internet, revendu à des sociétés pour leur permettre de cibler des consommateurs sénégalais pour leurs articles. Également, sur les réseaux sociaux comme Facebook et WhatsApp, l'accessibilité des données publiées par plusieurs pose un problème[33]. Enfin, en matière de commerce électronique, les cybermarchands collectent des informations de façon disproportionnée[34]. Outre les insuffisances relatives au respect de certains droits numériques, d'autres sont relatives à certains droits humains.

B. Les faiblesses relatives au respect de certains droits humains

Plusieurs manquements relatifs à certains droits humains peuvent être décriés car ils portent un gros coup sur l'équité procédurale et impactent négativement sur la conduite loyale de la procédure pénale[35]. D'abord, en matière de recherche de la preuve dans l'univers numérique, la stratégie juridique de renforcement du processus de répression face à la cybercriminalité ne se soumet pas toujours à ces contraintes de politique criminelle. À cet effet, l'absence de limitation de la durée de l'interception donnée par l'autorité judiciaire et le défaut de droit de recours contre la décision judiciaire d'interception, constituent de réels dangers susceptibles de favoriser des atteintes à la vie privée des citoyens.

Ensuite, l'habilitation expresse donnée aux officiers de police judiciaire par l'article 677-39 du Code de procédure pénale (CPP) pour recourir aux nouveaux mécanismes de recherche de preuves, à savoir l'interception de données de contenu et la conservation rapide de données « *pour les nécessités de l'enquête* », nous paraît dangereuse pour les libertés individuelles,

dont le seul garant est le juge. En effet, en cas de commission d'une cyberinfraction flagrante, les officiers de police judiciaire seraient habilités, en raison du caractère coercitif de l'enquête, à intercepter des données, sans recueillir le consentement des intéressés ni requérir une autorisation judiciaire. Cette situation est préjudiciable aux libertés individuelles.

Enfin, les articles 90-4 et 90-17 de la loi n° 2016-30 du 08 novembre 2016 modifiant la loi n° 65-61 du 21 juillet 1965 portant Code de procédure pénale permettent à un juge d'instruction d'ordonner à des « *personnes ayant une connaissance particulière* » d'un système informatique ou d'un service de communication, de chiffrement ou de transmission des données, de fournir des informations sur le fonctionnement de ce système et sur la manière d'accéder à des données dans une forme compréhensive. Il va sans dire que ces textes attribuent de façon regrettable au juge instructeur le pouvoir d'ordonner, même pendant une durée limitée, certaines mesures particulièrement attentatoires à la vie privée, telles que les interceptions de correspondances téléphoniques ou émises par la voie électronique. Pis encore, l'article 90-16 de ladite loi prévoit l'impossibilité d'exercer un recours contre la décision d'interception.

Certes, ces interceptions pourraient être légitimes pour défendre l'État contre les cyberattaques, mais il faut des garanties pour permettre d'éviter l'arbitraire. Cela signifie que le système doit reposer sur une loi précise, viser une personne déterminée suspectée d'avoir commis des infractions via internet. D'ailleurs, si l'on se fie au rapport explicatif de la Convention de Budapest sur la cybercriminalité, « *la modification des données de trafic aux fins de faciliter les communications anonymes (comme dans le cas des activités des systèmes de réexpédition anonyme) ou la modification des données aux fins d'assurer la protection des communications (chiffrement, par exemple) assurent la protection légitime de la vie privée et, de ce fait, se réalisent de façon légitime.* »

De façon générale, l'infiltration aux enregistrements dissimulés qui prennent la forme d'écoutes téléphoniques, la captation de données informatiques, la sonorisation, la géolocalisation ne sont pas incompatibles avec l'intégrité physique, le secret des correspondances et l'intimité de la vie privée, valeurs sociales auxquelles les citoyens sont particulièrement attachés et dont les Conventions internationales assurent la protection.

Dans le même ordre de pensées, les articles 8 et 10 de la loi n° 2016-33 du 14 décembre 2016 relative aux Services de renseignement[36] autorise les opérations de sonorisation et de captation d'images dans des lieux publics ou privés. De tels dispositifs nous paraissent peu conformes aux exigences imposées par les textes internationaux relatifs aux droits humains.

Conclusion

En dernière analyse, l'étude s'est proposée de revisiter « *la politique criminelle au Sénégal à l'aune de la lutte contre la cybercriminalité* ». Le constat inspirateur est celui d'une appréciation de la stratégie juridique et sociale adoptée face à l'extension de la criminalité sur internet. Ainsi, s'il faut dresser le bilan de cette stratégie, on se rend compte qu'en dépit de l'intensification de la politique criminelle pour répondre adéquatement à cette forme de criminalité, celle-ci continue, malgré tout, à susciter quelques insuffisances. C'est dire alors qu'un nouveau chantier s'ouvre au législateur sénégalais, celui qui consiste à mettre en place une stratégie efficiente tout en sauvegardant les droits et libertés fondamentaux. Il est à espérer que les refontes substantielles, annoncées avant fin 2020, de la loi sur la cybercriminalité et celle sur les données personnelles apporteront les correctifs nécessaires.

Notes :

1 D. NZOUABETH, « Les preuves pénales à l'épreuve de la métamorphose des règles de la procédure pénale sénégalaise », Annales africaines, nouvelle série, Revue de la Faculté des Sciences Juridiques et Politiques de l'Université Cheikh Anta Diop, vol. 2, n° 9, déc. 2018, pp. 111 et s.

2 Ch. LAZERGES, La politique criminelle, PUF, 1987, p. 6.

3 Voir M. DELMAS-MARTY, Les grands systèmes de politique criminelle, Paris, PUF, 1992 ; du même auteur, Modèles et mouve-

ments de politique criminelle, Paris, Économica, 1983 ; Ch. LAZERGES, « La défense sociale nouvelle a 50 ans. ; L'actualité de la pensée de M. Ancel », RSC 2005, pp. 165 et s.

4 D. NZOUABETH, « La tolérance en matière pénale », Annales africaines, nouvelle série, Revue de la Faculté des Sciences Juridiques et Politiques de l'Université Cheikh Anta Diop, vol. 2, n° 7, déc. 2017, pp. 157 et s.

5 D'une part, par la création d'incriminations nouvelles spécifiques aux technologies de l'information et de la communication (TIC) en vue de combler les vides juridiques constatés en législation et d'autre part, par l'adaptation des incriminations classiques aux dites technologies.

6 Il faut comprendre que la cybercriminalité n'est pas un phénomène criminel sénégalais ou africain ; c'est un phénomène criminel mondial. Donc, c'est bien d'avoir des instruments au plan communautaire et continental mais, la lutte doit se faire à l'échelle internationale parce que le phénomène est transnational. C'est pourquoi, l'adhésion du Sénégal à la Convention sur la cyber sécurité et la protection des données à caractère personnel de L'Union Africaine dite la « Convention de Malabo » adoptée le 27 juin 2014 et à la Convention sur la Cybercriminalité du Conseil de l'Europe dite « Convention de Budapest « du 23 novembre 2001 a permis de bénéficier une coopération avec tous les États : États-Unis, France, Afrique du sud, etc. Ce faisant, le Sénégal s'est inscrit dans la croisade internationale contre le phénomène de la cybercriminalité qui constitue une très sérieuse menace pour la sécurité des réseaux et le développement de la société de l'information.

7 Exposé des motifs de la loi n° 2008- 11 du 25 janvier 2008 sur la cybercriminalité, JORS, n°6406 du 03 mai 2008, p. 419.

8 Conscient du danger que représente la cybercriminalité, le Sénégal s'est doté d'un cadre juridique presque intégral, pas seulement de lutte contre la cybercriminalité, mais d'encadrement des phénomènes qui touchent la société de l'information. Pour plus d'informations, Th. A. NDIOGOU, Étude sur l'état des lieux de la cybersécurité et de la cybercriminalité au Sénégal, disponible sur le lien suivant : http://jonction.e-monsite.com/medias/files/etat-des-lieux-de-la-cybersecurite-et-de-la-cybercriminalite-au-senegal-par-dr-ndiogou.pdf

9 Loi n° 2016-29 du 08 novembre 2016 modifiant la loi n° 65-60 du 21 juillet 1965 portant Code pénal, JORS n° 6975 du 25 novembre 2016, p. 1613 ; Loi n° 2016-30 du 08 novembre 2016 modifiant la loi n°65-61 du 21 juillet 1965 portant Code de procédure pénale, JORS n° 6976 du 25 novembre 2016, p. 1627 ; Loi n° 2016-33 du 14 décembre 2016 relative aux Services de renseignement, JORS n° 6984 du samedi 07 janvier 2017.

10 La cybercriminalité, réalité protéiforme et difficile à cerner, n'a fait pas l'objet d'une définition légale au Sénégal.

11 En droit camerounais, la cybercriminalité est définie comme « l'ensemble des infractions s'effectuant à travers le cyberespace par les moyens autres que ceux habituellement mis en oeuvre et de manière complémentaire à la criminalité classique » (Loi n° 2010-12 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité au Cameroun, JORC du 21 décembre 2010, p. 3 et s.).

12 Heureusement que le Code pénal, en ses art. 431-7 à 431-62, prévoit et punit de telles infractions.

13 Le projet de loi qui sera dans les meilleurs délais soumis au conseil des ministres, s'inscrit dans la vision constructive et évolutive de la Stratégie Nationale de Cybersécurité du Sénégal (SNC 2022).

14 Selon M. CHAWKI, la cybercriminalité comme « toute action illicite associée à l'interconnexion des systèmes informatiques et des réseaux de télécommunication, où l'absence de cette interconnexion empêche la perpétration de cette action illicite » Essai sur la notion de cybercriminalité, IEHEI, juillet 2006, p. 23, disponible sur le lien suivant :https://www.ie-ei.eu/IE-EI/Ressources/file/biblio/cybercrime.pdf

15 A. CISSE, « Les déterminants juridiques à la promotion des technologies de l'information et de la communication (TIC) au Sénégal : enjeux, perspectives et méthodologie », Revue trimestrielle d'informations sur les télécommunications, la régulation et la recherche de l'ARTP, Oct., Nov., Déc. 2006, p. 20 et s.

16 À travers la réponse législative étatique, il est à noter qu'en général, la peine poursuit un but d'intimidation destiné à décourager d'éventuels délinquants ; sur le plan de la prévention spéciale, elle remplit une fonction d'intimidation individuelle en ce qu'elle vise à prévenir la récidive de l'individu déjà frappé.

17 De plus en plus, des établissements scolaires se voient dotés de nouveaux outils technologiques. Cependant, l'adaptation des élèves et enseignants est trop lente ; d'ailleurs, un nombre important d'enseignants se sentent démunis ou à l'écart face à ce nouveau matériel.

18 P.GUEYE, Criminalité organisée, Terrorisme et cybercriminalité : Réponses de politiques criminelles, L'Harmattan –Sénégal, 2018, pp. 330 et s.

19 Cette entité aura pour mission la préservation et la lutte contre la cybercriminalité en vue de promouvoir au Sénégal un environnement numérique de confiance. L'article 4 du décret portant organisation et fonctionnement, fait de ladite entité un « point de contact central national dans les échanges internationaux en matière d'enquête relative à la cybercriminalité ».

20 CP, art. 431-7 à 431-62.

21 D. NZOUABETH, « Les preuves pénales à l'épreuve de la métamorphose des règles de la procédure pénale sénégalaise », Op. cit., p. 117.

22 Article 10 de la loi n° 2016-33 du 14 décembre 2016 relative aux Services de renseignement : « Les services spéciaux de renseignement peuvent, lorsqu'ils disposent d'indices relatifs à l'une des menaces prévues à l'article 2 et en l'absence de tout autre moyen, recourir à des procédés techniques, intrusifs, de surveillance ou de localisation pour recueillir les renseignements utiles à la neutralisation de la menace ».

23 Th. A. NDIOGOU, « Réflexions sur la nouvelle législation sénégalaise antiterroriste », in Droits fondamentaux, Revue électronique du CRDH, Université Paris II Panthéon-Assas (France), n° 16, janvier 2018, disponible sur le lien suivant : http://droits-fondamentaux.u-paris2.fr/article/2018/reflexions-nouvelle-legislation-senegalaise-antiterroriste

24 L'avant-projet de loi sur les données personnelles propose la création d'une autorité administrative indépendante dénommée « Autorité de Protection des Données à caractère Personnel » en abrégé « APDP » pour remplacer la « Commission de Protection des Données à Caractère Personnel » la « CDP ».

25 En France, les articles 60-1, 77-1-1 et 99-3 du Code de procédure pénale.

26 Une nouvelle loi sera certainement adoptée avant la fin de l'année 2020.

27 Pour illustration, voir le lien suivant : https://www.bbc.com/afrique/37780270

28 Vidéosurveillance, collecte par internet, téléphone ou formulaire, fichiers du personnel, collecte de données personnelles en cas de recrutement, fichiers de gestion des accès, etc.

29 Exploitation, archivage, transfert, traitement intelligent des données et les nouveaux usages qui en résultent tel que le Big data, open data, data mining, etc.

30 Risque de vol de données, d'usurpation d'identité, d'exclusion, de discrimination, de stigmatisation, etc.

31 Envois de messages SMS ou Mail pour les promotions de services sans information.

32 Orange Money s'est mis en conformité.

33 Les géants du net, Google (propriétaire de Facebook et de WhatsApp) ont entamé la mise en conformité. Sur WhatsApp, par exemple, les données sont maintenant cryptées pour en assurer la sécurité.

34 Données non indispensables pour les transactions sollicitées par le client.

35 L'article 6 alinéa 1er de la loi n°2008-10 du 25 janvier 2008 portant loi d'orientation relative à la Société de l'information (LOSI), a posé les bases d'une cyberéthique en énonçant que le principe de la sécurité « garantit les droits fondamentaux des

personnes et les droits sur les biens et sauvegarde l'ordre public ainsi que les valeurs fondamentales de la société de l'information ».

36 Art. 8 de la loi n° 2016-33 du 14 décembre 2016 relative aux Services de renseignement : « Les entités d'enquête peuvent, avec l'autorisation et sous le contrôle du procureur de la République compétent, recourir aux moyens d'investigation prévus à l'article 10. Les preuves régulièrement recueillies par ces moyens sont recevables en justice et sont laissées à l'appréciation des juridictions pénales compétentes ».

Art. 10 de la même loi : « Les services spéciaux de renseignement peuvent, lorsqu'ils disposent d'indices relatifs à l'une des menaces prévues à l'article 2 et en l'absence de tout autre moyen, recourir à des procédés techniques, intrusifs, de surveillance ou de localisation pour recueillir les renseignements utiles à la neutralisation de la menace ».

OUVRAGES RÉCENTS

RGPD :
LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

19 FICHES POUR RÉUSSIR ET MAINTENIR VOTRE CONFORMITÉ

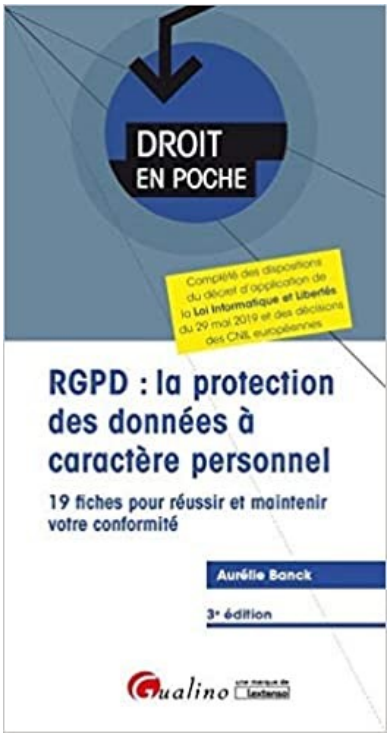
AUTEUR : AURÉLIE BANCK

ÉDITEUR : GUALINO EDITEUR

Résumé

19 fiches pratiques pour avoir une vision globale du RGPD et réussir votre mise en conformité

Le 20 juin 2018, la loi relative à la protection des données personnelles a été promulguée, elle adapte la loi Informatique et Libertés de 1978 au paquet européen constitué du RGPD, du règlement du 27 avril 2016 ainsi que d'une directive dite "Directive police". Toutefois, cette loi n'a eu qu'une durée de vie limitée puisque le Gouvernement français a été autorisé à prendre par voie d'ordonnance les mesures relevant du domaine de la loi nécessaire à la réécriture de la loi du 6 janvier 1978 afin d'adopter des corrections formelles et les adaptations nécessaires à la mise en cohérence du RGPD et des textes nationaux. Cette ordonnance prise après avis de la CNIL a été publiée le 12 décembre 2018 (Ord. n° 2018-1125). Elle est entrée en vigueur en même temps que le décret d'application n°2019-536 précisant ses modalités d'application.



1 an après, cet ouvrage vous propose de faire un point sur les principales règles de la protection des données en France et en Europe. Il intègre les dispositions du décret n°2019-536 pris pour l'application de la nouvelle loi Informatique et Libertés

CRIMINOGÉNÉITÉ DU FOOTBALL PROFESSIONNEL : CONSIDÉRATIONS À L'AUNE DES AFFAIRES JUDICIAIRES SECOUANT LA BELGIQUE NATIONALE

MICHAËL DANTINNE

PROFESSEUR - SERVICE DE CRIMINOLOGIE - FACULTÉ DE DROIT, DE SCIENCE POLITIQUE ET DE CRIMINOLOGIE DE LIÈGE (BELGIQUE)

Avec les contributions de Camille CLOES et de Valentine DOFFINY, assistantes de recherche.

Beaucoup de ceux qui l'étudient ou, plus simplement, l'apprécient le soulignent : le football constitue un objet très particulier. Dynamiteur de passions pouvant mener à la transfiguration des individus ou encore coeur de processus identificatoires forts, le foot demeure, par exemple, l'un des rares moteurs d'unification dans des pays parfois par ailleurs divisés, ce qui traduit la force et la cohésion qu'il peut exhaler.

Toute médaille a cependant son revers puisque ces mêmes éléments émotionnels, s'ils peuvent résonner positivement, sont aussi ceux susceptibles de déclencher des comportements inadaptés, voire répréhensibles. Tels sont notamment les cas des manifestations antisociales de supportérisme, comme l'hooliganisme, et qui se traduisent, par exemple, par des affrontements parfois extrêmement violents (entre fans, avec les forces de l'ordre) ou encore des propos et chants injurieux et/ou racistes entonnés depuis les tribunes des stades.

La présence d'argent dans le sport, en général, ne constitue ni une surprise ni une nouveauté sur le plan historique. Il n'est donc nullement étonnant – puisqu'il est dans beaucoup de pays le sport de loin le plus populaire – de la retrouver aussi dans un football qui aurait même été la première pratique sportive passée du loisir à l'exercice à titre principal contre rémunération, ce qui est l'élément principal définissant la professionnalisation.

I. Contextualisation : financiarisation du football et accroissement des opportunités délinquantes

Cette professionnalisation du football a cependant rapidement dépassé la seule rémunération des joueurs ayant décidé d'en faire leur métier. En effet, elle a ouvert la porte à une authentique financiarisation du football, qui n'a cessé d'aller *crescendo ;* l'arrêt ou la pause (selon les compétitions) imposé par le confinement en lien avec la pandémie de coronavirus ayant frappé le monde fin début 2019 - début 2020 a rappelé cette prépondérance de l'argent sur, entre autres, les considérations sportives, puisque les impératifs économiques ont lourdement pesé sur la reprise de certains championnats[1].

Il est possible de pointer différents leviers ayant présidé à cette évolution, sans ici aucune prétention d'exhaustivité. L'investissement fort, dans les années 1980, des grands équipementiers sportifs, ainsi que celui de grosses entités industrielles et financières, a constitué la première injection substantielle de capitaux dans le football professionnel. Mais cet apport était sans commune mesure avec ce

qu'a représenté ultérieurement l'explosion des montants liés aux « droits TV » et ce, à partir des années 90. Elle a créé une forme d'interdépendance footbalistico-médiatique jamais connue auparavant et les clubs ont désormais besoin, de manière financièrement vitale, des médias, au même titre d'ailleurs, que certains médias (a fortiori ceux qui sont exclusivement sportifs) ont besoin des clubs[2]. La libéralisation des transferts, à la suite du célèbre arrêt Bosman de la Cour de justice des Communautés européennes (15 décembre 1995), a profondément remis en question le rapport contractuel unissant joueurs et clubs. Cette décision judiciaire a dopé tant le montant des transferts que celui des salaires de joueurs : devenu terriblement concurrentiel, le marché a vu ses prix s'envoler en raison d'un point d'équilibre redéfini entre offre et demande. Pour ce qui est du foot européen à proprement parler, l'arrivée massive d'argent d'origine non continentale (Moyen-Orient, ex-URSS, ...) dans les capitaux d'un ensemble de clubs des plus grands championnats a encore accentué cette financiarisation, contraignant les instances sportives à prendre des mesures pour tenter – en vain – de limiter le gouffre grandissant créé par ces différentiels de capitalisation entre une élite très restreinte de grands clubs (comprenez « riches ») et les autres (comprenez « moins riches » voire « pauvres »), notamment avec les règles du « Fair-play financier » si chères à l'Union des associations européennes de football (UEFA)[3].

Au-delà des constats de nature économique et historique, cet avènement de l'argent dans le football professionnel peut aussi être perçu, plus spécifiquement, comme ayant à la fois engendré et multiplié les opportunités criminelles en lien avec cette activité. Dans la mesure où, de manière générale, la criminalité économique et financière peut être lue à travers le prisme des théories dites « opportunistes », qui soutiennent que l'explication du passage à l'acte résulte de l'exploitation de ce qui est perçu, par les criminels, comme des opportunités délinquantes, le brassage d'argent consubstantiel au football professionnel a, de manière quasi inévitable, induit une hausse de cette criminalité spécifique[4].

En octobre 2018, le football belge a été frappé par une onde de choc baptisée « Footbelgate » par les médias nationaux. S'inscrivant dans la continuité d'une première salve de révélations fracassantes liées aux « Football leaks » (novembre 2016), le début de ce séisme footballistique belge a été provoqué par une vague coordonnée de perquisitions et d'arrestations dans le pays et à l'étranger, mettant en cause des agents de joueurs, des dirigeants de clubs (au sens large), des entraîneurs, des joueurs et des arbitres. Ces devoirs d'instruction judiciaire furent rapidement rejoints, à l'instar des dominos tombant en cascade, par d'autres enquêtes mettant en cause les mêmes catégories d'intervenants, comme en témoignent des perquisitions menées en septembre 2019 et fin janvier 2020.

Au moment de rédiger ces lignes, aucune de ces procédures n'est achevée et il est dès lors impossible, tant à cause du respect dû à la présomption d'innocence que du caractère imprévisible de l'issue de la procédure, de dessiner les contours exacts de ce que ces enquêtes vont mettre à jour. Toujours est-il que la palette de comportements délinquants incriminés est très large et l'on peut citer, en vrac, et dans une acception non strictement juridique : fraude fiscale, corruption privée, blanchiment de capitaux, truquage de matchs, participation à une organisation criminelle, etc. Toute la panoplie y passe donc, faisant de la situation du football professionnel belge, certainement pas une réalité exclusive et/ou inédite ou une sorte de particularisme local (qui ne peut de toute façon exister dans un foot par essence globalisé, ce qui vaut aussi pour ses pratiques frauduleuses), mais bien un excellent révélateur de la criminogénéité de ce secteur d'activité qu'il peut être intéressant d'étudier.

II. Une criminalité endémique ?

Lorsqu'on prend la peine de se pencher sur la « sale » histoire du football, ce « sein que la plupart des supporters demandent de cacher car ils ne sauraient le voir », les exemples de « dérapages » ne manquent pas. Cette récurrence contraste, au passage, avec les réactions de surprise systématique qui teintent les prises de parole des acteurs du foot, dès lors qu'une « affaire » ou un « scandale » éclate et éclabousse leur sport, car cela n'a rien de nouveau et donc d'étonnant[5].

Même à la stricte échelle belge, le « Footbelgate » révélé par les faits de 2018 évoqués ci-dessus ne peuvent nullement être considérés comme la première confrontation du monde du foot avec la fraude. En effet, et par exemple, en 1982, le foot belge fut déstabilisé par « l'affaire Standard-Waterschei » : en vue de s'assurer du titre de champion national, le Standard de Liège acheta, à l'époque, plusieurs joueurs du club de Waterschei afin que ceux-ci lèvent le pied lors de la rencontre opposant les deux équipes. Objectif ? S'assurer, pour le Standard, le titre de champion de Belgique en limitant l'énergie dépensée et préserver, de la sorte, ses joueurs à quelques jours d'une finale de coupe européenne[6]. De même, « l'affaire Yé », survenue en 2005-2006, avait déjà mis en évidence la potentialité de truquages de matches de la compétition belge, non plus à des fins strictement sportives mais avec l'objectif de fausser des paris sportifs. Zheyun Yé, se présentant comme un homme d'affaires, écuma les clubs de football belges - le plus souvent financièrement exsangues - pour leur proposer des contrats de sponsoring et même des investissements en cas d'actionnaires. S'il fut éconduit par bon nombre de phalanges méfiantes, certaines furent cependant moins regardantes, ce qui permit à l'intéressé, avec la complicité judiciairement avérée d'un dirigeant de club, d'un avocat et d'un « agent » non officiel, d'approcher des joueurs et des entraîneurs afin que ceux-ci « lèvent le pied » dans certaines rencontres. La finalité de ce dispositif frauduleux était de favoriser le succès d'importants paris, tantôt placés sur des plateformes légales, tantôt auprès de bookmakers asiatiques opérant de manière underground, par la corruption de ces acteurs du foot.

Le trucage de matches n'est pas une invention belge ; tous les pays ont été ou sont concernés et il suffit, pour s'en convaincre, de jeter un oeil sur l'actualité judiciaro-sportive d'un ensemble de compétitions. *Calciopoli* et *Calcioscommese* en Italie (2006), *Koriopolis* en Grèce (2011), l'affaire *Hoyzer* en Allemagne (2005) ou encore *Sike Davasi* en Turquie (2011), les exemples ne manquent pas ! L'un des opérateurs de monitoring des paris sportifs, Federbest, estime que ce ne sont pas moins de 510 matchs de football intervenus au cours de la saison 2013/2014 qui présentaient des éléments suspects tandis que 110 d'entre eux montraient des éléments clairs et patents de manipulation[7].

Il convient de garder à l'esprit que les quelques illustrations ci-dessus ne concernent que les manipulations de matches, soit à des fins de paris sportifs, soit à des fins de falsifications de compétitions et que, en outre, elles sont loin d'être exhaustives de ce seul comportement illégal. La palette d'infractions (si l'on veut utiliser une grille de lecture juridique) est néanmoins bien plus large et si, en plus, l'on quitte le prisme juridique pour celui de l'éthique, la liste des comportements s'allonge très significativement.

Si l'expression « crime en col blanc » est quasi passée dans le langage courant, peu connaissent son origine et les travaux de E.H. Sutherland desquels elle a émergé[8]. Dans son ouvrage de référence, plus que finalement la criminalité des dirigeants d'entreprise (les cols blancs), Sutherland démontrait la délinquance des entreprises, comme structures, personnes morales, et le traitement préférentiel, hors de la chaîne pénale classique, caractérisant ce contentieux. Mais Sutherland soulignait aussi la récurrence des infractions commises par certaines des plus grandes sociétés US scrutées par ses soins, sur une période d'analyse de plus de 30 ans : les individus changeaient mais la délinquance demeurait, ce qui plaide en faveur d'une analyse des causes de la délinquance qui dépasse la stricte responsabilité individuelle, même si celle-ci, à bien des égards, est plus confortable à concevoir puisqu'elle empêche toute (re)mise en cause plus large.

Il n'en va pas autrement du football professionnel que de l'analyse de Sutherland. La persistance des comportements frauduleux doit être analysée comme la manifestation possible d'un terreau fertile pour la fraude, en ce que ce secteur d'activité recèle alors un nombre significatif de facteurs criminogènes. Ces facteurs doivent dès lors être explorés afin de poser le débat de manière correcte, ce qui est la condition nécessaire (mais pas suffisante) pour des actions correctrices efficaces. En outre, il est également possible de questionner cette récurrence frauduleuse à l'aulne de l'hypothèse

d'un marché, celui du football professionnel, au sein duquel les illégalismes commis ne sont pas ou plus le fait d'individus, plus ou moins isolés, transgressant ponctuellement les lois mais bien celui d'individus utilisant des méthodes proches de celles auxquelles ont recours les organisations criminelles.

A. Collection de facteurs criminogènes

Le concept de « facteur criminogène », s'agissant de délinquances à formes économiques, renvoie à des caractéristiques propres à un secteur d'activité qui, selon les cas et par ordre d'influence croissante, exercent une influence « facilitative », « incitative » ou « obligative » dès lors qu'il s'agit de fraudes *sensu lato*[9].

Il est possible, sans prétention d'exhaustivité dans une contribution de volume réduit telle que la présente, d'évoquer un ensemble de facteurs criminogènes généraux caractérisant le foot pro. Par « facteurs généraux », il faut ici entendre des facteurs qui concernent toutes les facettes du football professionnel.

Il y a tout d'abord l'important volume des capitaux brassés par ce secteur, qui représente une activité économique à part entière, qui crée à la fois une forme d'attractivité tant pour des acteurs respectueux de la loi que pour certains délinquants potentiels. L'omniprésence de l'argent dans le foot professionnel est évidente mais elle contraste avec l'opacité forte qui l'entoure car le monde du ballon rond réussit à maintenir ce paradoxe : l'argent y est partout, tout le monde parle d'argent mais, au final, de l'argent dans le foot, on ne sait pas grand-chose de précis. Combien gagne réellement tel joueur ou coach, quel est le montant exact de tel transfert ? Les protagonistes du foot se font particulièrement discrets dès lors qu'il s'agit d'être précis. L'activité footballistique est par ailleurs transnationale par essence, comme mentionné *supra*, ce qui crée l'opportunité d'une justification permanente de flux à l'échelle planétaire.

Déjà envisagées seules, l'importance des sommes, l'opacité et la transnationalité, sont des facteurs de risques classiquement reconnus, par exemple, mais pas limitativement, en matière de blanchiment de capitaux, et les autorités publiques ne s'y trompent pas[10].

Mais il y a plus, bien plus, même… Le football professionnel à plusieurs vitesses décrit ci-dessus engendre une dichotomie des moyens qui, couplée à la précarité forte d'un ensemble de clubs (et à travers eux d'actionnaires, de personnel, etc.), crée la potentialité d'une infiltration de capitaux d'origine criminelle dans ce secteur. Luttant tous les jours pour leur survie financière et sportive, les deux étant le plus souvent liées tantôt dans une rétroaction positive, tantôt dans une rétroaction négative, les clubs au bord du gouffre peuvent être tentés de succomber à de l'argent dont l'odeur nauséabonde n'a pourtant pas dû totalement leur échapper : l'affaire « Yé », dans le foot belge évoquée auparavant, n'en est qu'un des nombreux exemples.

L'avidité des acteurs du foot, notamment celle des joueurs qui doivent rentabiliser une carrière de sportif professionnel par essence limitée dans le temps et chez qui le goût du « bling-bling » est parfois très prononcé, rencontre celles d'autres professionnels du secteur, comme par exemple les agents/intermédiaires, et leur goût partagé de l'argent tisse alors la trame de leur parcours commun. Ce goût de l'argent, et la spirale sans fin qui peut le caractériser, est un des moteurs de la fraude, mais aussi de l'enracinement dans une éventuelle trajectoire criminelle, par les changements de valeurs, de style de vie, et de fréquentation des groupes de pairs qu'il induit.

Les accointances économiques entre le football professionnel et d'autres secteurs d'activité (parfois en plein essor) est un autre facteur général potentiellement criminogène. L'on pense notamment à l'industrie des paris qui, après s'être affranchie d'un ensemble de monopoles d'état, a déployé sa toile, en y capturant les sports et, parmi eux, le foot pro. Les sociétés de paris ne se contentent d'ailleurs plus d'organiser des mises sur le football, elles sont parfois devenues les sponsors principaux de plusieurs équipes de pointe, lorsqu'elles ne sont pas les partenaires officiels de ligues ! Il n'y a dès lors rien d'étonnant à ce que cet entrelacs argenté (au sens premier) crée les conditions de possibles truquages de matches à des fins sportives : les gains des fraudeurs peuvent être

astronomiques et la dissimulation de leurs malversations dans une masse de paris devant désormais être envisagée à l'échelle mondiale, est sans cesse plus aisée.

Enfin, les contrôles exercés sur les clubs de football professionnel sont, depuis longtemps, pointés comme largement lacunaires[11]. L'existence de nombreux conflits d'intérêts au sein des instances décisionnelles et régulatrices qui sont en charge de la rédaction des règlements (fédérations) ou des compétitions (ligues) rajoute à l'inefficacité du contrôle et mine toute velléité (pour autant qu'elle soit sincère) d'autorégulation. Il est difficile de concevoir que des gendarmes puissent se contrôler eux-mêmes…

Au vu de ces quelques facteurs brossés à gros traits, l'on perçoit mieux en quoi l'essence même du football professionnel, comme secteur d'activité, rend celui-ci propice à des exploitations criminelles en tous genres. Mais ce n'est pas tout…

B. Les fraudes liées aux transferts et contrats en particulier

Au sein de ce tableau général des facteurs de criminogénéité caractérisant l'industrie footballisique professionnelle, il faut détailler ceux qui concernent les transferts et contrats, en particulier. Ces facteurs spécifiques s'additionnent donc aux facteurs généraux précités pour faire des transferts entre clubs (et des contrats y afférents) la pierre angulaire des fraudes commises. L'on peut dès lors presque évoquer une « surcriminogénéité » mais aussi envisager, sur un plan fonctionnel, les illégalismes inhérents aux transferts et contrats, comme l'origine d'une masse de capitaux illicites, qui vont être les leviers d'un ensemble d'autres actes délinquants.

Parmi ces facteurs de criminogénéité spécifiques, il convient d'abord de pointer la subjectivité très importante qui caractérise la valeur d'échange d'un joueur. Aux facteurs intrinsèques liés au sportif, comme l'âge, le poste, l'historique/expérience, le fait de jouer en sélection nationale ou non, d'être gaucher/droitier, viennent se superposer des réalités sportives et économiques (comme les finances des clubs concernés par la transaction ou leurs besoins de recrutement purement sportifs). Dès lors qu'il n'existe pas ou très peu de balises financières dans ce type d'opérations, il est simple de sous-payer ou de surpayer le montant du transfert d'un joueur. Il n'en va d'ailleurs pas autrement des conditions salariales conclues au moment de la même opération de transfert.

Cette importante subjectivité de la valeur d'échange permet, le cas échéant, de « doper » une vente, parfois de plusieurs millions d'euros, et dont une partie est éventuellement destinée à être redistribuée discrètement à des acteurs qui ont été concernés par le deal. Ceci permet de réaliser une corruption privée (inciter les détenteurs du pouvoir de droit/fait sur l'opération à la conclure). Mais ce schéma permet aussi (ou en plus) d'organiser une fraude fiscale destinée à payer la « prime à la signature » du joueur, les commissions des agents impliqués, voire en réglant, « en noir » et donc en échappant à toute forme de fiscalité, une partie du salaire du joueur.

La prolifération des intermédiaires, en particulier des « agents de joueurs » plus ou moins reconnus (selon les exigences nationales), et le rôle sans cesse plus important qu'ils jouent dans le monde footballistique professionnel, constitue un autre facteur de risque. S'il ne s'agit certainement pas ici d'affirmer que tous les agents sont des fraudeurs, le rôle central qu'ils peuvent jouer en matière d'illégalité sur les transferts est bien connu, et depuis très longtemps. La forte concurrence et l'instabilité du lien contractuel (mandat) unissant joueur/entraîneur et agent, couplée à la grande concurrence du marché des intermédiaires constituent deux premiers facteurs de criminogénéité. L'intéressement de la rémunération de l'agent à la conclusion de l'opération - soit un modèle de rémunération connu dans d'autres professions – peut parfois agir comme un incitant fort à transgresser la loi : être prêt à tout pour conclure un transfert et toucher alors une commission par définition inexistante si l'opération n'est pas bouclée.

Plus loin, ce sont les rapports et relations (et leurs modalités) entre agents et autres protagonistes du monde du foot qui sont potentiellement à risque. Certains agents sont, par exemple, les intermédiaires attitrés, points de passage obligés,

de certains clubs, et ce, pour toute opération entrante ou sortante, au point de parfois supplanter d'autres employés du club pourtant assignés à cette tâche, par exemple en remplissant quasi la fonction de directeur sportif ou technique ou de responsable du recrutement. Certains d'entre eux (parfois les mêmes !) sont aussi les agents des coaches qui dirigent les équipes dans les noyaux au sein desquels figurent un ou plusieurs joueurs de leur portefeuille. L'on conçoit alors aisément que ces relations multiples et malsaines puissent conduire tantôt à des convergences d'intérêt, tantôt à des conflits d'intérêts. Payer un coach pour qu'il aligne un joueur, ou s'appuyer sur le mandat qui lie l'agent et l'entraîneur pour arriver à la même fin, voilà une autre forme de corruption privée sévissant dans le monde du football professionnel. Sans oublier le cas, que l'on n'oserait qualifier « d'idéal », de clubs plus ou moins discrètement sous la direction actionnariale d'agents de joueurs, ce qui est totalement contraire aux règlements sportifs en vigueur mais aussi formidablement créateur d'opportunités criminelles de natures polymorphes…

La commission de l'agent, dont l'encadrement est plus ou moins contraignant selon les réglementations applicables en fonction des championnats concernés, peut également servir de point de départ à la création d'une authentique comptabilité parallèle, synonyme d'organisation des rapports humains. La « rétro-commission », souvent présentée improprement comme la seule fraude ayant cours dans le foot professionnel, est un formidable exemple de la manière insidieuse dont les choses peuvent se dérouler. L'intermédiaire, ayant conclu un transfert, a droit à une commission (pourcentage du prix de la transaction et/ou pourcentage de la rémunération annuelle brute du joueur perçue par celui-ci dans son nouveau club). Ce montant de commissionnement peut être artificiellement gonflé par toutes ou certaines parties à la transaction. La somme devient alors potentiellement (et discrètement) redistribuable à ceux qui ont rendu l'opération possible, et qui ont donc permis à la commission d'exister (directeurs sportifs, entraîneurs, joueurs, …). Le magot agit alors comme un levier de la corruption, mais aussi comme celui d'une fraude fiscale de grande envergure puisqu'elle n'a aucune existence légale, plus spécifiquement fiscale. C'est là un des points névralgiques du schéma frauduleux puisqu'il contente tout le monde : le joueur atterrit dans le club de ses désirs, l'agent gagne sa vie, les dirigeants sont heureux d'attirer le renfort recherché, les corrompus arrondissent leurs fins de mois et les supporters sont aux anges. En fait, seul un acteur est mécontent parce que spolié, c'est le fisc qui, comme l'État qui l'incarne, peut être l'objet d'un ensemble de techniques de neutralisation qui vont faciliter sa victimisation et donc le passage à l'acte frauduleux[12].

À coups d'enveloppes remplies de cash et remises sous le manteau, de cadeaux sous la forme de biens de luxe (montres, costumes, …), l'argent est alors redistribué aux « méritants ». Dans la mesure où, dans le football professionnel, les paiements se réalisent le plus souvent sous la forme d'échéanciers complexes (il est, en effet, rare qu'une somme de transfert soit réglée en une fois ; le plus souvent son paiement est échelonné en plusieurs tranches), il se crée alors une forme d'économie parallèle, illégale qui suit ces mêmes plannings de distribution. L'intermédiaire devient dès lors, en plus de ses autres prérogatives, une espèce de « comptable-notaire » des paiements occultes. Dans la mesure où il est bien connu que les relations économiques entre créanciers et débiteurs sont des organisateurs de rapports humains, en ce compris dans l'illégalité, l'agent peut alors créer un système de redevabilités croisées qui est de nature à perpétuer le système illégal créé.

Poussé à échelle moyenne, voire grande, ce système crée à la fois un matelas économique et un tissu relationnel que les acteurs impliqués peuvent mobiliser au gré de leurs envies/besoins. La finalité de cette mobilisation peut, bien entendu, être illégale, mais elle peut aussi servir, et c'est ce qui fait sa force, des desseins légaux. Ce dernier emploi est particulièrement insidieux puisque, en effet, adossée à des complicités passées, il permet d'utiliser des solidarités criminelles préexistantes (et renforcées par le fait, par exemple, que toutes les sommes dues n'ont pas encore été perçues) pour mener des opérations, quant à elles, dépourvues

de tout illégalisme[13] ! Ce « système » pourrait, entre autres choses, être mis en lumière par les développements judiciaires du scandale du « Footbelgate » précédemment évoqué…

III. Criminalité organisée

En 2006, Denis Robert titrait son ouvrage pionnier consacré aux fraudes dans le football : « Le milieu du terrain »[14]. Outre le jeu de mots, ce choix traduisait l'idée d'un ensemble d'acteurs impliqués dans les fraudes liées au football fonctionnant selon le modèle du « milieu », soit celui des organisations criminelles.

L'idée mérite assurément d'être traitée comme une hypothèse de recherche car un ensemble d'indicateurs la rend a priori crédible. Il y a tout d'abord la récurrence des comportements frauduleux évoquée *supra* et, parmi ceux-ci, l'implication démontrée de plusieurs organisations reconnues comme criminelles par les États concernés (Grèce, Italie, Turquie, …). La présence des nombreux facteurs criminogènes évoqués dans la section précédente de la présente contribution éclaire ce constat à travers le prisme des théories opportunistes caractérisant le plus souvent les délinquances financières[15]. Mais il est possible d'aller plus loin…

Dans une approche non-juridique et au-delà des différences entre les législations nationales, il est possible de considérer que les organisations criminelles sont caractérisables par l'implication de plusieurs personnes (au moins 3), dans une association relativement pérenne, structurée, appliquant la discrétion sinon la loi du silence, à tout le moins une grande discrétion, poursuivant un objectif de profit, et usant de moyens tels que l'intimidation, la violence et/ou la corruption. Certaines modélisations théoriques ajoutent, à ces caractéristiques, une imbrication systématique entre activités légales et illégales.

Force est de constater que les révélations apportées à ce stade par un ensemble d'affaires, dont le « Footbelgate », semblent démontrer la réunion de ces éléments. Les gains sont potentiellement très importants et ils titillent l'avidité de certains personnages peu scrupuleux qui en font leur objectif « coûte que coûte ». Des connexions stables entre individus ont été mises à jour et elles sont apparues comme ayant eu cours pendant une période de temps significative, parfois « importées » dans différents clubs, selon les mêmes schémas. Le monde du foot est par ailleurs un univers où le mensonge est roi, en plus de l'opacité préalablement décrite, et beaucoup de choses sont tues, en tout cas vers l'extérieur du microcosme footballistique (ce qui inclut la sphère judiciaire) : tout « de polichinelle » qu'ils soient, les secrets sont légion ! Si les violences sont exceptionnelles, l'intimidation, quant à elle, semble bel et bien exister. Si elle est rarement physique, elle semble cependant souvent « économique » : ceux qui ne se plient pas aux diktats des « plus forts », économiquement parlant, se trouvent exclus des opérations les plus lucratives, voire carrément du marché tout entier.

Toutefois, ce n'est pas ici l'hypothèse d'acteurs criminels organisés désirant « infiltrer » le monde du football professionnel qui se dessine, mais bien celle de protagonistes déjà actifs dans ce secteur, ayant pignon sur rue, alternant actes légaux et illégaux, qui émerge. Ce « système criminel » entretiendrait des relations, non pas parasitaires, mais symbiotiques avec le « système légal », les deux ayant de multiples interrelations de sorte que, peut-être, ils ne soient aujourd'hui même plus clairement dissociables. Cette situation contribuerait alors à créer le paradoxe stigmatisé par M. Punch et qui expliquerait la profondeur du problème rencontré par le foot, même s'il le formulait en regard de l'activité d'autres industries : « Crime is simultaneously normal and deviant »[16].

Si l'hypothèse ainsi précisée venait à être empiriquement soutenue, c'est toute l'appréhension de la problématique qui s'en trouverait bouleversée. En effet, la délinquance liée au football ne devrait alors plus être perçue comme le fait d'acteurs individuels décidant de transgresser épisodiquement la loi dans une forme de dérive, mais comme le fait de personnages liés qui exploitent le football pour y développer une activité criminelle sinon principale, à tout le moins substantielle. L'impact éventuel de cette confirmation d'hypothèse emporterait des conséquences sur le plan théorique, rendant pertinente la mobilisation de

cadres propres à la criminalité organisée, ce qui permettrait de mieux comprendre le phénomène, les comportements et les acteurs qui lui donnent corps. Mais il s'exercerait aussi sur le plan de l'intervention, qu'il s'agisse de la prévention ou de la répression, qu'elles concernent les autorités judiciaires ou sportives, et dont l'efficacité serait rehaussée par l'utilisation de cadres théoriques adaptés.

En conclusion, le tableau du football professionnel qui précède est – il faut en convenir – assez sombre. Il n'est toutefois en aucun cas une diatribe à l'encontre de ce sport et de l'activité économique qu'il nourrit et il n'entend pas non plus nier que les mêmes problèmes (ou d'autres) caractérisent d'autres sports. Néanmoins, il doit interpeller à un ensemble de niveaux. La récurrence des comportements illégaux, qu'elle traduise la puissance incitative voire « obligative » des facteurs criminogènes mis en évidence et/ou la mise en place de formes organisées de criminalité, témoigne en tous cas de l'incapacité, jusqu'à présent, des tentatives d'assainissement du secteur, exogènes ou endogènes.

Au-delà, on peut considérer que toute crise, quelle qu'en soit la nature, agit comme un révélateur. Appliquée au monde du football, et comme souligné précédemment, celle liée au coronavirus a exhibé et exacerbé la fragilité financière des clubs. Et pour en revenir au prisme qui a servi de point de départ à la présente contribution, la Belgique et ses clubs de football n'ont pas du tout fait exception à cette règle : déjà fragiles en comparaison de nombre de leurs concurrents européens, les cercles nationaux en ressortent encore davantage précarisés. L'on sait que si une crise peut réveiller les consciences, la précarité économique est un facteur criminogène majeur…

La crise du « Footbelgate », dont il est difficile d'estimer la date de l'accouchement judiciaire – dans une procédure toujours longue dès lors qu'il s'agit d'affaires à dominante financière -, est/sera un deuxième révélateur pour le football professionnel belge, dont on peut alors dire qu'il se retrouve à la croisée des chemins.

En réalité, plus qu'une croisée des chemins, c'est une bifurcation qui se dessine. Soit le football belge – et à travers lui, tout le foot car il n'en est qu'un exemple - se réinvente et change de cap, soit il poursuit son chemin et ne se réforme pas.

L'option du changement suppose une grande radicalité : il faudra faire preuve de davantage de raison, faire oeuvre d'un fort assainissement des pratiques souvent plus qu'à « la limite » et tenir bon dans un marché particulièrement concurrentiel sur lequel, dès lors qu'un opérateur vient à impunément violer les règles, et de surcroît avec des succès à la clé, ce sont tous les acteurs qui subissent la tentation de l'imiter… Toutefois, dans une activité où prévaut le court terme, celui du match, du résultat, du classement, des trophées, il y a comme une contradiction avec cette réinvention qui ne pourra sortir des bénéfices au mieux qu'à moyen terme, plus vraisemblablement à long-terme. Cette contradiction ne dope pas forcément l'optimisme ouvert par la perspective d'un changement, tandis qu'il renforce la crainte de l'option de l'attente de la fin de l'orage et, donc, de la résurgence des déviances/délinquances comme des faux plis tenaces. L'histoire des scandales de délinquance liée au monde des affaires et à l'argent est, malheureusement, jalonnée de la cyclicité des comportements frauduleux. Qui vivra verra…

Notes :

1 PRO LEAGUE DE FOOTBALL, « Le chiffre d'affaires des clubs belges progresse de 18%, atteignant €378,5 millions pour la saison 18/19, mais leur rentabilité reste fragile », Communiqué de presse, 3 juin 2020, 4 pages.

2 Voir not. MARCHETTI, D., SOUANEF, F. (2017), « La médiatisation du football : un jeu sous contrôle », *Pôle Sud*, Vol. 2, N°47, 61-78.

3 Pour plus d'infos, voir not. PETER, H., ARN, J. (2017), « Gouvernance sportive: le système du fair-play financier de l'UEFA est-il correctement conceptualisé? » *in*: A. LEUBA et al., *Le droit en question: Mélanges en l'honneur de la Professeure Margareta Baddeley*, Genève, Schultess Editions Romandes, 429-457.

4 Sur le lien entre criminalité économique et financière et opportunités, voir not. BENSON, M., SIMPSON, S. (208), *White-Collar Crime: An Opportunity Perspective*, Londres, Rouledge, 276 p.

5 Sur ce distinguo entre « affaire » et scandale, voir l'intéressante analyse de Pierre Lascoumes – LASCOUMES, P. (1997), Elites irrégulières, Paris, Gallimard, 304 p.

6 La similitude avec le scénario du célèbre match FC Valenciennes / Olympique de Marseille de 1993 est évidente et le fait que l'entraîneur du Standard de Liège (1982) et de l'OM (1993) fut le même (R. Goethals) ne peut pas être une pure coïncidence.

7 MORICONI, M. (2018), "The official football match-fixing prevention discourse as a cognitive limitation (the cases of Iberian countries)", *Soccer & Society*, Vol. 19, N°2, pp. 271-287.

8 Voir not. la version intégrale de l'ouvrage majeur de Sutherland: SUTHERLAND, E.H. (1983), *White collar crime – The uncut version*, Londres, Yale university Press, 320p.

9 Sur ce concept de marché criminogène, voir l'étude fondatrice : FABERMAN, H. (1975), « A Criminogenic Market Structure: The Automobile Industry », *The Sociological Quarterly*, 1975, vol. 16, N° 4, pp. 438-57.

10 Dès 2009, le GAFI consacrait un rapport spécial aux risques de blanchiment de capitaux à travers le secteur du football – FATF (2009), *Money Laundering through the Football Sector*, 42p.

11 DI RONCAO, A., LAVORGNA, A. (2015), "Fair play? Not so much: Corruption in the Italian football", *Trends in Organized Crime*, Vol. 18, pp. 176–195.

12 Il faut se référer ici aux travaux fondateurs de Matza et Sykes qui, à travers leur théorie des techniques de neutralisation, expliquent comment les délinquants soulèvent les barrières morales qui, normalement, devraient les dissuader de passer à l'acte – MATZA, D., SYKES, G.M. (1957), « Techniques of Neutralization : A Theory of ² », *American Sociological Review*, Vol. 22, N°6, pp. 664-670.

13 Sur ce concept de loyautés criminelles, dans le spectre du radicalisme cette fois, voir not. TRUONG, F. (2017), *Loyautés radicales – L'Islam et les « mauvais garçons » de la Nation*, Paris, La Découverte, 238 p.

14 ROBERT, D. (2006), *Le milieu du terrain*, Paris, les Arènes, 240p

15 On peut résumer ces théories opportunistes dans le champ de la délinquance économique et financière par l'adage anglophone « If it could be done, some one will do it » - ROSOFF, M, et al. (2013), *Profit Without Honor: White Collar Crime and the looting of America*, 6ème edition, Pearson, 664p.

16 PUNCH, M. (1996), *Dirty Business*, Londres, Sage, 318p.

OUVRAGES RÉCENTS

LE JIHADISME FRANÇAIS

QUARTIERS, SYRIE, PRISONS

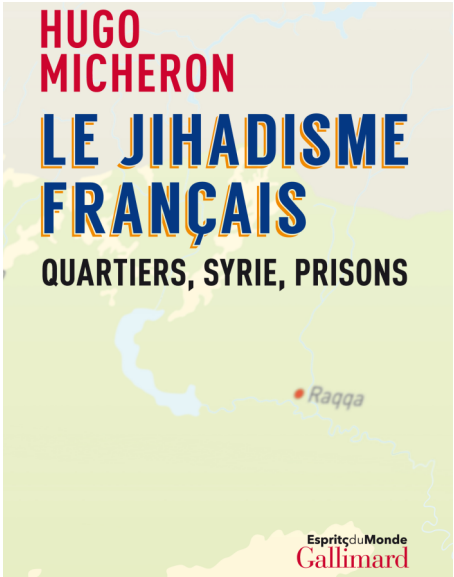
AUTEUR : HUGO MICHERON

ÉDITEUR : GALLIMARD

Résumé

Cinq ans après les attentats qui ont ensanglanté la France - de la tuerie de Charlie Hebdo au massacre du Bataclan -, ce livre est le premier récit de l'intérieur du processus qui a vu croître le jihadisme français. Né dans les «cités» enclavées des banlieues populaires, il a mené ses activistes, en passant par le «califat» de Daech au Levant, jusqu'aux prisons de l'Hexagone.

À partir de quatre-vingts entretiens avec des terroristes incarcérés, Hugo Micheron analyse la nature du jihadisme français.



Loin d'être coupée du reste de la société, la prison est en interaction constante avec les quartiers. Dans quel terreau français se creuse le jihadisme ? Comment se transplante-t-il dans le jihad syrien ? Comment s'épanouit-il dans les prisons de l'Hexagone ? Voici le récit édifiant d'une emprise moderne, méthodique, qui a bouleversé les profondeurs de la société