LA REVUE DU
GRASCO

www.grasco.eu
www.larevuedugrasco.eu

N°29— Janvier 2020

Parution trimestrielle
Gratuite
ISSN 2272-981X

EDITORIAL

JOCELYNE KAN

RÉDACTRICE EN CHEF DE LA REVUE DU GRASCO

La rédaction présente ses meilleurs voeux à ses lectrices et lecteurs pour 2020.

Le Groupe de Recherches Actions Sur la Criminalité Organisée (GRASCO) publie sa revue depuis près de 8 ans. La revue n'a de cesse d'informer sur la prévention et la répression de la criminalité organisée dans sa dimension économique et financière.

La criminalité organisée, qui a des formes variées et tentaculaires et qui est généralement transnationale, évolue malgré l'arsenal juridique aux niveaux national, européen, international. Elle progresse plus vite que les lois.

Toute personne, physique ou morale, est une victime potentielle de la criminalité organisée. Elle ne concerne pas que les acteurs qui s'emploient à la prévenir, à la poursuivre, à la sanctionner. Nous sommes tous concernés. C'est ainsi qu'il faut s'informer, se former pour connaître et reconnaître toutes les formes de la criminalité organisée. Il faut se sensibiliser à ce phénomène pour être moins vulnérable. Cela rendrait un peu plus difficile l'action des criminels à l'affût des faiblesses et des opportunités. À cet effet, les pouvoirs publics devraient encourager ces formations, ces sensibilisations. Aussi, il est regrettable de voir supprimer, dans quelques mois, des structures telles que l'Institut national des hautes études de la sécurité et de la justice (INHESJ) qui a justement pour mission de proposer des formations de qualité sur la criminalité et la délinquance à des hauts responsables des secteurs public et privé.

Il est acquis que le rôle de la société civile est primordial dans la lutte contre la criminalité organisée. Il convient de se féliciter de l'évolution de la fonction Conformité dans les secteurs bancaires, industriels, qui assure au mieux l'éthique des affaires. De même, la fonction de référent déontologue ne peut qu'être encouragée dans la mesure où elle prévient des conflits d'intérêts. La récente directive du Parlement européen et du Conseil de l'Union européenne du 7 octobre 2019 sur la protection des lanceurs d'alerte qui signalent des violations du droit de l'Union devrait permettre d'accroître la révélation de faits délictueux d'une gravité certaine.

SOMMAIRE

ÉDITO....1

INTERVIEW :

GIANLUCA ESPOSITO, SECRÉTAIRE EXÉCUTIF DU GROUPE D'ÉTATS CONTRE LA CORRUPTION DU CONSEIL DE L'EUROPE....4

DOCTRINE SCIENCES CRIMINELLES

DARKWEB ET ENQUÊTE PÉNALE : LA DIFFICILE CONCILIATION ENTRE EFFICACITÉ, PROTECTION DES DONNÉES ET CONFORMITÉ AU RGPD PAR ADEL JOMNI ET FLORIAN PERRETIN....9

DOCTRINE JURIDIQUE

LA RÉGULATION DES CRYPTO-ACTIFS : UN DÉFI EN TERMES DE COMPTABILITÉ DES NORMES ET CLARTÉ DE LA LOI EN MATIÈRE DE LCB-FT PAR DELYA DOUGLAS....17

FOCUS SUR LES CAS DE DÉNONCIATION OBLIGATOIRE AU PARQUET DE FAITS DE FRAUDE FISCALE DOROTHÉE GOETZ....22

DU CÔTÉ DES PRATICIENS

LES NOUVEAUX ENJEUX DE LA LUTTE CONTRE LA CRIMINALITÉ FINANCIÈRE AU SEIN DE LA DIRECTION CENTRALE DE LA POLICE JUDICIAIRE PAR THOMAS DE RICOLFIS....25

LA RECHERCHE DE LA PREUVE NUMÉRIQUE PAR LA GENDARMERIE NATIONALE PAR CYRIL DEBARD....31

Mais, la lutte contre la criminalité organisée demeure un véritable défi dans la mesure où elle nécessite des moyens. L'accumulation de textes répressifs d'application parfois complexe, l'adoption de plans d'action, la création de nouveaux services préventifs ou répressifs tant dans les secteurs public que privé, resteront insuffisantes pour lutter efficacement contre la criminalité organisée faute de moyens matériels et humains suffisants. Régulièrement, les spécialistes, qui contribuent à la revue du GRASCO, dénoncent ce manque récurrent de moyens. Partant de ce même constat, en janvier 2019, François Molins, procureur général prés la Cour de cassation avait souligné, lors de l'audience solennelle de rentrée de la Cour, que « le ministère public souffre d'un manque de moyens » et s'adressant à la Garde des Sceaux, il avait ajouté qu'il faut « dans une véritable direction de projet, augmenter les moyens humains et matériels dont disposent les parquets, moyens en magistrats mais aussi par une véritable assistance à ces magistrats ». Dans le même sens, dans un référé du 12 décembre 2018 rendu public le 4 mars 2019, la Cour des comptes a noté que l'organisation et les moyens consacrés par les ministères de l'Intérieur et de la Justice à la lutte contre la délinquance économique et financière faisaient apparaître des faiblesses. Il convient de mentionner également le rapport intitulé « Évaluation de la lutte contre la délinquance financière » remis par les députés Ugo Bernalicis et Jacques Maire le 28 mars 2019, dans lequel ils ont suggéré une augmentation des effectifs de police spécialisés et la hausse des effectifs du parquet national financier. De même, le 26 novembre 2019, les députés Jean-Luc Warsmann et Laurent Saint-Martin ont remis, à la ministre de la Justice et au secrétaire d'État auprès du ministre de l'Intérieur, leur rapport intitulé « Investir pour mieux saisir, confisquer pour mieux sanctionner », dans lequel ils font 36 propositions afin de faire de la saisie un réflexe et donner aux services d'enquête et aux juridictions les moyens de mettre en oeuvre les nouvelles orientations de la politique de saisie et de confiscation.

La lutte contre la criminalité organisée exige également un échange d'informations, de renseignements. Elle nécessite une véritable coopération aux niveaux national, européen, international et une entraide judiciaire sans faille. Il est indispensable que ces collaborations, coopérations, entraides, qui sont prévues par de nombreux textes, conventions et traités, puissent s'appliquer avec moins de difficulté.

Souhaitons qu'en 2020 tous les manquements précités soient revus à la baisse. Sinon, il sera légitime de se demander s'il existe une volonté affirmée de garantir que le crime ne paie pas.

LA REVUE DU GRASCO

Numéro ISSN : 2272-981X

Université de Strasbourg, UMR-DRES 7354

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

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

Adresse mail : information@grasco.eu

Directrice de la revue du GRASCO : Chantal CUTAJAR

Rédactrice en chef : Jocelyne KAN

Rédacteur adjoint—Conception : Sébastien DUPENT

COMITÉ SCIENTIFIQUE DU GRASCO

FALLETTI François

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

LABORDE Jean-Paul

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

LEBLOIS-HAPPE Jocelyne

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

MATHON Claude

Avocat général honoraire à la Cour de cassation (chambre criminelle). Après avoir Développé une carrière essentiellement comme procureur de la République, il a dirigé le Service Central de prévention de la Corruption (2001). Spécialisé en intelligence économique, il a présidé à la rédaction de trois rapports : « Entreprise et intelligence économique, quelle place pour la puissance publique ? - 2003 », « Intelligence économique et corruption - 2004 », « la protection du secret des affaires : enjeux et propositions-2009 ».

PRADEL Jean

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

SORDINO Marie-Christine

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

STRICKLER Yves

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

STORCK Michel

Professeur émérite à l'Université de Strasbourg.

INTERVIEW

GIANLUCA ESPOSITO,

SECRÉTAIRE EXÉCUTIF DU GROUPE D'ÉTATS CONTRE LA CORRUPTION (GRECO) DU CONSEIL DE L'EUROPE

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

L.R.D.G. : Quelle est la genèse de la création du GRECO par le Conseil de l'Europe en 1999 ?

Au milieu des années 1990, il y a eu une reconnaissance croissante de la part de nos États membres du fait que la corruption sape les valeurs qui sont au coeur du Conseil de l'Europe, à savoir la démocratie, l'État de droit et les Droits de l'Homme. La corruption empêche aussi le développement social et économique de nos sociétés car elle freine les investissements, réduit les revenus fiscaux, rend les services publics inefficaces, augmente les inégalités, et met en péril les institutions financières. Plusieurs affaires de corruption ont éclaté à cette époque dans nombreux États membres, comme par exemple l'enquête « Mani Pulite » (« Mains Propres ») en Italie.

Dans ce contexte, les ministres européens de la Justice, réunis en 1994 à Malte et 1997 à Prague, ont convenu la mise en place d'un cadre conventionnel et institutionnel afin, d'abord, d'harmoniser les cadres juridiques nationaux et, ensuite, de s'assurer – par le biais d'un mécanisme de contrôle international – la mise en oeuvre effective de ces normes. C'est ainsi que les 20 Principes directeurs pour la lutte contre la corruption (Résolution (97) 24), les Conventions pénale et civile sur la corruption (STE 173 & 174), et les Recommandations sur les codes de conduite pour les agents publics (Recommandation n° R (2000) 10) et sur les règles communes contre la corruption dans le financement des partis politiques et des campagnes électorales (Recommandation Rec (2003) 4) ont été adoptés.

Le 2e Sommet des chefs d'État et de gouvernement des États membres du Conseil de l'Europe a décidé de la création du Groupe d'États contre la Corruption (connu sous l'acronyme « GRECO ») qui a vu le jour deux ans plus tard en 1999 sous forme d'un Accord partiel et élargi.

Il s'agit d'un Accord « partiel » car, à l'époque de sa création, certain États européens estimaient que la lutte contre la corruption n'était pas une priorité dans leur Pays. Depuis, les choses ont changé et, à partir de 2010, tous les 47 États membres du Conseil de l'Europe sont devenus membres du GRECO devant reconnaître que la corruption nous concerne tous. Elle

n'est pas liée à l'appartenance nationale, mais à l'intégrité individuelle de chacun et chacune d'entre nous. L'Accord créant le GRECO est aussi « élargi » car des États non-membres du Conseil de l'Europe peuvent y adhérer. Le Bélarus et les États-Unis d'Amérique sont membres à part entière du GRECO. Le Kazakhstan va bientôt le devenir et la Tunisie a demandé l'adhésion et a été invitée à y adhérer. Le GRECO est donc un mécanisme anti-corruption qui dépasse largement les frontières de l'Europe.

Le GRECO est l'un des quatre mécanismes anti-corruption dans le monde. Les trois autres sont celui de l'Organisation des États américains (OEA) basée à Washington D.C., celui de l'Organisation de coopération et de développement économiques (OCDE) basée à Paris, et enfin celui de la Conférence des États parties à la Convention des Nations Unies contre la corruption basée à Vienne.

L.R.D.G. : Quels sont le rôle et le fonctionnement du GRECO ?

Le rôle du GRECO est d'assurer le respect et l'application effective des normes anti-corruption par ses 49 États membres. Nous le faisons par le biais d'un processus dynamique d'évaluation et de pression mutuelles par les pairs.

Le GRECO procède par cycles, appelés « cycles d'évaluation », lesquels couvrent chacun des thèmes spécifiques. Le premier cycle d'évaluation du GRECO (2000-2002) a traité la question de l'indépendance, de la spécialisation et des moyens utilisés par les organes nationaux engagés dans la prévention et la lutte contre la corruption. Le deuxième cycle d'évaluation (2003-2006) a porté sur l'identification, la saisie et la confiscation des produits du crime, la prévention et la détection de la corruption dans l'administration publique et la prévention de la pratique consistant à utiliser des personnes morales (sociétés, etc.) pour dissimuler les faits de corruption. Le troisième cycle d'évaluation (lancé en 2007) s'intéresse aux incriminations prévues par la Convention pénale sur la corruption et à la transparence du financement des partis politiques. Le quatrième cycle d'évaluation (lancé en 2012) se concentre sur la prévention de la corruption des parlementaires, juges et procureurs. Le cinquième cycle d'évaluation (lancé en 2017) vise à prévenir la corruption et promouvoir l'intégrité au sein des gouvernements centraux (hautes fonctions de l'exécutif) et des services répressifs.

Pour remplir sa mission, le GRECO suit une procédure en deux étapes comprenant une évaluation mutuelle et un programme de conformité, qui est appliquée à tous ses membres pour chaque cycle d'évaluation.

Le GRECO est le seul des quatre mécanismes mondiaux anti-corruption à pouvoir entamer des évaluations ad hoc urgentes lorsqu'une réforme institutionnelle, une initiative législative ou une modification procédurale dans un État pourraient entraîner une violation grave d'une norme anticorruption du Conseil de l'Europe. Nous avons entamé quatre procédures d'urgence à ce jour envers la Roumanie, la Pologne, la Slovénie et la Grèce. Ces procédures sont en cours.

L.R.D.G. : Comment fonctionne le processus d'évaluation et quelles actions mènent le GRECO pour inciter les pays membres à se mettre en conformité à ses recommandations ?

Les procédures d'évaluation du GRECO comprennent le recueil d'informations grâce à un ou plusieurs questionnaire(s), des visites dans le pays évalué permettant à l'équipe d'évaluation de solliciter des informations plus détaillées au cours d'entretiens de haut niveau avec les acteurs locaux les plus qualifiés, et la rédaction de Rapports d'évaluation. Ces Rapports offrent une analyse poussée de la situation dans chaque pays et sont adoptés par le GRECO lors des réunions plénières. Les conclusions de ces rapports font état de la législation et de la pratique, et de leur adéquation ou non avec les dispositions examinées. Elles peuvent mener à des recommandations, qui appellent à la prise de mesures de la part de l'État membre. Les autorités de celui-ci sont alors sommées de soumettre un rapport explicatif des mesures prises, qui sont ensuite examinées par le GRECO au cours de la procédure de conformité.

Dans le cadre de la procédure de conformité, le GRECO contrôle la mise en oeuvre de ses recommandations faites au pays dans le Rapport d'évaluation. L'estimation de la mise en oeuvre satisfaisante, partielle ou l'absence de mise en oeuvre est basée sur un rapport de situation et de documents explicatifs soumis par le pays évalué. Lorsque toutes les recommandations n'ont pas été mises en oeuvre, le GRECO examine à nouveau la situation à intervalles réguliers. Les Rapports de

conformité adoptés par le GRECO contiennent également une conclusion générale de la mise en oeuvre de toutes les recommandations, dont l'objectif est de décider s'il faut clore la procédure de conformité à l'égard de ce membre. Enfin, le Règlement du GRECO prévoit une procédure spéciale, basée sur une approche graduée, appliquée aux membres dont la réponse aux recommandations faites par le GRECO est jugée globalement insatisfaisante.

En cas de non-respect systématique de ses recommandations, le GRECO peut publier une déclaration de non-conformité d'un État membre avec les standards anti-corruption de l'Organisation, avec le rappel de l'action entreprise par le membre concerné en réponse aux recommandations formulées dans le Rapport d'évaluation mutuelle. Le GRECO a adopté une telle déclaration une seule fois, en mars 2019, envers le Bélarus. Cette déclaration a un impact réputationnel et économique non négligeable sur l'État concerné.

Les procédures d'évaluation, suivies par celles de conformité, permettent un dialogue et une pression constante sur les États pour avancer dans leur processus de réformes. La publication des rapports génère un débat public qui, lui aussi, contribue aux réformes, notamment lorsque la société civile y participe activement.

L.R.D.G. : Depuis la décision du 10 juillet 2019 du Comité des Ministres du Conseil de l'Europe, l'Union européenne est observateur auprès du GRECO ; quelle est la valeur ajoutée de cette participation ?

La participation de l'Union européenne au GRECO en tant qu'observateur est une avancée très importante. Elle permettra de continuer et renforcer la coopération entre nos deux institutions et assurer la cohérence de l'action anti-corruption sur le plan européen.

Il est important de noter que même avant cette décision, la coopération entre le GRECO et l'UE était très positive. Les évaluations du GRECO servent souvent de textes de référence au sein de l'UE dans le cadre de son activité interne (ex. les rapports « CVM », les rapports élaborés dans le cadre du semestre européen, les procédures devant la Cour de justice de l'Union européenne, les rapports du Parlement européen, les travaux de l'OLAF, etc...) et externe (ex. : dans la cadre des processus d'adhésion des Pays tiers à l'UE, les programmes de voisinage, la coopération dans le cadre du « Partenariat pour la bonne gouvernance » et des Pays des Balkans occidentaux). Le statut d'observateur de l'UE au GRECO va faire monter d'un cran cette coopération.

L'objectif à terme est la pleine adhésion de l'UE au GRECO. Lors du Conseil « Justice et affaires intérieures » de l'UE, 7-8 octobre 2019, une nette majorité de ministres était favorable à ce que l'UE devienne un membre à part entière du GRECO.

L.R.D.G. : Quels sont les nouveaux défis spécifiques que posent la lutte contre la corruption au XXIe siècle ?

Dans l'imaginaire collectif, la corruption se réduit à une somme d'argent payée à un fonctionnaire public en échange d'une faveur. En réalité, la corruption peut être beaucoup plus subtile qu'une mallette pleine d'argent. Il est important de savoir la reconnaître : elle peut prendre des formes multiples, par ex., des cadeaux, des invitations, des médailles honorifiques, des emplois, des faveurs pour un membre de la famille, de la nourriture (par ex. : du caviar), des services de toute nature, et ainsi de suite. Il suffit pour le corrupteur de découvrir le point faible du potentiel corrompu pour que « l'achat » soit fait.

Au XXIe siècle, nous avons encore beaucoup de défis. Dans certains États, non seulement nous ne voyons pas les progrès espérés, mais nous constatons des retours en arrière qui sont contraires aux standards anti-corruption. Dans d'autres, l'indépendance de la justice est mise en péril par des interférences externes. Dans d'autres États enfin, le financement et le soutien politique, notamment lorsqu'il vient de l'étranger - qu'il soit en argent ou « en nature » - reste opaque, ce qui pose un défi démocratique pour nos sociétés.

Plus fondamentalement, nous devons exiger des représentants publics l'exemplarité qu'imposent leurs fonctions. Sans cette exemplarité, et sans cette volonté politique, nous ne pourrons pas avancer avec les réformes nécessaires. Cette exemplarité doit être aussi exigée des institutions internationales.

Enfin, nous devons faire face à un véritable défi technologique. Alors que les nouvelles technologies sont une source extraordinaire pour prévenir et lutter

contre la corruption, il faudra veiller à ce que nous ne passions pas de la corruption politique à la « corruption technologique ».

Le GRECO reste prêt à relever tous ces défis.

L.R.D.G. : En matière de coopération internationale, quels sont les liens qu'entretient le GRECO avec les agences nationales anti-corruption, le réseau international des agences anti-corruption créé le 16 octobre 2018, et les autres enceintes internationales de suivi anticorruption, telles que l'OCDE, l'ONUDC, l'OEA (Organisation des États Américains) ?

Le GRECO a une coopération extrêmement étroite avec les agences nationales anti-corruption. Elles sont des partenaires à part entière du GRECO. Ce n'est donc pas un hasard si le GRECO a promu la création du Réseau de Šibenik des agences nationales anti-corruption et continue à en assurer son élargissement et son fonctionnement.

Le GRECO coopère aussi étroitement avec les autres trois mécanismes de suivi anti-corruption. Nous nous rencontrons une fois par an pour échanger des informations et des bonnes pratiques ; des contacts réguliers se déroulent au niveau des évaluations par Pays lorsque le Pays et les thématiques sont proches ; nous arrivons même à réaliser des visites sur place en commun lorsque c'est possible et utile. Les quatre mécanismes de suivi anti-corruption restent, toutefois, différents en termes de mandat, cadre juridique, composition géographique, focus thématique des cycles d'évaluation, etc.

L.R.D.G. : Quel bilan faites-vous des activités du GRECO qui a fêté ses 20 ans lors d'une conférence de haut niveau organisée sous les auspices de la Présidence française du Comité des Ministres du Conseil de l'Europe, le 17 juin 2019 ?

Avec plus de 500 rapports en presque 20 ans de travail, le GRECO a permis des changements profonds dans nos États membres (et dans nos institutions). Qu'il s'agisse de changements de législations ou de réglementations, de la création ou de la réforme d'institutions nationales, de réformes constitutionnelles, d'adoption de mesures visant à accroître la transparence du financement politique ou l'éthique dans les institutions publiques, l'impulsion du GRECO a été essentielle. Voilà quelques exemples :

– Le premier grand succès du GRECO a été de réveiller les consciences, notamment dans les Pays qui estimaient être immuns à la corruption.

– Aussi, il y a 20 ans, les « pots-de-vin » payés aux fonctionnaires publics étrangers étaient déductibles des impôts dans certains Pays. Aujourd'hui, ce n'est heureusement plus le cas...

– Il y a 20 ans, les États incriminaient les diverses infractions de corruption de manière assez diverse et lacunaire. Aujourd'hui, dans la plupart des cas, les États incriminent les infractions de corruption de manière à peu près similaire. Ceci est important, entre autres, pour faciliter la coopération internationale. Ces formes d'incrimination incluent également la corruption dans le secteur privé.

– Dans les années 1990, il était difficile d'imaginer dans de nombreux États membres qu'une personne morale puisse être responsable pénalement. Aujourd'hui, les personnes morales peuvent aussi être soumises à une responsabilité pénale.

– À la fin des années 1990, les États hésitaient encore à utiliser les techniques spéciales d'enquête pour des enquêtes en matière de corruption. Aujourd'hui, il est généralement admis qu'il serait très difficile de lutter contre la corruption sans l'utilisation de ces moyens d'enquête.

– L'immunité est de moins en moins synonyme d'impunité.

– Au fil du temps, les États ont mis en place des systèmes, plus ou moins performants, pour protéger les lanceurs d'alerte.

– Il y a des années, le financement des partis politiques et des campagnes électorales était opaque ou non existant. Aujourd'hui, la plupart de nos Pays se sont dotés d'un cadre normatif permettant plus de transparence et de contrôle sur la manière dont l'argent entre et est utilisé dans le système politique.

– Le GRECO a enfin joué un rôle clé dans le développement des standards d'intégrité des élus et des responsables publics : conflits d'intérêts, incompatibilités, cadeaux, déclaration de patrimoine, pantouflage, etc.

Le bilan du GRECO est donc certainement très positif, même s'il reste encore beaucoup de travail à faire pour libérer nos sociétés du fléau de la corruption.

L.R.D.G. : Quelles sont les perspectives d'avenir du GRECO ?

Le GRECO a seulement 20 ans. Il est relativement jeune et va donc continuer à grandir, à plusieurs niveaux.

Le GRECO va tout d'abord continuer de poursuivre sans relâche ces évaluations, s'appuyant sur son mécanisme de conformité pour faire en sorte que ses recommandations ne restent pas lettre morte. Le GRECO va ensuite continuer de poursuivre ses évaluations ad hoc : de véritables « interventions chirurgicales » pour intervenir là où le moment le demande et pour empêcher des dérives. Mais le GRECO va également évoluer dans ces fonctions de « conseil ». Il ne suffit plus de dire aux États ce qu'il faut améliorer ; il faut également leur montrer comment le faire. Le GRECO va devenir ainsi un véritable centre de référence en Europe et dans le monde en matière d'intégrité publique.

Enfin, le GRECO va continuer de maintenir sa vocation globale. Après la Kazakhstan et la Tunisie, d'autres États dans le monde pourraient s'intéresser à nos travaux et rejoindre notre Groupe. En tout cas, c'est ce que nous allons poursuivre dans le cadre de notre coopération avec les Nations Unies, le G20 et le G7.

OUVRAGES RÉCENTS

RECEL ET BLANCHIMENT

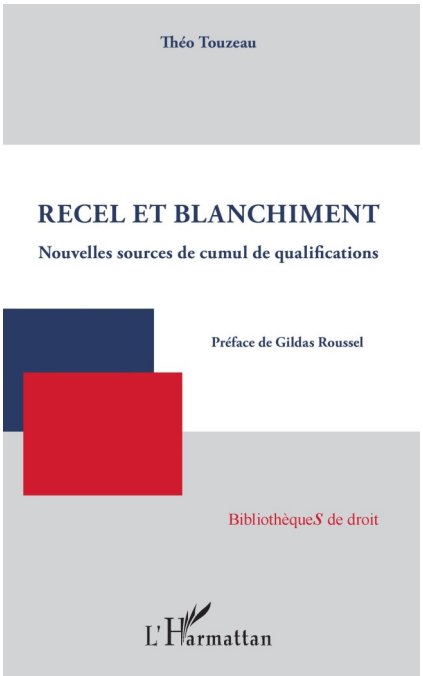
NOUVELLES SOURCES DE CUMUL DE QUALIFICATIONS

AUTEUR : THÉO TOUZEAU

ÉDITEUR : L'HARMATTAN

Résumé

À la lumière de la jurisprudence, la question de l'impossible cumul de l'infraction d'origine avec celle du recel de choses concernant un même auteur mérite de nouveau d'être posée. C'est que les juges de la Chambre criminelle, malgré leur opposition à ce cumul, ont depuis admis la condamnation d'un individu tant pour une première infraction que pour le blanchiment subséquent. Cette différence de traitement des deux infractions interroge nécessairement. Cet ouvrage, dressant le constat de la possibilité de dépasser les arguments qui fondent le rejet de « l'auto-recel », invite le lecteur à mettre de côté ses certitudes et à prendre position : rien ne semble s'opposer à l'admission du cumul de l'infraction d'origine et du recel de choses.



DARKWEB ET ENQUÊTE PÉNALE : LA DIFFICILE CONCILIATION ENTRE EFFICACITÉ, PROTECTION DES DONNÉES ET CONFORMITÉ AU RGPD

ADEL JOMNI

ENSEIGNANT-CHERCHEUR À L'UNIVERSITÉ DE MONTPELLIER

FLORIAN PERRETIN

DOCTORANT, JURISTE CHEZ HAAS AVOCATS

Dans son roman *Neuromancien*[1], William Gibson utilise pour la première fois le terme de « *Cyberespace* », et décrit un lieu de rencontre de toutes les productions numériques. L'informatique et les communications pouvant être utilisées à des fins aussi bien légitimes que malveillantes, tout système informatique peut être la source ou la cible d'abus. Le *Cyberespace* correspond à un espace qui offre des perspectives de créativité et de croissance à l'échelle de la planète mais qui génère aussi une criminalité sans frontière.

Aujourd'hui, parmi les composantes du Cyberespace, on trouve le *Darkweb* où agissent, avec une facilité déconcertante, de nombreux réseaux criminels. Il est ainsi possible de retrouver sur cette partie du Cyberespace :

- des sites sur lesquels les pirates publient des informations personnelles et confidentielles d'individus ou d' entreprises (doxing) ;

- de nombreuses « boutiques » permettant d'acheter des cigarettes de contrebande, des faux papiers (passeports, carte d'identité, carte SNCF…), de la fausse monnaie (euros, livres, dollars…), des armes… ;

- des sites de dons à des organisations terroristes ;

- de la pédopornographie ;

- des services de « Hack-as-a-Service » proposant des virus prêts à l'emploi (RAT, Trojans, DDoS) ;

- des forums de conseils en piratage et des sites d'échanges entre criminels.

Après avoir dressé un portrait réaliste de la cybercriminalité sur le *Darkweb* (I), nous verrons comment concilier l'efficacité des nouvelles techniques d'enquête avec la protection des données (II).

I. Portrait de la cybercriminalité sur le Darkweb

L'activité criminelle présente sur le *Darkweb* est devenue très professionnelle. Véritable marché guidé par la demande, le crime s'y est organisé en adaptant la qualité et la diversité de ses offres de service. De véritables plateformes de « *Crime-as-a-Service* » (CaaS) voient régulièrement le jour dans le cyberespace, offrant aux apprentis hackers les moins expérimentés la possibilité de paramétrer en quelques clics son « *ransomware* » personnalisé.

À titre d'exemple, du 19 au 23 février 2019, le site de veille informatique « zataz.com » a identifié 14 entreprises de tailles diverses qui ont vu leurs jeux de données revendus sur le Darkweb.

La cybercriminalité présente sur le *Darkweb* trouve principalement son essor du fait de la spécificité de l'infrastructure technique sur laquelle elle repose (A), mais aussi du véritable écosystème existant sur ce réseau qui joue un rôle de facilitateur dans les transactions illicites (B). Face à ce constat, il apparaît plus que nécessaire de développer de nouvelles techniques d'investigation (C) afin de doter

les forces de l'ordre d'outils d'enquête performants.

A. Spécificités de l'infrastructure technique du Darkweb

L'infrastructure technique sur laquelle repose le *Darkweb* s'appelle *Darknet*. Ce sont des « *ensembles de réseaux conçus pour assurer l'anonymat des utilisateurs par la mise en oeuvre d'une architecture décentralisée ainsi que de logiciels et d'autorisations d'accès spécifiques* »[2]. Les *Darknets* ne constituent donc pas des réseaux physiquement distincts, mais bien des protocoles de transmission qui fonctionnent au sein de réseaux déjà existants[3]. Ces protocoles ont volontairement été créés afin d'échapper à tout référencement possible par des robots d'indexation, et le plus souvent pour préserver l'anonymat des internautes.

Le fonctionnement du *Darknet* repose sur trois facteurs essentiels[4] :

- l'usage de l'infrastructure Internet ;
- l'existence de protocoles spécifiques permettant la constitution de « sous-réseaux » non indexables ;
- des architectures décentralisées de type « peer to peer » ou « *mix net* » afin de partager du contenu, le plus souvent anonymement.

Il existe une multitude de *Darknets* comme GNUnet ou *Retroshare*, I2P, ZeroNetmais le plus connu et le plus populaire d'entre eux reste le réseau *Tor*.

Le réseau *Tor* permet d'anonymiser les flux de connexions TCP/IP (ensemble des protocoles utilisés pour le transfert des données sur Internet) afin de rendre non identifiable la source d'une session de navigation Web ou de messagerie instantanée. Cependant, cette anonymisation du flux n'était pas suffisante étant donné que l'application peut potentiellement transmettre des informations annexes permettant d'identifier la personne. C'est la raison qui a poussé les équipes en charge du projet *Tor* à développer également un navigateur Web dédié à ce *Darknet* intitulé « *Tor Browser* », ainsi que d'autres applications spécialement modifiées pour préserver l'anonymat de leurs usagers[5]. Ce sont ces développements qui sont à l'origine des difficultés rencontrées lors des enquêtes menées par les forces de l'ordre sur le *Darkweb* : la quasi-intraçabilité des connexions rend le travail des enquêteurs extrêmement complexe.

Les adresses URL (« *Uniform Resource Locator* » ou adresse d'un site web) des plateformes de vente sur le *Darkweb* s'échangent soit sur des forums spécialisés difficilement identifiables soit en communication privée entre les individus. Ainsi, elles ne peuvent être cartographiées par des outils classiques. L'absence d'indexation permet aux cybercriminels d'effectuer une forme de cooptation en ne délivrant l'adresse de leurs plateformes cachées qu'aux membres initiés. Cette situation complique également le travail d'investigation.

B. Crypto-marchés, Crypo-actifs et Escrows : facilitateurs de transactions illicites et anonymes

Le relatif anonymat qui caractérise le *Darkweb* couplé à l'utilisation des *crypto-actifs*[6,7], notamment les monnaies virtuelles telles que le *Bitcoin*, facilite les transactions quasi intraçables par le biais de nombreuses places de marché sur le *Darkweb*, appelées « Marketplaces, « ou « *Crypto-marchés* [8]».

L'engouement médiatique pour les monnaies virtuelles, ou crypto-monnaies, a vu le jour à la suite de leur utilisation sulfureuse sur le Darkweb, bien avant leurs enjeux spéculatifs. L'opacité proposée par les transactions en monnaies virtuelles permet aux malfaiteurs de dissimuler assez aisément la provenance ou la destination de fonds utilisés à des fins illicites.

Les monnaies virtuelles sont utilisées comme unité de compte

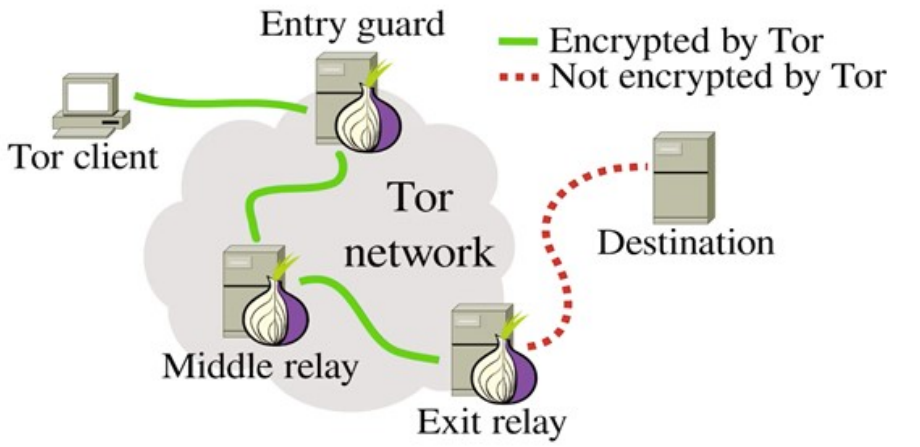


Illustration simplifiée du fonctionnement du Tor

dans un système open-source de transactions authentifiées appelées « *Blockchain* ». Elles sont créées, stockées et administrées sans tiers de confiance grâce à des moyens cryptographiques et des algorithmes complexes.

Sur le plan technique, il convient de rappeler que la *Blockchain* fonctionne comme un vaste registre public intégrant l'ensemble des transactions validées. Ce registre fait donc figure d'historique de toutes les transactions menées par tous les utilisateurs dès le début de la constitution du réseau.

Certaines plateformes offrent des services de "mixage" des crypto-monnaies. Le procédé consiste à mélanger les transactions de plusieurs utilisateurs en un seul groupe avant l'envoi des fonds. Mixer les monnaies virtuelles permet de brouiller encore les pistes sur les transactions. Il devient en théorie plus difficile de retracer la source initiale des transactions et d'analyser une *blockchain*. Cependant les mixeurs sont principalement utilisés par les cybercriminels et non par le tout public, ce qui réduit en pratique leur pouvoir opacifiant.

En ce qui concerne les crypto-marchés, ils se sont emparés du *Darkweb* et constituent un écosystème commercial souvent illégal et très rentable. Les plateformes utilisées par cet écosystème sont devenues les vecteurs naturels d'une cybercriminalité toujours plus florissante et très préjudiciable pour les organisations publiques et privées.

Sur ces crypto-marchés illicites, il est presque impossible de connaître son interlocuteur et aucun recours de l'acheteur n'est envisageable auprès du vendeur en cas de problème relatif à la transaction du fait de l'anonymat qui règne entre les parties. Afin de limiter ces risques, les acheteurs ont recours à des « tiers de confiance », appelés *escrows*. Ces derniers jouent un rôle d'intermédiaire dans la transaction. Ils proposent une mise sous séquestre de sommes d'argent qui ne seront déversées au vendeur qu'au moment de la réception de la livraison par l'acheteur. En cas de litige, ces *escrows* sont également en charge des procédures de médiation. Parfois, certains vendeurs jouissant d'une bonne réputation exigent une procédure de finalisation anticipée de la transaction appelée « *Finalize Early* », évitant ainsi les intermédiaires.

C. Émergence de nouvelles techniques d'investigation : Le *crypto-tracking*

L'explosion des fuites de données revendues sur des marchés noirs spécialisés, la variété et l'important volume de produits illicites proposés sur les crypto-marchés, l'anonymat qui caractérise les transactions en crypto-monnaies, les risques élevés de blanchiment de capitaux et de financement du terrorisme[9], imposent la recherche et le développement de nouveaux moyens d'investigation complétant les dispositifs traditionnels de recueil des preuves (aveux, empreintes, ADN, appels et messageries téléphoniques, traces sur les réseaux sociaux ou supports de stockages, etc.). Il s'agit, en effet, de combattre cette nouvelle délinquance sur son propre terrain : celui des crypto-marchés, des crypto-actifs et du Darkweb.

Parmi les nouvelles solutions étudiées, on trouve le crypto-tracking. Le but poursuivi par le crypto-tracking est de remonter jusqu'à l'adresse *Bitcoin* (par exemple), d'un service de portefeuille en ligne ou d'une plateforme d'échange de monnaies virtuelles selon un principe de « *follow the money* ». Il devient alors possible d'identifier les cyberdélinquants utilisant les monnaies virtuelles comme moyen d'échange[10].

Dans le cadre du projet de recherche iTRAC[11] (investigation par Traitement et Analyse des Crypto-monnaies) sur lequel nous travaillons, il est proposé un nouvel outil d'investigation s'appuyant sur le crypto-tracking. Ce projet vise deux objectifs :

- fournir aux autorités publiques, Gendarmerie Nationale, Douanes... un démonstrateur fondé sur un ensemble d'outils d'analyse et d'investigation de flux financiers opérés sur les monnaies virtuelles afin d'avoir une vision globale des échanges et ainsi d'améliorer la capacité de lutte contre la cybercriminalité et le blanchiment,

- utiliser ce démonstrateur pour fournir aux autorités publiques une cartographie dynamique leur permettant de connaître, d'évaluer, d'investiguer et de suivre ces usages

dans le temps et ainsi d'approfondir leur connaissance des usages des monnaies.

Le projet iTRAC s'intéresse principalement à la monnaie virtuelle Bitcoin, mais les outils d'analyse, de visualisation et d'investigations développés dans le cadre de ce projet seront réutilisables pour toute autre monnaie où les transactions sont publiques. iTRAC propose un outil dit de « *Dark Hunting* » permettant de fournir des éléments de preuve sur les transactions effectuées en Bitcoin sur le Darkweb. L'idée est de fournir aux forces de l'ordre un « *anti-Bitcoin Mixer* ». Techniquement, trois types de traitements ont été prévus par l'outil développé : le traitement d'analyse de flux financiers en *Bitcoin* issus du *Clearweb*[12], le traitement de *crawling*[13] issu du Darkweb, le traitement issu de la mise en corrélation des données issues du *Darkweb* avec les flux financiers *Bitcoin*.

II. Quelles régulations entre investigation, recevabilité de la preuve et protection des données ?

Les nouvelles preuves digitales issues du crypto-tracking se heurtent comme toutes les preuves numériques au problème de leur recevabilité. Ainsi, les services d'enquête sont amenés à justifier du respect du principe général de loyauté de la preuve, lequel revêt désormais une double facette : la loyauté de la collecte de la preuve pénale et la loyauté des traitements de données à caractère personnel mis en oeuvre. La directive « Police-Justice » n° 2016/680 du 27 avril 2016 du Parlement européen et du Conseil constitue le socle de cette nouvelle notion et vise précisément à encadrer les opérations de traitement à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales.

Comment, dans ce contexte, concilier efficacité et conformité des nouveaux outils d'enquête au regard du droit de la protection des données à caractère personnel ?

Les outils[14] permettant de tracer les transactions en monnaie virtuelle réalisées sur le *Darkweb* pourraient être un début de réponse à cette question. Il convient néanmoins de confronter ce type d'outils de « crypto tracking » aux notions de données à caractère personnel (A) et de traitement de données (B). Cette confrontation permettra d'appréhender l'impact des contraintes réglementaires sur l'utilisation de tels outils au stade de l'enquête (C).

A. Crypto-tracking et données à caractère personnel

Les technologies de crypto-tracking reposent sur l'étude approfondie des transactions en monnaies virtuelles, lesquelles sont inscrites de manière indélébile sur le registre de la *Blockchain*. Par un croisement des données via l'utilisation de puissants algorithmes, il est dès lors possible de retracer l'ensemble des flux de transactions jugées suspectes. Le but recherché par le crypto-tracking est de remonter jusqu'à l'adresse Bitcoin d'un service de portefeuille en ligne, ou d'une plateforme d'échange de monnaies virtuelles selon un principe de « *follow the money* » suite à la commission d'une infraction. Seules les transactions effectuées en Bitcoin seront étudiées ici.

De prime abord, les données présentes sur la *Blockchain* Bitcoin ne semblent pas relever de la catégorie des données à caractère personnel[15]. La *Blockchain* Bitcoin est connue du grand public pour l'« anonymat » qu'elle offre dans ses transactions, aussi il est légitime de s'interroger sur la présence ou non de données à caractère personnel.

Cependant, au travers de l'arrêt Breyer[16] en date du 19 octobre 2016, partiellement confirmé en jurisprudence interne[17], la Cour de justice de l'Union européenne (CJUE) fait une interprétation particulièrement extensive de la notion de « moyens raisonnablement susceptibles » permettant d'identifier un individu. Elle considère en l'espèce qu'une adresse IP dynamique constitue une donnée à caractère personnel dans la mesure où celle-ci peut être recoupée avec l'historique des connexions tenu par les fournisseurs d'accès à Internet. Dès lors qu'un recoupement est possible avec une table de correspondance existante chez un tiers, la qualification de donnée à caractère personnel s'applique. On parlera alors de données pseudonymisées permettant une identification indirecte de l'individu.

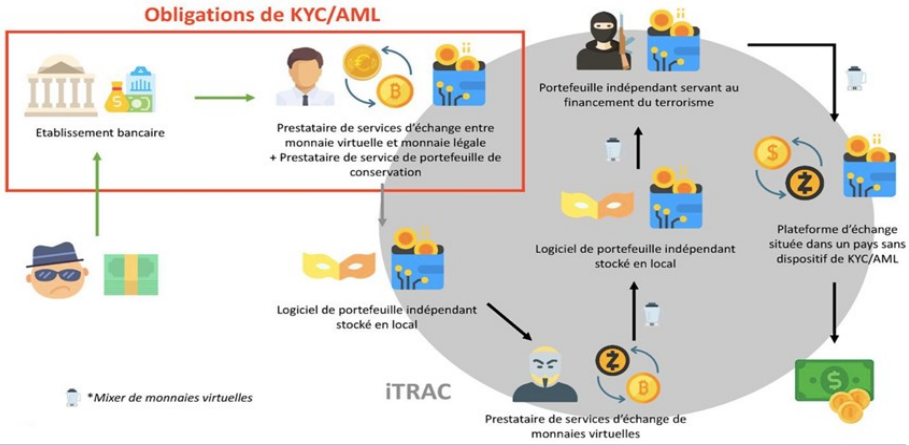
La nouvelle directive anti-blanchiment[18] n° 2018/843 du Parlement européen et du Conseil

du 30 mai 2018 vient compléter l'arsenal législatif français[19] en imposant aux prestataires de services d'échange entre monnaies virtuelles et monnaies légales (PSEMV) et aux prestataires de services de portefeuille de conservation (PSPC) l'identification de leurs clients (KYC), mais aussi des bénéficiaires effectifs de la transaction. Les éléments d'identification fournis doivent présenter un caractère probant, que les clients soient occasionnels ou non.

En somme, la cinquième directive anti-blanchiment impose la création systématique d'une table de correspondance permettant de recouper les titulaires de comptes sur ces plateformes, et donc les adresses Bitcoin associées, avec l'identité réelle de l'internaute. On peut alors conclure que les adresses Bitcoin sont des données à caractère personnel.

Notons également que le panel de métadonnées issues de la *Blockchain* permet de renforcer ce pouvoir identifiant indirect de l'adresse Bitcoin, et donc de renforcer l'identification des individus. Il est alors raisonnable d'avancer que les métadonnées « techniques » issues de la *Blockchain*, par agrégation, peuvent également être considérées comme des données à caractère personnel. Le pouvoir identifiant se dégage ici uniquement de l'agrégat de ces données, dans le prolongement du paradoxe de sorite énoncé par Eubulide de Milet.

Même si l'outil iTRAC manipule des données disposant d'un faible pouvoir identifiant, encore faut-il que des « traitements de données à caractère personnel » au sens de la réglementation soient générés.



Fonctionnement du dispositif testé dans le projet iTRAC

B. Crypto-tracking et traitements de données à caractère personnel

La présence de traitements de données à caractère personnel conditionne l'applicabilité de la directive « Police-Justice »[20]. Cependant l'appréciation de cette notion n'est pas unitaire mais varie selon l'interprétation donnée par la CNIL, à visée extensive[21], ou celle donnée par le juge pénal, à visée restrictive.

Le courant jurisprudentiel porté par la Chambre criminelle de la Cour de cassation entend, sans doute par opportunisme, limiter l'application du droit de la protection des données en matière pénale. Dans un arrêt en date du 16 mars 2004, le juge a ainsi estimé, sous couvert du principe de stricte application de la loi pénale, que « *l'utilisation d'un appareillage informatique ne suffit pas, à elle seule, à caractériser un traitement automatisé au sens de l'article 5 de la loi « informatique et libertés », et que rien ne permet de retenir que les informations collectées aient fait l'objet d'un traitement automatisé, ni même qu'elles aient été conservées au-delà de leur édition sur support papier* »[22].

Dans deux autres arrêts en date du 13 janvier 2009[23] et du 16 juin 2009[24] en matière de lutte contre les pratiques du « *peer to peer* », la Chambre criminelle a considéré que les recherches ponctuelles faites sur Internet par un agent assermenté grâce à son logiciel de pair à pair ne constituent pas un traitement, alors que la CNIL avait adopté une position radicalement opposée sur ce point[25]. Pour le professeur Anne Debet : « *cette solution ne semble respectueuse ni de la lettre, ni de l'esprit de la loi, mais elle est sans doute dictée par la nécessité pour la Cour de cassation de sauver un grand nombre de procédures pénales* »[26].

Au-delà des juridictions françaises et de l'appréciation de la notion de traitement, il est également intéressant d'évoquer, en droit de la concurrence, la décision du Tribunal de l'Union européenne du 8 septembre 2016[27] qui fonde ses motivations en partie sur des éléments de preuve obtenus de manière illégale par un employé d'une

société concurrente, via des enregistrements portant atteinte au droit au respect de la vie privée. Le juge estime que la production de telles preuves n'était pas prohibée aux motifs qu'« *il résulte de la jurisprudence de la CEDH, citée aux points 54 et 55 ci-dessus, que l'utilisation en tant que moyen de preuve d'un enregistrement illégal ne se heurte pas en soi aux principes d'équité consacrés par l'article 6, § 1, de la [Convention européenne], y compris lorsque cet élément de preuve a été obtenu en violation des exigences de l'article 8 de la [Convention européenne], lorsque, d'une part, la partie requérante en cause n'a pas été privée d'un procès équitable ni de ses droits de la défense et, d'autre part, cet élément n'a pas constitué le seul moyen de preuve retenu pour motiver la condamnation* ». Certes, cet arrêt ne concerne que la matière du droit de la concurrence, mais au vu des propos assez généraux avancés par le Tribunal de l'Union européenne, on pourrait tout à fait imaginer une extension de cette jurisprudence au profit de l'efficacité de la preuve, et donc au détriment de sa légalité.

Et pourtant, au regard des motivations du célèbre arrêt *Breyer*[28] couplé avec la directive « Police-Justice » transposée en droit français et de la récente étude de la CNIL sur la *Blockchain*[29], tout semble converger vers la réelle présence de traitements de données à caractère personnel pour un outil comme celui proposé dans le projet iTRAC.

Ce nouvel engouement, tant législatif que doctrinal et jurisprudentiel, pourrait sonner le glas des arrêts d'opportunité qui ont, un temps, écarté la protection des données à caractère personnel de la sphère pénale.

C. Crypto-tracking et enjeux de conformité

Si les outils d'enquête réalisent des traitements de données à caractère personnel au sens de la directive « Police- Justice », ils devront respecter à la lettre les dispositions spécifiques transposées aux articles 70-1 et suivants de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. En substance, le but de cette réglementation est de protéger les droits et libertés des personnes physiques et d'éviter la mise en place d'un système de contrôle « *orwellien* »[30] de la population, qui trouve déjà écho en Chine avec le « social ranking »[31].

Reprenant les principaux points visés par le RGPD, la directive encadre les collectes de données à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales[33].

Ces collectes devront ainsi reposer sur un texte spécial, respecter les principes de proportionnalité de la collecte et être mises en oeuvre dans le respect des concepts de *Privacy by Design* et *Privacy by Default* visant à garantir un niveau de protection suffisant en matière de protection de la vie privée dès la conception d'un produit et par défaut. Le responsable du traitement devra quant à lui désigner un délégué à la protection des données, tenir un registre des activités de traitement, effectuer des analyses d'impacts sur la protection des données. En somme, les services d'enquête devront satisfaire à un ersatz de « responsabilisation »[34], cher aux yeux du législateur européen, qui tend à insuffler un vent de « soft law » dans les voiles de l'Union.

Outre ces contraintes, pouvant être vécues comme de nouvelles « lourdeurs administratives »[35], la directive impose aux autorités une dégradation partielle ou totale des éléments collectés lors de l'enquête au travers de la mise en place de durées de conservation.

Ces durées seront en pratique « déterminées » en fonction de la qualité des personnes concernées qu'il faudra obligatoirement distinguer[36] et des typologies de données (données de faits, appréciations subjectives, données sensibles[37]), ou au mieux « déterminables » par des procédés d'audits lourds visant à juger la pertinence et la qualité d'une information. On imagine aisément l'incommodité de la mise en place de tels processus pour des outils d'enquête dédiés aux « cold-case »[38] ou encore des outils de veille à l'instar de l'outil développé dans le cadre du projet de recherche iTRAC.

Conclusion

En raison de la reconnaissance inévitable de traitements de données à caractère personnel dans la sphère pénale, le juge français prêtera le flanc à un argumentaire musclé de la part de la défense qui n'hésitera pas à écarter les preuves ne respectant pas le grand principe de

loyauté. Avec une réglementation aussi riche, souple et complexe, il est extrêmement délicat d'embrasser complétement la conformité imposée par le RGPD.

Face à ce constat, il faut souhaiter une évolution de la jurisprudence française, avec un certain assouplissement de l'appréciation de la loyauté de la preuve au bénéfice d'un dispositif plus pragmatique de balance des intérêts en présence afin de ne pas voir les éléments probatoires récoltés tombés les uns après les autres. Une appréciation *in concreto* de la loyauté permettra ainsi de prendre en considération le principe de réalité de l'enquête.

Notes :

1 GIBSON William, Neuromancien, Paris, J'ai Lu, 1984.

2 Avis de la Commission d'enrichissement de la langue française publié au Journal Officiel du 26 septembre 2017 - Numéro 225.

3 P. Biddle, P. England, M. Peinado, B. Willman, The Darknet and the Future of Content Protection, in Digital Rights Management, 2003.

4 S. Mansfield-Devine, Darknets, in Computeur Fraud & Security, Vol. 2009, Issue 12, Décembre 2009.

5 « The Tor Project FAQ », sur trac.torproject.org

6 Un crypto-actif est un actif virtuel stocké sur un support électronique permettant à une communauté d'utilisateurs l'acceptant en paiement de réaliser des transactions sans avoir à recourir à la monnaie légale. Banque de France, Focus n°16, 5 mars 20 https://publications.banque-france.fr/sites/default/files/medias/documents/focus-16_2018_03_05_fr.pdf

7 Les crypto-actifs s'appuyant sur la technologie Blockchain (ou chaînes de bloc) pour sécuriser et valider les transactions entre deux ou plusieurs entités sont les moteurs de ce nouveau marché.

8 Exemples de crypto-marchés : Silk Road, AlphaBay market, Cannazone market, Hansa market.

9 Voir Cons. 8, 9, 10 et 11 du projet de directive abrogeant la directive 2015/849 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, modifiant le règlement (UE) no 648/2012 du Parlement européen et du Conseil et abrogeant la directive 2005/60/CE du Parlement européen et du Conseil et la directive 2006/70/CE de la Commission http://data.consilium.europa.eu/doc/document/PE-72-2017-INIT/en/pdf

10 Bien que prometteuses, les technologies de crypto-tracking en sont encore à leur balbutiement. De plus, certaines monnaies virtuelles comme Zcash, Monero ou Dash proposent un anonymat beaucoup plus important que le Bitcoin, rendant quasi-impossible les techniques de crypto-tracking.

11 iTRAC : projet de recherche public-privé regroupant des universitaires (Paris et Montpellier) et des partenaires privés comme Thalès, Haas Avocats, etc. L'objectif est de fournir aux forces de l'ordre un « anti-Bitcoin Mixer ». Les idées et propositions figurant dans cet article sont les fruits des réflexions et recherches, dans le cadre du projet iTRAC, produites par l'équipe de l'Université de Montpellier dirigée par Adel Jomni.

12 Correspond à la partie d'Internet accessible à tous via les moteurs de recherche usuels de type Google, Yahoo, Bing, etc. Ces moteurs de recherche utilisent des logiciels d'indexation, aussi appelés « robot d'indexation ». C'est à partir de cet espace que seront effectuées les études sur le registre des transactions effectuées sur la Blockchain Bitcoin.

13 Consiste à parcourir et indexer le Web afin d'en établir la cartographie. Le programme qui réalise cette tâche de façon automatique est appelé Web crawler (ou Web spider, Webbot...).

14 Exemple de l'outil développé dans le cadre du projet « iTRAC », destiné aux forces de l'ordre et permettant de tracer les transactions en monnaie virtuelle réalisées sur le Darkweb.

15 Les données à caractère personnel sont définies dans le Règlement général sur la Protection des données (RGPD) et la directive Police-Justice selon leur pouvoir identifiant, qui peut être direct ou indirect. Pour déterminer si une personne physique est identifiable, le texte précise qu'il faut « prendre en considération l'ensemble des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne pour identifier la personne physique directement ou indirectement ».

16 CJUE 19 octobre 2016, Patrick Breyer c/ Bundesrepublik Deutschland, C-582/14.

17 La Chambre civile de la Cour de cassation a repris les motivations de l'arrêt dans un arrêt en date du 3 novembre 2016 (n° 15-22595) qui met fin à une incertitude jurisprudentielle.

18 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 (Texte présentant de l'intérêt pour l'Espace économique européen (EEE).

19 Art L 561-2 et s. du Code monétaire et financier.

20 Art. 2 de la directive « Police-Justice ».

21 Voir en ce sens le Pack de conformité « Véhicules Connectés et Données personnelles » qui assimile à des données personnelles « l'état d'usure des pièces [de véhicule] ».

22 Cass. Crim., 16 mars 2004, n°04-80048.

23 Cass. Crim., 13 janvier 2009 n°08-84088.

24 Cass. Crim., 16 juin 2009 n°08-88560

25 V. Délibération CNIL n°2006-294 du 21 décembre 2006 autorisant l'association de lutte contre la piraterie audiovisuelle de procéder à un traitement de données à caractère personnel ayant pour finalité principale la recherche des auteurs de contrefaçon audiovisuelle.

26 A. DEBET, La notion de traitement, in Informatique et Liberté, la protection des données à caractère personnel en droit français et européen, 2015.

27 Trib. UE, 8 sept. 2016, aff. T-54/14, Goldfish BV et voir Le principe de loyauté probatoire a-t-il encore un avenir dans le contentieux de la concurrence ? – Mustapha Mekki – D. 2016. 2355.

28 Prévu pour 2020, le système de notation des citoyens chinois vise à récompenser les bons comportements et punir les mauvais via notation par points. Ce système de « crédits sociaux » donne accès à plus ou moins de services selon le score attribué à chaque citoyen : transports publics, logements sociaux, offres de prêt, limitation de l'accès à Internet, accès à certains emplois de la fonction publique...

29 CJUE 9 octobre 2016, Patrick Breyer c/ Bundesrepublik Deutschland, C-582/14.

30 CNIL, Blockchain, Premier éléments d'analyse de la CNIL, septembre 2018.

31 G. ORWELL, 1984, Ed. Gallimard (1950).

32 Règlement (UE) n°2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

33 Pour une analyse complète, voir l'article de J. MARTINON « RGPD, législation nationale et directive « Police/justice » : quelles applications pour l'institution judiciaire ? »

34 Art. 5.2 du RGPD.

35 Ces contraintes sont inspirées des certifications de type « ISO » ou « AFNOR ». Notons également que le processus de conformité à la protection des données à caractère personnel est déjà particulièrement lourd pour les acteurs privés (environ 3 à 5 ans de chantier pour une parfaite conformité). Il le sera encore plus pour les acteurs publics, qui ne

disposent généralement pas des ressources nécessaires, tant budgétaires qu'humaines, pour embrasser complétement la conformité.

36 Suspects ; personnes reconnues coupables d'une infraction pénale ; victimes et autres parties, tels que les témoins ; personnes détenant des informations ou des contacts utiles ; complices de personnes soupçonnées et de criminels condamnés...

37 Données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, ou l'appartenance syndicale, et le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

38 Affaires non-classées. À titre d'exemple, on peut évoquer la mise en examen de Murielle BOLLE en 2018 dans l'affaire dite du « Petit Grégory » en partie justifiée par des recoupements d'informations permis par le logiciel d'enquête AnaCrim.

OUVRAGES RÉCENTS

LA PROTECTION DES DONNÉES PERSONNELLES

LE RGPD ET LA LOI FRANÇAISE DU 20 JUIN 2018

AUTEUR : GUILLAUME DESGENS-PASANAU

ÉDITEUR : LEXISNEXIS

Résumé

C'est une petite révolution qui se joue.

Le RGPD (règlement général européen sur la protection des données) remplace, depuis le 25 mai 2018, la célèbre loi « informatique et libertés » adoptée il y a plus de 40 ans en France.

Si les grands principes de protection des données restent globalement inchangés, les modalités de gestion de la conformité sont totalement bouleversées, et les risques en cas de non-conformité (sanctions pénales, sanctions financières de la CNIL et risque d'image) sont significativement renforcés.

Au-delà, le RGPD ambitionne d'améliorer la protection des personnes fichées, dans le contexte du développement exponentiel des technologies (de la prédominance des algorithmes en passant par les objets connectés et les nouveaux usages que tout un chacun fait de l'internet) et l'exploitation de nos données personnelles par des opérateurs établis dans le « nuage informatique », (des tigres asiatiques

en passant par les « GAFAM » américains ou les prestataires de services de l'océan indien).

Chaque professionnel se doit donc désormais d'être au clair sur la nouvelle réglementation : les obligations qui lui incombent, les droits que les personnes fichées tiennent du texte européen et les actions de mise en conformité à engager sans tarder.

La quatrième édition - enrichie et actualisée - du présent ouvrage vise à confier au lecteur les principales « clés » de décryptage du RGPD et de la nouvelle loi française du 20 juin 2018. Il s'adresse tant au professionnel désireux de vérifier son niveau de conformité qu'au citoyen soucieux de la protection de sa vie privée et de ses données personnelles.

Guillaume Desgens-Pasanau est magistrat et professeur des universités associé au Conservatoire national des arts et métiers (CNAM), où il a créé en 2012 un certificat de spécialisation pour les référents et délégués à la protection des données. Il a travaillé 8 ans à la CNIL où il a exercé les fonctions de responsable du contentieux et de chef du service des affaires juridiques. Ancien avocat, il a accompagné pendant de nombreuses années des responsables de traitement issus tant du secteur privé que du secteur public dans leurs opérations de mise en conformité à la réglementation « informatique et libertés ». Auteur de plusieurs ouvrages et MOOC de référence, il est unanimement reconnu comme l'un des meilleurs experts français du droit à la protection des données.

LA RÉGULATION DES CRYPTO-ACTIFS : UN DÉFI EN TERMES DE COMPTABILITÉ DES NORMES ET CLARTÉ DE LA LOI EN MATIÈRE DE LCB-FT

DELYA DOUGLAS

CONSULTANTE RÉGLEMENTAIRE À B-PART CONSULTING, MEMBRE DE L'OBSERVATOIRE DE LA LUTTE ANTI-BLANCHIMENT ET CONTRE LE FINANCEMENT DU TERRORISME (OLAB)

Le projet de création du crypto-actif « Libra » par Facebook prévu au premier semestre 2020 a récemment soulevé de nombreuses inquiétudes de la part du G7[1] ainsi que des États-Unis. Ces derniers sont même allés jusqu'à présenter un projet de loi spécifique visant à interdire l'émission de crypto-actifs, encore qualifiés de « crypto-monnaie » ou « monnaie virtuelle », par les entreprises technologiques[2]. Les risques politiques mais également juridiques, résultant de l'absence de réglementation stabilisée à l'échelle internationale, d'un tel projet ont été soulignés.

Dans les faits, l'augmentation significative du nombre des déclarations de soupçon liées à des opérations impliquant des crypto-actifs relevée en 2018 par Tracfin, la cellule de renseignement financier nationale, a mis en lumière le niveau élevé des risques de blanchiment de capitaux et de financement du terrorisme (BC-FT) de ces activités[3]. Ainsi, une augmentation de 54% du nombre de déclarations de soupçon, soit 528 déclarations de soupçon, a été constatée. Ce phénomène a également souligné la nécessité de mettre en place une réglementation adaptée afin de réguler les activités impliquant l'utilisation de crypto-actifs.

De plus, le développement rapide du marché des crypto-actifs pose un certain nombre de difficultés liées à l'application des obligations de lutte contre le blanchiment des capitaux et le financement du terrorisme (LCB-FT) pour les organismes financiers : anonymat fréquent des opérations, difficulté à obtenir des justificatifs quant à l'origine des fonds, caractère transnational des services liés à cette catégorie d'actifs...

Ces évolutions rapides ont donné lieu à des positionnements variés à l'échelle internationale qui se sont traduits par des normes et principes similaires applicables aux prestataires de services sur crypto-actifs (I). Parallèlement, le cadre juridique réglementant les activités liées aux crypto-actifs a été récemment instauré à l'échelle nationale (II).

I. Les normes et principes applicables aux prestataires de services sur crypto-actifs

A. La révision des recommandations du Groupe d'Action Financière (GAFI)

i. Un champ d'application large des recommandations du GAFI

À l'échelle internationale, le G20 a fait part de l'urgence de créer un cadre de régulation des activités liées aux crypto-actifs et a appelé le GAFI à étendre le champ d'application de ses recommandations. Lors de sa réunion plénière du 18 octobre 2018[4], le GAFI a ainsi procédé à la modification :

- de son glossaire, afin d'y insérer une définition des « actifs virtuels[5]» et des prestataires de services d'actifs vituels[6] ;

- de la recommandation 15 relative aux nouvelles technologies, afin de préconiser la régulation LCB-FT de ces prestataires de services et leur enregistrement ou leur agrément par les États membres du GAFI[7].

De plus, le GAFI a retenu un champ d'application large de ses recommandations :

- les activités de conversion des actifs virtuels contre des monnaies ayant cours légal ;

- la conservation ou la gestion d'actifs virtuels ou d'instruments permettant d'exercer un contrôle sur des actifs virtuels ;

- les activités de conversion d'actifs virtuels contre d'autres actifs virtuels ;

- les transferts d'actifs virtuels ;

- la participation à la fourniture et la fourniture de services financiers liés à une offre d'émission ou à une vente d'actifs virtuels.

ii. Des obligations de LCB-FT identiques à celles des autres catégories d'organismes assujettis

Les mesures de vigilance en matière de LCB-FT applicables aux prestataires de services sur actifs virtuels et aux États membres ont ensuite été précisées par le GAFI le 21 juin 2019 par une note interprétative contraignante[8]. Celle-ci soumet d'une part, les États membres aux obligations suivantes :

- réaliser une évaluation des risques de BC-FT liés à l'utilisation des actifs virtuels ;

- enregistrer ou agréer les prestataires de services sur actifs virtuels par l'autorité nationale de supervision compétente et soumettre ces derniers à une supervision efficace. À noter que la supervision par un organisme d'autorégulation est exclue ;

- mettre en place un régime de sanctions et autres mesures coercitives en cas de violation des obligations de LCB-FT à l'égard de ces prestataires.

Il est intéressant de relever que les États membres ont la possibilité d'interdire toute activité impliquant des actifs virtuels après avoir procédé à une évaluation des risques de BC-FT y étant associés ou afin de poursuivre des objectifs de politique générale. Cette possibilité reflète probablement la nécessité d'aboutir à une décision de compromis entre tous les États membres du GAFI, notamment avec la Chine, qui a affirmé vouloir interdire toute activité liée aux crypto-actifs en avril 2019[9].

D'autre part, les prestataires de services d'actifs virtuels devront mettre en oeuvre les obligations de LCB-FT suivantes[10] :

- réaliser une évaluation des risques de BC-FT associés à leurs activités ;

- mettre en oeuvre toutes les mesures de prévention de BC-FT telles que prévues par les recommandations du GAFI (obligations de vigilance, obligation de conservation des documents, obligation de déclaration de soupçon et filtrage de toutes les opérations au regard des sanctions financières) de la même manière que les autres catégories d'organismes assujettis ;

- se coordonner avec les autorités nationales compétentes à l'égard des règles de protection des données personnelles et autres règles similaires afin de s'assurer de leur compatibilité avec les exigences en matière de LCB-FT.

Il apparaît que les obligations pesant sur les prestataires de services sur crypto-actifs sont identiques en ce qui concerne les mesures de vigilance. Le GAFI a fait le choix d'un régime unifié pour toutes les entités assujetties à ces recommandations, ce qui est préférable à la mise en place d'un régime spécifique, tant le rythme des évolutions dans ce domaine est intense et difficilement prévisible.

En outre, l'identité de traitement de toutes les entités assujetties permet de créer des « règles du jeu équitable » (*level playing field*) sur le marché des crypto-actifs et ainsi éviter une fragmentation de régimes juridiques pour les entités agréées pour plusieurs types de services financiers. En effet, nombre d'acteurs tels que les établissements de paiement et les établissements de monnaie électronique, le plus souvent agréés[11] et soumis à la supervision de l'Autorité de Contrôle Prudentiel et de Résolution (ACPR), envisagent de se lancer ou se sont d'ores et déjà lancés dans les services liés aux crypto-actifs. L'application de toutes les recommandations du GAFI leur impose de réaliser une évaluation des risques de BC-FT détaillée selon leurs activités tout en leur permettant de mettre en oeuvre toutes les mesures de vigilance prévues, en les adaptant si besoin en fonction du niveau de risque de chaque activité.

iii. Une surveillance spécifique de l'application des principes applicables aux prestataires de services liés aux crypto-actifs

Le GAFI a en effet prévu de procéder à une revue de l'application de ces nouvelles obligations pour une durée de 12 mois à compter du mois de juin 2020[12]. Enfin, des « *Lignes directrices sur l'approche par les risques des crypto-actifs et les prestataires de services sur crypto-actifs* » ont été publiées par le GAFI le 21 juin 2019, reprenant ainsi les travaux du groupe de travail du GAFI dédié à ce sujet depuis septembre 2018[13].

Sans surprise, le G20 a officiellement fait part de son soutien à

la nouvelle régulation par le GAFI des activités liées à des crypto-actifs et sa volonté de s'y conformer dans une déclaration publiée lors du sommet du 29 juin 2019 qui s'est tenu à Osaka[14].

À la suite de travaux intenses découlant de l'urgence posée par les activités liées aux crypto-actifs, le GAFI est parvenu à réviser ses recommandations afin d'inclure ces nouveaux acteurs. Ainsi, ces recommandations révisées sont susceptibles d'inspirer d'autres États non membres du GAFI, tout en conservant une formulation suffisamment large des obligations prévues pour ne pas gêner l'application de la réglementation élaborée à l'échelle de l'Union européenne.

B. Un nouveau cadre européen pour les activités liées aux crypto-actifs

i. Un champ d'assujettissement plus restreint que celui du GAFI

L'article 2 de la directive 2015/849 du 20 mai 2015 dite « 4ème directive anti-blanchiment[15]» révisée par la directive n° 2018/843 du 30 mai 2018, prévoit explicitement l'assujettissement aux obligations de LCB-FT des plateformes de change de *« monnaies virtuelles »* contre des monnaies ayant cours légal ainsi que des prestataires de services de portefeuilles de conservation.

Les « *monnaies virtuelles* » sont définies à l'article 3 de la directive susmentionnée révisée comme des *« représentations numériques d'une valeur qui ne sont émises ou garanties ni par une banque centrale ni par une autorité publique [...], mais qui sont acceptées comme moyen d'échange par des personnes physiques ou morales et qui peuvent être transférées, stockées et échangées par voie électronique[16] »* ce qui devrait permettre de couvrir toutes les catégories de crypto-actifs existants et à venir. Le service d'échange d'un crypto-actif contre un autre crypto-actif a été exclu étant donné que l'absence de conversion en monnaie légale ne permet pas de procéder à la dernière étape du blanchiment de capitaux, à savoir l'intégration dans le système financier légal de fonds d'origine illicite.

Les prestataires de services de portefeuilles de conservation sont quant à eux définis comme étant des entités « *fournissant des services de conservation de clés cryptographiques privées pour le compte de ses clients à des fins de détention, de stockage et de transfert de monnaies virtuelles[17] »*. Ces prestataires devront ainsi fournir les trois services énumérés dans la définition, ces conditions étant cumulatives. Il est intéressant de remarquer qu'il existe en effet des prestataires fournissant exclusivement le service de garde de clés cryptographiques privées pour le compte des clients, qui sont ainsi exclus du champ d'application de la 4ème directive anti-blanchiment révisée. Il s'agit d'un choix logique, étant donné que ces prestataires n'ont aucun pouvoir sur les crypto-actifs des clients au nom desquels ils sont gardés.

ii. Une surveillance des acteurs assurée à travers l'obligation d'immatriculation

L'article 47 de la 4ème directive anti-blanchiment révisée prévoit que les États membres s'assurent que les prestataires de services d'échange entre monnaies virtuelles et monnaies ayant cours légal et les prestataires de services de portefeuilles de conservation soient immatriculés. Cette obligation a pour finalité de définir un cadre minimal de surveillance, sans toutefois imposer un agrément à ces entités. Cependant, la directive étant d'harmonisation minimale, les États membres demeurent libres d'adopter des mesures plus contraignantes et d'instaurer une obligation d'agrément pour tous ces acteurs dans leur droit national[18].

Cette obligation d'immatriculation implique également le respect de l'obligation de compétence et d'honorabilité des dirigeants et des bénéficiaires effectifs des prestataires de services sur crypto-actifs, plus communément appelée obligation de « *fit and proper* ». Cette exigence s'inspire fortement du régime juridique applicable aux établissements de crédits issu de la directive 2013/36 du 26 juin 2013 concernant l'accès à l'activité des établissements de crédit et la surveillance prudentielle des établissements de crédit et des entreprises d'investissement (directive CRD IV)[19], aux organismes d'assurance et organismes de retraite professionnelle issu de la directive 2009/138 du 25 novembre 2009 sur l'accès aux activités de l'assurance et de la réassurance et leur exercice (directive Solvabilité II)[20]. On ne peut que se réjouir que cette obligation issue de la réglementation post-crise économique de 2008 ait été reprise pour cette nouvelle catégorie d'organismes assujettis au vu des risques élevés de BC-FT que présentent leurs activités.

Dès la transposition de la 4ème directive anti-blanchiment révisée, ces prestataires seront assujettis aux obligations de LCB-FT dans tous les États membres de l'Union européenne. En parallèle, le cadre juridique réglementant les activités liées aux crypto-actifs a été récemment instauré à l'échelle nationale.

II. Le cadre juridique national réglementant les activités liées aux crypto-actifs

Après des débats législatifs fournis, la loi dite « PACTE » du 22 mai 2019 relative à la croissance et la transformation des entreprises[21] a créé un cadre juridique applicable aux prestataires de services sur crypto-actifs ainsi qu'à leurs activités.

A. Les régimes d'autorisation et d'agrément des prestations des services sur crypto-actifs

La superposition des régimes d'autorisation et d'agrément est complexe à appréhender et non-conforme aux recommandations du GAFI.

Les crypto-actifs sont qualifiés « *d'actifs numériques* » par la loi PACTE à la différence de la formulation adoptée par le GAFI et de celle de la 4ème directive anti-blanchiment révisée, ce qui peut d'ores et déjà créer une difficulté de compréhension pour ces nouveaux acteurs.

Selon les services fournis, le régime applicable aux prestataires de services sur crypto-actifs est différent. Ainsi, l'article L.54-10-3 du Code monétaire et financier (CMF) prévoit que pour l'exercice de services de conservation pour le compte de tiers de crypto-actifs ou d'accès à des actifs numériques, et du service de conversion de crypto-actifs en monnaie ayant cours légal, les prestataires devront être enregistrés par l'Autorité des Marchés Financiers (AMF). L'enregistrement implique de contrôler l'honorabilité et la compétence des dirigeants et bénéficiaires effectifs du prestataire[22], conformément aux dispositions de la 4ème directive anti-blanchiment révisée. L'AMF doit également contrôler qu'un dispositif de contrôle interne propre à assurer le respect de ses obligations de LCB-FT a été mis en place par le prestataire.

Ce même article prévoit en outre que l'ACPR doit rendre un avis conforme dans le cadre de cette procédure, ce qui ajoute un niveau de contrôle supplémentaire et risque d'allonger les délais d'enregistrement des prestataires de services de conservation et de conversion de crypto-actifs[23]. De potentielles divergences d'interprétation pourraient également survenir. Toutefois, le silence gardé par l'AMF pendant 6 mois vaut acceptation de la demande d'enregistrement (article. R. 54-10-4 du CMF).

Pour tous les services mentionnés dans la liste dressée à l'article L.54-10-2 du CMF, à la condition qu'ils soient fournis « *à titre de profession habituelle* », un régime d'agrément optionnel par l'AMF s'applique. L'agrément requiert de respecter plusieurs critères tels que la mise en place d'un dispositif de sécurité et de contrôle interne adéquat, la mise en place d'un système de gestion des conflits d'intérêts... La liste des prestataires agréés est publiée par l'AMF en précisant les services pour lesquels ceux-ci ont été agréés[24].

Par conséquent, les prestataires fournissant des services autres que la conservation et la conversion de crypto-actifs (par exemple, l'exploitation d'une plateforme de négociation de crypto-actifs) pourront exercer leurs activités sans être agréés ni même enregistrés auprès de l'AMF. Ce cadre juridique ne peut être considéré comme étant conforme à la recommandation 15 du GAFI relative aux nouvelles technologies.

B. L'assujettissement aux obligations de LCB-FT et la supervision non-exhaustifs des prestataires de services sur crypto-actifs

D'une part, la supervision des prestataires des services de conservation et de conversion de crypto-actifs est assurée par l'ACPR en matière de LCB-FT[25], alors que leur enregistrement relève de la compétence de l'AMF. Pour rappel, l'agrément des prestataires souhaitant fournir des services autres que les deux services susmentionnés est réalisé par l'AMF.

D'autre part, la supervision des émetteurs de jetons, représentant un ou plusieurs droits sur un crypto-actifs[26], dans le cadre d'une offre publique (Initial Coin Offering dit ICO) relève de la compétence de l'AMF[27]. Une nouvelle fois, on ne peut que souligner la complexité du cadre juridique applicable aux activités liées à des crypto-actifs.

En outre, la supervision des prestataires de services sur crypto-actifs pour les obligations autres que la LCB-FT (obligations professionnelles, protection du consommateur...) est assurée par l'AMF en vertu de l'article L.621-9 du CMF, à la condition qu'ils soient agréés.

Seuls les prestataires de services sur crypto-actifs enregistrés ou agréés sont assujettis aux obligations de LCB-FT, ce qui n'est une nouvelle fois pas conforme à la recommandation 15 du GAFI relative aux nouvelles technologies. L'assujettissement partiel à ces obligations est par ailleurs regrettable au vu des risques élevés de BC-FT posées par ces activités. En effet, l'article L.561-2 du CMF dans sa nouvelle rédaction vise les prestataires fournissant les

services de conservation et de conversion de crypto-actifs et les prestataires agréés respectivement au 7° bis et 7° quater. Les émetteurs de jetons ayant obtenu le visa de l'AMF dans le cadre d'une offre publique sont également assujettis à ces obligations[28]. Néanmoins, le visa de l'AMF demeure optionnel[29].

Il en résulte de multiples divisions de compétences entre l'ACPR et l'AMF, tant au lancement des activités liées aux crypto-actifs qu'au cours de leur exercice, ce qui risque d'être source de confusion pour les prestataires de services sur crypto-actifs.

Ainsi, le cadre juridique créé par la loi PACTE se révèle à la fois incomplet, en ce que toutes les activités liées aux crypto-actifs ne sont pas soumises à un agrément ou un enregistrement par une autorité de supervision, et à la fois complexe, du fait du fractionnement marqué des compétences entre l'ACPR et l'AMF. L'épreuve de l'application pratique de ces nouvelles normes s'annonce décisive.

Notes :

1. Article de presse « Défiance et détermination au G7 Finances face au projet Libra », 18/07/2019, Les Echos.
2. Article de presse « Un projet de loi US vise à empêcher le lancement de Libra, la cryptomonnaie de Facebook », 15/07/2019, LSA-Commerce connecté.
3. Rapport annuel d'activité Tracfin 2018.
4. Outcomes FATF Plenary, 17-19 October 2018.
5. Un actif virtuel est la représentation numérique d'une valeur qui peut être échangée de manière digitale, ou transférée, et qui peut être utilisée à des fins de paiement ou d'investissement. Les actifs virtuels n'incluent pas les représentations numériques des monnaies fiduciaires, titres et autres actifs financiers qui font déjà l'objet d'autres dispositions des Recommandations du GAFI. https://www.fatf-gafi.org › fatf › documents › recommendations › pdfs
6. Le terme prestataire de services lié à des actifs virtuels désigne toute personne personne physique ou morale qui ne fait pas l'objet d'autres dispositions des Recommandations du GAFI, et qui exerce à titre commercial une ou plusieurs des activités ou opérations suivantes au nom d'un client ou pour son compte :
   i. échange entre actifs virtuels et monnaie fiduciaire;
   ii. échange entre une ou plusieurs formes d'actifs virtuels ;
   iii. transfert d'actifs virtuels;
   iv. conservation et/ou administration d'actifs virtuels ou d'instruments permettant le contrôle d'actifs virtuels ; et
   v. participation à et prestation de services financiers liés à l'offre d'un émetteur et/ou à la vente d'actifs virtuels.

   https://www.fatf-gafi.org › fatf › documents › recommendations › pdfs
7. quater https://www.fatf-gafi.org › fatf › documents › recommendations › pdfs
8. Public Statement on Virtual Assets and Related Providers, 21/06/2019.
9. À ce sujet, voir l'article de presse « Cryptomonnaies : quand la Chine mine le marché », 09/04/2019, Boursier.com.
10. Public Statement on Virtual Assets and Related Providers, 21/06/2019.
11. Les articles L.522-6 et L.526-7 du CMF prévoient respectivement que les établissements de paiement et les établissements de monnaie électronique doivent obtenir un agrément délivré par l'ACPR. Néanmoins, des exemptions d'agrément pour ces entités sont possibles si ces entités satisfont aux critères prévus aux articles L. 521-3, L. 525-5 et L. 525-6 du CMF.
12. Public Statement on Virtual Assets and Related Providers, 21/06/2019.
13. Pour plus de précisions, voir les Lignes directrices sur l'approche par les risques des crypto-actifs et les prestataires de services sur crypto-actifs.
14. Pour plus d'informations, voir la Déclaration des Leaders du G20 du sommet d'Osaka.
15. Directive n° 2015/849 du 20 mai 2015 révisée par la directive n° 2018/843 du 30 mai 2018.
16. Ibidem.
17. Ibidem.
18. Cf. article 5 de la directive 2015/849 du 20 mai 2015 révisée.
19. Directive 2013/36/UE du Parlement européen et du Conseil du 26 juin 2013 concernant l'accès à l'activité des établissements de crédit et la surveillance prudentielle des établissements de crédit et des entreprises d'investissement, modifiant la directive 2002/87/CE et abrogeant les directives 2006/48/CE et 2006/49/CE.
20. Directive 2009/138/CE du Parlement européen et du Conseil du 25 novembre 2009 sur l'accès aux activités de l'assurance et de la réassurance et leur exercice.
21. Loi n° 2019-486 du 22 mai 2019 relative à la croissance et la transformation des entreprises.
22. L'article L.500-1 du Code monétaire et financier a été modifié afin d'inclure les prestataires de services sur crypto-actifs.
23. À noter que la procédure de radiation, également prévue à l'article L.54-10-3 du Code monétaire et financier, est identique conformément au parallélisme des formes.
24. Cf. article L.54-10-5 VI du Code monétaire et financier.
25. Cf. article L.561-36-1 du Code monétaire et financier.
26. Les jetons sont définis à l'article L.552-2 du Code monétaire et financier comme « tout bien incorporel représentant, sous forme numérique, un ou plusieurs droits pouvant être émis, inscrits, conservés ou transférés au moyen d'un dispositif d'enregistrement électronique partagé permettant d'identifier, directement ou indirectement, le propriétaire dudit bien. »
27. Cf. article L.561-36 2° du Code monétaire et financier dans sa nouvelle rédaction.
28. La possibilité d'obtention d'un visa de l'AMF dans le cadre d'une offre publique d'émission de jetons (ICO) est prévue à l'article L.552-4 du Code monétaire et financier.
29. Il faut préciser que les émetteurs qui n'auront pas reçu le visa de l'AMF ne pourront pas démarcher le grand public.

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

FOCUS SUR LES CAS DE DÉNONCIATION OBLIGATOIRE AU PARQUET DE FAITS DE FRAUDE FISCALE

DOROTHÉE GOETZ

DOCTEUR EN SCIENCES CRIMINELLES, ASSISTANTE SPÉCIALISÉE

AU PARQUET DU TRIBUNAL DE GRANDE INSTANCE DE STRASBOURG

La loi relative à la lutte contre la fraude du 23 octobre 2018, qui a réécrit l'article L.228 du Livre des procédures fiscales (LPF), a modifié la mise en oeuvre des poursuites pénales en cas de fraude fiscale en procédant à une levée au moins partielle du « verrou de Bercy[1] ». Depuis ce texte, si l'impossibilité, pour la justice, d'engager des poursuites pénales pour fraude fiscale sans plainte du ministère de l'économie et des finances[2], n'a pas totalement disparu, le « verrou de Bercy » a été nettement desserré[3]. En effet, si l'administration conserve une part d'initiative des poursuites sur avis conforme de la Commission des infractions fiscales (CIF), elle est, dans certains cas, tenue de dénoncer au procureur de la République les faits de fraude fiscale considérés comme étant les plus graves.

Le 2 juillet 2019, le Conseil constitutionnel a été saisi par le Conseil d'État d'une question prioritaire de constitutionnalité (QPC) posée par l'Association française des entreprises privées, remettant en cause la conformité à la Constitution des cas de dénonciation obligatoire au parquet visés par l'article L.228 du LPF dans sa rédaction résultant de la loi du 23 octobre 2018. Dans sa décision n° 2019-804 QPC du 27 septembre 2019, le Conseil constitutionnel a déclaré conformes à la Constitution le premier alinéa et les 1° à 3° du paragraphe I de l'article L.228 du LPF.

I. L'assouplissement progressif du verrou de Bercy

En application de l'article 1 du Code de procédure pénale (CPP), la mise en mouvement de l'action publique relève en principe de l'initiative du ministère public. Dans certains cas, elle peut toutefois être confiée à des administrations pour la poursuite des infractions qui lèsent les intérêts dont elles ont la charge.

Jusqu'à la loi du 23 octobre 2018, l'article L.228 du LPF, tel qu'interprété par la jurisprudence constante de la Cour de cassation, attribuait à l'administration fiscale un pouvoir discrétionnaire concernant l'initiative des poursuites pour fraude fiscale qui, sans aller jusqu'à lui réserver la décision de mise en mouvement de l'action publique, subordonnait celle-ci au dépôt d'une plainte de sa part. Depuis 1977, le pouvoir d'initiative ainsi accordé à l'administration fiscale était conditionné à l'avis conforme de la CIF. Cette double exigence préalable à l'engagement des poursuites était communément appelée le « verrou de Bercy ».

Ce mécanisme puise ses racines dans le privilège reconnu dès la Révolution à la Régie des contributions indirectes concernant l'engagement des poursuites pénales pour les infractions à la législation spécifique à ces impositions. Cette prérogative, interprétée par la Cour de cassation comme excluant toute mise en mouvement de l'action publique par le parquet, fut ensuite étendue par le législateur, mais sous une forme infléchie, pour la répression du délit général de fraude fiscale. La loi du 25 juin 1920 portant création de nouvelles ressources fiscales accorda en effet à l'administration fiscale la faculté de demander l'engagement des poursuites,

mais non celle de les exercer. En présence de faits de cette nature, l'article 112 de cette loi prévoyait uniquement que « les poursuites seront engagées à la requête de l'administration compétente et portées devant le tribunal correctionnel dans le ressort duquel l'impôt aurait dû être acquitté ».

Le ministère public, auquel il revient normalement d'être informé par toutes les autorités administratives de la commission d'infractions et d'apprécier s'il est opportun d'en poursuivre les auteurs (articles 40 et 40-1 du CPP) ne pouvait donc engager des poursuites pour fraude fiscale sans l'initiative préalable de l'administration, formalisée par un dépôt de plainte. Cette prérogative restrictive du libre exercice des poursuites par le parquet était justifiée par la volonté du législateur d'assurer une plus grande efficacité répressive dans la lutte contre la fraude fiscale, partant de l'idée que les services fiscaux sont les plus à même de détecter ce type de comportements et de distinguer ceux à l'égard desquels l'application de sanctions administratives, dont le prononcé relève de leur compétence exclusive, doit se doubler d'une répression pénale.

En dépit de la limitation apportée au pouvoir discrétionnaire de l'administration par l'entremise de la CIF, le « verrou de Bercy » a souvent fait l'objet de critiques récurrentes lui reprochant de compromettre l'efficacité de la répression en laissant toujours au ministre du Budget la faculté d'empêcher l'engagement d'une procédure pénale.

Après plusieurs tentatives parlementaires de suppression du « verrou de Bercy », à l'occasion notamment des travaux préparatoires à la loi du 6 décembre 2013 relative à la lutte contre la fraude fiscale et la grande délinquance économique et financière, il est revenu à la loi du 23 octobre 2018 de réformer le dispositif prévu à l'article L. 228 du LPF en imposant à l'administration de dénoncer au ministère public les faits de fraude fiscale les plus graves.

L'article 36 de cette loi a ainsi apporté plusieurs modifications au dispositif spécifique prévu à l'article L.228 du LPF, dont la plus importante – qui fait seule l'objet de la QPC précitée – tient à la mise en place d'un mécanisme de dénonciation obligatoire au parquet, sans avis préalable de la CIF, des faits les plus graves de fraude fiscale. Ce faisant, l'intervention du législateur a été animée par la volonté de renforcer la réponse pénale à l'égard des cas les plus graves de fraude fiscale en substituant au pouvoir discrétionnaire de l'administration des critères transparents qui entraînent obligatoirement un dépôt de plainte pour fraude fiscale par l'administration.

Le paragraphe I de l'article L.228 du LPF[4] est le plus innovant en ce qu'il impose à l'administration de dénoncer au procureur de la République les faits ayant conduit à l'application d'importantes pénalités fiscales sur des droits rappelés supérieurs à un seuil fixé par le législateur, à l'issue des procédures de contrôle que l'administration exerce en vertu de l'article L.10 du LPF. Le paragraphe II de l'article L.228 du LPF[5] maintient le « verrou de Bercy », c'est-à-dire la faculté pour l'administration de déposer plainte, sur avis conforme de la CIF, pour les faits qui ne répondent pas aux critères de transmission obligatoire au ministère public. Il en va notamment ainsi : des dossiers dans lesquels le montant des droits éludés est inférieur à 100 000 euros, quand bien même ils auraient donné lieu à l'application des majorations prévues aux 1° à 3° du paragraphe I de l'article L. 228 ; des dossiers portant sur des droits fraudés pour un montant supérieur à 100 000 euros ayant justifié l'application de majorations de 40 %, sans que la condition de réitération ne soit remplie. Dans ces hypothèses, l'administration recouvre donc son pouvoir d'appréciation de l'opportunité de déposer plainte ou non en sus des pénalités appliquées au contribuable.

II. L'apport de la question prioritaire de constitutionnalité du 2 juillet 2019

En l'espèce, le requérant reproche au législateur de méconnaître, dans ce texte qui instaurerait des différences de traitement inconstitutionnelles, les principes de personnalité des peines et d'égalité devant la loi.

Précisément, il dégage plusieurs distinctions visées par le texte qui, à ses yeux, sont injustifiées. Il mentionne à ce titre la distinction prévue par le législateur entre les contribuables pour lesquels l'administration est tenue de dénoncer au procureur de la République des faits susceptibles de caractériser le délit de fraude fiscale et les autres contribuables. Le caractère injustifié de cette distinction résulte également, selon lui, du silence gardé par le législateur sur la nécessité d'un avis conforme de la CIF. Ce faisant, c'est l'administration elle-même qui, selon les circonstances et de manière discrétionnaire, apprécierait d'instituer, ou non, une obliga-

tion de dénonciation des faits au parquet. Dans le même sens, il souligne qu'en retenant également, comme critère de dénonciation obligatoire le montant des droits éludés, le texte établit une différence de traitement injustifiée entre les sociétés bénéficiaires et déficitaires.

Avant de déclarer ce texte conforme à la Constitution, les Sages rappellent la distinction essentielle entre les faits visés à l'article L.228 du LFP, pour lesquels l'administration est dans l'obligation de procéder à des dénonciations au parquet et les autres faits, pour lesquels l'administration ne peut déposer plainte que sur avis conforme de la CFI. Si cette distinction a été établie par le législateur c'est, selon le Conseil constitutionnel, dans le but de soumettre systématiquement au procureur de la République, aux fins de poursuites pénales, les faits de fraude fiscale les plus graves dont a connaissance l'administration. Pour cette raison, pour délimiter les faits concernés par cette obligation de dénonciation au parquet, le législateur a nécessairement dû ériger des critères de choix. Pour les Sages, les critères retenus par le texte sont « objectifs et rationnels, en lien avec le but poursuivi ». En conséquence, les critères de dénonciation obligatoire visés par le texte ne génèrent pas de discrimination injustifiée entre les contribuables. En outre, les Sages fournissent une explication logique à l'absence d'avis conforme de la CIF en cas d'obligation de dénonciation. En effet, dès lors que les dispositions contestées instituent un mécanisme de dénonciation de plein droit au procureur de la République, l'absence d'avis conforme de la CIF, qui a pour objet de filtrer parmi les dossiers transmis par l'administration ceux justifiant effectivement des poursuites pénales, ne prive les contribuables d'aucune garantie.

En conséquence, les dispositions contestées sont déclarées conformes à la Constitution. Cette décision de conformité rappelle que la nécessité de lutter contre les grandes fraudes doit être une priorité. Précisément, parce qu'il doit s'agir d'un objectif prioritaire du législateur, le Conseil constitutionnel approuve la nécessité de mettre en oeuvre des moyens efficaces dans le traitement procédural de cette délinquance. La dénonciation obligatoire au parquet des faits de fraude fiscale prévue par l'article L.228 du LPF en fait incontestablement partie.

Ce choix était prévisible. En effet, cette question prioritaire de constitutionnalité entretient un lien de filiation évident avec la décision n° 2016-555 QPC du 22 juillet 2016 par laquelle le Conseil constitutionnel avait été amené à valider le principe même du monopole de dépôt de plainte de l'administration pour la poursuite du délit de fraude fiscale, emblématique du « verrou de Bercy[6] ».

Notes :

1 E. Verges, Loi n° 2018-898 du 23 octobre 2018, l'outil procédural au service de l'efficacité, RSC 2019. 155 ; E. Diard et E. Cariou, Rapport d'information du 23 mai 2018, de la mission d'information commune, sur les procédures de poursuite des infractions fiscales ; C. Cutajar, Partiellement déverrouillé, le verrou de Bercy résiste !, D. 2018. 2029.

2 A.-L. Cassard-Valembois, AJDA 2016. 1925.

3 M.-C. de Montecler, AJDA 2018. 1940.

4 Article L.228 du LPF : « I. – Sans préjudice des plaintes dont elle prend l'initiative, l'administration est tenue de dénoncer au procureur de la République les faits qu'elle a examinés dans le cadre de son pouvoir de contrôle prévu à l'article L. 10 qui ont conduit à l'application, sur des droits dont le montant est supérieur à 100 000 € :

1° Soit de la majoration de 100 % prévue à l'article 1732 du Code général des impôts ;

2° Soit de la majoration de 80 % prévue au c du 1 de l'article 1728, aux b ou c de l'article 1729, au I de l'article 1729-0 A ou au dernier alinéa de l'article 1758 du même code ;

3° Soit de la majoration de 40 % prévue au b du 1 de l'article 1728 ou aux a ou b de l'article 1729 dudit code, lorsqu'au cours des six années civiles précédant son application le contribuable a déjà fait l'objet lors d'un précédent contrôle de l'application des majorations mentionnées aux 1° et 2° du présent I et au présent 3° ou d'une plainte de l'administration.

L'administration est également tenue de dénoncer les faits au procureur de la République lorsque des majorations de 40 %, 80 % ou 100 % ont été appliquées à un contribuable soumis aux obligations prévues à l'article LO 135-1 du code électoral et aux articles 4 et 11 de la loi n° 2013-907 du 11 octobre 2013 relative à la transparence de la vie publique, sur des droits dont le montant est supérieur à la moitié du montant prévu au premier alinéa du présent I.

L'application des majorations s'apprécie au stade de la mise en recouvrement. Toutefois, lorsqu'une transaction est conclue avant la mise en recouvrement, l'application des majorations s'apprécie au stade des dernières conséquences financières portées à la connaissance du contribuable dans le cadre des procédures prévues aux articles L. 57 et L. 76 du présent livre.

Lorsque l'administration dénonce des faits en application du présent I, l'action publique pour l'application des sanctions pénales est exercée sans plainte préalable de l'administration.

Les dispositions du présent I ne sont pas applicables aux contribuables ayant déposé spontanément une déclaration rectificative. »

5 Article L.228 du LPF : « II. – Sous peine d'irrecevabilité, les plaintes portant sur des faits autres que ceux mentionnés aux premier à cinquième alinéas du I et tendant à l'application de sanctions pénales en matière d'impôts directs, de taxe sur la valeur ajoutée et autres taxes sur le chiffre d'affaires, de droits d'enregistrement, de taxe de publicité foncière et de droits de timbre sont déposées par l'administration à son initiative, sur avis conforme de la commission des infractions fiscales. La commission examine les affaires qui lui sont soumises par le ministre chargé du budget. Le contribuable est avisé de la saisine de la commission qui l'invite à lui communiquer, dans un délai de trente jours, les informations qu'il jugerait nécessaires. Le ministre est lié par les avis de la commission ».

6 Crim. 19 mai 2016, n° 16-81.857, Dalloz actualité, 9 juin 2016, obs. D. Goetz , Cons. const. 22 juill. 2016, n° 2016-555 QPC, note R. Salomon ; AJDA 2016. 1925 ; D. 2016. 1569 ; ibid. 2017. 1328, obs. N. Jacquinot et R. Vaillant ; Constitutions 2016. 532, chron. ; ibid. 651, chron. L. Alice Bouvier ; RSC 2016. 529, obs. S. Detraz.

DU CÔTÉ DES PRATICIENS

LES NOUVEAUX ENJEUX DE LA LUTTE CONTRE LA CRIMINALITÉ FINANCIÈRE AU SEIN DE LA DIRECTION CENTRALE DE LA POLICE JUDICIAIRE

THOMAS DE RICOLFIS

CONTRÔLEUR GÉNÉRAL À LA DIRECTION CENTRALE DE LA POLICE JUDICIAIRE (DCPJ),
SOUS-DIRECTEUR EN CHARGE DE LA SOUS-DIRECTION DE LA LUTTE
CONTRE LA CRIMINALITÉ FINANCIÈRE (SDLCF)

La Direction Centrale de la Police Judiciaire (DCPJ), direction hautement spécialisée du ministère de l'Intérieur, a pour coeur de mission la lutte contre le terrorisme, la criminalité organisée, la délinquance financière et la cybercriminalité.

Forte de près de 6.000 personnels, elle mène une stratégie proactive pour anticiper les évolutions des groupes et phénomènes criminels et adapter sa posture.

Elle dispose à la fois de services centraux, des sous-directions spécialisées composées pour la plupart d'offices centraux et d'un ancrage territorial composé de 58 implantations.

Jusqu'au 1er juillet 2019, une seule entité centrale coiffait le crime organisé et la délinquance financière, la sous-direction de la lutte contre la criminalité organisée et la délinquance financière (SDLCODF).

À cette date, la SDLCODF a été partagée en deux, une sous-direction de la lutte contre la criminalité organisée (SDLCO) et une sous-direction de la lutte contre la criminalité financière (SDLCF). Les synergies déjà existantes entre offices centraux seront maintenues et renforcées, le but n'étant pas d'avoir des silos de compétences étanches.

Cette réforme trouve ses origines dans l'impact grandissant de la criminalité financière sur la société (I) nécessitant une réponse stratégique plus cohérente (II).

I. L'impact grandissant de la criminalité financière

Chaque époque a connu ses affaires marquantes, le scandale des décorations en 1887, le canal de Panama en 1892, Stavinsky en 1934, la spéculation sur le sucre en 1974. À compter des années quatre-vingt, la justice a commencé à prendre possession du terrain financier, s'émancipant à travers à l'action de juges d'instruction précurseurs.

Le sommet de l'Arche en 1989[1] a érigé la lutte contre le blanchiment comme une priorité.

Peu à peu, des textes législatifs sont venus corriger les errements de certaines pratiques comme la loi Sapin I du 29 janvier 1993 relative à la prévention de la corruption et à la transparence de la vie économique et des procédures publiques.

Mais, il a fallu attendre le choc de la crise financière de 2008 pour qu'un mouvement plus durable s'enclenche.

A. La crise financière de 2008

Le facteur déclenchant de ce mouvement est la crise financière mondiale de 2008 symbolisée par des affaires retentissantes comme MADOFF, la faillite de LEHMANN BROTHERS aux États-Unis ou KERVIEL en France. Cette même année, un ancien cadre de la banque HSBC à Genève, Hervé FALCIANI, transmettait à l'administration fiscale française une liste d'évadés fiscaux.

Cette crise a non seulement fait apparaître la faiblesse du système économique mais aussi dévoilé au grand jour l'existence de circuits d'évasion des

capitaux particulièrement performants. Ce qui était jusqu'alors « toléré » ne le devenait plus.

Dès décembre 2008, une mission d'information de la Commission des finances, de l'économie générale et du contrôle budgétaire de l'Assemblée nationale s'est attaquée au sujet des paradis fiscaux. Dans son rapport d'information, rendu public en septembre 2009, la mission a préconisé un service fiscal d'enquêtes composé d'agents disposant de la qualité d'officier de police judiciaire sous l'autorité du parquet.

La loi n°2009-1674 du 30 décembre 2009 de finances rectificative pour 2009 a concrétisé cette proposition en créant la procédure de présomption de fraude fiscale (article L.228 du Livre des procédures fiscales) et les officiers fiscaux judiciaires (article 28-2 du Code de procédure pénale). Le décret n° 2010-1318 du 4 novembre 2010 a donné naissance à la Brigade nationale de répression de la délinquance fiscale (BNRDF), surnommée police fiscale, au sein de la DCPJ et qui a été le premier service de police judiciaire exclusivement dédié aux fraudes fiscales les plus complexes. Sa force est d'être composée d'officiers de police judiciaire (OPJ) et d'officiers fiscaux judiciaires (OFJ).

La loi n° 2010-7768 du 9 juillet 2010 visant à faciliter la saisie et la confiscation en matière pénale a renforcé fortement les mécanismes déjà existants et donnait naissance à l'Agence de gestion et de recouvrement des avoirs criminels saisis et confisqués (AGRASC).

B. Le tournant de 2013

L'année 2013 constitue le tournant décisif, tournant consécutif à ce qui est communément appelé l'affaire CAHUZAC, alors ministre du Budget, en charge de la lutte contre l'évasion fiscale. Le retentissement est tel qu'il aboutit à l'automne de la même année à l'adoption de textes législatifs fondateurs et à la mise en place de trois institutions complémentaires :

- Les lois organique n° 2013-906 et ordinaire n° 2013-907 du 11 octobre 2013 relatives à la transparence de la publique créant la Haute Autorité pour la transparence de la vie publique en remplacement de la Commission pour la transparence financière de la vie politique ;

- La loi ordinaire n° 2013-1117 du 6 décembre 2013 relative à la lutte contre la fraude fiscale et la grande délinquance économique et financière ;

- La loi organique n° 2013-1115 du 6 décembre 2013 relative au procureur de la République financier, créant le parquet national financier (PNF), en activité à compter du 1er février 2014 ;

- Décret n° 2013-960 du 25 octobre 2013 portant création de l'Office central de lutte contre la corruption et les infractions financières et fiscales (OCLCIFF) qui se substitue à la Division nationale des investigations financières et fiscale ;

Suite à des procédures judiciaires visant des assistants parlementaires tant nationaux qu'européens, sont promulguées les lois organique n° 2017-1338 et ordinaire n° 2017-1539 pour la confiance dans la vie politique, le 15 septembre 2017.

C. L'internationalisation

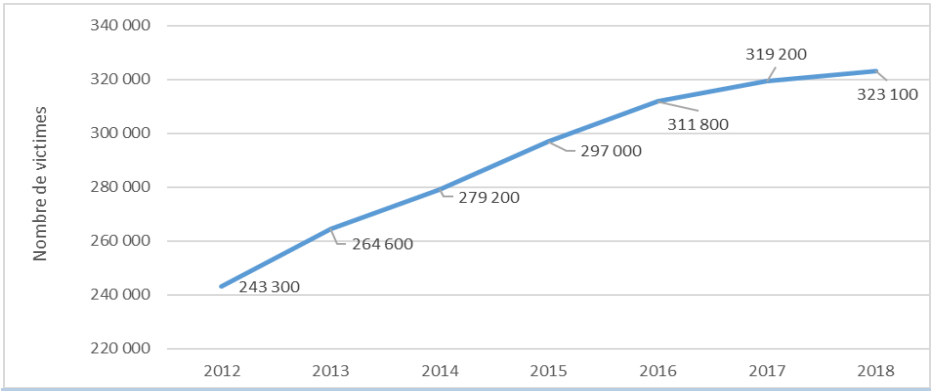
Au plan international, à compter de 2008 aussi, émergent deux phénomènes.

D'une part, la montée en puissance de l'extraterritorialité américaine qui se concrétise par de lourdes sanctions financières dans le cadre du mécanisme du « deffered prosecution agreement » (DPA), instrument de justice négocié, à l'encontre, notamment, de sociétés françaises. En réaction, la loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, dite loi Sapin II, mettait en place un dispositif innovant avec l'Agence française anticorruption (AFA), un corpus de conformité, la mise à niveau de dispositions du Code pénal et du Code de procédure pénale complété par un dispositif de justice transactionnel, la convention judiciaire d'intérêt public (CJIP)[2], inspiré du DPA.

D'autre part, la succession des « leaks » et « papers » sur les circuits internationaux de fraude fiscale et de blanchiment (Ubs Leaks, Lux Leaks, Panama Papers, Football Leaks, Paradise Papers, Malta Files, Dubaï Paper…) révélés par des groupements de journalistes comme l'ICIJ (International Consortium of Investigative Journalists) et parfois des lanceurs d'alertes, conduisent à la loi n° 2018-898 du 23 octobre 2018 relative à lutte contre la fraude créant, au 1er juillet 2019, le Service des enquêtes judiciaires des finances (SEJFI) qui prend la suite du Service national des douanes judiciaires. Le SEJFI a ainsi une compétence douanière et fiscale.

D. Des faits de criminalité financière plus nombreux

Les chiffres du Service statistique ministériel de la sécurité intérieure (SSMSI) montrent une tendance haussière des faits de criminalité financière. Les infractions économiques et financières représentent plus de 400.000 faits constatés en 2019, avec une progression de +20% entre 2013 et 2018. Plus de 90% des faits relèvent des escroqueries et infractions assimilées. Le graphique ci-contre sur la progression du nombre de victimes d'escroqueries et d'infractions assimilées enregistrées par les services illustre la prégnance du phénomène.



Champ : France métropole tous services [Agrégat EIEF Sous-agrégat Escroqueries et infractions assimilées : index 84 85 86 89 90 91 92. Note de lecture : le nombre de victimes d'escroqueries et infractions assimilées est passé de 243 300 en 2012 à 323 100 en 2018.

Source : SSMSI, Base des victimes de crimes et délits 2018, données provisoires.

E. Les missions d'évaluation

Parallèlement, de nombreuses missions se sont penchées en 2018 et 2019, sur le traitement de la délinquance économico-financière, parmi lesquelles, citons :

- Le référé n° S2018-3520 du 12 décembre 2018 de la Cour des comptes sur les moyens consacrés à la lutte contre la délinquance économique et financière par lequel la Cour formule 5 recommandations[3],

- Le rapport d'information du 28 mars 2019, déposé par le comité d'évaluation et de contrôle des politiques publiques et présenté par les députés Ugo Bernalicis et Jacques Maire, sur l'évaluation de la lutte contre la délinquance financière. Ce rapport comporte 25 propositions[4],

- Le rapport rendu au mois de juillet 2019 sur le traitement de la criminalité organisée et financière du groupe de travail présidé par François Molins, procureur général près la Cour de Cassation[5],

- Le rapport d'information du 25 septembre 2019, déposé par la mission d'information commune présenté par les députés Émilie Cariou et Pierre Cordier sur le bilan de la lutte contre les montages transfrontaliers. Ce rapport comporte 27 recommandations[6],

- Le rapport du 26 novembre 2019 intitulé « Investir pour mieux saisir, confisquer pour mieux sanctionner » des députés Laurent Saint-Martin et Jean-Luc Warsmann, qui préconise 34 propositions[7],

- Le rapport de novembre 2019 de la Cour des comptes sur la fraude aux prélèvements obligatoires. La Cour propose 11 recommandations[8].

Si ces rapports mettent en exergue les progrès accomplis (lois, nouvelles institutions…), ils critiquent les insuffisances récurrentes de la lutte contre la criminalité financière dues à une absence de stratégie globale.

Le référé de la Cour des comptes précité résume la situation : *« Face à l'évolution aussi bien quantitative que qualitative des infractions, l'organisation et les moyens consacrés par les ministères de l'Intérieur et de la Justice à la lutte contre la délinquance économique et financière font apparaître des faiblesses qui contribuent à expliquer le caractère partiel et tardif de la réponse pénale. La Cour recommande de mieux utiliser les moyens qui existent dans les deux missions budgétaires concernées et, dans le choix des affaires et leur traitement, d'adopter une approche plus sélective, et plus préoccupée de l'efficacité et du délai de la réponse pénale ».*

La criminalité financière est devenue un véritable enjeu sociétal qui vient percuter à la fois le pacte républicain quand il s'agit des atteintes à la probité et de la fraude fiscale mais aussi l'ordre public économique quand des systèmes bancaires parallèles se mettent en place pour blanchir l'argent des groupes criminels organisés.

C'est dans ce contexte que le ministère de l'Intérieur a confié à la Direction Centrale de la Police Judiciaire la mission d'adapter en profondeur le dispositif.

II. Une nécessaire réponse stratégique

La sous-direction de la lutte contre la criminalité financière (SDLCF) constitue le vecteur de la réponse de la DCPJ. Elle a pour objectif la prévention et la répression des formes complexes, organisées et transnationales de la criminalité financière. Elle s'appuiera évidemment sur le réseau dynamique des Divisions économiques et financières de la DCPJ.

Elle doit développer une ambitieuse stratégie de pilotage national en synergie et coordination avec les administrations partenaires, au premier desquelles l'autorité judiciaire, en inscrivant son action tant au plan national qu'international.

Cette stratégie passera par une priorisation renforcée des cibles, la qualité devant prévaloir sur la quantité. Il s'agira d'un changement de paradigme dans la gestion des flux d'enquêtes pour avoir un effet répressif et dissuasif multiplié.

La réforme a été planifiée en deux étapes.

Dans un premier temps, création de la sous-direction qui se structure à partir de trois entités déjà existantes à savoir les deux offices centraux financiers » (l'OCRGDF et l'OCLCIFF) et la Brigade nationale d'enquêtes économiques. Dans un second temps, s'y ajoute une division transversale nouvelle, la Division d'appui opérationnelle (DAO).

A. L'Office central de lutte contre la corruption et les infractions financières et fiscales (OCLCIFF)

Créé le 25 octobre 2013, l'OCLCIFF a pour finalité la lutte contre la criminalité financière commise par des auteurs socialement insérés, les « cols blancs ». Il est organisé en deux brigades :

- La brigade nationale de répression de la délinquance fiscale (BNRDF), composée de policiers, officiers de police judiciaire, et d'inspecteurs des finances publiques, officiers fiscaux judiciaires, a pour mission, selon l'article 28-2 du Code de procédure pénale, de rechercher et constater, sur l'ensemble du territoire national, les infractions prévues par les articles 1741 et 1743 du Code général des impôts et le blanchiment de ces infractions lorsqu'il existe des présomptions caractérisées que les infractions prévues par ces articles résultent d'une des conditions prévues aux 1° à 5° du II de l'article L. 228 du livre des procédures fiscales, ainsi que les infractions qui leur sont connexes.

- La brigade nationale de lutte contre la corruption et la criminalité financière (BNLCF), qui est compétente pour les infractions à la législation sur les sociétés, au financement de la vie politique, aux délits boursiers et aux atteintes à la probité (corruption, corruption d'agents publics étrangers, trafic d'influence, détournement de fonds publics, prise illégale d'intérêt, favoritisme, concussion).

B. L'Office central pour la répression de la grande délinquance financière (OCRGDF)

Créé le 9 mai 1990, à la suite du sommet de l'Arche de 1989, ce service a pour domaine de compétence, d'une part, la lutte contre la criminalité financière commise par des groupes criminels organisés : blanchiment, financement du terrorisme, lutte contre les fraudes communautaires, les escroqueries transnationales et, d'autre part, l'identification des avoirs criminels.

Il comprend :

- une section de lutte contre le blanchiment de fonds et le financement du terrorisme,

- une section de lutte contre les escroqueries internationales et les atteintes aux intérêts financiers de l'Union européenne,

- un groupe opérationnel chargé des enquêtes relatives aux « biens mal acquis »,

- une brigade de recherche et d'intervention financière nationale (BRIFN), antenne de l'office central de lutte contre le crime organisé (OCLCO) (unité de terrain spécialisée dans les surveillances, filatures et interpellations d'individus aguerris et/ou dangereux),

- la plate-forme d'identification des avoirs criminels (PIAC).

C. La Brigade nationale des enquêtes économiques (BNEE)

La BNEE est un service composé d'agents de la direction générale des Finances publiques, essentiellement des inspecteurs des finances publiques, mis à la disposition fonctionnelle de la DCPJ qui en est l'autorité d'emploi. Implantée sur 22 sites au sein des GREE (groupes régionaux d'enquêtes économiques), elle a un effectif de 51 agents dénommés, depuis l'arrêté interministériel du 25 novembre 1997, « attachés d'enquêtes de la police nationale »

Les agents ont une double mis-

sion. D'une part, ils portent une assistance technique au profit des policiers principalement dans la répression des infractions économiques et financières. D'autre part, ils participent à la programmation du contrôle fiscal.

D. La Division d'appui opérationnelle (OPA)

Elle comprend trois sections d'appui aux activités opérationnelles.

i. La section formation

La DCPJ pilote des formations financières de grande qualité.

L'IMEF pour Investigateur en matière économique et financière constitue la formation de référence au sein de la police nationale. D'une durée de 7 semaines séquencée en 3 périodes, elle délivre un bagage théorique et pratique approfondi indispensable aux enquêteurs assujettis à des épreuves écrites permettant, en cas de succès, l'obtention du brevet IMEF.

Par ailleurs, il existe des stages spécialisés de deuxième niveau portant sur blanchiment, probité, saisie des avoirs criminels, comptabilité.

ii. La section de la preuve numérique

Le recueil et l'exploitation de la preuve sont consubstantiels aux investigations judiciaires, la DCPJ étant la police de la preuve. En matière financière, elle occupe une place toute particulière. Les traces digitales et génétiques ne permettent pas de remonter les flux financiers. La trace numérique est l'ADN de l'enquêteur financier. Les archives papiers occupant des mètres linéaires ont laissé place au stockage numérique dont les unités de comptes sont le giga ou le téraoctet.

Composée d'investigateurs en cybercriminalité (ICC), l'unité dispose d'un laboratoire d'investigation opérationnelle du numérique (LION), plateforme dotée d'outils performants permettant la préservation de l'intégrité des supports et leur exploitation en profondeur.

iii. Le SIRASCO financier

Le renseignement criminel est un vecteur primordial de l'action de la police judiciaire afin d'orienter l'activité de ses unités et développer leurs capacités proactives.

À côté du SIRASCO central (Service d'information, de renseignement et d'analyse stratégique sur la criminalité organisée), le SIRASCO financier va venir investir le domaine du renseignement criminel financier et permettre de consolider le rôle des offices centraux tels que défini par l'article D8 du Code de procédure pénale. Eh effet, ces services ont la charge d'assurer, dans les matières relevant de leurs compétences respectives, la centralisation, la coordination et la diffusion nationales de l'information auprès des services de police et des unités de gendarmerie.

Par ailleurs, la Coordination nationale des groupes interministériels de recherche (CNGIR), actuellement au sein de la sous-direction de la lutte contre la criminalité organisée, rejoindra la SDLCF.

iv. La création de quatre nouveaux offices centraux

Au printemps 2020, de nouveaux offices centraux vont succéder à ceux existants.

Quatre grandes thématiques correspondantes aux priorités ont été retenues :

- la fraude fiscale dans ses formes les plus complexes,

- la corruption, à la fois les atteintes à la probité et le financement illicite de la vie publique,

- le blanchiment, infraction irradiante allant de la criminalité organisée au financement du terrorisme en passant par les fraudes dont les escroqueries,

- l'identification des avoirs criminels, colonne vertébrale des enquêtes, l'enquête patrimoniale doit devenir un réflexe.

À chacune de ces thématiques va répondre un nouvel office :

- l'office anti-fraude fiscal,

- l'office anti-corruption,

- l'office anti-blanchiment,

- l'office d'identification des avoirs, bureau de recouvrement des avoirs ou asset recovery office.

Les noms des offices procèdent de la volonté de donner plus de cohérence et de visibilité.

Cette réorganisation de la filière écofi de la DCPJ intervient au moment même où d'autres institutions s'adaptent.

La loi de programmation 2018/2022 et de réforme de la Justice du 23 mars 2019 a prévu que le tribunal judiciaire de Paris dispose d'une compétence nationale en matière de criminalité organisée, en ce compris sa dimension financière ce qui recouvre à la fois le blanchiment et les escroqueries en bande organisée. Ainsi, à côté de la JIRS

(juridiction interrégionale spécialisée) prend place la JUNALCO (Juridiction nationale chargée de la lutte contre la criminalité organisée).

Pour des raisons sensiblement similaires à celles ayant guidé la DCPJ, Europol réorganise ses unités financières. Au printemps 2020, l'office européen de police devrait mettre en place l'Economic Financial and Corruption Crimes Center (Centre de lutte contre la criminalité économique, financière et la corruption). La SDLCF se positionnera comme partenaire privilégié d'Europol.

Enfin, la SDCLF portera une attention toute particulière aux atteintes aux intérêts financiers de l'Union, pour lesquelles elle est déjà compétente, dans le cadre du futur Parquet européen.

Notes :

1 Le sommet du G7 organisé sous la présidence française du 14 au 16 juillet 1989, dans le quartier d'affaires de La Défense (Hauts-de-Seine).

2 L'article 41-1-2 du CPP prévoit une procédure permettant au procureur de la République de conclure avec une personne morale mise en cause ou mise en examen pour corruption, trafic d'influence, blanchiment de fraude fiscale ou pour des infractions connexes, une convention comprenant une ou des obligations déterminées dont l'exécution éteint l'action publique.

3 https://www.ccomptes.fr/system/files/2019-03/20190204-refere-S2018-3520-lutte-delinquance-economique-financiere.pdf

4 http://www.assemblee-nationale.fr/15/pdf/rap-info/i1822.pdf

5 http://www.justice.gouv.fr/la-garde-des-sceaux-10016/remise-du-rapport-du-groupe-de-travail-sur-les-jirs-32556.html

6 http://www.assemblee-nationale.fr/15/rap-info/i2252.asp

7 http://www.justice.gouv.fr/la-garde-des-sceaux-10016/remise-du-rapport-sur-la-mission-de-lagrasc-32809.html

8 https://www.ccomptes.fr/system/files/2019-12/20191202-rapport-fraude-aux-prelevements-obligatoires.pdf

OUVRAGES RÉCENTS

LA GUERRE DES CARTELS

TRENTE ANS DE TRAFIC DE DROGUE AU MEXIQUE

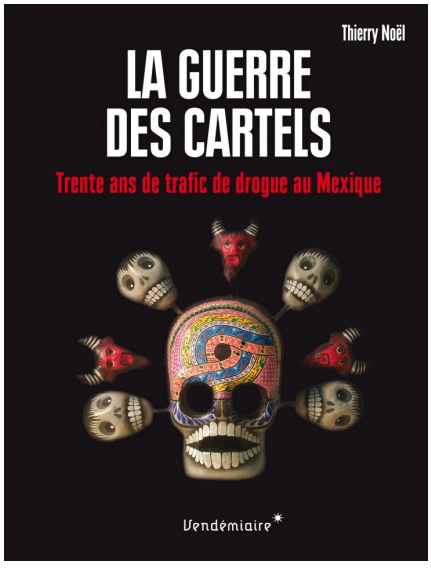
AUTEUR : THIERRY NOËL

ÉDITEUR : VENDÉMIAIRE

Résumé

Chaque mois, plus de 2 500 personnes sont assassinées au Mexique. Des villes sont transformées en champs de bataille, que des bandes ennemies parsèment de signaux macabres adressés à leurs adversaires : corps décapités, démembrés, pendus sous des ponts... On n'en finit plus de découvrir des charniers où les cadavres de civils sont laissés à l'abandon. La violence semble avoir atteint dans l'ensemble du pays un paroxysme que même la mobilisation de l'armée peine à empêcher.

Tandis que partout les trafiquants, les narcos, affichent leurs richesses, armes à la



crosse dorée à l'or fin à la main, que des chansons populaires sont composées à leur gloire et que les plus célèbres d'entre eux, tels Joaquín Guzmán Loera, dit El Chapo, ont acquis une réputation légendaire.

Comment en est-on arrivé là ?

Pour la première fois, un historien français remonte aux racines du mal, depuis la fin des années 1970 et le déferlement de la cocaïne colombienne jusqu'à la constitution de cartels organisés en véritables multinationales de la drogue, infiltrant tous les rouages de l'État. En leur sein, les narcos se battent sans merci pour imposer leur autorité. Faisant du pays le théâtre d'une guerre civile qui ne dit pas son nom et totalise à ce jour plusieurs centaines de milliers de victimes.

LA RECHERCHE DE LA PREUVE NUMÉRIQUE PAR LA GENDARMERIE NATIONALE

CYRIL DEBARD

LIEUTENANT-COLONEL DE LA GENDARMERIE NATIONALE, CHEF DU DÉPARTEMENT INFORMATIQUE - ÉLECTRONIQUE (INL) DE L'INSTITUT DE RECHERCHE CRIMINELLE DE LA GENDARMERIE NATIONALE (IRCGN), PÔLE JUDICIAIRE DE LA GENDARMERIE NATIONALE (PJGN)[1]

La technologie est au service de l'homme et au service de l'information. Elle est également au service de la criminalistique qui utilise ses larges possibilités pour contribuer à la démonstration de la vérité. Dans ce domaine, les experts doivent s'adapter aux mutations constantes des technologies, des moyens et des procédés mis en oeuvre afin de concourir le plus efficacement possible aux investigations et faire face aux nouvelles criminalités.

Le terme de cybercriminalité peut être employé, dans son acception large, afin de définir ces nouvelles formes de crime. Celui-ci recouvre alors les infractions commises sur Internet mais aussi l'utilisation exponentielle des technologies numériques par les criminels qui génère un impact non négligeable dans la pratique des utilisateurs tant auteurs que victimes.

La division criminalistique ingénierie numérique (DCIN) de l'IRCGN (Institut de Recherche Criminelle de la Gendarmerie Nationale) s'intéresse à toutes les formes de technologies numériques pour en extraire les indices et preuves qui permettront la révélation de la vérité.

Les smartphones, les ordinateurs, les disques durs, les véhicules et leur technologie embarquée, les terminaux de paiement électroniques, les GPS, les systèmes de vidéosurveillance, les enregistrements sonores, etc. n'ont pas de secret pour les experts de la DCIN.

I. La chaîne fonctionnelle criminalistique numérique de la Gendarmerie Nationale

Aveux et témoignages ont longtemps été suffisants pour convaincre les magistrats et un jury. Actuellement, c'est l'exploitation scientifique des indices qui constitue la base de toutes les investigations sur les scènes d'infraction. Afin de s'adapter à ce changement, la Gendarmerie Nationale a construit une chaîne criminalistique, reposant sur des spécialistes formés à la détection, au prélèvement, à l'analyse et l'interprétation de ces indices.

La chaîne fonctionnelle criminalistique numérique de la gendarmerie nationale comporte plusieurs niveaux dont la complémentarité fonde la cohérence de l'ensemble :

- **localement**, les unités élémentaires (brigades) réalisent les actes de criminalistique de premier niveau au travers de la recherche de traces et indices simples sur les scènes d'infractions liées à la délinquance de proximité. Elles s'appuient pour cela sur les C-NTECH (Correspondant - Enquêteur en Technologies Numériques).

- **au plan départemental**, la brigade départementale de

renseignements et d'investigation judiciaire (BDRIJ) et plus particulièrement les NTECH (Enquêteurs en Technologies Numériques) réalisent des actes techniques complexes. Ils animent par ailleurs le réseau des C-NTECH et peuvent mettre à leur disposition l'équipement collectif spécifique.

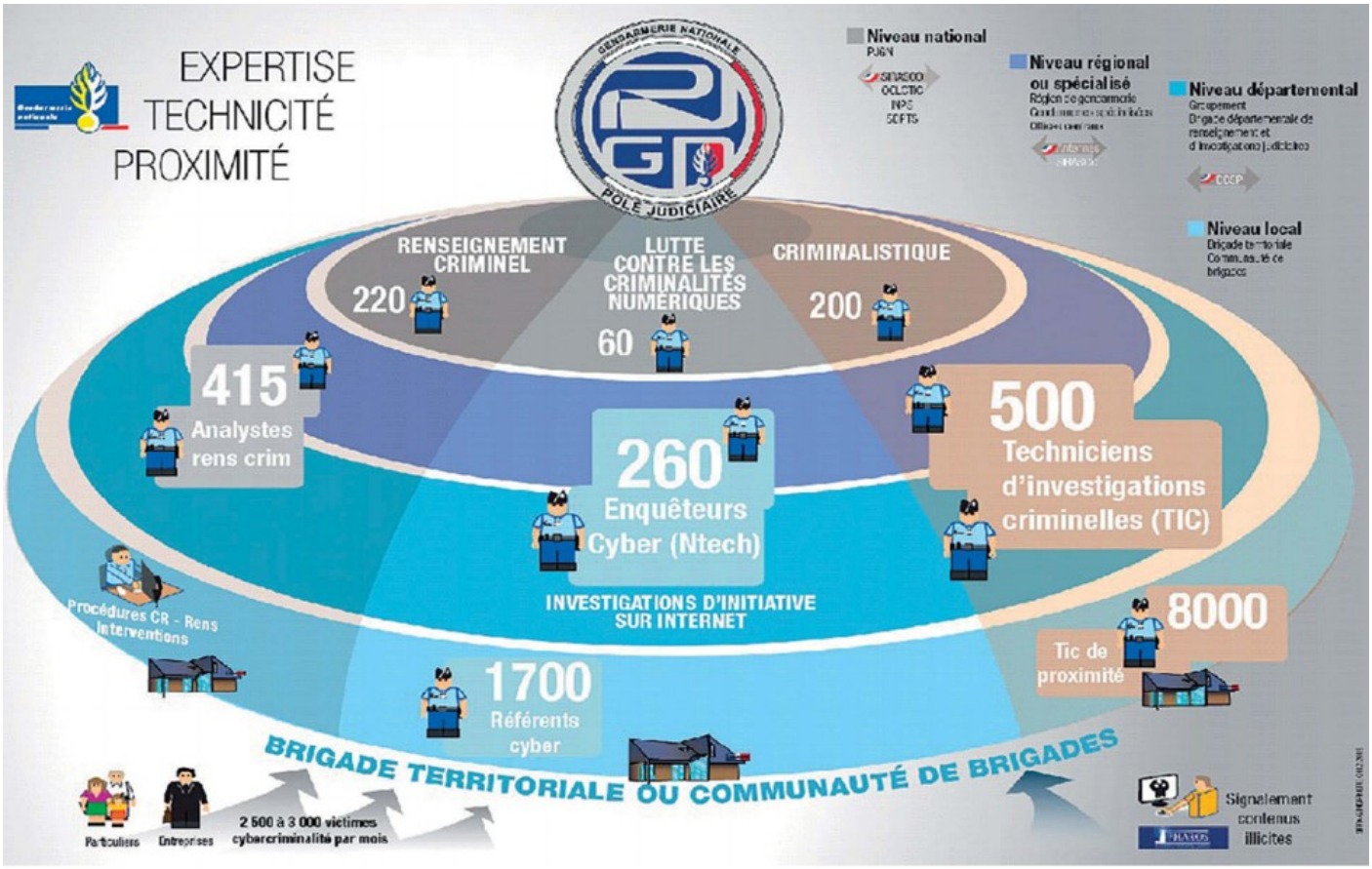
- **au plan national**, l'institut de recherche criminelle de la gendarmerie nationale (IRCGN) a pour mission de participer à l'établissement de la preuve des infractions pénales et apporter son assistance technique aux unités. La DCIN avec son département Informatique Électronique en est une des composantes.

Le C3N (Centre de Lutte Contre les Criminalités Numériques) du SCRCGN (Service Central de Renseignement Criminel de la Gendarmerie Nationale) vient compléter le dispositif. Il est chargé plus particulièrement d'assurer le pilotage et l'appui spécialisé de l'action de la gendarmerie contre la cybercriminalité et les criminalités numériques de façon plus générale. Le C3N mène ou coordonne les investigations d'ampleur nationale ayant trait à la cybercriminalité, et réalise une surveillance permanente de l'Internet.

II. Un défi à relever : l'accès à la donnée

Le cybercrime est un type de criminalité qui se développe de façon conséquente. En effet, de plus en plus de crimes dits "classiques" peuvent utiliser des outils informatiques. Cependant, contrairement au monde réel, où les preuves peuvent être collectées assez simplement, les preuves numériques sont cachées grâce aux nouvelles techniques telles que le « cloud », la cryptographie et les mots de passe complexes.

Les avancées technologiques et la normalisation de la cryptographie dans la vie de tous les jours ont considérablement augmenté le niveau de cybersécurité des utilisateurs et des entreprises de façon générale malgré une prise de conscience tardive. Néanmoins, elles ont aussi permis aux cybercriminels de cacher leurs données numériques et de les rendre inaccessibles



© Sirpa Gendarmerie

aux enquêteurs.

Ces mécanismes de sécurité ont rendu indispensable de mener de la R&D afin de trouver des vulnérabilités et de les exploiter pour retrouver les données en clair. De plus, les criminels, qu'ils soient de la criminalité organisée ou isolée (pédopornographie par exemple), utilisent régulièrement des téléphones « sécurisés ». Ces téléphones sont abandonnés et changés dès lors qu'ils sont cassés.

III. Une coopération européenne indispensable

Être de son temps, c'est utiliser les mêmes moyens que son environnement. Il revient aux forces de l'ordre et à la gendarmerie de concevoir le cas échéant les outils nécessaires pour accéder à cette information numérisée, la sélectionner très précisément, et la partager au juste besoin pour remplir l'ensemble de ses missions de sécurité. Il lui revient également de développer ses propres outils numériques et de veiller à leur appropriation par le gendarme sur le terrain. Il s'agit en outre et de manière concomitante d'observer avec le plus haut degré d'expertise, l'emploi ou le risque d'emploi du numérique à des fins malveillantes et de mettre en place les parades adaptées.

Dans ce contexte très changeant de lutte contre la criminalité organisée, le département Informatique Électronique est porteur du projet européen CERBERUS, avec pour partenaires le NFI (Netherlands Forensic Institute aux Pays-Bas) et l'UCD (University College Dublin en Irlande).

CERBERUS, co-financé par le Fonds Sécurité Intérieure (FSI), vise à créer une plateforme de cassage de mots de passe utilisable dans tous les pays de l'UE. Hébergée au PJGN, cette solution est complémentaire au service de cassage de mots de passe proposé par l'EC3 (Europol)[2].

Cette plateforme permettra aux enquêteurs de casser les mots de passe utilisés par les criminels afin de protéger leurs données numériques (images/vidéos pédopornographiques, transactions bancaires, etc.) ainsi que leurs communications textes/vocales. Elle donnera donc aux juges des preuves numériques supplémentaires qui sont actuellement inaccessibles en raison de mots de passe forts et de chiffrement robustes.

La dimension européenne du projet donnera la capacité à tous les États membres de l'UE d'extraire des données chiffrées et augmentera le rayonnement d'expertise de la Gendarmerie Nationale auprès des laboratoires européens. Cette expertise permettra notamment de fluidifier les échanges et d'augmenter les capacités en R&D de l'IRCGN.

IV. La révolution de l'Internet des Objets : IoT

L'IoT (Internet of Things ou Internet des objets) constitue la prochaine étape de la révolution numérique. Ce sont des milliards d'objets du quotidien qui seront connectés à l'horizon 2020.

Les objets connectés ont le pouvoir de simplifier la vie quotidienne et d'améliorer le bien-être des individus, chez eux, au bureau, en famille ou au sein de toute autre communauté.

La multiplication de ces objets dans la vie courante en fait des témoins permanents de nos activités et parfois des sources d'attaques. Dans le cadre de l'investigation judiciaire, la récupération des informations contenues dans ces objets peut éclairer les enquêteurs sur le déroulement de faits infractionnels et orienter les investigations judiciaires. Cependant, en raison de leur nouveauté, de leurs multiplicités aussi bien dans leur forme que leurs caractéristiques techniques et dans les données produites, la plupart de ces objets ne sont, pour l'heure, pas identifiés. Ils ne sont donc pas ou peu récupérés aujourd'hui lors d'une investigation sur une scène d'infraction.

Cependant, dans le cadre d'affaires récentes en Australie[3], au Royaume-Uni[4] et aux États-Unis[5], la récupération de données provenant d'objets connectés aussi disparates qu'une montre connectée, un stimulateur cardiaque ou un moniteur d'activité physique, a contribué à faire avancer significativement les enquêtes en montrant notamment les incohérences entre les témoignages des suspects et les informations recueillies par ces

objets du quotidien. La prise en compte des objets connectés par les enquêteurs de terrains constitue donc un vecteur essentiel dans la recherche de la preuve scientifique lors d'une enquête judiciaire.

Notes :

1 https://www.gendarmerie.interieur.gouv.fr/pjgn

2 https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

3 https://www.sfchronicle.com/crime/article/Murder-defendant-dies-A-Fitbit-device-linked-14432677.php

4 https://www.liverpoolecho.co.uk/news/liverpool-news/how-police-unmasked-iceman-assassin-15649613

5 https://www.journal-news.com/news/crime--law/using-pacemaker-data-stealing-personal-information-judge-middletown-arson-case-says/BAGH5WM0iCxOTwTPfM3P7J/

OUVRAGES RÉCENTS

3 MINUTES POUR COMPRENDRE

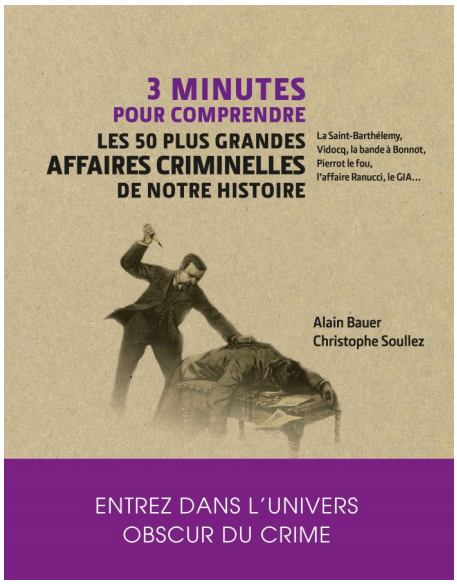
LES 50 PLUS GRANDES AFFAIRES CRIMINELLES DE NOTRE HISTOIRE

AUTEUR : ALAIN BAUER ET CHRISTOPHE SOULLEZ

ÉDITEUR : LE COURRIER DU LIVRE

Résumé

Les grandes affaires criminelles ont toujours fasciné le public et suscité des débats passionnés et passionnants ! Quelques figures criminelles mythiques ont marqué durablement notre histoire. Si elles provoquent un tel engouement, c'est parce que leurs crimes brisent tous les tabous, qu'ils sont un condensé des imperfections humaines, et qu'ils restent un formidable révélateur des forces et des faiblesses de notre société... et de nous-mêmes. Érigés en "héros négatifs", ces personnages charismatiques inspirent l'effroi et l'horreur, le doute et le mystère. Leur personnalité complexe et ambivalente, leur histoire exceptionnelle et pourtant humaine - qui peut faire écho à notre propre vie - nous choquent, nous répugnent et nous



attirent. Des compagnons de la Coquille au clan de la Brise de mer en passant par Landru, la bande à Bonnot ou Mesrine, cet ouvrage magnifiquement illustré vous plongera au coeur de notre histoire criminelle. Des anecdotes et portraits de criminels, mais aussi de personnalités policières visionnaires, vous entraîneront du côté sombre de l'esprit humain...

Alain Bauer est professeur de criminologie au Conservatoire national des arts et métiers (New York et Shanghai). Il est aussi le conseiller de diverses polices ou institutions dans le monde et auteur d'une cinquantaine d'ouvrages traduits en une dizaine de langues.

Christophe Soullez, universitaire, est le chef de l'Observatoire national de la délinquance et des réponses pénales. Il enseigne notamment à l'Institut d'études politiques de Paris et est l'auteur d'une quinzaine de livres sur la sécurité et la police.