LA REVUE DU
GRASCO

www.grasco.eu
www.larevuedugrasco.eu

N°19— Juillet 2017

Parution trimestrielle
Gratuite

EDITORIAL

CHANTAL CUTAJAR

DIRECTRICE DU GRASCO

Le projet de loi rétablissant la confiance dans l'action publique, présenté lors du Conseil des ministres du 14 juin 2017 par l'éphémère ministre de la Justice, François Bayrou[1], était en préparation bien avant l'élection présidentielle. Soumis au Conseil d'État dès le 31 mai 2017, soit 15 jours après l'investiture du Président de la République, le projet de loi vise à « moraliser la vie publique » : « La transparence à l'égard des citoyens, la probité des élus, l'exemplarité de leur comportement constituent des exigences démocratiques fondamentales. Elles contribuent à renforcer le lien qui existe entre les citoyens et leurs représentants, comme elles doivent affermir les fondements de notre contrat social » peut-on lire dans l'exposé des motifs...

Il s'agit d'une énième tentative destinée à renouer le lien de confiance entre les citoyens et les élus après les lois organique et ordinaire du 11 octobre 2013 relatives à la transparence de la vie publique à l'origine de la Haute Autorité pour la Transparence de la Vie Publique, la loi du 6 décembre 2013 relative à la lutte contre la fraude fiscale et la grande délinquance économique et financière créant le procureur de la République financier, la loi du 20 avril 2016 renforçant les obligations déontologiques des fonctionnaires et la loi du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique qui crée l'Agence Française Anticorruption.

Le Conseil d'État a été saisi d'un projet de loi ordinaire et d'un projet de loi organique[2]. L'indigence de l'étude d'impact relative au projet de loi ordinaire a été sévèrement critiquée par la Haute juridiction administrative qui recommande qu'elle soit enrichie notamment par des éléments de comparaison internationale. Les travaux de commission ont débuté le 23 juin 2017. 17 amendements ont, d'ores et déjà, été déposés.

Le projet de loi ordinaire comporte 14 articles répartis en six titres consacrés aux dispositions relatives à la peine d'inéligibilité en cas de crimes ou de manquements à la probité[5], à la prévention des conflits d'intérêts[6], à l'interdiction de l'emploi de membres de la famille des élus et des membres du gouvernement[7], à l'indemnité des membres du parlement, au financement de la vie politique[8] et aux représentants au Parlement européen[9].

On retiendra les axes principaux du projet de loi :

- L'instauration d'une peine complémentaire obligatoire d'inéligibilité en cas de crimes ou d'infractions matérialisant une atteinte à la probité pour les candidats aux élections législatives et sénatoriales. Les juridictions répressives auront l'obligation de la prononcer, **sauf décision spécialement motivée**[10].
- Les assemblées parlementaires devront élaborer les règles en matière

SOMMAIRE

EDITO 1

INTERVIEW :

CHARLES DUCHAINE, DIRECTEUR DE L'AGENCE FRANÇAISE ANTICORRUPTION. 4

CONSTATS ET PRECONISATIONS :

ISLAMISME RADICAL EN PRISON : LA DIFFICILE DÉFENSE DES DROITS FONDAMENTAUX , PAR AGATHE LOGEART 9

DOCTRINE SCIENCES CRIMINELLES :

LES PARTICULIERS VICTIMES D'ACTES DE CYBERMALVEILLANCE, PAR ADELINE CHAMPAGNAT 23

PARADIS FISCAUX ET MONDIALISATION, PAR ÉMILIE AUGUSTIN 30

DOCTRINE JURIDIQUE :

LA SAISIE ET LA CONFISCATION EN VALEUR EN DROIT PÉNAL FRANÇAIS , PAR STEPHEN ALMASEANU 35

LE JUGE ET LE RENSEIGNEMENT, PAR EMMANUEL FARHAT 42

LES CELLULES DE RENSEIGNEMENT FINANCIER : UN OBJECTIF COMMUN, DES APPROCHES DIFFÉRENTES, PAR GUILLAUME BÈGUE 51

RAPPORT :

COMPTE-RENDU DE LA RÉUNION DE LA COMPAGNIE RÉGIONALE DES COMMISSAIRES AUX COMPTES DE CAEN ET DES PROCUREURS DE LA RÉPUBLIQUE DU RESSORT DE LA COUR D'APPEL DE CAEN 57

REGARDONS AILLEURS :

LA LUTTE CONTRE LA CRIMINALITÉ FINANCIÈRE : QUEL RÔLE POUR L'UNITÉ MAROCAINE DE TRAITEMENT DU RENSEIGNEMENT FINANCIER ?, PAR IHSAN EL HASSANI 62

de prévention et de cessation des **conflits d'intérêts uniquement entre un intérêt public et des intérêts privés** dans lesquels peuvent se trouver des parlementaires et préciser les conditions dans lesquelles chaque député ou sénateur veille à faire cesser immédiatement ou à prévenir ces situations.

– C'est également aux assemblées de déterminer les modalités de tenue d'un **registre accessible au public** et recensant les cas dans lesquels un parlementaire a estimé devoir ne pas participer aux travaux du Parlement en raison d'une situation de conflit d'intérêts à laquelle il pourrait être confronté.

– Les assemblées devront définir les règles selon lesquelles les frais de mandat réellement exposés par chaque parlementaire lui sont remboursés sur présentation de justificatifs de ces frais et dans la limite de plafonds qu'elles déterminent.

– L'interdiction pour les membres du gouvernement, les parlementaires et les titulaires de fonctions exécutives locales d'employer des membres de leur famille proche. Le projet punit de trois ans d'emprisonnement et de 45 000 euros d'amende la violation de l'interdiction d'employer ou de nommer des membres de la famille proche comme collaborateurs parlementaires ou membres de cabinet. Est également prévue une obligation de remboursement des sommes versées en vertu de contrats conclus en violation de l'interdiction. Les contrats en cours qui méconnaîtraient l'interdiction prendront fin deux mois après la publication de la loi. La rupture du contrat sera constitutive d'un licenciement.

– Le projet renforce le contrôle des comptes des partis politiques et facilite leur financement et celui des campagnes électorales par l'institution d'un médiateur du crédit et la création, par ordonnance, d'une structure pérenne de financement destinée à palier les carences du financement bancaire privé.

Le lien de confiance entre les citoyens et leurs élus est un impératif catégorique pour que puisse s'épanouir une démocratie réelle qu'appelle de leurs voeux une grande majorité d'entre eux. La loi seule, est impuissante à le tisser si elle n'est pas accompagnée d'une réelle prise de conscience des élus et responsables publics, manifestée par des actes clairs et lisibles pour éradiquer les conflits d'intérêts.

Notes :

1. Le 21 juin, soit une semaine après la présentation du texte.
2. Projet de loi organique rétablissant la confiance dans l'action publique : http://www.senat.fr/dossier-legislatif/pjl16-580.html
   Projet de loi rétablissant la confiance dans l'action publique : http://www.senat.fr/dossier-legislatif/pjl16-581.htmlTexte n° 581 (2016-2017) de Monsieur François Bayrou, ministre d'Etat, garde des sceaux, ministre de la justice https://www.senat.fr/leg/pjl16-581.html
3. https://www.senat.fr/leg/etudes-impact/pjl16-581-ei/pjl16-581-ei.html
4. Titre I art. 1
5. Titre II, art. 2
6. Titre IV, art. 7
7. Titre V, art. 8 à 12
8. Titre VI, art. 13 et 14
9. Sont visées notamment les infractions en matière de faux administratifs (faux et usage de faux dans un document administratif, détention de faux document administratif, faux et usage de faux en écriture publique ou authentique, fourniture frauduleuse de document administratif, fausse déclaration pour obtention indue d'allocation, prestation, paiement ou avantage, obtention frauduleuse de document administratif), des infractions en matière électorale (infractions relatives aux élections, aux listes électorales, au vote, au dépouillement, au déroulement du scrutin...), des infractions en matière fiscale (fraude fiscale aggravée), des infractions en matière de délits d'initiés, des infractions en matière de financement des partis politiques (financement des campagnes électorales et des partis politiques), et des manquements aux obligations déclaratives à la Haute Autorité pour la transparence de la vie publique, dans la mesure où ces infractions portent atteinte à la confiance publique.

HATVP

HAUTE AUTORITÉ
POUR LA TRANSPARENCE
DE LA VIE PUBLIQUE

Règlement du prix
de la Haute Autorité pour la transparence de la vie publique

Lire le document : http://www.larevuedugrasco.eu/documents/Reglement-du-prix-de-recherche-2017.pdf

COMITÉ SCIENTIFIQUE DU GRASCO

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

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

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

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

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

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

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

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

INTERVIEW

CHARLES DUCHAINE, DIRECTEUR DE L'AGENCE FRANÇAISE ANTICORRUPTION

PROPOS RECUEILLIS PAR JOCELYNE KAN

L.R.D.G. : Quelle est la compétence de l'Agence française anticorruption (AFA), créée par la loi du 9 décembre 2016 relative à la lutte contre la corruption et à la modernisation de la vie économique (loi dite "Sapin II"), qui a remplacé le Service central de prévention de la corruption (SCPC), créé par la loi n du 29 janvier 1993 relative à la prévention de la corruption et à la transparence de la vie économique des procédures publiques (loi dite "Sapin") ? ?

Le Service central de prévention de la corruption (SCPC) créé par la loi n° 93-122 du 29 janvier 1993 relative à la prévention de la corruption et à la transparence de la vie économique et des procédures publiques, dirigé par un magistrat et placé auprès du ministre de la Justice, n'avait été doté par le législateur d'aucun pouvoir d'investigation. En dépit d'une composition interministérielle et d'une réelle volonté de faire, ce service n'a, faute de pouvoirs, jamais pu prendre la place qu'il aurait dû occuper au sein de nos institutions.

L'Agence française anticorruption (AFA), créée par la loi 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte

contre la corruption et à la modernisation de la vie économique est un service à compétence nationale tout à fait singulier puisqu'il est créé par la loi et placé auprès de deux ministres, celui de la Justice et celui en charge du Budget.

Ce service a pour mission :

1- d'aider les autorités compétentes et les personnes qui y sont confrontées à prévenir et à détecter les faits de corruption, de trafic d'influence, de concussion, de prise illégale d'intérêt, de détournement de fonds publics et de favoritisme (art.1) ;

2- de participer à la coordination administrative, de centraliser et diffuser les informations permettant d'aider à prévenir et à détecter les faits de corruption, d'apporter dans ce cadre son appui aux administrations de l'État, aux collectivités territoriales et à toute personne physique ou morale (art. 3). Le décret du 14 mars 2017 prévoit que l'AFA doit, à ce titre, préparer un plan national pluriannuel de lutte contre la corruption, assister les autorités françaises compétentes dans les organisations internationales, assurer des actions de formation, de sensibilisation et d'assistance sur la prévention et la détection des risques en matière de corruption et contribuer, par ses actions de coopération et ses missions d'appui et de soutien technique, à l'application des engagements internationaux

des autorités françaises.

3- d'élaborer des recommandations destinées à aider les personnes morales de droit public et de droit privé à prévenir et à détecter les faits de corruption.

4- de contrôler la qualité et l'efficacité des procédures mises en oeuvre pour prévenir et détecter les faits de corruption, de trafic d'influence, de concussion, de prise illégale d'intérêt, de détournement de fonds publics et de favoritisme, tant au sein des administrations de l'État, des collectivités territoriales, de leurs établissements publics et sociétés d'économie mixte et des associations et fondations reconnues d'utilité publique, qu'au sein des entreprises en veillant au respect des mesures et procédures de conformité énumérées au II de l'article 17.

5- d'exercer les attributions prévues à l'article 131-39-2 du Code pénal et aux articles 41-1 -2 et 764-44 du Code de procédure pénale, c'est-à-dire d'assurer le suivi de la peine de soumission à un programme de mise en conformité ou celui de la convention judiciaire d'intérêt public concernant les personnes morales.

6- d'aviser le procureur de la République compétent des faits dont elle a eu connaissance dans l'exercice de ses missions et qui sont susceptibles de constituer un crime ou un délit, elle en avise simultanément le parquet national financier si ces faits sont susceptibles de relever de sa compétence.

7- d'élaborer chaque année un rapport d'activité rendu public.

L.R.D.G. : De quels moyens dispose l'Agence sur le plan humain et matériel ?

Au 31 décembre 2017, l'AFA disposera d'un effectif de 70 agents, une vingtaine consacrée aux missions de conseil, d'analyse et aux actions internationales, une quarantaine dédiée aux missions de contrôle. Les autres emplois seront affectés aux fonctions support et de direction. Le budget devrait, pour un exercice plein, avoisiner les 8 M€.

L.R.D.G. : Comment l'AFA est-elle organisée pour accomplir ses différentes missions ?

Cette organisation est fixée par l'arrêté du 14 mars 2017. L'Agence française anticorruption comprend, outre la commission des sanctions et le conseil stratégique : la sous-direction du conseil, de l'analyse stratégique et des affaires internationales ; la sous-direction du contrôle ; le secrétariat général.

La sous-direction du conseil, de l'analyse stratégique et des affaires internationales est notamment chargée de centraliser et d'assurer la diffusion des informations et des bonnes pratiques permettant d'aider à prévenir et à détecter les faits de corruption ; à ce titre, elle bénéficie du concours des services du ministère de l'Économie et des Finances et du ministère de la Justice, notamment à des fins statistiques. Elle participe, dans les domaines de compétence de l'Agence, à la définition de la position des autorités françaises compétentes au sein des organisations internationales et propose et met en oeuvre des actions de coopération, d'appui et de soutien techniques auprès d'autorités étrangères.

Elle est composée du département de l'appui aux acteurs économiques et du département du conseil aux acteurs publics. Le sous-directeur dispose, en outre, d'un chargé de mission qui coordonne l'action internationale de l'Agence.

Le département de l'appui aux acteurs économiques élabore et actualise les recommandations destinées à aider les personnes morales de droit privé et établissements publics à caractère industriel et commercial à prévenir et à détecter les infractions ci-dessus énumérées. Il exerce, à la demande du Premier ministre, les attributions prévues au 5° de l'article 3 de la loi (mise en oeuvre de la loi de blocage).

Le département du conseil aux acteurs publics apporte son assistance aux administrations de l'État, aux collectivités territoriales, à leurs établissements publics et sociétés d'économie mixte, aux associations et fondations reconnues d'utilité publique ainsi qu'aux personnes physiques. Il élabore et actualise les recommandations destinées à aider ces personnes à prévenir et à détecter les infractions d'atteinte aux devoirs de probité.

La sous-direction du contrôle est composée du département du contrôle des acteurs économiques et du département du contrôle des acteurs publics.

Le département du contrôle des acteurs économiques contrôle, sur pièces et sur place, le respect par les personnes morales de droit privé et les établissements publics à caractère industriel et commercial qui y sont

soumis, des mesures et procédures de conformité prévues à l'article 17 de la loi du 9 décembre 2016. Il veille à l'exécution des décisions rendues par la commission des sanctions et contrôle l'exécution de la peine prévue à l'article 131-39-2 du Code pénal et du programme de mise en conformité prévu à l'article 41-1-2 du Code de procédure pénale en exécution des conventions judiciaires d'intérêt public.

Le département du contrôle des acteurs publics contrôle, sur pièces et sur place, la qualité et l'efficacité des procédures mises en oeuvre dans les administrations de l'État, les collectivités territoriales, leurs établissements publics et sociétés d'économie mixte et les associations et fondations reconnues d'utilité publique en vue de prévenir et de détecter les infractions d'atteinte aux devoirs de probité.

Le secrétariat général est chargé de la gestion administrative et financière de l'Agence française anticorruption, en liaison avec le secrétariat général du ministère de l'Économie et des Finances et le secrétariat général du ministère de la Justice. Il propose et met en oeuvre la politique de communication institutionnelle et de relations publiques de l'Agence. Il assure le secrétariat de la commission des sanctions et celui du conseil stratégique.

L.R.D.G. : Quelles sont les relations de L'AFA avec la Haute Autorité pour la transparence de la vie publique (HATVP) ?

L'article 3 de la loi prévoit que l'AFA dispose par principe du pouvoir d'initier des contrôles mais il prévoit aussi que ces contrôles peuvent être effectués à la demande du président de la HATVP. C'est le seul lien fonctionnel existant entre ces deux institutions mais nous entendons bien, de part et d'autre ne pas en rester là et nous envisageons de nouer un partenariat plus étroit, dans des conditions restant à définir et évidemment conformes aux textes et aux principes applicables.

En réalité, les missions de la HATVP et celles de l'AFA, sont complémentaires mais totalement différentes : la HATVP s'intéresse à la probité des hommes qui prétendent à l'exercice de certaines fonctions publiques, l'AFA s'intéresse aux entreprises et aux administrations et plus précisément aux conditions dans lesquelles elles tentent de se prémunir contre les risques de corruption.

L.R.D.G. : Comment vont s'organiser les relations avec les collectivités territoriales en matière de prévention et d'aide à la détection de la corruption ?

La relation avec les collectivités territoriales et plus généralement avec les acteurs publics peut se nouer aussi bien dans le champ du conseil que dans celui du contrôle. Le 3° de l'article 3 de la loi du 9 décembre 2016 dispose en effet que l'AFA *« contrôle, de sa propre initiative, la qualité et l'efficacité des procédures mises en oeuvre au sein des administrations de l'État, des collectivités territoriales, de leurs établissements publics et sociétés d'économie mixte, et des associations et fondations reconnues d'utilité publique pour prévenir et détecter les faits de corruption, de trafic d'influence, de concussion, de prise illégale d'intérêt, de détournement de fonds publics et de favoritisme. »*

Malheureusement, et à l'inverse de ce qui a été prévu à l'article 17 pour les acteurs économiques, la loi n'a posé aucune obligation particulière de conformité à la charge de ces personnes publiques, ce qui engendre deux interrogations et un regret : quel sera le contenu d'un programme de conformité anticorruption pour un personne publique et partant, quel sera le référentiel de contrôle de l'AFA ? pourquoi réserver un traitement différent aux personnes publiques et aux acteurs économiques alors qu'ils sont en la matière susceptibles de lier leurs sorts dans un pacte de corruption ?

Des obligations de conformités, non pas identiques mais comparables à celles posées à l'article 17 pour les entreprises, auraient pu être imposées aux acteurs publics sans aucunement entraver leur libre administration.

Comme pour les entreprises, les relations avec les acteurs publics vont s'organiser dans la concertation, l'objectif n'étant pas d'alourdir encore le poids de la « règlementation », mais de dégager des recommandations, des bonnes pratiques, permettant d'appliquer celle existante dans le souci permanent de limiter les risques de corruption. Le contrôle de l'AFA ne sera pas « un contrôle de plus » mais un contrôle qui, s'il portera parfois sur les mêmes éléments que d'autres contrôles existants, aura une autre orientation et une autre finalité.

L.R.D.G. : Comment envisagez-vous le contrôle du respect, par les grandes entreprises, de l'obligation de vigilance dans le domaine de la lutte contre la corruption et le trafic d'influence et de la mise en oeuvre des sanctions en cas de manquement à cette obligation ? Élaborez-vous des programmes adaptés aux risques de chacune des entreprises ?

L'obligation de vigilance ne sera efficace que si elle recueille l'adhésion des dirigeants énumérés à l'article 17 et que ceux-ci la mette en oeuvre avec sincérité et volontarisme. Les dispositifs imposés par la loi ne serviraient à rien si l'entreprise les vivait simplement comme une obligation et ne cherchait pas à leur donner une traduction réelle dans la mise en oeuvre de sa politique. Partant, le contrôle ne sera pas simplement un contrôle formel, il faudra mettre les dispositifs à l'épreuve en vérifiant de quelle manière ils sont appliqués dans la pratique de l'entreprise.

Dès que nous serons en capacité de le faire, nous émettrons des recommandations à l'usage des entreprises. Elles constitueront un socle applicable au plus grand nombre. Il n'est pas envisageable pour notre Agence d'élaborer des programmes adaptés aux risques de chacune d'entre elles et je ne pense d'ailleurs pas que ce soit souhaitable. L'Agence pourra, au-delà des recommandations à portée générale, apporter un soutien plus individualisé, mais il ne lui appartient pas de se substituer à l'entreprise en lui disant ce qu'elle doit faire. L'Agence est là pour aider, le plus concrètement possible, à la mise en oeuvre des dispositions légales en rappelant l'objectif à atteindre, elle ne saurait imposer à l'entreprise le choix des moyens pour y parvenir ni davantage lui délivrer une quelconque certification au vu des moyens mis en oeuvre.

La loi prévoit que le directeur peut adresser des avertissements. Même si ces avertissements ne constitueront probablement pas une injonction de faire, il est vraisemblable qu'ils engendreront la nécessité de contrôles a posteriori pour s'assurer de ce qui a été fait. Si rien n'a été fait et que l'inertie apparaît fautive, la commission des sanctions sera saisie. En réalité c'est elle qui, par ses décisions, donnera le ton et permettra à l'Agence d'élaborer sa stratégie en la matière.

L.R.D.G. : Que va vous apporter le droit de communication, par les représentants de l'entité contrôlée, de tout document professionnel ou de toute information utile ?

L'existence formelle au sein de l'entreprise d'un programme de conformité anticorruption répondant en tous points aux huit obligations posées par l'article 17 de la loi est une chose, la sincérité de ses auteurs et leur volonté de le mettre effectivement en oeuvre ne peut, elle, se vérifier qu'à l'examen concret, par sondage, du déroulement de certaines opérations. L'examen de certains documents financiers, bancaires ou commerciaux pourra seul permettre de mesurer cette volonté et, le cas échéant, de détecter des failles dans la vigilance voire des infractions consommées.

L.R.D.G. : Existera-t-il un positionnement particulier de l'Agence par rapport aux lanceurs d'alerte ?

Même si le législateur n'a rien prévu de manière expresse, l'AFA est au nombre des autorités administratives susceptibles de recevoir les alertes en l'absence de diligence de la personne initialement destinataire dans les conditions prévues par l'article 8 de la loi du 9 décembre 2016.

Par ailleurs, de simples dénonciations pourront être et sont même déjà adressées à l'AFA qui, rappelons-le, dispose d'un pouvoir d'auto-saisine et peut donc, si elle l'estime opportun, déclencher un contrôle sans avoir à rendre compte à quiconque des conditions par lesquelles elle s'est convaincue de son opportunité.

L.R.D.G. : Quel sera le rôle de l'Agence à l'international ?

En application des dispositions de l'article 2 de l'arrêté du 14 mars 2017, l'AFA participe, dans ses domaines de compétence, à la définition de la position des autorités françaises compétentes au sein des organisations internationales et propose et met en oeuvre des actions de coopération, d'appui et de soutien techniques auprès d'autorités étrangères. Dans ces champs, l'AFA participe aux travaux de l'OCDE, du G20, de l'ONUDC ou du GRECO, mais elle souhaite aussi nouer des relations bilatérales avec d'autres pays, en ou hors Union européenne, pour asseoir, à terme, son rôle au plan international. La convention de l'OCDE sur la lutte contre la corruption d'agents publics étrangers dans les transactions commerciales internationales n'a pas entendu confier une compétence exclusive

à tel ou tel pays, bien au contraire, elle dispose que *« lorsque plusieurs Parties ont compétence à l'égard d'une infraction présumée visée dans la présente Convention, les Parties concernées se concertent, à la demande de l'une d'entre elles, afin de décider quelle est celle qui est la mieux à même d'exercer les poursuites »*. Cette concertation est de nature à éviter les doubles poursuites – qui ne sont d'ailleurs pas d'usage dans le champ de la répression des infractions de droit commun- et à réfréner les appétits de certains, parfois moins épris de justice qu'animés par le goût du lucre ou par une volonté d'éliminer la concurrence. Seul un véritable positionnement de l'ensemble des pays sur ces questions permettra d'assurer cette concertation nécessaire. La France doit donc clairement se positionner et, dans le cadre de la coopération bilatérale, apporter son soutien à tous les pays tiers qui souhaiteraient en faire de même.

L.R.D.G. : Quelles sont vos priorités pour l'année à venir ?

Nous sommes actuellement 6 ou 7 et nous n'avons rejoint nos locaux que depuis le 22 mai dernier. La priorité est d'abord d'achever la construction du service, c'est-à-dire de réaliser les recrutements jusqu'au dernier, nous sommes actuellement à environ 50% mais les recrues n'ont pas encore rejoint leur poste ! Nous devons installer le mobilier, l'informatique, le téléphone…nous devrons ensuite définir nos procédures de travail et notamment de contrôle, ce qui est un travail très lourd que nous ne pourrons véritablement mener à bien que lorsque les effectifs suffisants et compétents seront à pied d'oeuvre.

Nous devons exprimer de manière extrêmement détaillé notre besoin informatique pour créer une application métier, ce qui revient à « décortiquer » toutes les phases de notre activité en envisageant toutes les variables possibles et ce, aussi bien dans l'activité de conseil que dans celle de contrôle ou d'exécution des mesures judicaires.

Nous devrons, aussi rapidement que possible, élaborer des recommandations à l'intention des acteurs économiques. Certains attendent sans doute de connaître notre niveau d'exigence pour engager des moyens, d'autres aussi attendent peut- être des contrôles pour se convaincre de la nécessité d'en engager…Nous laisserons un temps de répit aux entreprises, les contrôles n'interviendront probablement pas avant 2018.

LA REVUE DU GRASCO

Numéro ISSN : 2272-981X

Université de Strasbourg, UMR-DRES 7354

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

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

Adresse mail : information@grasco.eu

Directrice de la revue du GRASCO : Chantal CUTAJAR

Directrice adjointe de la revue du GRASCO : Jocelyne KAN

Rédacteur en chef -Conception : Sébastien DUPENT

Relecture - Correction : Claudia-Vanita DUPENT

Isabelle FISHER

ISLAMISME RADICAL EN PRISON : LA DIFFICILE DÉFENSE DES DROITS FONDAMENTAUX

AGATHE LOGEART

CONTRÔLEURE AUPRÈS DE LA CONTRÔLEURE GÉNÉRALE DES LIEUX DE PRIVATION DE LIBERTÉ (CGLPL)

Le 11 juin 2015, la Contrôleure générale des lieux de privation de liberté (CGLPL) publiait un rapport sur la prise en charge de la radicalisation islamiste en milieu carcéral, accompagné d'un avis publié au journal officiel.

Un an plus tard, le 7 juin 2016, un deuxième rapport, consacré à l'ouverture des unités dédiées aux personnes détenues radicalisées, était publié.

Ces deux documents ont été communiqués aux ministres de la Justice qui se sont succédés, Mme Christiane Taubira, puis M. Jean-Jacques Urvoas, qui ont souhaité y répondre[1].

Par la suite, le 25 octobre 2016, M. Urvoas a présenté un nouveau plan de lutte contre la radicalisation en prison qui revenait pour partie sur la création des unités dédiées, annonçait une réorientation du dispositif et une augmentation considérable du nombre de places réservées aux personnes détenues radicalisées.

Ce sont ces étapes que l'article ci-dessous va retracer, ainsi que la démarche et la méthode choisies par la Contrôleure générale des lieux de privation de liberté.

Définie par la loi du 30 octobre 2007 modifiée, la mission de la Contrôleure générale des lieux de privation de liberté, autorité administrative indépendante, est de veiller au respect des droits fondamentaux des personnes privées de liberté. C'est à ce titre qu'il a été décidé d'examiner les mesures nouvelles mises en place par l'administration pénitentiaire dans le cadre du plan de lutte contre le terrorisme annoncé le 21 janvier 2015 par le Premier ministre, et principalement le principe de la création de cinq unités dédiées et du regroupement de personnes détenues à raison de leur radicalisation islamiste.

À l'automne 2014, une expérience de regroupement de personnes détenues islamistes avait été organisée à la Maison d'arrêt de Fresnes, à l'initiative de son directeur, qui entendait par cette mesure enrayer les manoeuvres prosélytes de personnes radicalisées, dont l'influence grandissante perturbait la détention. Cette mise à l'écart ne concernait que les personnes prévenues ou condamnées pour des faits de terrorisme en lien avec une pratique radicale de l'islam. La garde des Sceaux, dont les services n'avaient pas été consultés, s'était déclarée « très réservée » sur cette expérience, et l'inspection des services pénitentiaires avait rendu un rapport très critique sur sa mise en oeuvre.

Pourtant, un contexte dramatique allait modifier l'approche de la question. En effet, le choc des attentats de janvier 2015 a conduit les autorités à décider de prendre des mesures dans l'urgence. Il est vite apparu que le parcours pénal de certains auteurs, le rôle de la prison dans leur radicalisation, le fait que des personnes impliquées dans des actes de terrorisme aient pu s'être rencontrées alors qu'elles étaient détenues pour des faits de droit commun et soient restées en contact à leur sortie de prison, a suscité un émoi profond auquel les pouvoirs publics ont alors décidé de répondre, en reprenant pour partie le schéma

de Fresnes, bien qu'il ait jusque là été observé avec beaucoup de réserves.

Ainsi, la création de cinq quartiers dédiés étaient-elle annoncée comme une « duplication » de l'expérience de Fresnes où elle se poursuivrait, à Fleury-Mérogis, Osny, et Lille-Annoeullin. Ces unités assureraient pour certaines l'évaluation des personnes détenues et/ou leur prise en charge. Des appels d'offre étaient lancés pour poursuivre des « recherches-actions » (en centrale, en milieu ouvert et chez les mineurs) ; des aumôniers musulmans devaient être recrutés ; des modules d'éducation civique et d'histoire des religions et des modules sur la citoyenneté et la laïcité devaient être mis en place. Des grilles de détection de la radicalisation devaient être renouvelées.

Pour élaborer son premier rapport sur ce sujet, la CGLPL a réuni des informations de types différents, à partir de sources diversifiées et de visites sur place (Fresnes, Réau, Bois d'Arcy, Osny). Il s'est agi de rassembler les éléments les plus objectifs possibles sur les phénomènes de radicalisation en détention, leur évolution et leur traitement. Les observations de la direction de l'Administration pénitentiaire (DAP), des services de renseignement et des acteurs de terrain ont été recueillies. Des entretiens ont été menés avec des chercheurs, des policiers, des magistrats, des avocats, des représentants syndicaux, des familles de détenus, des membres des services pénitentiaires d'insertion et de probation (SPIP), des responsables associatifs. Les politiques publiques développées dans des pays étrangers ont été examinées.

Ce travail a duré plusieurs mois. Si la plupart des interlocuteurs institutionnels de la CGLPL ont fait montre d'une grande ouverture d'esprit, il est arrivé que certains manifestent des réticences, voire de l'incompréhension à l'égard de sa démarche. Dans une période d'une telle gravité, était-il vraiment nécessaire de se pencher sur la question des droits fondamentaux ? Porter un regard tatillon, voire aux yeux de quelques-uns complaisant à l'égard de personnes détenues, était-il de mise ? À ces critiques à peine voilées, la CGLPL a tenu à répondre, dès la première page de son rapport du 11 juin 2015 : « Sans négliger les problèmes de sécurité, en parfaite conscience de la gravité et de l'ampleur du phénomène de radicalisation dans la société toute entière et dans les établissements pénitentiaires - et en particulier des risques que fait peser le prosélytisme sur les personnes détenues les plus vulnérables- le CGLPL a souhaité déterminer quelles conséquences en matière de droits fondamentaux peut entraîner la création d'un mode de surveillance particulier qui ne correspond à aucune catégorie connue jusqu'ici. »

Au cours des entretiens avec les différentes catégories de personnels intervenant en détention dans les établissements visités, un désarroi profond s'est régulièrement exprimé. Les interlocuteurs de la CGLPL ont expliqué que la question de la radicalisation n'était pas pour eux une découverte, qu'auraient ravivée les attentats. Depuis des années, ont-ils expliqué, ils tiraient la sonnette d'alarme, mais n'étaient pas écoutés. Certains affirmaient même avoir été « taxés d'islamophobie », lorsqu'ils mettaient leur hiérarchie en garde contre un phénomène croissant qu'ils étaient impuissants à contenir. Des notes faisant état de l'inquiétude des intervenants de terrain communiquées à la CGLPL étaient ainsi restées sans réponse, regrettaient-ils. Autre reproche : le poids trop grand que les pouvoirs publics comme l'opinion feraient peser à l'administration pénitentiaire dans le développement de la radicalisation islamiste. Nombre de personnes rencontrées déploraient une tentative de renvoyer la responsabilité des failles du système de repérage à une institution aux moyens faibles, débordée par une surpopulation galopante.

Au cours d'une visite de deux jours à Fresnes, au mois de janvier 2015, les 22 personnes détenues regroupées ont été rencontrées par les contrôleurs qui ont pu s'entretenir avec elles individuellement et en toute confidentialité. Plusieurs enseignements ont été tirés de ces entretiens et des observations faites sur place, la direction et les différentes catégories d'intervenants s'étant longuement exprimées. La plupart des personnes détenues ont expliqué aux contrôleurs ne pas comprendre ce qui les avait conduites à ce mode d'incarcération spécifique, consistant en un isolement de principe du reste de la détention, et craindre une forme de stigmatisation préjudiciable à leur parcours pénal, ainsi que le fait d'être mêlées « à des personnes détenues plus ancrées dans le

processus de radicalisation ». Aucun programme de prise en charge spécifique n'était mis en place. Hormis la promenade et une partie des activités sportives, les autres activités se déroulaient en compagnie d'autres personnes détenues, ce qui démontrait aisément que le principe d'étanchéité entre les différentes parties de la détention n'existait pas.

S'agissait-il vraiment de « dupliquer » ce modèle ? Deux visites à la Maison d'arrêt d'Osny aux mois de mars et d'avril 2015 permettaient de poursuivre la réflexion. En effet, dans cet établissement, se déroulait depuis plusieurs mois une expérience de « recherche-action » conduite par des sociologues très impliqués depuis longtemps dans la recherche en milieu pénitentiaire. Leur mission consistait à élaborer des outils de prise en charge de la radicalisation avec des personnes détenues volontaires, sans qu'un regroupement soit alors envisagé. Investir la période de détention pour limiter et amoindrir la dangerosité, tenter de faire évoluer les certitudes, instiller du doute, réfléchir au parcours de violence : la démarche paraissait à l'opposé de celle qui avait été mise en oeuvre à Fresnes, où, de même qu'il existe des « sorties sèches » de prison, on assistait à un mode d'incarcération consistant en un « regroupement sec », une mise à l'écart sans prise en charge. Les critères d'affectation retenus à Fresnes (l'incrimination ou la condamnation pour des faits en relation avec une entreprise terroriste) ne paraissaient pas satisfaisants aux yeux de la CGLPL, puisqu'ils ne concernaient pas les personnes détenues pour des faits de droit commun, mais qui pouvaient être engagés dans une démarche d'islamisme violent.

Dans sa conclusion, la CGLPL, bien consciente que les expériences étrangères ne permettent nullement de définir une approche modélisable, comme le montrent d'ailleurs les changements de pied répétés souvent opérés au gré de l'actualité, et tout en comprenant parfaitement la difficulté de la tâche, a regretté que la France ait tardé à prendre en compte la question de la radicalisation islamiste en détention. Elle a critiqué le fait que le placement dans des unités dédiées, décidé de façon discrétionnaire par la direction des établissements concernés, ne soit susceptible d'aucune des voies de recours habituelles, alors qu'il présente le risque de restreindre les droits fondamentaux des personnes détenues et de détériorer leurs conditions de détention. En effet, selon l'analyse de la CGLPL, aucune disposition légale existante ne correspond au statut d'une personne détenue dans un quartier dédié, dont le régime ne s'apparente ni tout à fait à la détention ordinaire ni à la mise à l'isolement. L'absence d'information -à ce stade- sur les modalités d'encadrement et de précisions sur le régime de détention laisse plutôt craindre un glissement vers une forme d'isolement qui ne dit pas son nom. C'est pourquoi la CGLPL a considéré qu'il ne pouvait être favorable au regroupement tel qu'il a été présenté par les autorités.

Les programmes de prise en charge, dès lors qu'ils sont affichés comme destinés à un public volontaire, ne suscitaient en revanche pas de réserve de principe, mais devraient faire l'objet d'évaluations régulières. La CGLPL préconisait enfin une réflexion approfondie des pouvoirs publics sur la prise en charge des personnes de retour des zones de conflit, estimant que l'incarcération ne pouvait être le seul mode de traitement de cette situation.

Considérant que l'importance du sujet et des risques encourus, la CGLPL a décidé de publier au JO un avis reprenant les principaux éléments de ce rapport et des enseignements qu'il en a tirés.

Dans une lettre du 26 juin 2015, la garde des Sceaux a répondu aux observations et réserves de la CGLPL. Il y est notamment contesté que les personnes détenues dans une unité dédiée soient assujetties à un régime de détention spécifique, ce qui expliquerait le choix du mot « unité » et non celui de « quartier ». L'ensemble des droits de ces personnes y seraient respectés, (maintien des liens familiaux, accès aux activités de travail, de formation, et socio-culturelles). Les décisions d'affectation seraient « des mesures d'ordre intérieur ». À l'avenir, même si les personnes dirigées vers les unités dédiées seraient « principalement » des personnes écrouées pour des faits liés à l'islamisme radical, celles considérées comme radicalisées et prônant une action violente mais incarcérées pour des faits de droit commun pourraient aussi à l'avenir y être dirigées. Des précisions étaient apportées sur la répartition des personnes détenues concernées : sur la base du volontariat, les personnes « accessibles à une remise en question » seraient plutôt envoyées à Osny et Fleury-Mérogis, tandis que « les plus opposantes » seraient transférées à Lille-Annoeullin, où l'unité dédiée installée dans le quartier maison

centrale serait par nature plus sécurisée. Pour « les plus dangereux », ils continueraient à être soit dispersés soit placés à l'isolement.

Avec un peu de retard sur le calendrier prévu, l'ouverture des cinq unités dédiées s'est échelonnée de la fin janvier à la fin mars 2016. Comme elle l'avait annoncé, la CGLPL a donc décidé de mener une nouvelle enquête sur la mise en pratique du programme. Trois contrôleurs ont été chargés d'une mission spécifique dans les quatre établissements concernés. La mission s'est déroulée du début du mois de février jusqu'à la remise du deuxième rapport à la fin du mois de mai, et à sa publication le 7 juin 2016.

Là encore, cette démarche a provoqué des réactions -cette fois de franche hostilité- de la part de l'administration qui la jugeait prématurée et la supposait par avance partiale. Au contraire, la Contrôleure générale a estimé qu'il était logique de poursuivre le travail entamé un an plus tôt. Après avoir pointé de possibles atteintes aux droits fondamentaux, il convenait d'examiner la façon dont étaient mises en place les unités dédiées, de voir quel chemin avait été parcouru et de vérifier si les craintes et réserves exprimées dans le premier rapport étaient ou non fondées. Il ne pouvait évidemment s'agir que d'un travail d'étape, le sujet méritant de faire l'objet de contrôles ultérieurs, en fonction de la mise en place progressive des programmes et de leur adaptation au fil du temps.

Un an plus tôt, l'urgence qui guidait la commande publique passée à l'administration pénitentiaire pouvait être analysée comme devant répondre à la nécessité de faire obstacle au prosélytisme et à la « contagion » de l'islamisme radical. Donc à faire tous les efforts nécessaires pour séparer des personnes détenues radicalisées de celles, vulnérables, sur lesquelles elles pourraient exercer une néfaste influence. Depuis, une réflexion nettement plus élaborée avait été menée, nourrie notamment de la recherche-action. Les attentats de novembre 2015 avaient encore douloureusement avivé la volonté d'aboutir à la mise en place de structures pérennes.

Le 10 février 2016, une « doctrine d'emploi » rédigée par la DAP était transmise aux directeurs interrégionaux.

L'encellulement individuel devait être la règle pour les 117 places, réservées aux hommes majeurs dans quatre établissements, selon la répartition suivante :

- à Fresnes, l'unité dédiée (transformée en unité d'évaluation) était prévue pour 26 places ;

- à Fleury-Mérogis, 2 unités dédiées de 20 places ;

- à Osny, 1unité dédiée de 23 places ;

- à Lille-Annoeullin,1 unité dédiée de 28 places.

Une nouvelle fois, la DAP affirmait qu'il s'agirait d'un régime de détention ordinaire et en aucune manière d'isolement, même si les personnes concernées devraient « autant que possible être séparées des autres ».

En principe, il était prévu que le passage en unité d'évaluation dure huit semaines, au cours desquelles serait établi le risque d'un passage à l'acte violent fondé sur l'extrémisme religieux et examiné « le risque de nuisance » à l'égard des autres personnes détenues. Une synthèse rédigée à l'issue de cette période serait transmises aux autorités, y compris au juge d'instruction et au juge de l'application des peines, ainsi qu'à la personne concernée si elle en faisait la demande. La personne détenue serait ensuite orientée soit vers une unité de prise en charge, soit en détention ordinaire, soit placée à l'isolement.

La durée de séjour en unité dédiée de prise en charge ne devait pas excéder six mois.

64 personnes étaient incarcérées dans ces unités au moment des visites des contrôleurs. À l'exception de 3 d'entre elles, toutes ont accepté les entretiens, qui se sont là aussi déroulés individuellement et dans une totale confidentialité. Nombre d'entre elles ont assuré n'avoir pas eu le choix de leur affectation en unité dédiée, l'avoir souvent apprise la veille ou le jour -même, ce qui remettait en cause le volontariat supposément requis. Certaines paraissaient très contentes de bénéficier de conditions de détention meilleures (locaux propres, encellulement individuel), et appréciaient d'être regroupées avec des codétenus partageant les mêmes idées. Cet « entre soi » pouvait être perçu comme favorisant le sentiment d'appartenir « au gratin », et induisait une forme d'héroïsation par rapport au reste de la détention. D'autres au contraire considéraient leur placement en unité dédiée comme une mesure discriminatoire, une punition qui les avait contraintes à abandonner du jour au lendemain formation, travail et activités auxquels elles avaient auparavant accès. La crainte que ce placement influence négativement les juges

les perturbait également. Ainsi, « l'étiquette d'irrécupérable » selon les termes d'une personne détenue, « collée à ceux de Lille-Annoeullin » ne pourrait qu'aggraver la perception portée sur leur avenir à la fois pénitentiaire et pénal. Une autre disait « ne pas voir l'intérêt de nous mettre tous ensemble, si l'idée c'est de nous sortir de là ».

Si certains éléments des programmes de prise en charge ont pu être portés à la connaissance des contrôleurs, au moment des visites peu avaient déjà été mis en place. Il était donc prématuré d'apporter une analyse sur ce sujet. Toutefois, il paraissait clair qu'au moins dans un établissement -Osny- le fait qu'une recherche-action s'y soit déroulée plus d'une année avant l'ouverture de l'unité dédiée et se soit passée en bonne intelligence avec les acteurs locaux, favorisait la création d'ateliers, de groupes de parole et d'activités auxquels les personnes détenues semblaient accepter volontiers de participer.

Une très grande autonomie a été laissée aux directions d'établissement pour concevoir l'aménagement et l'organisation des unités dédiées. Les personnels se sont emparés des projets, avec une forme d'enthousiasme, assez rare dans le difficile exercice de leur métier pour être relevée. Les différents agents se sont engagés de façon très volontaire et impliquée dans ce qui leur apparaissait comme un défi majeur, non seulement pour leur administration mais aussi pour l'ensemble de la société.

Au cours des visites, les contrôleurs ont porté une attention particulière aux binômes de soutien (un éducateur, un psychologue) nouvellement créés, soit vingt-six postes. Formés en quelques semaines, souvent tout juste diplômés, n'ayant pour la plupart aucune expérience du monde carcéral pas plus que des phénomènes de radicalisation, assujettis à un régime précaire (CDD d'un an renouvelable), ces jeunes professionnels ont paru particulièrement peu assurés. Ainsi, à Lille-Annoeullin, les binômes étaient-ils rattachés au renseignement pénitentiaire, tandis qu'à Osny, il était hors de question pour les personnes interrogées que leurs rapports puissent même être transmis aux magistrats, en raison de leur conception du secret professionnel.

Alors que la mission de la CGLPL était en cours, le Premier ministre présentait le 9 mai 2016 un deuxième volet du plan de lutte antiterroriste, le PART (Plan d'action contre la radicalisation et le terrorisme), où étaient annoncées de nouvelles mesures spécifiques au monde carcéral. Le principe des unités dédiées y était réaffirmé et complété. La création notamment d'un service de renseignement de plein exercice appartenant au second cercle de la communauté du renseignement était annoncée, ainsi que le développement des programmes de prise en charge après le passage en unité d'évaluation, la mise en place d'une grille d'indicateurs de sortie de la radicalisation, l'adaptation du cadre législatif des fouilles.

Les autorités expliquaient alors vouloir prendre en compte « le changement d'échelle » du phénomène de radicalisation islamiste, dont l'évolution « exponentielle » allait de plus en plus peser sur le fonctionnement de la justice et des établissements pénitentiaires, du fait en particulier des cas de retours de Syrie et d'Irak. Alors que la France représentait le plus important contingent de combattants européens dans ces zones de conflit, les chiffres montraient une explosion du nombre de procédures : au cours de l'année 2015, 2010 procédures et 67 informations judiciaires avaient été ouvertes, soit 249 procédures au total à la fin de l'année. 260 personnes avaient été mises en examen dans le cadre des filières irako-syriennes (contre respectivement 9 et 4 en 2012). Désormais, la plupart des personnes étaient incarcérées dès leur retour en France. Une évolution significative de la politique pénale du parquet de Paris, compétent en matière de terrorisme, expliquait aussi cette nouvelle approche. Le recours quasi-systématique à la qualification criminelle d'association de malfaiteurs pourrait à l'avenir conduire au prononcé de peines allant jusqu'à 20 ans de réclusion. La loi du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement prévoyait dans son article 11 la possibilité de porter la période de sûreté à 30 ans pour les crimes punis de la réclusion criminelle à perpétuité. Interrogée par la CGLPL, la DAP admettait volontiers que cette spectaculaire inflation changeait la donne : l'expérimentation des unités dédiées pourrait à l'avenir être « exportée » dans chaque direction interrégionale. Dans un deuxième temps, lorsque le système serait « modélisé », les mineurs et les femmes, jusqu'ici

complètement exclus du programme pourraient être eux aussi concernés.

La CGLPL faisait un bilan des visites et entretiens conduits de façon approfondie pendant les quatre mois qu'a duré sa mission.

Sur la question du regroupement, son avis restait le même : il présente plus d'inconvénients que d'avantages. Alors que ses critiques sur l'absence de cadre légal donné au placement en unité dédiée avaient été rejetées par les responsables de l'administration pénitentiaire, la CGLPL notait avec satisfaction que la loi du 3 juin 2016 dans son article 726-2 du Code de procédure pénale prévoyait que la mesure d'affectation pouvait désormais faire l'objet d'un recours devant le juge administratif.

La CGLPL regrettait que la qualification terroriste reste le critère unique d'affectation, même si l'entrée par une « deuxième voie », pour des personnes incarcérées pour d'autres faits était en théorie, mais en théorie seulement, envisagée. Le régime particulier de détention organisé dans les unités dédiées entraînait des effets pervers. Ainsi, l'accès au travail, à la formation professionnelle étaient rendus pratiquement impossible. En contradiction avec les objectifs affichés, l'étanchéité des unités dédiées des autres quartiers n'était pas du tout assurée. Si les contacts étaient de fait limités, ils continuaient d'exister, ne serait-ce qu'au cours des mouvements. Plusieurs incidents ont montré que la communication entre personnes détenues dans les unités dédiées et les autres subsistaient. Au sein même des unités dédiées -plusieurs témoignages de personnes détenues en font état- la coexistence entre djihadistes appartenant à des factions rivales créée des tensions potentiellement extrêmement dangereuses. Il a paru paradoxal aux contrôleurs -et ceci a été relevé par plusieurs interlocuteurs- que l'administration rassemble des personnes que la justice poursuit pour association de malfaiteurs.

La CGLPL a aussi pointé le rôle de la surpopulation pénale sur la création de ces unités. En effet, particulièrement sensible dans les établissements de la région parisienne où sont détenues la plupart des personnes mises en cause dans des dossiers de terrorisme islamiste en raison de la spécialisation du TGI de Paris, la surpopulation est mise en avant par l'administration pour justifier le regroupement. Alors que le surencombrement des établissements est -comme il n'est plus besoin de le démontrer- un frein à la réinsertion, la prise en charge de personnes radicalisées nécessitant une attention particulière y serait dans ces conditions empêchée.

La CGLPL a été saisi à plusieurs reprises par les avocats de leurs clients détenus en unité dédiée. Au-delà des conditions de détention proprement dites, ils insistent sur les conséquences négatives que cela entraîne dans l'esprit des magistrats, pour qui le fait d'être affecté en unité dédiée peut constituer un indice de dangerosité supplémentaire. La CGLPL a considéré ces observations comme légitimes.

L'ambiguïté du rôle des binômes de soutien devrait faire l'objet d'une clarification déontologique : il n'est pas acceptable aux yeux de la CGLPL que, en particulier pour ce qui concerne les psychologues, les personnes détenues ne sachent pas quel usage peut être fait des entretiens qu'elles ont avec elles. Mentionnée à plusieurs reprises au cours de la mission, la difficulté pour les prévenus de s'exprimer sur les faits qui leur sont reprochés ne saurait leur porter grief : elles sont en effet présumées innocentes, et il a paru aux contrôleurs particulièrement attentatoire à leurs droits qu'il soit possible d'en tirer argument.

En conclusion, ce deuxième rapport estimait que l'extension du modèle expérimental des unités dédiées n'était pas réaliste, car il paraissait sous-dimensionné en regard des enjeux. Et potentiellement dangereux car il est porteur par sa nature-même de risques quant à l'exercice de certains droits fondamentaux.

Dans une lettre datée du 6 juillet 2016, le ministre de la Justice, Jean-Jacques Urvoas répondait au rapport du CGLPL. Il précisait qu'aucune décision d'extension des unités dédiées n'avait été prise, ni ne le serait tant qu'une évaluation fine ne serait pas faite. Le regroupement n'aurait pas eu pour but de rendre « étanche » les unités dédiées du reste de la détention, mais de « faciliter la prise en charge des personnes détenues sans les isoler du reste de la population de l'établissement ». Une clarification du rôle des binômes de soutien serait opérée. Si les personnes placées en unité dédiée ne l'ont en effet pas été sur la base du volontariat et si certaines d'entre elles ont manifesté leur désaccord, de meilleures conditions de détention et un intérêt pour les programmes de prise en charge auraient levé

leurs réticences.

Quant à la modicité des structures, il devrait y être remédié par la mise en place en parallèle, de programmes de prévention de la radicalisation dans 27 établissements pénitentiaires. Contrairement aux témoignages recueillis, le ministre de la Justice affirmait que le placement en unité dédiée ne pouvait être organisé sans l'accord formel du magistrat compétent.

Réputées particulièrement sécurisées et encadrées bien davantage que d'autres secteurs de la détention, les unités dédiées ne sont pas pour autant à l'abri d'incidents graves. Le 4 septembre 2016 en début d'après-midi, un homme condamné à cinq ans de prison pour avoir tenté de se rendre en Syrie a agressé deux surveillants qui le conduisaient à la promenade. Il utilisait une pointe métallique confectionnée à partir d'un élément de la fenêtre de sa cellule. L'arme d'une trentaine de centimètres a été utilisée en direction de la tête du premier agent, et comme le montrent les enregistrements de vidéosurveillance, avec une extrême violence. Un deuxième surveillant venu à la rescousse de son collègue a lui aussi été blessé en l'évacuant. Des circonstances particulières, qui n'ont jamais été publiquement expliquées, n'ont pas permis aux forces d'intervention d'arriver rapidement. Il leur a fallu trois heures pour se rendre sur place pendant lesquelles l'unité a été livrée à elle-même. Les vidéos enregistrées ont montré que des personnes détenues dans l'unité dédiée circulaient librement, disposaient d'autres armes blanches confectionnées à partir de débris de miroir, et que l'agresseur s'était livré à des actes particulièrement odieux avec le sang du surveillant blessé.

Cet acte d'une gravité extrême, où la vie d'un voire de deux surveillants a été mise en danger, la passivité sinon la complicité de certaines des personnes détenues dans la même unité que l'agresseur, la lenteur des forces d'intervention ont provoqué un état de choc dans l'administration pénitentiaire. N'ayant pas été saisie, la CGLPL ne s'est pas rendue à Osny, une enquête sur cet épisode dramatique n'étant pas, en soi, dans son domaine de compétence. Pour autant, cela ne l'a pas empêchée d'observer les conséquences entraînées par ces faits.

Sans qu'il soit possible d'y voir un lien direct, mais considérant que la double agression d'Osny avait inévitablement été prise en compte dans la réflexion qui a conduit à une refonte des mesures concernant les détenus radicalisés, la CGLPL a pris connaissance du nouveau plan rendu public le 25 octobre 2016 pour la sécurisation des prisons et contre la radicalisation violente en détention. Présenté dans la presse, sans démenti du ministère de la Justice, comme « la fin des unités dédiées », le nouveau dispositif, de fait les consacre, mais en élargissant et en modifiant leur implantation. Le garde des Sceaux, en préambule, précise la philosophie qui sous-tend le nouveau dispositif, ce qui paraissait cruellement manquer dans les phases précédentes : « Il est indispensable de préciser ici nos intentions, écrivait le ministre. Il semble illusoire de « déradicaliser » une personne. Car si la radicalisation est un facteur de risque, elle n'est pas en elle-même une menace, et seule la violence qu'elle peut induire doit être combattue par les pouvoirs publics (…). Plus que tout, nous devons oeuvrer à faire que ces personnes rompent avec la violence, qu'elles s'engagent dans un processus de désistement de la fureur qui les habite et les conduit à passer à l'acte. Ce faisant, l'univers carcéral renoue avec une mission trop souvent oubliée : aider la personne détenue à se rédimer, à rejoindre la société dans une meilleure disposition que celle ayant justifié sa condamnation à la réclusion ou l'emprisonnement. »

Se félicitant de la pertinence et du caractère fécond de l'approche pluridisciplinaire mise en oeuvre lors de la création des unités dédiées, il regrette en revanche l'absence d'évaluation des premières personnes incarcérées dans ces nouvelles structures. L'absence d'approche unifiée des prises en charge -relevée aussi par la CGLPL- lui paraît regrettable. Une décision importante est prise : le regroupement ne s'appliquera désormais qu'aux détenus dont l'ancrage dans la radicalisation est la plus forte, la sécurité de leurs conditions de détention sera renforcée.

Le nombre de places devrait augmenter de façon importante : 27 établissements (il s'agit d'une confirmation) devraient mettre au point des programmes de prise en charge pour des personnes considérées comme susceptibles de s'éloigner de la violence. Une centaine de places seraient réservées en Maison

d'arrêt pour « les profils les plus dangereux », et 190 places d'isolement mises à disposition. Des quartiers spécifiques d'évaluation remplaceraient les structures en place et de nouveaux devraient être ouverts en province (Bordeaux et Marseille). Contrairement à ce qu'avait considéré le ministère de la Justice dans sa réponse à la CGLPL, la question des femmes et des mineurs engagés dans un processus de radicalisation islamiste a fini par préoccuper les autorités, entraînant la décision d'ouvrir 100 places destinées aux femmes radicalisées. En ce qui concerne les mineurs -sujet longtemps négligé et qui n'a commencé à préoccuper l'administration que lorsque les retours de Syrie sont devenus plus nombreux- ils pourraient, par groupes de cinq, être admis en établissements pour mineurs (EPM). La question des jeunes filles -impliquées notamment dans des filières de « mariages express » par téléphone et internet avec des djihadistes- devrait être l'objet de recherches et d'une attention particulière.

D'importantes embauches de personnel sont prévues : notamment un quasi-doublement des binômes de soutien, qui devraient faire l'objet d'une formation et d'un encadrement renforcés.

Que s'est-il passé depuis ? La CGLPL n'a pas encore organisé de nouvelle mission spécifique à ce sujet. En revanche, elle est saisie régulièrement désormais par des avocats, mais aussi par des personnes détenues. Ce sont les mêmes sujets qui reviennent dans la plupart des courriers : l'incompréhension des motifs de placement dans des unités dédiées alors que les personnes étaient détenues en régime ordinaire où elles pouvaient avoir accès à des activités ; la durée bien plus longue qu'annoncée dans l'unité d'évaluation (neuf mois au lieu des huit semaines…) ; l'interdiction de travailler -y compris en cellule- en raison de l'incrimination terroriste ; et surtout, depuis l'agression d'Osny, un régime de détention d'exception, appliqué, selon les courriers reçus, dans plusieurs établissements. Selon les témoignages, du jour au lendemain, les activités auraient été suspendues, qu'il s'agisse de programmes de prise en charge ou d'activités classiques comme le culte collectif, l'enseignement ou le sport ; les changements de cellule seraient fréquents et imprévisibles ; la quantité d'effets personnels autorisée limitée de façon conséquente ; les fouilles -y compris à corps- incessantes ; les parloirs difficiles à obtenir, et les familles victimes de vexations et de contrôles à la rigueur inhabituelle. Plusieurs témoignages parvenus à la CGLPL relèvent l'inquiétude d'intervenants devant l'évolution de personnes détenues placées dans les unités dédiées. Comme la CGLPL en avait émis la crainte lors de son premier rapport, le sentiment d'appartenance à une entité particulière dans la prison, géographiquement clairement identifiée, soumise au même régime dérogatoire de détention, et faisant l'objet d'attentions très particulières des personnels de surveillance, entraîne des solidarités, et des réflexes de défense collectifs. Certaines personnes détenues, qui avaient pu être partie prenante des programmes de prise en charge, auraient récemment opéré un repli sur elles-mêmes, se rendant difficilement accessibles y compris à leurs avocats, qui expriment leur crainte de voir leurs clients s'enfoncer dans un processus de radicalisation de plus en plus profonde.

Dans ce domaine, les faits dont la CGLPL recueille le témoignage ne peuvent être considérés, en eux-mêmes, comme avérés. Des visites sur place nous paraissent parfois nécessaires. Des rapports thématiques, tels que ceux évoqués ici, nous permettent d'étudier les questions soulevées en profondeur.

Des demandes d'explications sont envoyées aux établissements, aux directions d'administration. Il n'est pas rare qu'il faille attendre les réponses pendant plusieurs mois, quand elles arrivent. Et elles n'arrivent pas toujours.

Même si son obstination peut parfois agacer, la CGLPL ne se lasse pas. Toute personne privée de liberté, quelle qu'elle soit, mérite que l'exercice de ses droits fondamentaux soit garanti et respecté.

Notes :

1. Ces documents sont disponibles sur le site du CGLPL, cglpl.fr

COMMENT VIVRE AU TEMPS DU TERRORISME

AUTEURS : ALAIN BAUER, FRANÇOIS FREYNET, CHRISTOPHE SOULLEZ

EDITEUR : FIRST EDITIONS

La France a inventé le concept de terrorisme pendant les années révolutionnaires d'après 1789. Elle a expérimenté à peu près tous les modèles d'attaques, d'opérateurs, de modes opératoires, du couteau de Ravaillac frappant Henri IV à la machine infernale rue Saint Nicaise contre Bonaparte, en passant par la plupart des armes à feu, les explosifs, les enlèvements, etc.

Pourtant, le terrorisme ne fait l'objet d'aucun consensus international sur sa définition.

Jusqu'en 1989, les opérateurs étaient des militants qui passaient à la violence. Comme une continuité extraordinaire du combat politique par d'autres moyens, pour détourner encore une fois Clausewitz.

Depuis la chute du mur de Berlin, le terrorisme est devenu pluriel. On peut désormais parler de terrorismes. Les traditionnels terrorismes d'État ont disparu lentement. Les terrorismes nationalistes irlandais, basques ou colombiens ont opté pour le chemin de la paix.

En 1995 déjà, on assiste à l'apparition d'une toute nouvelle catégorie d'opérateurs : l'hybride, mi-criminel, mi-terroriste. Khaled Kelkal en fut le prototype. Le protagoniste suivant sera Mohammed Merah, 17 ans plus tard.

Pendant cette période, ce qu'on croit devoir appeler Al Qaida génère un hyper terrorisme à partir des unités de combats formées par l'Occident contre les Soviétiques en Afghanistan et qui se révoltent contre leurs créateurs après le départ des troupes russes.

Depuis, le terrorisme a muté et offre une diversité de profils allant du militant en mission au malade mental utilisant les panoplies du moment pour justifier ses actes.

Si le terrorisme d'État est presque silencieux, on assiste à la poussée d'acteurs qui brisent tous les profils traditionnels.

Plus jeunes, plus féminisés, plus convertis, ils couvrent un champ dont la diversité est considérable.

Parfois, ils ne disposent même d'aucune logistique majeure. Ils sont juste mus par une impulsion. On peut dire qu'ils peuvent obéir directement à un ordre de l'État Islamique (puisque c'est son nom, que cela nous plaise ou pas), ce sont alors les lions du Califat. Ils peuvent aussi devenir des sous-traitants, disposant d'une large autonomie (les soldats du Califat). Certains sont eux totalement inconnus et agissent en surfant sur la communication de l'État Islamique qui décidera alors de revendiquer l'opération en termes soigneusement choisis. Il y a une forte décentralisation des attentats selon une logique du nid de guêpes et sans nécessité d'une direction centrale.

En matière de ce qu'on appelle improprement « radicalisation », on découvre que le phénomène prend plus de temps qu'on ne le croit mais l'évolution, eu égard au passé qui nécessitait des voyages et des formations dans des camps d'entraînement, souligne une

accélération sensible. Internet permet de booster le passage à l'acte.

Seules notre capacité à l'amnésie et notre cécité parfois volontaire devant les enjeux d'un monde plus globalisé qui subit la revanche, voire la vengeance, de l'histoire et de la géographie, tout en devant traiter son remords colonial, a généré un affaiblissement de la capacité à répondre aux risques et à trouver des solutions adaptées aux problèmes posés (dont nous sommes souvent les créateurs, plus ou moins involontaires).

Ce que l'État Islamique tente désespérément, c'est d'affaiblir son adversaire au coeur. Attaquer la France dans sa diversité et pousser à l'affrontement fait partie de sa stratégie.

Voici pourquoi il nous a paru utile de publier un guide, outil pratique de « survie en milieu hostile », mais aussi ouvrage permettant de s'y retrouver dans la confusion ambiante sur un sujet plus complexe qu'il n'y paraît.

Certains, angoissés devant la multiplication des risques, peuvent avoir raison et apparaître lucides en parlant de guerre civile. Mais nous ne partageons pas leur pessimisme.

Face au terrorisme, on peut, c'est naturel, décider de se sauver. Tous les ouvrages et toutes les recommandations le disent : « S'échapper, se cacher, alerter ». Il faut sans doute suivre ces recommandations.

Mais nous savons aussi que quelques individus plus courageux, des « héros », ont réussi à désarmer l'agresseur du Thalys, abattre deux des terroristes du Bataclan mettant fin au massacre, dévier le camion de Nice, etc. Et combien d'autres inconnus ont pu sauver des dizaines de vies ?

Se sauver sans doute. Mais on peut aussi se demander si on peut sauver les autres. Surtout dans un contexte où la prise d'otages terroriste régresse face au massacre de masse.

La non-assistance à personne en danger est un objet complexe. Selon le Code pénal « quiconque pouvant empêcher par son action immédiate, sans risque pour lui ou pour les tiers, soit un crime, soit un délit contre l''intégrité corporelle de la personne, s'abstient volontairement de le faire est puni de cinq ans d''emprisonnement et de 75 000 euros d''amende. Sera puni des mêmes peines quiconque s''abstient volontairement de porter à une personne en péril l''assistance que, sans risque pour lui ou pour les tiers, il pouvait lui prêter soit par son action personnelle, soit en provoquant un secours ».

Ce risque pour soi-même est réel. Il ne faut pas le sous-estimer. Mais rien n'empêche justement de le considérer.

La France apprend douloureusement à devenir vigilante, résiliente. Il lui faudra aussi se montrer résistante.

Accepter de vivre avec le terrorisme, c'est accepter que les espaces publics ne soient pas à l'abri d'une attaque et que tous les lieux ne soient pas défendables. La participation des citoyens à la sécurisation de leur environnement immédiat est donc un impératif.

Au travers de l'action de chacun, la sécurité de tous peut être améliorée.

Plus qu'un guide individuel de survie en cas d'attaque, le propos de cet ouvrage est donc de comprendre les mesures mises en oeuvre par les gestionnaires publics ou privés d'espaces ouverts au public et de donner les clés pour inscrire l'action individuelle dans ce dispositif collectif.

La puissance, le nombre et la diversité des attaques menées contre la France remettent en cause l'organisation publique et privée de la sûreté. Notre pays ne peut pas protéger toutes les cibles potentielles, depuis les cibles supposées « dures » (le Stade de France ou le Bataclan le 13 novembre 2015) jusqu'aux cibles dites « molles » (les terrasses de café le 13 novembre ou la promenade des Anglais à Nice, le 14 juillet 2016).

Dès lors, les espaces dans lesquels nous évoluons doivent être sécurisés par l'action individuelle autant que collective, c'est une condition pour que les prochaines attaques, s'il doit y en avoir, soient moins meurtrières.

Dans ce contexte, l'attitude des citoyens dans les espaces publics peut être résumée dans l'ordre suivant :

1. Être attentif à l'environnement physique et humain : ne pas être surpris par les personnes et les lieux, savoir

reconnaître lesquels sont le plus à risque, y adapter son attitude, se reconnecter avec son environnement pour détecter les alertes éventuelles.

2. Anticiper une attaque et repérer les points d'échappatoire latéraux et arrière et de mise à l'abri :, se placer en fonction de ceux-ci, être en capacité de ne pas repartir par l'endroit où on est arrivé. En fonction du niveau de criticité de son environnement, il est possible de gagner de précieuses secondes, en ayant anticipé la direction dans laquelle il est le plus juste de se déplacer et les endroits où l'on peut le mieux se protéger (même quand ils sont derrière soi).

3. Réagir en cas d'attaque avec des réflexes de survie, fuir en se baissant, se mettre à l'abri, puis porter secours. Par défaut, se cacher.

4. Accepter l'événement et faire face est aussi une possibilité. Il y aura des héros à chaque attaque, sauveurs ou sauvés, et ils pourront faire partie des survivants. Le combat, même inégal, est soit une ultime réaction, soit un choix instinctif qui ne mène pas toujours au sacrifice. Il n'y a pas de bon ou de mauvais comportement, il y a une première condition qui est de rester vivant pour porter assistance et/ou se défendre, chaque action portant en elle son contenu d'héroïsme et d'humanité.

Les nouveaux modes de revendication

La nécessité de vivre avec le terrorisme pour le citoyen, potentiel témoin ou victime, doit être comprise comme la nécessité de vivre avec l'acte terroriste, qui n'est plus un concept lointain, télévisé, virtuel.

Aussi, au-delà des définitions possibles du terrorisme, il est utile de comprendre ce qui caractérise l'acte terroriste et donc, ce qui le différencie de l'acte criminel simple.

Parmi les théories qui se sont développées en la matière, une des plus largement acceptées est celle dite du « triangle du passage à l'acte ».

Selon cette analyse, qui sous-tend l'essentiel des politiques publiques et privées de lutte contre la criminalité depuis plus de 50 ans, il faut réunir trois conditions pour qu'un criminel passe à un acte réfléchi :

- La motivation : qui peut être l'appât du gain, la revanche, la haine personnelle, la passion, etc.
- La facilité, qui doit être considérée comme relative, c'est-à-dire en rapport à un autre espace ou un autre temps qui générerait la même motivation, mais serait mieux protégé.
- L'anonymat ou l'impunité, condition pour ne pas être pris ou ne pas être trop fortement puni, là encore relativement à un autre espace ou un autre moment qui générerait la même motivation.

Ces conditions sont effectivement présentes dans la plupart des actes criminels, en dehors des phénomènes dits d'impulsion ou d'opportunité où aucune n'est réellement nécessaire. Ainsi un toxicomane en manque, passant devant une agence bancaire, va entrer, menacer un employé avec sa seringue en affirmant qu'il est porteur du sida et demander quelques dizaines d'euros. Il va être bloqué dans le sas, filmé par le système de vidéoprotection, arrêté, mais il est quand même passé à l'acte, sans réelle motivation, sans tenir compte de la difficulté ni du risque, mais en ayant pu faire des victimes.

Mais pour tout acte réfléchi, cette idée du calcul d'un rapport enjeu/facilité/risque est un puissant moyen déterminant et donc un puissant outil de travail pour ceux qui luttent contre le crime : baisser les motivations, augmenter la difficulté du passage à l'acte, limiter l'anonymat et l'impunité.

L'ensemble des politiques développées par les services publics et privés de sûreté est basé, sans toujours le savoir, sur cette théorie qui tient lieu de prose. On a ainsi réduit les fonds stockés dans les banques (motivation), augmenté les mesures de protection – blindages, sas, guichets – (facilité) et mis en oeuvre des moyens d'identification avec la vidéoprotection (anonymat).

Les conditions de passage à l'acte sont plus complexes à appréhender dans le cadre d'un acte terroriste :

- la motivation est bien présente sous forme d'une idéologie ou d'une croyance.
- La facilité relative est effectivement présente, mais à

une échelle différente comme nous le verrons par la suite.

– L'anonymat ou l'impunité, par contre, ne rentre que peu en jeu, voire agit dans des proportions inverses.

La revendication caractérise l'acte terroriste

Au final, et au regard de ces trois conditions, ce qui différencie un acte terroriste d'un acte criminel simple est la revendication exprimée ou supposée : le contenu des actes criminels menés dans le cadre d'une action terroriste a toujours une qualification de droit pénal commun. Cette action ne devient « terroriste » que lorsqu'elle est revendiquée par un groupe ou un individu qui alors la justifie.

On a ainsi constaté lors des vagues d'attentats commis depuis les années 1970 que la recherche de notoriété ou de reconnaissance était systématiquement présente car elle permettait la revendication par des groupes ou des individus qui, autrement, auraient eu des difficultés à s'approprier l'événement.

Les groupes « historiques » avaient mis en place des moyens de revendication parfois particulièrement élaborés.

Ainsi, les « terroristes irlandais ou corses » disposaient de codes de reconnaissance avec les autorités publiques, de façon à être certains qu'un acte ne pouvait pas être revendiqué par d'autres. Ces réseaux, fonctionnaient pour la plupart comme les institutions qu'ils combattaient, de manière pyramidale, avec une hiérarchie, un leader, des disciplines individuelles et collectives, des règles énoncées, etc. Nous étions en univers connu.

Petit à petit, ces groupes ont évolué, ils ne fonctionnent plus comme un organisme centralisé mais presque comme un réseau social et des dérives individuelles ou collectives extrêmement rapides et fluctuantes.

De ce point de vue, Al Qaïda a généré un moment charnière avec, en même temps, des formes de terrorisme à l'ancienne et, déjà, des éléments modernes. Si on devait caricaturer, les criminels des attentats du 11 septembre sont devenus des « terroristes », lorsqu'ils ont retiré leurs casquettes en passant sous les caméras de vidéosurveillance des aéroports pour être sûrs d'être identifiés *a posteriori*. Ils signaient ainsi leurs actes à venir.

L'absence d'anonymat est devenue un moyen de revendication, même dans le cas de l'État Islamique qui tente une revendication post/ante centralisée d'actes impulsifs individuels plus ou moins provoqués, automotivés, organisés. Mais qui insiste beaucoup sur l'allégeance préalable.

Ce constat détermine les moyens de lutte : le levier de l'anonymat n'est plus une condition de passage à l'acte, le levier de la reconnaissance l'est.

C'est une des difficultés que nous allons devoir affronter dans les années qui viennent, nos méthodes traditionnelles sont très peu efficaces dans ce domaine. Nous ne pouvons agir contre la motivation que de manière marginale, les risques liés à la rupture d'anonymat ou d'impunité sont sans effet. Il ne nous reste qu'à travailler sur la facilité, avec un rendement de plus en plus faible.

Cette faiblesse structurelle du corpus théorique explique une grande partie de l'impuissance de la plupart des États ciblés qui ont fondé toute leur protection sur cette « prose ». On a déjà voulu faire perdre la nationalité aux auteurs d'actes terroristes. On pourrait tout autant promettre la peine de mort aux kamikazes que cela n'aurait guère d'effet sur eux.

Le levier de la reconnaissance est une piste de travail forte pour les services de renseignement. La rapidité avec laquelle les assaillants sont identifiés *a posteriori* démontre que les données disponibles sont bien présentes. L'enjeu est de transformer ces informations en moyens de lutte *a priori*.

L'espace de moins en moins défendable

Au-delà du triangle du passage à l'acte, l'autre grand champ théorique qui a guidé les 50 dernières années de la sécurité publique est celui dit de « prévention situationnelle ».

Les urbanistes Oscar Newman et Jane Jacobs sont à l'origine du concept de prévention situationnelle (ou de prévention par l'architecture – « *defensible space* »), au début des années 1970. L'idée consistait alors à réduire le passage à l'acte criminel et le sentiment

d'insécurité par l'urbanisme et l'architecture.

En 1961, Jane Jacobs émettait l'hypothèse que les rues sont plus sûres si les habitants peuvent les identifier comme leur propre espace. D'après elle, les rues sont dangereuses parce qu'elles sont désertes.

La solution consistait donc à :

- rétablir une distinction claire entre espace privé et espace public,
- orienter les constructions vers la rue pour faciliter une surveillance naturelle des habitants sur les espaces extérieurs à partir de leur logement,
- augmenter la fréquentation des rues jusqu'à en faire des lieux d'activité continue.

De fait, si l'occupation de la rue est une manière d'appropriation de l'espace, elle génère aussi plus d'opportunités de délits, provoque une augmentation des nuisances. En outre, si la surveillance est rendue possible, elle n'est pas pour autant effective, car elle dépend des motivations individuelles à intervenir. Jacobs fondait sa théorie sur le mythe d'un citoyen parfait.

Dix ans plus tard, Oscar Newman développe le même point de vue dans *Defensible Space*. Les espaces extérieurs seront mieux défendus contre la criminalité s'ils sont mieux surveillés par les habitants. Il faut donc dessiner un urbanisme qui facilite la surveillance informelle.

Newman fut fortement critiqué pour le déterminisme de sa théorie. Ces critiques le conduisirent à revoir le concept d'espace défendable selon lequel des communautés d'intérêts peuvent émerger sur des groupes d'habitants possédant le même mode de vie, le même âge et le même cycle familial. Il faut construire des immeubles pour des personnes de la même communauté d'intérêts, l'architecture et l'urbanisme étant des facteurs de cohésion ou de désorganisation sociales.

Certes, la réalité a montré depuis que le concept est très critiquable et que les affectations massives de populations à profils identiques ont également mené à des désordres dans les quartiers, voire à des émeutes.

Cependant, les principes de prise en compte des contraintes de sûreté dans les politiques d'aménagement et d'urbanisme ont été formalisés. La séparation entre espace privé et espace public, le marquage territorial, la limitation de la hauteur des bâtiments, les nouveaux procédés de surveillance formelle et informelle, l'appropriation « naturelle » de l'espace découlent de Jacobs et Newman.

La prévention situationnelle est une voie qui tente d'influencer à la fois les comportements criminels et les actions civiques.

Pour les premiers, une plus grande surveillance, un meilleur management des espaces sont des éléments contraignants. Pour les seconds, un environnement concourt à une augmentation des comportements civiques.

L'application réglementaire de ces principes s'adapte aujourd'hui à l'évolution des menaces terroristes et tend à agir dans le sens de l'espace défendable, c'est-à-dire à durcir les cibles, à mieux contrôler les accès, avec le support de la vidéoprotection, à améliorer la résistance des bâtiments, etc.

Mais, comme on l'a vu dans le retour d'expérience, cette notion d'espace défendable a perdu une partie de son sens pour plusieurs raisons.

Les moyens de durcissement des cibles, agissant sur la facilité du passage à l'acte perdent de leur efficacité lorsqu'ils doivent être dimensionnés par rapport à des risques d'attaques par des moyens de guerre. Pour schématiser, on ne peut pas construire la Canopée des Halles en la dimensionnant pour résister à un risque de bombardement. Comme pour le reste de nos moyens de défense de temps de paix, les bâtiments et les aménagements sont prévus pour résister à des attaques de temps de paix.

Le contrôle des accès n'a de sens que si les espaces peuvent être fermés et que les publics présents à l'extérieur et à l'intérieur sont différents (en laissant *a priori* les attaquants plutôt à l'extérieur). Or, on l'a vu, les attaquants sont, pour beaucoup, déjà à l'intérieur, et les points de filtrage ne constituent en fait qu'un point de passage entre un espace ouvert et un autre espace ouvert, avec les mêmes personnes présentes dedans et dehors.

Les moyens d'identification, notamment la vidéoprotection, ont aujourd'hui un rôle préventif

faible sur ces attaques terroristes même s'ils sont déterminants pour l'analyse *a posteriori*.

L'augmentation du risque du passage à l'acte a peu de sens face à des individus qui viennent pour mourir, le risque majeur pour eux étant de ne pas réussir à emporter avec eux un suffisamment grand nombre de victimes.

La réduction des gains et des excuses pour le passage à l'acte n'a pas de sens dans le cadre d'actes terroristes qui ont leur propre logique de bénéfice, souvent irrationnelle et difficile à comprendre *a priori*.

Enfin, la surveillance naturelle (ou par les citoyens) ne peut fonctionner que dans un cadre clair de cohérence entre l'action publique et la situation individuelle, ce qui n'est quasiment plus jamais atteint dans la situation actuelle. D'une part, on l'a vu, l'incapacité de l'État à graduer le niveau d'alerte est génératrice d'une « dés-adhésion » citoyenne, d'autre part, on ne peut pas cacher qu' il existe des sympathisants aux causes terroristes.

Encore faudrait-il que l'action citoyenne attendue soit clairement identifiée et dispose d'un rôle dans le panel des réponses institutionnelles, ce qui n'est pas le cas lorsque l'ensemble des réponses se résume en une « punch line » : « fuyez et cachez-vous » (« *run and hide* ») et une supplique immédiate et impérative : « ne stigmatisez pas ».

Cette succession d'actes terroristes aboutit de fait à une remise en cause d'une certitude: elle signe en réalité la fin de la théorie de l'espace défendable. Plus tôt nous comprendrons ce phénomène, plus vite nous mettrons en place des outils de résistance et non plus de simple résilience.

Le fait d'accepter la notion d'espace indéfendable amène à une logique différente de celle développée aujourd'hui. La concentration des moyens de sûreté n'est plus dans la protection statique d'un espace, mais dans la protection dynamique des personnes qui s'y trouvent.

Dans des attaques en mouvement, la ligne du temps est devenue un risque et plus un allié. Si l'on doit caricaturer, sur les actes terroristes récents il y a un acte initial qui produit rapidement un grand nombre de victimes, puis une progression avec des victimes supplémentaires, qui va plutôt en diminuant au rythme de la diffusion de l'alerte, puis une réaction qui termine la phase d'action terroriste.

Ainsi, chaque attaque connaît son lot de drames, d'individualismes, de désespoirs et d'espoirs, et aussi de héros. Les soldats américains qui sont intervenus lors de l'attaque du Thalys se sont comportés en héros et ils ont évité des dizaines de morts.

Toutes les victimes d'un attentat terroriste sont des héros, précipités dans un univers de violence auquel elles n'étaient ni destinées ni généralement préparées. Mais certaines iront au-delà des recommandations de précaution et de survie et choisiront de combattre. Cela fait partie de l'acceptation de l'acte terroriste.

Il ne doit pas y avoir d'échelle de valeurs dans ces termes, le héros, mort ou vivant, est celui qui a contribué à sauver des vies dans des circonstances où il s'est mis lui-même en danger. Il n'y a pas de bon choix dans ces circonstances. Tous les choix sont mauvais et peuvent potentiellement mener à une mise en danger supplémentaire.

Que ce serait-il passé si les passagers du Thalys avaient fui au lieu de combattre? Combien de vies l'homme qui a précipité son scooter sous le camion-bélier de la promenade des Anglais a-t-il sauvées en ralentissant ou déviant le camion ?

Alors, évidemment, aucun d'entre nous ne sait comment il réagirait s'il était confronté à un tel événement, y compris ceux qui l'ont déjà vécu. Évidemment, l'État ne peut demander à personne d'agir avec héroïsme et il ne suggère finalement que la fuite et la survie. Évidemment, aucun des dispositifs collectifs que nous avons décrits ne peut se baser sur ces réactions individuelles exceptionnelles.

Mais vivre avec le terrorisme, c'est aussi accepter une situation de guerre à un moment donné de notre vie en paix. C'est vivre en citoyen actif. Et être prêt à la réaction combattante lorsqu'il n'y a plus d'autre choix.

LES PARTICULIERS VICTIMES D'ACTES DE CYBERMALVEILLANCE

ADELINE CHAMPAGNAT

COMMISSAIRE DE POLICE,
CONSEILLER À LA DÉLÉGATION MINISTÉRIELLE AUX INDUSTRIES DE SÉCURITÉ ET À LA LUTTE CONTRE LES CYBERMENACES (DMISC)

Le 18 juin 2015, lors de la présentation de la stratégie pour la sécurité du numérique du Gouvernement, le Premier ministre, Manuel VALLS, annonçait la mise en place à venir, d'un dispositif national d'assistance aux victimes d'actes de cybermalveillance.

La cybermalveillance peut être définie comme "*l'intention criminelle de nuire à quelqu'un, de porter atteinte à sa personne, à ses biens*"[1] lorsqu'il est un utilisateur des réseaux informatiques. Ce mot rappelle aussi l'expression "*logiciel malveillant*" ou "*maliciel*" (en anglais : *malware*), programme informatique développé dans le but de nuire à des systèmes informatiques (virus, Vers, chevaux de Troie notamment).

Juridiquement, le concept de "*cybermalveillance*" englobe celui de "*cybercriminalité*", c'est-à-dire "*l'ensemble des infractions pénales commises sur les réseaux de télécommunication, en particulier Internet*"[2]. On distingue généralement les infractions ciblant les systèmes d'information (SI) de celles commises via les systèmes d'information[3].

Il reste aujourd'hui difficile de mesurer la menace "cyber". Lorsqu'elle est réalisée par les éditeurs de solution de sécurité informatique, cette mesure peut être discutée et parfois manquer d'objectivité.[4] Par ailleurs, les crimes et délits enregistrés par la police et la gendarmerie ne peuvent pas recenser la totalité des cybermalveillances commises : ces infractions ne couvrent qu'une partie des cybermalveillances touchant les particuliers, toutes les victimes d'actes de cybermalveillance ne se font pas connaître et ces agressions d'un nouveau genre peuvent passer inaperçues.

Mais on constate quand même un alignement des diagnostics : escalade de la menace, multiplication des actes de cybermalveillance, sophistication des attaques et aggravation des dommages causés ; les particuliers sont, au même titre que les entreprises ou les collectivités, de potentielles cibles (I). Parce qu'il est de sa responsabilité de protéger ses citoyens dans le cyberespace, l'État améliore sans cesse le traitement des victimes d'actes de cybermalveillance, mais il ne peut agir seul (II).

I. Les actions de cybermalveillance qui touchent les particuliers

Elles sont aujourd'hui réalisées à grande échelle par des groupes criminels qui se sont organisés et ont gagné en efficacité (A). Dans la grande majorité des cas, elles ont pour objectif un gain financier. Ces agressions informatiques peuvent aussi être réalisées à des fins crapuleuses (B).

A. Des cybermalveillances pratiquées à grande échelle par des groupes criminels organisés qui ont gagné en efficacité

"*Organised crime is dynamic and adaptable and law enforcement authorities across the EU are challenged to keep peace with the changing nature of this substantial and significant threat.*"[5]

L'expérience opérationnelle montre en effet l'accélération de la transformation numérique du

paysage de la criminalité organisée.

Trafiquants de stupéfiants, cyberescrocs, réseaux de pornographie enfantine, contrefacteurs..., Internet offre de multiples possibilités pour ces groupes criminels organisés d'atteindre un grand nombre de victimes potentielles, à court terme, à très faible coût et avec de nombreux avantages : éloignement par rapport aux victimes, échanges facilités entre complices, anonymisation, caractère transfrontalier de la fraude, possibilités multiples de blanchiment d'argent provenant de leurs activités illicites.

Ces groupes relevant de la criminalité organisée traditionnelle se sont très vite appropriés le net, non seulement pour commettre leurs méfaits mais aussi pour la vente des marchandises mal acquises. Produits stupéfiants, armes, faux billets, images pédopornographiques, données bancaires ou personnelles volées...sont vendus et achetés en monnaies virtuelles (telles que le *Bitcoin*) sur des marchés parallèles (notamment sur le *darkweb*[6]).

Ainsi, "*à l'origine conçue comme une succession de défis à la sécurité des réseaux, la cybercriminalité se teinte désormais d'une coloration mafieuse, donnant naissance à de véritables « marchés noirs » d'informations piratées, allant des atteintes à l'identité et à la propriété intellectuelle et artistique, aux fraudes à la carte bancaire. La criminalité classique et la criminalité informatique entretiennent des liens étroits, et les cybercriminels font de plus en plus partie de réseaux internationaux très organisés.*" [7]

En effet, peu de criminels ont les connaissances et/ou les capacités nécessaires à la création de logiciels malveillants. Ils vont donc s'offrir les services de programmeurs ou codeurs de haut niveau qui fabriquent derechef ou sur demande des virus, chevaux de Troie, Vers ou autres maliciels. Ces concepteurs de logiciels malveillants les utilisent eux-mêmes ou les vendent sur Internet, généralement sur des forums spécialisés et confidentiels, y compris sur le *darkweb*, proposant même parfois un service d'aide en ligne. Ils doivent aussi louer des serveurs pour lancer leur attaque, recruter des individus prêts à servir de mules pour acheter des marchandises avec des données bancaires volées ou les réceptionner, s'acheter les services d'experts en montage financier pour blanchir leurs profits et brouiller les pistes de la fraude ainsi que d'autres personnels spécialisés dans le domaine des télécommunications pour agir en toute discrétion (notamment avec l'utilisation de techniques d'anonymisation et de chiffrement).

Il reste aussi possible pour les criminels de faire appel aux botmasters, ces délinquants qui contrôlent les BotNets (contraction de "*Robots of the Network*"), qui permettent notamment la diffusion ou l'installation de virus de récupération de données personnelles (y compris bancaires) ou l'envoi de spam de *phishing*. Les BotNets sont des réseaux de machines (ordinateurs, téléphones mobiles, tablettes...) qui ont été infectés par un logiciel malveillant permettant leur contôle à distance (on parle alors de machines Zombies). Ils sont composés de plusieurs milliers voire plusieurs centaines de milliers d'ordinateurs.

On voit que contrairement à ce que l'on peut penser de prime abord, il ne suffit pas de fabriquer ou d'acquérir un logiciel malveillant pour réussir une cyberattaque, mais bien de pouvoir compter sur un réseau de criminalité plus ou moins structuré.

B. Des actions de cybermalveillance plus ou moins ciblées

i. Des actions de cybermalveillance génériques

Les actions les plus nombreuses sont génériques, en ce sens qu'elles ne visent aucune cible particulière. Il s'agit notamment des attaques par spam qui véhiculent l'essentiel des escroqueries[8] sur Internet (*Phishing*, les escroqueries aux faux héritages, contrats de travail, épargnes, loteries, spam sms[9], spam vocaux[10]...) et logiciels malveillants tels que les malwares bancaires (qui permettent la récupération des données bancaires) ou encore les *rançongiciels*.

Les *rançongiciels* (*Ransomware* en anglais) sont une catégorie particulière de logiciels malveillants qui bloquent l'ordinateur des internautes et réclament le paiement d'une rançon (généralement en *Bitcoin*), pour en obtenir à nouveau l'accès. Depuis 2013, une variante est apparue avec des virus chiffrants ou cryptovirus[11]. Cette nouvelle forme de rançongiciels chiffre les documents se trouvant sur l'ordinateur cible, voire sur des serveurs qui hébergent les données. Les cybercriminels communiquent généralement la clé de déchiffrement une fois le

paiement de la rançon effectué, mais ce n'est jamais une garantie. De tels procédés relèvent de l'extorsion de fonds et non pas de l'escroquerie. En effet, ils se caractérisent par une contrainte physique - le blocage de l'ordinateur - obligeant à une remise de fonds non volontaire. L'infraction d'atteinte à un système de traitement automatisé de données (STAD) peut aussi être retenue soit du fait d'une modification frauduleuse de données soit d'une entrave au bon fonctionnement d'un STAD[12]. La commission de ces infractions requiert en principe la mise en oeuvre de différentes compétences et donc l'intervention de plusieurs personnes (conception, injection du virus, expédition du mail infecté, collecte de la rançon), caractérisant ainsi la circonstance aggravante de bande organisée. Pour l'année 2016, ce sont 10 475 infractions d'atteinte aux systèmes de traitement automatisé de données (STAD) qui ont été traitées par les services de police et de gendarmerie[13].

ii. Des actions de cybermalveillance ciblées

Les particuliers peuvent être aussi victimes d'attaques plus ciblées. Il s'agit notamment des escroqueries aux fausses annonces sur Internet, des escroqueries à la romance ou à la fausse amitié, ou encore du chantage à la webcam. Ces actes de cybermalveillance ne font appel à aucune technique d'attaque particulière, mais elles sont facilitées par l'Internet, voire dans les cas de harcèlement, de "*revenge porn*"[14], de diffamation ou d'injures publiques, amplifiées[15] par la caisse de résonnance des réseaux sociaux (Facebook, Twitter, Google +). On parle dans ce dernier cas de diffusion virale de tels propos.

L'enquête annuelle de victimation "cadre de vie et sécurité"[16] montre une augmentation du nombre de victimes en France de menaces ou d'injures commises par courrier électronique ou sur les réseaux sociaux entre 2006 et 2016. En 2006, 95 000 personnes déclaraient ainsi avoir subi au moins une menace par courrier postal, électronique ou sur réseaux sociaux au cours des deux années précédentes tandis qu'elles sont au nombre de 197 000 en 2015 (+106%). Le nombre de victimes d'injures augmente aussi, passant de 104 000 en 2007 à 160 000 en 2016 (+ 53%).

L'usurpation d'identité "numérique"[17] est une autre infraction commise sur un réseau de communication au public en ligne (messageries électroniques, sites web, messages publiés en ligne et profils en ligne sur les réseaux sociaux). Le préjudice effectif ou éventuel s'analyse en un trouble de la tranquillité de la personne dont l'identité est usurpée ou celle d'un tiers, ou en une atteinte à son honneur ou à sa réputation[18].

Certains professionnels sont aussi victimes d'actes de cybermalveillance. C'est le cas des artistes victimes des sites de streaming ou de téléchargement illégal[19], des personnels humanitaires qui sont régulièrement ciblés dans les pays dans lesquels ils exercent. Kim Aumonier des brigades de paix internationales fait notamment état d'attaques régulières à l'encontre des "défenseurs des droits humains": ces attaques visent leurs données personnelles ou sont commises sur les réseaux sociaux (menaces...)[20].

Les cyberattaques peuvent aussi spécifiquement viser le fonctionnement même des processus démocratiques. Ce risque a d'ailleurs été jugé d'un niveau suffisamment élevé pour que le Gouvernement décide de retirer la possibilité pour les Français résidant à l'étranger, de voter en ligne aux législatives de juin 2017[21].

Enfin, les nouveaux usages du numérique (objets connectés[22], smart cities[23]), peuvent comporter des risques pour leurs utilisateurs. À titre d'illustration, la presse s'est faite l'écho du piratage possible de véhicules roulant connectés allant jusqu'à leur prise de contrôle[24].

II. Le traitement des victimes d'actes de cybermalveillance

" *L'État a le devoir d'assurer la sécurité en veillant, sur l'ensemble du territoire de la République, [...] à la protection des personnes et des biens*" [25].

Il revient à l'État, et en premier lieu au ministère de l'Intérieur, d'assurer la protection des particuliers contre les cybermalveillances. La nouvelle délégation ministérielle aux industries de sécurité et à la lutte contre les cybermenaces (DMISC)[26] a été chargée de jeter les bases de la stratégie du ministère de l'Intérieur en matière de lutte contre les cybermenaces afin d'assurer une protection efficace et adéquate des utilisateurs des réseaux informatiques. Elle compte deux volets opérationnels : le premier est celui de la prévention. Il est en effet essentiel de prévenir et d'éduquer, de trouver des parades techniques, culturelles et comportementales à ces agressions d'un nouveau

type (A). Le second volet opérationnel est celui de la réaction (B).

A. La prévention

Pour être en capacité d'adapter la réponse à apporter aux atteintes à la cybersecurité, le ministère de l'Intérieur s'est organisé pour disposer d'un état actualisé chiffré et qualitatif des cybermenaces. Les directions concernées concourent à l'élaboration d'une synthèse recensant l'état des cybermenaces contre la France, ses réseaux gouvernementaux, ses intérêts fondamentaux, ses acteurs économiques et sa population.

i. Une campagne de sensibilisation des internautes

La sensibilisation des internautes sur les risques encourus et les moyens de protection existants contribue aussi dans une large mesure à réduire les risques numériques et à motiver les utilisateurs des réseaux informatiques à participer activement au renforcement de leur propre cybersécurité. Aussi, près de 550 référents de la police nationale, de la préfecture de police et de la gendarmerie nationale ont vu leurs compétences renforcées afin de permettre aux particuliers, aux entreprises et aux collectivités qu'ils conseillent de mieux se prémunir contre les cybermenaces.

L'opération « Permis Internet » initiée en 2014 et conduite par les services de police et de gendarmerie, permet aux élèves de CM2 et à leurs parents, d'assimiler plus facilement les règles élémentaires de prudence et de civilité, que chacun doit adopter sur Internet. Ce sont à ce jour 750 000 élèves qui ont pu bénéficier de cette sensibilisation et acquérir les gestes réflexes de la navigation sur le net.

Des actions de sensibilisation sur les risques de cybermalveillance sont aussi mises en oeuvre par un certain nombre d'associations, telles que le CECyF (Centre Expert contre la cybercriminalité Français)[27], Antibot[28], Signal Spam[29], Phishing Initiative[30], la plateforme 33 700[31] (qui permet de lutter contre les spam sms et spam vocaux), l'AFPI (l'association française des prestataires de l'Internet) notamment dans le cadre de sa mission de lutte contre les contenus odieux sur Internet[32], ou l'association e-enfance[33].

Des actions complémentaires devraient à terme être mises en oeuvre par l'État. Un groupe de travail placé sous la présidence conjointe de l'Agence nationale de sécurité des systèmes d'information (ANSSI)[34] et du ministère de l'Intérieur entre mars et octobre 2015 a émis un certain nombre de propositions dans le domaine de la sensibilisation :

- développer une campagne de sensibilisation annuelle à destination du grand public, comme il existe en matière de sécurité routière ;

- co-produire ou co-développer, avec les médias appropriés ou des prestataires privés, des programmes courts audiovisuels de sensibilisation (sous forme de fictiopns ou de programmes éducatifs). Il est aussi envisagé de donner une visibilité plus forte à des contenus créés par des partenaires externes qui seraient ensuite recommandés voire labellisés.

- fédérer l'ensemble des outils et campagnes de sensibilisation touchant au cyber sous une même signalétique ou "marque" et référencer l'ensemble d'entre elles sur un portail d'information qui pourrait accueillir des contenus complémentaires. Il s'agit là d'une proposition complémentaire au programme "Internet sans crainte"[35] à destination des jeunes publics, développé sous l'égide de l'Agence du numérique.

ii. Des mesures de blocage et de déréférencement de certains sites Internet

Le législateur a élargi le cadre préventif. La loi du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme permet de mieux prévenir un certain nombre de comportements cybercriminels.

L'OCLCTIC (office central de lutte contre la criminalité liée aux technologies de l'information et de la communication) a été désigné comme autorité administrative chargée de mettre en oeuvre, à titre préventif, les mesures de blocage et de déréférencement les sites Internet à caractère pédopornographique ou faisant l'apologie du terrorisme voire concourrant à sa provocation. En 2016, 834 demandes de blocage, 1929 demandes de déréférencement et 3129 demandes de retrait ont été adressés par l'OCLCTIC aux professionnels de l'Internet. Des milliers de connexions à des pages pédopornographiques et à de la propagande terroriste ont ainsi été empêchées, protégeant les internautes du visionnage d'un contenu choquant et potentiellement dangereux accessible au hasard des navigations et des liens proposés.

iii. Un dispositif d'assistance aux victimes d'actes de cybermalveillance

D'autres outils sont aussi mis à

disposition des particuliers telle que la plateforme téléphonique info-escroqueries, hébergée par la direction centrale de la police judiciaire (DCPJ) et chargée d'informer, de conseiller et d'orienter les personnes qui pensent être victimes d'une escroquerie. Composée de policiers et de gendarmes, cette plateforme reçoit une centaine d'appels par semaine. Ils concernent essentiellement des fausses annonces sur Internet, du phishing, des escroqueries à la romance, chantage à la web-cam et ransomwares.

L'internaute qui, au cours de sa navigation sur Internet, se trouve confronter à des contenus ou comportements illicites doit aussi pouvoir compter sur la présence de l'État dans le cyberespace. C'est l'un des objectifs de la plateforme de signalement des contenus illicites de l'Internet, dénommée PHAROS, du nom de l'île qui pendant près de dix-sept siècles porta le phare d'Alexanderie. En 2016, PHAROS a reçu des internautes 170 721 signalements : 49% concernaient des escroqueries, 11% des atteintes aux mineurs, 10% des discriminations et 7% des faits d'apologie et de provocation au terrorisme. Ces signalements sont pour partie exploités judiciairement et peuvent aboutir à l'interpellation de l'auteur des contenus ou comportements.

Les victimes d'actes de cybermalveillances sont encouragées à déposer plainte, auprès des services de police et de gendarmerie ainsi que de ceux de la justice qui s'adaptent progressivement à traiter ce type d'affaires. L'État développe des outils pour mieux répondre aux attentes de proximité des internautes. Il poursuit ainsi la dématérialisation des démarches citoyennes. Deux téléservices devraient être proposés à plus ou moins court terme aux internautes victimes : le dispositif de signalement en ligne des usages frauduleux de cartes bancaires (PERCEVAL) et un système de plainte en ligne dédié aux escroqueries sur Internet (THESEE).

Enfin, les victimes, outre la possibilité de déposer plainte en cas d'infractions cyber, doivent aussi par exemple pouvoir être orientées vers un service de traitement de l'incident informatique. le Gouvernement a ainsi décidé la mise en place d'un dispositif d'assistance aux victimes d'actes de cybermalveillances. Il repose sur une plateforme numérique intéractive. Cette plateforme devra faciliter la mise en relation des victimes après un parcours d'auto-diagnostic (sur la base d'un formulaire d'orientation) avec une assistance de proximité : intervenants susceptibles d'assister techniquement les victimes (réparateurs informatiques, associations d'entraide, sociétés spécialisées dans la réponse à incident informatique) et services de l'Etat concernés (police nationale, gendarmerie nationale, coordinateurs territoriaux de l'ANSSI et autres).

B. La réaction

i. Les services centraux spécialisés de la police et de la gendarmerie

Il est aussi très vite apparu que, pour faire face à l'augmentation des cybermalveillances et à l'utilisation des outils numériques par les terroristes, le ministère de l'Intérieur devait se doter de moyens importants pour améliorer l'efficacité de son action. Les services centraux spécialisés de la police (la sous-direction de la lutte contre la cybercriminalité ou SDLC) et de la gendarmerie (le Centre de lutte contre la criminalité numérique ou C3N) ont été renforcés.

Les 12 laboratoires d'investigation opérationnelle du numérique (LION) récemment installés par la SDLC dans les services territoriaux et centraux de la DCPJ, et les plateaux criminalistiques départementaux de la gendarmerie nationale doivent permettre de mieux traiter la preuve numérique indissociable du travail d'enquête, lutter contre les organisations criminelles qui sévissent sur ou à partir du Web et traiter la délinquance numérique de proximité.

ii. Un renfort législatif face aux nouvelles menaces

Pour faire face aux actions cybercriminelles, il faut aussi au besoin adapter le cadre juridique. Dès 2014, face à l'émergence de nouvelles menaces terroristes, le législateur a prévu de nouvelles dispositions qui permettent de mieux réprimer ces comportements. Certaines dispositions visent singulièrement à mieux appréhender la cybercriminalité et à renforcer la répression pénale des faits de provocation aux actes de terrorisme et d'apologie du terrorisme.

La loi n° 2016 -731 du 3 juin 2016 renforce encore l'efficacité de la lutte contre la criminalité organisée et le terrorisme. Ce texte durcit la réponse pénale. Il vise à lutter plus efficacement contre la propagande djihadiste en ligne.

La loi s'est aussi adaptée en créant un nouveau critère de compétence : celui du domicile

de la victime: "*tout crime ou tout délit réalisé au moyen d'un réseau de communication électronique, lorsqu'il est tenté ou commis au préjudice d'une personne physique résidant sur le territoire de la République [...], est réputé commis sur le territoire de la République*"[36]. Cet ajout s'explique par la difficulté à lutter contre cette délinquance complexe et souvent internationale[37].

Toutefois, en créant ce nouveau critère de compétence, le législateur ne consacre pas pour autant une compétence universelle des juridictions françaises. Un arrêt de la Cour de cassation en date du 12 juillet 2016 a en effet rappelé que la compétence des juridictions françaises ne peut être rentenue que si les contenus illicites sont à destination du public français[38].

La loi a aussi instauré une compétence concurrente de la juridiction parisienne (procureur de la République, pôle de l'instruction, tribunal correctionnel et Cour d'assises de Paris) en matière de cybercriminalité. L'article 706-72 nouveau du Code de procédure pénale dispose en effet que les atteintes aux systèmes de traitement automatisés de données (STAD)[39] sont poursuivis, instruits et jugés selon des règles particulières fixées par les articles 706-72-1 à 706-72-6 du Code de procédure pénale. Toutefois, les infractions commises au moyen des technologies de l'information, soit pour véhiculer des contenus illicites, soit pour faciliter la commission d'une autre infraction, ne sont pas concernées par cette compétence concurrente.

Dans l'intérêt des victimes et afin de tenir compte des nouvelles méthodes et techniques d'investigation, de recueil et de conservation des preuves (y compris numériques), la loi n° 2017-242 du 27 février 2017 double les délais de prescription de l'action publique de droit commun en matière criminelle et délictuelle, tout en maintenant leur point de départ au jour de la commission de l'infraction. Des régimes dérogatoires pour certaines infractions relevant de la cybercriminalité sont en revanche maintenus : le délai dérogatoire de 10 ans à compter de la majorité de la victime s'applique toujours aux délits de proposition sexuelle à un mineur de quinze ans via un moyen de communication électronique, et à ceux de fabrication, transport, diffusion ou commerce d'un message à caractère violent ou pornographique, ainsi que les infractions relatives au matériel pédopornographique. Il doit enfin être noté que les délits de provocation ou d'apologie du terrorisme ou de consultation habituelle de sites terroristes se prescrivent par vingt années révolues à compter de la date à laquelle la décision de condamnation est dévenue définitive[40].

Enfin, la loi sur la République numérique pénalise le "*revenge porn*"[41], c'est-à-dire le fait de partager des photos sexualisées d'une personne sans son consentement, à des fins malveillantes, généralement après une rupture.

iii. La participation du secteur privé à la lutte contre les cybermalveillances

Les cyberattaques, pour la grande majorité d'entre elles sont organisées et lancées depuis l'extérieur du territoire français. Les données utiles à l'orientation des enquêtes sont donc détenues par des acteurs étrangers de l'Internet. La lutte contre les cybermalveillances ne saurait donc s'envisager sans la participation active du secteur privé, singulièrement de l'industrie du net. C'est dans cet esprit qu'a été institué le groupe de contact permanent (GCP) avec les principaux acteurs américains et français de l'Internet, pour faciliter le travail des enquêteurs dans les affaires les plus graves, et obtenir le retrait rapide de contenus illicites.

Ce groupe travaille aussi avec la Délégation interinistérielle à la lutte contre le racisme, l'antisémistisme et la la haine anti-LGBT (DILCRAH)[42] sur la lutte contre les contenus haineux sur Internet. Ils s'appuient notamment sur l'accord intervenu le 31 mai 2016 entre la commission européenne et les grands opérateurs de l'Internet comprenant une série d'engagements pour lutter contre la diffusion en ligne de discours de haine illégaux en Europe.

iv. La coopération internationale entre les services d'enquête

Il est aussi essentiel de disposer d'un réseau de collaboration actif à l'international sur lequel les enquêteurs français peuvent s'appuyer.

Cette coopération prend la forme de contacts bilatéraux, notamment avec les pays sources de cybercriminalité, tels que avec l'Afrique pour lutter contre les escroqueries sur Internet ou encore avec la Roumanie pour lutter contre la criminalité liée aux cartes bancaires; elle passe aussi par des échanges entre les services compétents des

différents États au sein des instances européennes ou Internationales, telles que Europol, Eurojust et Interpol. Outre le partage d'information, notre objectif est aussi la définition d'approches et de solutions partagées sinon communes. C'est le cas par exemple des travaux européens menés dans le domaine de la disponibilité et de l'accès à la preuve numérique.

Notes :

1. Définition de la "malveillance" par le dictionnaire académique, 1986.
2. Définition de l'Encyclopédie Larousse.
3. Cf. par exemple la distinction opérée par le magistrat Marc Robert dans son rapport « Protéger les internautes, Rapport sur la cybercriminalité ». Pour le télécharger, cliquez sur le lien http://www.ladocumentationfrancaise.fr/rapports-publics/144000372/
4. Cf. le rapport « Etat de la menace liée au numérique en 2017 », produit par la délégation ministérielle aux industries de sécurité et à la lutte contre les cybermenaces, pour le télécharger, cliquez sur le lien :http://www.ladocumentationfrancaise.fr/rapports-publics/174000226/index.shtml
5. Rob Wainwright, Directeur de Europol, présentant le rapport d'Europol *"Massive changes in the criminal landscape: Exploring tomorrow's organised crime", 2 march 2015-03-20, https://www.europol.europa.eu/content/massive-changes-criminal-landscape*.
6. Le *darkweb*, partie du *deepweb* ou web profond par opposition au web de surface, est accessible uniquement au moyen de logiciels d'anonymisation (types TOR) et de configurations spécifiques.
7. Myriam QUEMENER, « Concilier la lutte contre la cybercriminalité et l'éthique de liberté », *Sécurité et stratégie*, 1/2011 (5), p. 56-67. http://www.cairn.info/revue-securite-et-strategie-2011-1-page-56.htm
8. Article 313-1 et article 313-2 du Code pénal.
9. Messages SMS indésirables.
10. Appels vocaux indésirables.
11. Tels que cryptolocker, cryptoDefense, cryptoBit et plus récemment locky, petya ou cryptowall.
12. La loi n° 2015-912 du 24 juillet 2015 relative au renseignement a doublé les peines d'amende encourues (de 75.000 euros à 150.000 euros). Depuis 2013, la détention ou la cession d'un rançongiciel, sans motif légitime, est passible des mêmes peines.
13. Cf. le rapport État de la menace liée au numérique en 2017, publié par la délégation ministérielle aux industries de sécurité et à la lutte contre les cybermenaces (DMISC).
14. Le "*revenge porn*" ou "vengeance pornographique sur Internet" consiste à diffuser un contenu sexuellement explicite sur Internet, sans le consentement de la personne concernée et à des fins malveillantes. Cette pratique est désormais incriminée par l'article 226-2-1 du Code pénal.
15. Articles 29, 32 de la loi du 29 juillet 1881, sur la liberté de la presse.
16. L'enquête "Cadre de vie et sécurité" (INSEE/ONDRP/SSMSI) est une enquête annuelle de victimation réalisée auprès de résidents français de logements ordinaires, dont la collecte a débuté en 2007. Les informations recueillies dans cette enquête portent sur les deux années précédant la collecte et couvrent donc les années 2005-2006 à 2014-2015. Les atteintes liées aux cyberespace ne font pas l'objet d'un module spécifique de l'enquête CVS même si des parties du questionnaire relatives à certaines atteintes (menaces, injures et débits fruduleux) contiennent des questions liées au domaine de l'Internet. Ainsi, les données collectées ont donc d'un côté une acception extensive – car ne distinguant pas le courrier postal du courrier électronique – et de l'autre restrictive dans la mesure où elles ne couvrent qu'une partie des cybermalveillances touchant les personnes physiques et dépend du fait que la personne interrogée ait effectivement connaissance d'une telle atteinte.
17. Article 226-4-1 al. 2 du Code pénal.
18. L'auteur de l'infraction, personne physique, encourt un an d'emprisonnement et 15.000€ d'amende. La condamnation peut atteindre 75.000€ lorsque l'auteur de l'infraction est une personne morale.
19. Selon Médiamétrie, pour l'année 2015, 30% des internautes français ont consulté au moins une fois par mois un site de streaming ou de téléchargement de films et séries. Soit près de 14,1 millions de Français contre 13,4 millions en 2014. http://www.alpa.paris/nouvelle-etude-alpa-sur-la-consommation-illegale-de-films-et-series/
20. Propos de Ms. Kim AUMONIER, Peace Brigades International, conférence UNESCO, "*Construire la paix et la sécurité internationales de la société numérique*", acteurs publics, acteurs privés, rôles et responsabilités 6-7 avril 2017.
21. Voir: http://www.diplomatie.gouv.fr/fr/services-aux-citoyens/actualites/article/francais-de-l-etranger-modalites-de-vote-aux-elections-legislatives-06-03-17
22. On parle d'objets connectés pour définir des types d'objets dont la vocation première n'est pas d'être des périphériques informatiques ni des interfaces d'accès au web, mais auxquels l'ajout d'une connexion Internet a permis d'apporter une valeur supplémentaire en terme de fonctionnalité, d'information, d'interaction ..."Objet connecté | Agence web 1min30, Inbound marketing et ... https://www.1min30.com/dictionnaire-du-web/objet-connecte
23. Une "smart city", en français "ville intelligente" utilise les technologies de l'information et de la communication (TIC) pour « améliorer » la qualité des services urbains ou encore réduire ses coûts.
24. Par exemple: voir l'article de l'Express: "Piratage d'une Tesla: ils transforment une voiture connectée en jouet téléguidé", "http://lexpansion.lexpress.fr/high-tech/piratage-d-une-tesla-ils-transforment-une-voiture-connectee-en-jouet-teleguide_1832943.html
25. Cf. Article L.111-1 alinéa 2 du Code de la sécurité intérieure.
26. Délégation ministérielle aux industries de sécurité et à la lutte contre les cybermenaces (acronyme DMISC) créée par décret n°2017-58 en date du 23 janvier 2017.
27. https://www.cecyf.fr/
28. http://www.antibot.fr/
29. https://www.signal-spam.fr/
30. https://phishing-initiative.fr/
31. http://www.33700.fr/
32. http://www.afpi-france.com/
33. http://www.e-enfance.org/
34. ANSSI: Agence nationale de sécurité des systèmes d'information, laquelle dépend du Premier ministre. http://www.ssi.gouv.fr/
35. Programme "Internet sans crainte", voir: http://www.internetsanscrainte.fr/
36. Article 113-2-1 du Code pénal.
37. Dans un souci de cohérence, la loi du 3 juin 2016 a par ailleurs étendu les critères de compétence des articles 42, 52 et 382 du Code de procédure pénale au lieu de résidence des victimes de l'infraction autorisant la poursuite de l'enquête par le premier parquet saisi et évitant ainsi le dessaisissement au profit du parquet de résidence de l'auteur une fois ce dernier identifié.
38. Cour de cassation, criminelle, Chambre criminelle, 12 juillet 2016, 15-86.645, Publié au bulletin.
39. Articles 323-1 à 323-4-1 et 11-9 du Code pénal.
40. Article 133-3, alinéa 2 du Code pénal.
41. Article 226-2-1 du Code Pénal.
42. Délégation Interministérielle à la Lutte Contre le Racisme, l'Antisémitisme et la Haine anti-LGBT, http://www.gouvernement.fr/dilcrah

PARADIS FISCAUX ET MONDIALISATION

ÉMILIE AUGUSTIN

DOCTEUR EN SCIENCES ÉCONOMIQUES, ÉCONOMISTE, MINISTÈRE DE L'ÉCONOMIE ET DES FINANCES

Le récent scandale des Panama papers a rappelé, une fois encore, la place significative des paradis fiscaux, devenus de puissants rouages du système financier globalisé. Plus de 11,5 millions de documents provenant du cabinet d'avocats panaméen Mossack Fonseca ont révélé des listes de noms de sociétés offshores et de personnalités impliquées. Ils ont surtout souligné les volumes d'argent considérables concernés par ce détournement.

Alors que la libéralisation financière s'impose comme la doctrine à suivre, la circulation des capitaux est largement facilitée. Par ailleurs, les transactions liées à la finance « offshore » et impliquant les paradis fiscaux est partie intégrante d'un système de plus en plus autonome, avec ses propres mécanismes et effets d'entraînement. Un paradis fiscal renvoie avant tout à un territoire fiscal non coopératif. Il n'a pas de statut illégal mais ces utilisations parfois criminelles posent la question de leur positionnement. L'OCDE (Organisation de Coopération et de Développement Économique) a précisé la définition du paradis fiscal en fixant trois critères : une taxation nulle ou insignifiante sur le capital, l'absence de transparence et enfin de fortes réticences à communiquer la moindre information à une autorité étrangère. Pour Bernard Castelli (2005), quatre transformations structurelles illustrent le succès des paradis fiscaux : le mimétisme des techniques de placement pour les capitaux acquis légalement ou non, la présence croissante d'acteurs criminels dans le secteur légal, la flexibilité géographique et fonctionnelle et enfin la faible pression répressive sur ces activités.

Cependant, il est légitime de se demander si ces transactions, légales et illégales via notamment les paradis fiscaux sont sous contrôle. Si oui, qui en est responsable ? Les États ? Les réseaux criminels ? Ces systèmes peuvent-ils devenir complètement indépendants du système de contrôle international ? Dans ce cas, peuvent-ils être à l'origine de crise dans la sphère de la finance légale et, par effet d'entraînement, de l'économie réelle ? Quels sont les différents types de réponses que les pouvoirs publics peuvent apporter à l'échelle nationale comme mondiale ?

I. La circulation des capitaux est-elle toujours sous contrôle ?

A. Les vertus affichées du libéralisme financier

Élément nécessaire au bon fonctionnement du marché intérieur européen, la circulation des capitaux est un complément indispensable de la libre circulation des marchandises, des personnes et des services. Les vertus affichées sont, entre autres, la réduction des coûts de paiements et l'accroissement de l'efficacité des systèmes nationaux. À l'échelle de l'Union européenne (UE), toutes les restrictions aux mouvements de capitaux entre les États

membres et les pays tiers doivent être levées (articles 63 à 66 du Traité du Fonctionnement de l'Union européenne). À partir du 1er janvier 1993, le marché financier de l'UE est complètement libéralisé : la capitalisation boursière totale représentait ainsi 8 400 milliards d'euros fin 2013 (environ 65 % du PIB) contre 1 300 milliards en 1992 (22 % du PIB).

La littérature économique considère la finance offshore comme une réponse normale à la surtaxation des pays riches. Au niveau international, selon la théorie économique classique, la mobilité des capitaux permettrait aux pays qui ont des ressources d'épargne limitées d'attirer des financements pour leurs projets d'investissement internes. La justification théorique de la libéralisation repose sur le principe d'allocation optimale. L'élimination des capitaux diminue le rôle de l'État et cette tendance ne semble pas se renverser à moyen terme. La science économique justifie les paradis fiscaux par des arguments classiques, soutenus par la pensée libérale et néolibérale (théorie des avantages comparatifs). La circulation des capitaux fait de plus en plus fi des frontières géographiques et physiques.

B. La place menacée de l'État

L'État apparaît de prime abord comme la principale autorité de contrôle de la circulation des capitaux. Le rôle de l'État est effectivement central. Les agents affichent alors un fort niveau de confiance, cette relation reposant sur la notion de puissance exclusive et de souveraineté de l'État sur le sujet. « *Celui qui contrôle l'argent de la nation contrôle la Nation* » déclara Thomas Jefferson, 3ème président des États-Unis.

Pourtant, l'État, autorité ayant le monopole de la violence légitime (Max Weber, 1919), a de plus en plus de difficultés à assumer son rôle de superviseur.

La disparition progressive de l'argent liquide affaiblit en outre l'efficacité des politiques de régulation et de contrôle étatique ou supra-étatique. Le processus de circulation de la monnaie est géré traditionnellement par les Banques centrales qui sont en charge non seulement de la création monétaire mais également de la régulation (par les prix ou les stocks) de la masse monétaire en circulation. Les Banques centrales jouent également le rôle de prêteur en dernier ressort en cas de crise.

Mais, la position de domination et de contrôle de l'argent par les pouvoirs publics va-t-elle perdurer ? La Banque centrale européenne a récemment supprimé le billet de 500 euros, en cherchant à lutter contre le blanchiment des bénéfices des trafics illicites et donc les activités criminelles. Cette action confirme la tendance de disparition de l'argent physique. Un effet de report va s'opérer, de l'argent physique à la monnaie virtuelle. La monnaie numérique ne cesse de s'affirmer comme une alternative crédible, non seulement pour les opérations légales mais également illégales. Parmi les exemples les plus connus : le Bitcoin. D'un point de vue global, l'État subit une perte de pouvoir notable.

Cependant, d'aucuns soutiennent en contre-pied qu'il n'y pas de diminution du pouvoir de la force étatique mais seulement une évolution de son rôle (Vincent Piolet, 2013). L'État a toujours la mainmise sur la circulation de l'argent. Et c'est justement la connivence des Nations qui assure la pérennité des paradis fiscaux. Le Royaume-Uni, les États-Unis mais également la France auraient en effet trouvé leur intérêt à soutenir l'existence de tels dispositifs dérogatoires.

La circulation des capitaux, du fait de la libéralisation des transactions financières mais également de leur criminalisation rend donc le contrôle des pouvoirs publics délicat et relativement peu efficace. La puissance étatique est de plus en plus démunie pour assurer le suivi des transactions financières. La dérégulation a certes levé les barrières aux transactions mais elle a surtout accéléré la perte de contrôle de la puissance étatique, facilitant le développement de pratiques illicites. L'exemple des paradis fiscaux est révélateur de cette nouvelle opacité des circuits financiers dans un système pourtant de plus en plus globalisé. Et parallèlement, la coopération internationale « *bute encore sur la disparité des lois et des procédures dans les différents pays concernés* » (Gudrùn Kopp, 2006).

Se pose alors la question de la caractérisation des liens entre libéralisation des capitaux et criminalisation des transactions. Autrement dit, la circulation facilitée des capitaux a-t-elle entraîné la criminalisation de la sphère financière ? À l'extrême, pourrait-on envisager une situation d'indépendance de la finance offshore par rapport à la finance traditionnelle voire à l'économie réelle ?

C. Le développement des paradis fiscaux : une réponse aux stratégies d'optimisation fiscale des multinaltionales

Les paradis fiscaux proposent des régimes fiscaux avantageux aux multinationales. Cette concurrence, lancée à l'échelle de l'UE se traduit par des politiques attractives de quelques pays comme les Pays-Bas ou le Luxembourg. Les documents publiés par l'ICIJ (International Consortium of Investigative Journalists) lors du scandale du Luxembourg Leaks en 2014 a mis en exergue les enjeux de cette circulation de capitaux, aux frontières de la légalité, entre optimisation et évasion fiscales. La stratégie d'optimisation fiscale a pour objectif une réduction des impôts *via* le plus souvent la création d'une holding. Différents outils sont détaillés dans les documents publiés : prêts internes, versement royalties...autant de stratégies au coeur des accords passés entre le Grand-Duché et les firmes multinationales.

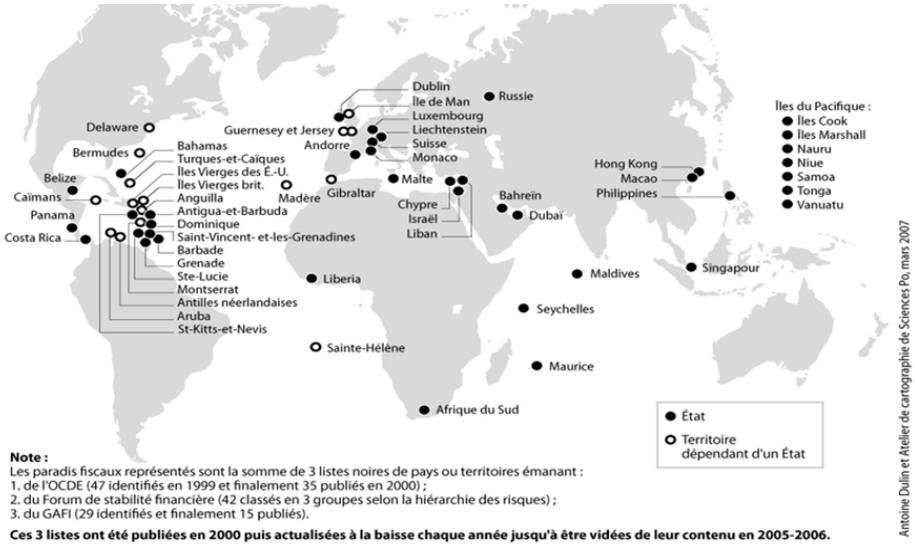
Ci-après la carte des paradis fiscaux proposée par Christian Chavagneux et Ronen Palan (2006).

II. Les paradis fiscaux, générateurs d'externalités négatives dans un contexte de mondialisation

La recrudescence des paradis fiscaux est imputable directement à la mondialisation. Autrement dit, le processus d'intégration économique et financière a conduit à faire émerger des opportunités en termes de fiscalité. La compétition entre les pays à l'échelle d'une zone géographique se traduit par des pratiques de concurrence déloyale et d'optimisation fiscale. Le manque à gagner significatif pour les États est l'une des conséquences notables à l'échelle macroéconomique mais il convient d'admettre les externalités connexes à savoir le renforcement du sentiment d'injustice fiscale ou l'affaiblissement du lien entre Souveraineté (à travers la capacité de collecte de l'impôt) et Globalisation. Ces pratiques introduisent des distorsions et génèrent des situations d'inefficience que les pouvoirs publics tentent de réduire à travers des lois dissuasives. Enfin, le recours à des paradis fiscaux par les multinationales et les plus riches a pour conséquence l'augmentation des inégalités. La science économique ne s'intéresse qu'à la marge à ce phénomène à travers le prisme, pourtant fondamental : celui des externalités négatives et des motivations non économiques (par exemple le degré d'opacité), arguments privilégiés par les organisations criminelles par exemple.

A. La criminalisation croissante des transactions financières à l'échelle internationale

Il paraît justifié de se demander s'il n'existe pas un risque d'instrumentalisation de ces législations par les groupes criminels. En effet, ces réseaux disposent d'outils sophistiqués pour réaliser leurs transactions en toute discrétion : sociétés-écrans domiciliées dans les pays bénéficiant de règlementations laxistes, plateformes de paiement alternatives pour contourner le système bancaire traditionnel. L'utilisation du web invisible (*darknet*) présente de nouvelles opportunités pour les fraudeurs. Ces derniers ont la possibilité d'effectuer des mouvements de fonds par le biais de monnaies virtuelles et ce, en concurrence avec le système bancaire international. La suppression de l'argent liquide, support des principales fraudes, joue un fort rôle incitatif et les monnaies virtuelles deviennent un moyen de paiement de substitution. Mais le recours au Bitcoin n'est pas sans risque (crise de gouvernance, crise de croissance).



Note :
Les paradis fiscaux représentés sont la somme de 3 listes noires de pays ou territoires émanant :
1. de l'OCDE (47 identifiés en 1999 et finalement 35 publiés en 2000) ;
2. du Forum de stabilité financière (42 classés en 3 groupes selon la hiérarchie des risques) ;
3. du GAFI (29 identifiés et finalement 15 publiés).

Ces 3 listes ont été publiées en 2000 puis actualisées à la baisse chaque année jusqu'à être vidées de leur contenu en 2005-2006.

Par ailleurs, l'hétérogénéité des cadres juridiques apparaît clairement comme un facteur incitatif qui s'est traduit par un net accroissement des facilités non seulement pour les contribuables à la recherche d'opportunités de placements très rentables mais également par le crime organisé : « *L'usage croissant de territoires extra-territoriaux correspond d'ailleurs au passage d'une spécialisation initiale presque exclusivement centrée sur l'évasion fiscale à une fonction plus diversifiée de protection des profits licites ou non des acteurs économiques publics et privés du monde entier* » (Bernard Castelli, 2005).

B. Les risques de l'autonomisation de la finance offshore

Parallèlement, la finance offshore ou « shadow banking » gagne en autonomie par rapport aux États, si bien qu'il est pertinent de se poser la question des risques inhérents à cette indépendance croissante. Certains secteurs de l'économie réelle sont devenus particulièrement vulnérables aux pratiques du blanchiment. La NSA (National Security Agency), agence britannique de lutte contre le crime organisé, a révélé les principaux secteurs à risque : les secteurs bancaire et immobilier, les cabinets de conseil fiscal et juridique, les casinos etc. Grâce aux possibilités offertes par la finance offshore, ces activités se sont montrées particulièrement vulnérables aux pratiques frauduleuses voire criminelles. Dans cette perspective, les paradis fiscaux extraterritoriaux pourraient avoir joué un rôle crucial dans le déclenchement de la crise financière de 2008. Paul Krugman (2013), dans un article pour le *New York Times* intitulé *« Tax heavens trauma »*, cite dans ce sens l'ouvrage référence de Nicholas Shaxson (2012) et reprend cette idée de lien de corrélation entre crise financière et accélération des mouvements de capitaux *via* les paradis fiscaux. "*Not only do they bleed revenues from cashstrapped governments and enable corruption; they distort the flow of capital, helping to feed ever-bigger financial crises*" *(Krugman, 2013).*

III. Des tentatives de régulation globale : un succès encourageant bien qu'insuffisant

Devant le constat du caractère internationalisé des paradis fiscaux, les réponses qui doivent être apportées par les pouvoirs publics seront nécessairement globales. Tout d'abord, les experts mettent en avant le rôle ambigu des conventions fiscales avec certains pays ou territoires non coopératifs.

À l'échelle européenne, des succès sont à noter, laissant croire à une amélioration de la situation, notamment à l'échelle de l'UE. Le 21 octobre 2015, la Commission européenne a condamné des filiales de *Fiat* et de *Starbucks* pour des pratiques de « *tax rulings* » c'est-à-dire des accords passés entre l'État (respectivement le Luxembourg et les Pays-Bas) et les multinationales en vue de diminuer les impôts à verser à l'administration fiscale. En réalité, cette décision est plus que symbolique puisqu'elle affirme le caractère illégal des « *tax rulings* », dépassant la notion, plus neutre, d'optimisation fiscale. Une décision du même ordre a été prise le 30 août 2016 concernant la société *Apple* pour des arrangements passés avec l'Irlande. Au final, la multinationale devrait régulariser la situation avec une amende de plus de 13 milliards d'euros.

La transparence demandée aux multinationales est de plus une condition *sine qua non* de la réussite de ces politiques. La loi Sapin II introduit une obligation de reporting financier public par pays (nombre de salariés, chiffre d'affaires, impôts sur les bénéfices, etc.), sous certaines conditions. Celle-ci n'entrera en vigueur qu'après l'adoption d'une directive européenne similaire et au plus tard au 1er janvier 2018.

Parallèlement, il convient de souligner l'importance de lutter contre un phénomène connexe et toutefois fortement corrélé à la persistance des paradis fiscaux à savoir la corruption. La Loi Sapin II constitue un exemple récent des avancées positives dans le sens de la transparence et de la lutte contre la corruption. Parmi les mesures introduites, il est désormais possible de poursuivre une entreprise en cas de corruption à l'étranger, le texte créant une infraction de « *trafic d'influence d'agent public étranger* ». Comme aux EÉtats-Unis, la justice française pourra donc condamner pour des actes de corruption à l'étranger des entreprises étrangères ayant tout

ou partie de leur activité économique en France.

Conclusion

Les paradis fiscaux sont, depuis quelques années, un sujet d'actualité à part entière qui alimente le débat public au sein non seulement de la recherche académique mais également de la société civile. Régulièrement représentés comme une des parts d'ombre de la mondialisation, les paradis fiscaux restent globalement un sujet peu analysé en détail, souvent à cause de son caractère intrinsèquement complexe et opaque. En réalité, ils sont considérés comme l'un des maillons centraux de la finance et de l'économie informelle. Leur utilisation par les multinationales et les groupes criminels génère des externalités négatives, souvent relayés au second rang par la théorie économique classique. Cet aspect est davantage étudié par le prisme des caractéristiques propres des paradis fiscaux (Robin Thomas Naylor, 2003). En économie politique internationale, Christian Chavagneux (2010), explicite le développement des pratiques offshore (pavillon de complaisance, zones franches) à travers le prisme de l'évolution et des transformations du lien entre la souveraineté des États et le capitalisme. Enfin, un discours émergent met en exergue l'implication indirecte de la finance offshore dans le déclenchement de la crise des surprimes. Le rôle des paradis fiscaux se révèle donc globalement ambigu : ils facilitent nombre de transactions (prêts internationaux, assurance, investissement) mais favorisent parallèlement la criminalité et réduisent l'autonomie des politiques (refus du principe de souveraineté politique). Enfin, ils génèrent une instabilité financière sous-jacente tout en participant à l'accroissement des inégalités économiques à l'échelle internationale.

Notes :

1. Référence aux Pentagon Papers de la guerre au Vietnam, nom donné au dossier secret de 7 000 pages révélé au public en 1971 par le New York Times.
2. ICIJ (International Consortium of Investigative Journalists) : groupement de journalistes et medias émanant de lanceurs d'alertes.
3. Publication par ICIJ de 28 00 documents sur les montages financiers des FMN (Firmes Multinationales) pour transférer leurs profits vers le Luxembourg. Plus de 340 multinationales seraient impliquées par le scandale.
4. Au Luxembourg par exemple, l'impôt sur les sociétés fixé à 29 % atteint en pratique un taux compris entre 1% ou 5%.
5. Un agent économique ou groupe d'agents économiques exerce une externalité lorsque son activité procure à autrui une utilité ou un avantage de façon gratuite ou au contraire une désutilité, un dommage sans compensation. Tirole « *Economie du bien commun* » (2017).

Bibliographie :

Castelli B. (2005), Une autre mondialisation : les mutations du blanchiment contemporain, *Mondes en développement*, n° 131, p. 111-130.

Chavagneux, C. (2010). *Economie politique internationale*. La Découverte.

Chavagneux, C., & Palan, R. P. (2006). Les paradis fiscaux. Paris: la Découverte.

Kopp, P. (2006). La lutte contre le blanchiment. Les banques entre droit et économie.

Krugman, P. (2013). Treasure Island Trauma. *New York Times*, 13.

Naylor, R. T. (2003). Towards a General Theory of Profit-Driven Crimes. *British Journal of Criminology*, *43*(1).

Piolet, V. (2013), Géopolitique des paradis fiscaux. Politique étrangère. p.175-187.

Shaxson, N. (2012). Treasure islands: tax havens and the men who stole the world. Random House.

Tirole, J. (2016). Économie du bien commun. *Presses Universitaires de France*.

Weber, M. (1919). Le savant et le politique, préface de R. Aron, *traduction de J. Freund: Flon*.

Inscription à la newsletter et à la revue du GRASCO

Par mail : abonnement@larevuedugrasco.eu

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

Par mail : information@grasco.eu

1 après validation de la rédaction

LA SAISIE ET LA CONFISCATION EN VALEUR EN DROIT PÉNAL FRANÇAIS

STEPHEN ALMASEANU

VICE-PROCUREUR DE LA RÉPUBLIQUE PRÉS LE TIBUNAL DE GRANDE INSTANCE DE PARIS

L'auteur de cet article n'exprime que des opinions personnelles qui n'engagent nullement le parquet de Paris

En droit pénal français, la saisie et la confiscation en valeur n'ont cessé, depuis trente ans, de voir leur champ d'application s'étendre, à l'instar d'ailleurs de leur rôle en droit international et européen. Après plusieurs évolutions législatives décisives, notamment opérées par les lois des 27 mars 2012 et 6 décembre 2013, la pratique s'est suffisamment emparée de cette possibilité pour qu'un premier bilan en soit tiré.

L'article 131-21 du Code pénal, souvent modifié, siège de l'ensemble de la matière, prévoit quels sont les biens qui peuvent être confisqués à titre de peine complémentaire en droit français, et donc quels sont les biens qui peuvent être saisis en cours de procédure, étant précisé que ces peines complémentaires sont encourues de plein droit pour les crimes et pour les délits punis d'une peine d'emprisonnement d'une durée supérieure à un an, à l'exception des délits de presse.

On le sait, peuvent, aux termes de ce texte, être ainsi saisis et confisqués les biens ayant servi d'instrument de l'infraction (article 131-21 alinéa 2), les biens objets ou produits directs ou indirects de l'infraction (article 131-21 alinéa 3), les biens dont la confiscation est prévue par l'incrimination (article 131-21 alinéa 4), les biens dont la personne, ne peut justifier de l'origine alors qu'elle encourt une peine d'au moins cinq ans d'emprisonnement (article 131-21 alinéa 5), tous les biens du patrimoine du condamné quand ce dernier l'a été sur le fondement d'une des infractions le prévoyant expressément (article 131-21 alinéa 6), les biens dangereux, nuisibles ou dont la détention est illicite (article 131-21 alinéa 7). Peut enfin être prononcée une confiscation « *en valeur* » (article 131-21 alinéa 9).

À première lecture, le texte même de l'article 131-21 alinéa 9 du Code pénal n'est ni d'une grande précision, ni d'une grande clarté : « *La confiscation peut être ordonnée en valeur. La confiscation en valeur peut être exécutée sur tous biens, quelle qu'en soit la nature, appartenant au condamné ou, sous réserve des droits du propriétaire de bonne foi, dont il a la libre disposition. Pour le recouvrement de la somme représentative de la valeur de la chose confisquée, les dispositions relatives à la contrainte judiciaire sont applicables* ».

Le texte de l'article 706-141-1 du Code de procédure pénale, sur la saisie en valeur, n'est guère plus explicite : « *La saisie peut également être ordonnée en valeur. Les règles propres à certains types de biens prévues aux chapitres III et IV du présent*

titre s'appliquent aux biens sur lesquels la saisie en valeur s'exécute ».

Ces deux textes sont l'aboutissement d'une longue évolution du droit français ayant eu lieu sous l'influence des textes internationaux et européens. Les dernières modifications textuelles datant de 2012 et de 2013, il est aujourd'hui possible, à l'aide d'une jurisprudence désormais relativement fournie de synthétiser l'utilisation de la saisie en valeur en droit français, tant en ce qui concerne son champ d'application (I) que sa mise en oeuvre par les juridictions (II).

I. Le champ d'application de la saisie et de la confiscation en valeur

A. Les origines internationales

La nécessité de pouvoir saisir non seulement le produit des infractions mais également leur équivalent a très vite été dégagée dans les premiers textes internationaux s'intéressant à la répression du trafic de stupéfiants, de la criminalité organisée et du blanchiment[1].

La Convention de Vienne contre le trafic illicite de stupéfiants et de substances psychotropes conclue dans le cadre de l'ONU le 20 décembre 1988, qui s'inscrit dans la longue série des conventions internationales concernant les stupéfiants depuis la fameuse Convention internationale de l'opium de 1912, marque néanmoins un tournant important en partant du principe que, pour lutter efficacement contre le trafic de stupéfiants, il est nécessaire de porter l'effort sur le financement de ce trafic, et donc sur le blanchiment, les saisies et les confiscations. C'est à ce titre que la Convention demande aux États signataires d'adopter les mesures nécessaires pour permettre la confiscation *« des produits tirés d'infractions* (…) *ou des biens dont la valeur correspond à celle desdits produits* » (article 5 § 1 a.) [2].

La Convention de Vienne a très fortement influencé les premières 40 recommandations du GAFI[3] de 1990, et notamment les recommandations n°8 (« *Les pays devraient, en tant que de besoin, adopter des mesures similaires à celles indiquées dans la Convention de Vienne, y compris des mesures législatives, afin que leurs autorités compétentes soient en mesure de confisquer les biens blanchis, les produits en découlant, ainsi que les instruments utilisés ou devant l'être pour commettre toute infraction de blanchiment, ou encore des biens de valeur correspondante* ») et n° 38 (« *Il serait souhaitable que l'on puisse prendre des mesures rapides en réponse. À des requêtes émanant de gouvernements étrangers demandant d'identifier, de geler, de saisir et de confisquer les produits, ou d'autres biens d'une valeur équivalente à ces produits, tirés du blanchiment d'argent ou des délits sur lesquels repose l'activité de blanchiment* »)[4].

La Convention de Strasbourg du 8 novembre 1990 relative au blanchiment, au dépistage, à la saisie et à la confiscation des produits du crime, signée dans le cadre du Conseil de l'Europe, prévoit que « *chaque partie adopte les mesures législatives et autres qui se révèlent nécessaires pour lui permettre de confisquer des instruments et des produits ou des biens dont la valeur correspond à ces produits* » (article 2 § 1), mais également, au titre de la coopération internationale, que « *chaque partie adopte les mesures législatives et autres qui se révèlent nécessaires pour lui permettre de répondre* (…) *aux demandes de confiscation de biens particuliers consistant en des produits ou instruments, ainsi que de confiscation des produits consistant en l'obligation de payer une somme d'argent correspondant à la valeur du produit* » (article 7 § 2 a.).

Il est ainsi intéressant de noter que, dès 1990, sont donc combinées dans un texte international deux conceptions différentes mais complémentaires de la saisie et de la confiscation en valeur, et sur lesquelles nous aurons l'occasion de revenir en droit interne : d'une part, celle de « *biens de valeur équivalente* » ou « *correspondante* » à saisir et à confisquer et, d'autre part, pour favoriser le recouvrement, notamment transfrontière, des confiscations, celle d'une « *somme en valeur* », sorte d'amende équivalente au produit de l'infraction[5].

B. L'influence européenne

En droit communautaire également, et dans un même souci d'efficacité, les différents textes ont très vite prévu la confiscation en valeur. La décision-cadre du Conseil 2001/500/JAI du 26 juin 2001 concernant le blanchiment d'argent, l'identification, le dépistage, le gel ou la saisie et la confiscation des instruments et des produits du

crime doit être tout particulièrement citée car elle lui consacrait son article 3 : « *Chaque État membre prend les mesures nécessaires pour que sa législation et ses procédures relatives à la confiscation des produits du crime permettent aussi, au moins dans le cas où ces produits ne peuvent être appréhendés, la confiscation des biens d'une valeur correspondant à celle des produits, dans le cadre tant de procédures purement internes que de procédures engagées à la demande d'un autre État membre, y compris des demandes d'exécution d'ordres de confiscation étrangers* (...) ». On retrouve bien sûr la saisie et la confiscation en valeur dans les autres textes communautaires pertinents[6], et notamment dans la décision-cadre 2003/577/JAI du 22 juillet 2003 relative à l'exécution dans l'Union européenne des décisions de gel de biens ou d'éléments de preuve (article 2 d.), dans la décision-cadre 2005/212/JAI du 24 février 2005 relative à la confiscation des produits, des instruments et des biens en rapport avec le crime (article 2 § 1), dans la décision-cadre 2006/783/JAI du 6 octobre 2006 relative à l'application du principe de reconnaissance mutuelle aux décisions de confiscation (articles 2 d) i. et 7) et, enfin, dans la directive 2014/42/UE du 3 avril 2014 concernant le gel et la confiscation des instruments et des produits du crime dans l'Union européenne (articles 4 et 6).

C. Les évolutions corrélatives en droit français

Le droit français se devait donc d'évoluer, et cette évolution a connu trois étapes principales.

i. L'édiction du nouveau Code pénal en 1994

Dans l'ancien Code, l'article 11, disposition générale sur la peine complémentaire de confiscation, ne prévoyait pas la possibilité de confisquer en valeur. Seule était admise « *la confiscation spéciale, soit du corps du délit, quand la propriété en appartient au condamné, soit des choses produites par le délit, soit de celles qui ont servi ou qui ont été destinées à le commettre* » (on parlerait aujourd'hui d'objet, du produit et de l'instrument de l'infraction). Fort logiquement, la Cour de cassation avait donc rejeté toute tentative de confiscation en valeur par les juridictions[7] .

Le législateur du nouveau Code pénal a profité de la réforme pour se conformer aux standards internationaux précités en prévoyant dans le nouvel article 131-21 (à l'époque dans l'alinéa 4 de ce texte) la confiscation en valeur, mais en l'assortissant, comme le permettait d'ailleurs la décision-cadre 2001/500/JAI du 26 juin 2001 *précitée*, de conditions : « *Lorsque la chose confisquée n'a pas été saisie ou ne peut être représentée, la confiscation est ordonnée en valeur. Pour le recouvrement de la somme représentative de la valeur de la chose confisquée, les dispositions relatives à la contrainte judiciaire sont applicables* ». Il était alors clair, à la lecture des deux phrases de ce texte, que le législateur avait certes fait progresser le droit français en admettant la confiscation en valeur, mais en réalité de façon somme toute limitée, en la conditionnant à l'absence de saisie ou d'identification de la chose devant être confisquée et, de plus, en semblant la limiter à une seule des deux modalités de la saisie en valeur vue plus haut, celle de la somme mise à la charge du condamné[8].

Cette possibilité subsidiaire de confiscation en valeur fut très peu utilisée, même après l'édiction de la loi du 9 juillet 2010 révolutionnant le droit français des saisies et des confiscations.

ii. La loi du 27 mars 2012 de programmation relative à l'exécution des peines

La deuxième étape de l'évolution eut justement pour but de mettre fin à cet échec, en France, de la saisie et de la confiscation en valeur. Elle fut opérée par la loi du 27 mars 2012 de programmation relative à l'exécution des peines, sur amendement déposé par Jean-Luc Warsmann, à l'époque président de la Commission des lois. Grâce à cet amendement furent supprimées les conditions vues *supra* qui faisaient de la confiscation en valeur une mesure résiduelle.

L'article 131-21 alinéa 9 du Code pénal, ne fait désormais plus référence qu'à une possibilité, sans condition : « *La confiscation peut être ordonnée en valeur* ». Le législateur décida, dans la même loi, d'introduire dans le Code de procédure pénale, dans les saisies spéciales, un texte spécifique permettant la saisie en valeur, l'article 706-141-1 rappelant que la saisie en valeur devait bien sûr respecter les règles spécifiques à la saisie de certains biens (par exemple l'inscription des saisies immobilières, y compris en valeur, en application de l'article 706-151 du Code de procédure pénale, ou

encore le transfert à l'AGRASC des saisies de sommes inscrites au crédit de compt bancaires, y compris en valeur, en application de l'article 706-160 2° du même Code).

De son côté, la Cour de cassation a décidé que si l'application de la nouvelle confiscation en valeur ne pouvait bien sûr concerner que des faits postérieurs à l'entrée en vigueur de la loi du 27 mars 2012 – puisqu'il s'agit de l'aggravation d'une peine –, la nouvelle saisie en valeur était, elle, immédiatement applicable aux affaires en cours en application de l'article 112-2 2° du Code pénal[9].

iii. La loi du 6 décembre 2013

La troisième et dernière étape de l'évolution fut accomplie par la loi du 6 décembre 2013, à la demande de l'AGRASC[10] : alors que la loi précitée du 27 mars 2012 avait étendu les confiscations élargies des alinéas 5 et 6 (confiscation de biens d'origine injustifiée et confiscation générale du patrimoine) de l'article 131-21 du Code pénal aux biens dont la personne avait la libre disposition, sous réserve bien sûr des droits du propriétaire de bonne foi, cette application de la libre disposition n'était pas prévue pour la confiscation en valeur, ce qui était un handicap majeur à une époque où les délinquants organisent leur insolvabilité et n'ont quasiment plus de biens en leur nom.

La loi prévoit donc, désormais, que la confiscation (et donc la saisie) en valeur « *peut être exécutée sur tous biens, quelle qu'en soit la nature, appartenant au condamné ou, sous réserve des droits du propriétaire de bonne foi, dont il a la libre disposition* »[11] , la logique voulant que cette nouvelle disposition soit immédiatement applicable aux affaires en cours au jour de l'entrée en vigueur de la loi du 6 décembre 2013 pour les saisies[12] et non, bien sûr, pour les confiscations.

II. La mise en oeuvre de la saisie et de la confiscation en valeur

A. La saisie et la confiscation en valeur : aspects pratiques

Aux termes de l'évolution que nous venons d'étudier, la saisie et la confiscation en valeur ont donc désormais, en France, un champ d'application particulièrement étendu : les possibilités de les utiliser sont, par conséquent, extrêmement larges pour les magistrats. Selon quelles modalités ? En pratique, il nous faut répondre à trois questions complémentaires : de quelle valeur parle-t-on ? Sous quelle forme peut-on la saisir ? Comment l'évaluer ?

i. De quelle valeur parle-t-on ?

Comme nous l'avons vu, les premiers textes internationaux et européens font référence à la valeur du ou des produits dégagés grâce aux infractions commises. Rien de tout cela en droit français. On s'accorde bien sûr à admettre la saisie et la confiscation tant de la « *valeur du produit* » que de la « *valeur de l'objet* » de l'infraction, qui sont très proches (par exemple, dans le blanchiment, les sommes blanchies sont l'objet du délit, pas son produit)[13] .

Il faut y ajouter, conformément d'ailleurs aux textes les plus récents, la saisie et la confiscation de la valeur de l'instrument de l'infraction. Ainsi, ont déjà été saisis, en France, à un trafiquant de stupéfiants, des biens d'une valeur équivalente à celle du puissant véhicule qui avait servi de voiture ouvreuse dans un « *go fast* », véhicule qui était la propriété d'une société de location. On voit le grand intérêt de cette saisie : le véhicule, instrument de l'infraction[14], était, lui insaisissable car, même à démontrer la libre disposition du trafiquant, rien ne permettait d'établir la mauvaise foi du loueur…

ii. Confisquer la valeur, sous quelle forme ?

Il est donc clair que la valeur du produit, de l'objet ou de l'instrument de l'infraction peut être saisie et confisquée. Mais sous quelle forme ? Nous avons vu que deux formes de confiscations en valeur avaient été dégagées, tant en matière internationale qu'en France : la confiscation de biens déterminés de valeur équivalente, ou la fixation d'une somme équivalente aux biens qui pourraient être confisqués.

L'avantage du droit français est de clairement permettre d'utiliser ces deux modalités, qui ne correspondent d'ailleurs pas du tout aux mêmes besoins judiciaires :

-Si une enquête patrimoniale peut être menée et des saisies effectuées, la saisie de biens déterminés correspondant à la valeur du produit, de l'objet

ou de l'instrument sera bien sûr privilégiée : le ou les biens (immeubles, meubles, sommes, créances, etc.) seront saisis, selon les règles respectives qui s'appliquent à eux aux articles 706-141 et s. du Code de procédure pénale, et pourront, à titre de peine, être confisqués par la juridiction de jugement. Dans ce cas, la saisie et la confiscation en valeur peuvent être qualifiées, de façon plus explicite, de saisie et de confiscation par équivalent, et la confiscation est exécutée par l'AGRASC[15].

-En revanche, si aucun bien n'a pu être saisi et même si aucune enquête patrimoniale n'a pu être menée, il est toujours possible pour la juridiction de jugement de confisquer une somme qu'elle détermine en fonction de ce qu'elle estime être le produit, l'objet ou l'instrument de l'infraction. Cette somme confisquée sera alors recouvrée, en application de l'article 707-1 du Code de procédure pénale, par le comptable public compétent. Cette forme de confiscation en valeur est très utile, par exemple pour les comparutions immédiates. Certes, son exécution, alors qu'elle n'a pas été précédée de saisies, ne sera pas simple, mais c'est souvent la seule façon, avec l'amende, dans ce type de procédures, de sanctionner le délinquant sur le terrain patrimonial…

iii. Quelle évaluation pour la valeur ?

Il reste alors à évaluer cette somme ou les biens à saisir et à confisquer, cette évaluation étant d'autant plus sensible que la Cour de cassation s'est montrée inflexible : il est impensable de saisir ou de confisquer un euro de plus que cette valeur[16].

Un montant considéré par la Cour de cassation comme maximal pour les confiscations, mais également pour les saisies

Cette jurisprudence se comprend aisément pour la confiscation, car il s'agit là de respecter la logique même de ce fondement. Ainsi, par exemple, s'il est établi que le délinquant a gagné 100.000 euros, il est normal qu'on lui confisque donc 100.000 euros, ou des biens d'une telle valeur ; s'il a blanchi un million d'euros, la loi du 27 mars 2012 de programmation relative à l'exécution des peines lui confisquer un million d'euros, etc. Nous ne sommes en effet pas là dans le contrôle, de plus en plus classique, de la proportionnalité[17], mais dans celui de l'équivalence.

Qu'il nous soit permis d'être en revanche critique concernant les saisies : en affirmant que « *le montant d'une saisie pénale en valeur ne doit pas excéder la valeur du bien susceptible de confiscation* »[18], la Chambre criminelle limite fortement les saisies possibles sans pour autant qu'une telle limite soit indispensable pour assurer la protection des intéressés. C'est le cas de toutes les saisies qui ne peuvent se scinder, et notamment la saisie pénale immobilière. En effet, un immeuble est saisi ou ne l'est pas, la saisie de l'article 706-150 du Code de procédure pénale comme l'inscription à la publicité foncière de l'article 706-151 du même Code ne se fractionnant pas. Rappelons ici que la saisie pénale immobilière ne dépossède nullement l'intéressé de sa propriété et de sa possession : elle ne fait que l'empêcher de céder son immeuble sans l'autorisation du juge saisissant (qu'il est possible d'obtenir, avec un report de la saisie sur le prix, en application de l'article 706-152 du Code de procédure pénale).

Affirmer de façon générale que « *le montant d'une saisie pénale en valeur ne doit pas excéder la valeur du bien susceptible de confiscation* » empêche donc la saisie de biens (immeubles, mais aussi créances inscrites sur des contrats d'assurance-vie, etc.) dont la valeur est supérieure à la valeur à récupérer, et donc parfois la mise en place de toute saisie. Ainsi, si un délinquant, propriétaire d'un immeuble d'une valeur d'un million d'euros, commet des délits pour des montant inférieurs, son immeuble ne pourra jamais être saisi…

Cela semble d'autant plus critiquable si on raisonne sur ce qui pourrait se passer à la fin de la procédure : la cour permettrait la saisie de biens d'une valeur supérieure au produit, à l'objet ou à l'instrument, leur confiscation se ferait évidemment selon des règles permettant le prélèvement de la seule valeur (en proposant à l'intéressé de verser cette somme pour récupérer son immeuble, ou en vendant l'immeuble, ne versant la somme confisquée en valeur qu' à l'État et en restituant le reste à l'intéressé). L'intéressé ne subirait donc aucun préjudice, si ce n'est d'avoir réglé la somme à laquelle il avait été condamné…

Pour pouvoir saisir et confisquer en valeur, il est indispensable de fixer une ou deux valeurs

Une évaluation est toujours indispensable pour permettre le

contrôle juridictionnel : celle du produit, de l'objet ou de l'instrument utilisé au cours de l'infraction. Cette tâche, essentielle, est parfois simple (par exemple en cas d'escroqueries : il s'agit de collationner l'ensemble des valeurs escroquées), et parfois plus compliquée (par exemple en matière de trafic de stupéfiants, où il faudra déterminer l'importance du trafic et des sommes perçues, ce qui sera d'ailleurs également très utile pour apprécier la gravité des faits délictueux et fixer la peine principale d'emprisonnement).

Une question se pose à ce stade : il convient bien sûr d'évaluer de la façon la plus juste possible le produit, l'objet ou l'instrument. Concrètement, pour le produit, que faut-il prendre en compte : le chiffre d'affaires du trafic (c'est-à-dire l'ensemble des ventes) ou seulement le profit (les ventes moins les charges, c'est-à-dire moins les coûts d'approvisionnement, de stockage, de distribution, etc.) ? Il semblerait plus juste de ne compter que le profit, mais ce serait accepter la déduction, dans la sanction pénale, de charges illégales, ce qui ne semble pas envisageable. Dans les États où la saisie et la confiscation en valeur se sont fortement développées, au point d'être souvent devenues le fondement le plus utilisé[19], les débats judiciaires se focalisent sur ces questions...

Une autre évaluation doit être effectuée en cas de saisie ou de confiscation en valeur de biens déterminé : celle de la valeur de ces, afin de pouvoir comparer cette dernière avec la valeur du produit, de l'objet ou de l'instrument. Là aussi, il convient d'être juste en évaluant les biens ainsi saisissables – rappelons ici que comme ils sont saisis par équivalent, ils n'ont nullement à être d'origine illicite ou même à avoir été acquis pendant la période de prévention –, c'est-à-dire de ne ni les sous-évaluer ni les surévaluer. Ainsi, pour un immeuble, il ne suffira pas de disposer d'une évaluation fiable ; il faudra également regarder si une ou plusieurs hypothèques, ou un privilège de prêteur de deniers, sont inscrits, et en déduire le montant des remboursements effectués. En effet, les créanciers antérieurs étant désintéressés en cas de confiscation en application de l'article 131-21 alinéa 10 du Code pénal, leurs créances obèrent la valeur de l'immeuble à hauteur des sommes non encore remboursées...

Notes :

1. Voir, pour une présentation générale des différents textes internationaux, Massé M., « L'évolution du droit en matière de gel et de confiscation », RSC 2006, p. 453 et s.

2. Voir également l'article 12 de la Convention de Palerme du 12 décembre 2000 contre la criminalité transnationale organisée et l'article 31 de la Convention de Mérida contre la corruption du 31 octobre 2003.

3. Le « *Groupe d'action financière* » (GAFI, FATF en anglais pour « *Financial Action Task Force* ») est un organisme intergouvernemental placé sous le giron de l'OCDE. Créée lors du Sommet de l'Arche à Paris en 1989, comprenant désormais 37 membres, il a pour objectif l'élaboration des normes et la promotion de la mise en oeuvre effective de mesures législatives, réglementaires et opérationnelles en matière de lutte contre le blanchiment de capitaux, le financement du terrorisme et les autres menaces liées pour l'intégrité du système financier international.

4. Il s'agit aujourd'hui, dans leur version de 2012, des recommandations n° 4 et n° 38.

5. On retrouve bien sur cette dualité de la saisie et de la confiscation en valeur dans la Convention de Varsovie du 16 mai 2005 – et ratifiée par la France le 8 décembre 2015 – relative au blanchiment, au dépistage, à la saisie et à la confiscation des produits du crime et au financement du terrorisme ayant succédé à la Convention de Strasbourg (articles 3§1 et 15§2 a.).

6. Sur ces textes et la logique de cette évolution, v. Lelieur J., « Le dispositif juridique de l'Union européenne pour la captation des avoirs criminels », AJ pénal 2015, p. 232 et s.

7. Voir notamment Crim., 29 juin 1826 (*Bull. crim.*, n° 169), Crim., 23 octobre 1963, n° 62-92.318 et Crim., 14 décembre 1982, n° 81-90.682. Sur cette ancienne jurisprudence et les changements introduits par le nouveau code pénal en matière de confiscation en valeur, voir not. Matsopoulou H., « La confiscation spéciale dans le nouveau code pénal », *RSC* 1995, p. 301 et s., spéc. § 20 p. 311.

8. Voir, en ce sens, le commentaire de J. Pradel : « *Au lieu de prononcer la confiscation, le juge prononcera donc une confiscation pécuniaire égale à la valeur de l'objet* (...). [Cette évolution] *témoigne encore d'un accroissement des pouvoirs du juge, qui se trouve ainsi investi du droit de prononcer "une sorte d'amende supplémentaire"* » (Pradel J., « Le nouveau code pénal (partie générale) », *D.* 1993, p. 163 et s., spéc. n° 71).

9. Crim., 24 septembre 2014, n° 13-88.602, *AJ pénal* 2014, p. 592 et s., obs. Ascensi L. Voir déjà Crim., 9 mai 2012, n° 11-85.522.

10. « Rajout du concept de libre disposition pour les confiscations en valeur de l'article 131-21 alinéa 9 du Code pénal », AGRASC, Rapport 2013, p. 29.

11. Parmi les premières applications, voir Crim., 25 février 2015, n° 13-81.946 : validation d'une saisie en valeur d'une créance de dividendes de plus de 43 millions d'euros appartenant à plusieurs sociétés placées sous le contrôle de l'intéressé, qui détenait la totalité du capital de l'une d'elles, ces éléments légitimant pour la Cour que la condition de libre disposition ait été remplie.

12. Voir en ce sens, implicitement, Crim., 12 novembre 2015, n° 15-83.114, *D. Actualités*, 7 décembre 2015, obs. S. Fulcini.

13. Pour une saisie en valeur de l'objet blanchi, voir Crim., 7 décembre 2016, n° 16-81.280.

14. Voir la directive 2014/42/UE du 3 avril 2014 précitée, qui insiste beaucoup sur la confiscation de biens dont la valeur correspond à l'instrument de l'infraction (voir notamment les considérants n° 14, n° 15 et n° 17 et surtout l'article 4 § 1 du texte : « *Les États membres prennent les mesures nécessaires pour permettre la confiscation de tout ou partie des instru-*

ments et des produits ou des biens dont la valeur correspond à celle de ces instruments ou produits (...) ».

15. Article 707-1 alinéa 2 du Code de procédure pénale : « (...) *les poursuites pour le recouvrement des amendes et l'exécution des confiscations en valeur sont faites au nom du procureur de la République par le comptable public compétent ou, dans les cas où la confiscation en valeur s'exécute sur des biens préalablement saisis, par l'Agence de gestion et de recouvrement des avoirs saisis et confisqués* ».

16. Voir notamment, parmi de nombreux arrêts, Crim., 14 janvier 2015, n° 14-85.486 ; Crim., 30 septembre 2015, n° 15-81.744 et Crim., 12 novembre 2015, n° 15 -83.114, *D. Actualités*, 7 décembre 2015, obs. S. Fulcini.

17. Sur lequel voir, récemment, JH Obert, « Les confiscations et les mesures de leur proportionnalité », *JCP*, 9 janvier 2017, 13 (à propos de deux arrêts Crim., 7 décembre 2016 n° 16-81.280 et n°16-80879).

18. Crim., 12 novembre 2015, n° 15-83.114 précité.

19. Nous pensons ici notamment aux Pays-Bas, lesquels font d'ailleurs souvent exécuter leurs confiscations en valeur sur le territoire français grâce aux mécanismes de l'entraide pénale internationale. Suivant une vision avant tout commerciale des choses, la justice néerlandaise n'hésite pas à comptabiliser tous les frais engendrés par les délits, notamment les trafics de stupéfiants, pour les déduire des gains des trafiquants avant de leur demander paiement...

OUVRAGES RÉCENTS

HISTOIRE SECRÈTE DES RG :

FIGURES, COULISSES, MÉTHODES & SECRETS D'UNE POLICE QU'IL N'AURAIT PEUT-ÊTRE PAS FALLU SUPPRIMER...

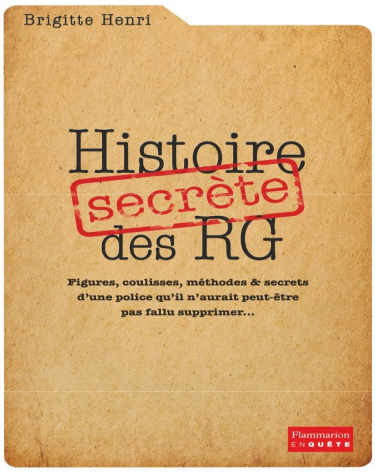
AUTEUR : BRIGITTE HENRI

EDITEUR : FLAMMARION ENQUËTE

Présentation de l'éditeur

En 2008, les Renseignements généraux disparaissent pour laisser place à la DCRI, une nouvelle structure censée incarner la modernité. Neuf ans plus tard, le constat est sans appel : c'est un échec. Pourquoi en est-on arrivé là ?

Tout n'a pas toujours été irréprochable au sein des RG.Le service a endossé un habit politique dont il a eu du mal à se défaire et plusieurs scandales ont terni son image. L'affaire des écoutes du PS tien-elle du simple malentendu ou de l'espionnage politique au profit du parti au pouvoir? Et qu'est-il arrivé au pasteur protestant et militant homosexuel Joseph Doucé, retrouvé mort dans la forêt de Rambouillet en 1990 ?



L'ancien parton des RG, Yves Bertrand, aurait-il fourni les faux listings de l'affaire Clearstream à la demande de Dominique de Villepin, comme l'a soupçonné Nicolas Sarkory ?

Affaires, efficacité du service, rôles des politiques... Brigitte Henri, une ancienne de la maison, raconte et sonde, documents à l'appui, l'histoire, les hommes, les réussites et les carences des RG, pour en dessiner un portrait loin des passions. Elle déplore leur disparition, notamment à la lumière des actions terroristes soudaines et violentes qu'a connues la France.

LE JUGE ET LE RENSEIGNEMENT

EMMANUEL FARHAT

MAGISTRAT DÉTACHÉ AU SERVICE DE LA PRÉVENTION DU TERRORISME
DE L'OFFICE DES NATIONS UNIES CONTRE LA DROGUE ET LE CRIME (ONUDC)

Les opinions exprimées dans cet article reflétent celles de son auteur et n'engagent en rien l'Organisation des Nations Unies.

L'ancien directeur adjoint du service juridique de la CIA, Fred F. Manget, comparaît l'interaction entre le monde du renseignement et le monde judiciaire aux mouvements de la tectonique des plaques en géologie : de manière générale, ils sont indécelables pour l'observateur situé en surface. Mais ils peuvent, de temps à autres, donner lieu à des manifestations visibles, et parfois spectaculaires.

À première vue, le juge, dont le rôle principal est de trancher de manière indépendante des litiges en application des règles de droit, et les services de renseignement, services de l'exécutif chargés de rassembler des informations nécessaires à la protection des intérêts fondamentaux de la Nation, semblent en effet opérer dans des sphères totalement différentes.

Alors que, dans un État de droit, la justice est supposée intervenir au plus tard du cheminement criminel, en se plaçant a posteriori par rapport à des faits déjà accomplis ou sur le point de l'être, les services de renseignement travaillent aussi et surtout de manière préventive et prospective afin de fournir aux décideurs des éléments destinés à permettre une évaluation objective et réaliste d'une situation donnée. Alors que la justice se rend en principe au vu et au su de tous (principe de l'audience publique [1]), après que chacun a pu présenter son point de vue (principe du contradictoire), le recueil du renseignement doit s'effectuer dans la plus grande discrétion, afin notamment de protéger les agents, les sources et les méthodes. De la même manière, les contraintes de temps, voire l'urgence, pesant sur l'action des services de renseignement sont a priori difficilement conciliables avec le temps judiciaire, nécessairement plus long puisqu'il s'agit pour le juge de « fermer les portes » et limiter au maximum les risques d'erreur.

Il n'est donc pas surprenant que justice et renseignement aient longtemps opéré de manière hermétique l'un par rapport à l'autre, dans une ignorance mutuelle aussi compréhensible qu'assumée. Loin d'être conçue comme une faiblesse, l'absence de lien entre ces deux mondes a même été théorisée de manière explicite, en particulier aux États-Unis d'Amérique, où les juristes qualifiaient cette séparation de « Mur » (Wall), en réaction notamment aux systèmes mis en place par l'Allemagne nazie et l'Union soviétique, où les missions de renseignement, de sécurité et de police étaient confiées à un même service. Ainsi, jusqu'aux réformes consécutives aux attentats du 11 septembre 2001, la loi fédérale et la jurisprudence interdisaient aux agences de renseignement, en particulier la CIA, de disposer d'un quelconque pouvoir d'enquête judiciaire, et réciproquement,

les services d'enquête tel que le FBI n'étaient pas autorisés à recueillir ou partager du renseignement [2].

En France, la situation fut longtemps sensiblement la même, quoique la séparation n'ait jamais été envisagée de manière aussi rigide. Comme aux États-Unis, la lutte contre le terrorisme s'est révélée ces dernières années comme un puissant moteur d'innovations juridique et pratique en la matière, le manque de circulation de l'information étant désormais unanimement considéré comme une faiblesse au regard des objectifs de protection de la sécurité et de l'ordre public. Se situant au carrefour des deux mondes, la lutte contre le terrorisme a ainsi largement contribué à la mise en place d'une dynamique résolument nouvelle entre le juge et le renseignement.

À la faveur notamment des affaires terroristes, l'action des services de renseignement fait désormais l'objet d'une attention renouvelée dans l'opinion publique, le monde politique, mais également chez les magistrats. Dans ce contexte, de nombreuses initiatives législatives et réglementaires sont intervenues en France [3] au cours des dernières années relativement aux services de renseignement, intérieur et extérieur. L'un des enjeux est aujourd'hui de permettre une plus grande efficacité dans l'action de la justice et des services de renseignement, tout en organisant un contrôle adapté et conforme aux principes de l'État de droit.

Dans notre pays, la dynamique nécessairement complexe entre le juge et le renseignement apparaît traversée par un double mouvement qui se caractérise par le développement contemporain d'une coopération de plus en plus étroite et mutuellement profitable entre le juge et les services de renseignement, et par l'émergence d'une nouvelle mission de contrôle par le juge sur l'activité des services.

I. Le développement d'une coopération réciproquement profitable

L'époque récente se caractérise par un phénomène d'interpénétration croissante des sphères du renseignement et de la justice, favorisée notamment par les objectifs de renforcement de la lutte contre le terrorisme et la criminalité organisée.

A L'extension de l'office du juge

Au cours des dernières décennies, l'office du juge a évolué de manière significative dans le sens d'un accroissement de son champ d'intervention.

i. Le renforcement de l'État de droit

Cette extension de l'office du juge s'inscrit d'abord dans le cadre du mouvement de fond de renforcement de l'État de droit, sous l'effet combiné de la jurisprudence interne (judiciaire, administrative et désormais constitutionnelle) et de la jurisprudence supranationale, notamment basée sur l'application de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales du Conseil de l'Europe.

ii. L'influence de la lutte contre le terrorisme et la criminalité organisée

Surtout, depuis la fin des années 1980, le législateur français a progressivement créé un régime juridique, administratif et pénal, exorbitant du droit commun pour permettre aux praticiens de la justice pénale de répondre plus efficacement aux défis posés par la criminalité organisée et le terrorisme. S'agissant de l'office du juge, ces réformes ont eu pour effet d'anticiper le seuil de déclenchement de l'intervention du juge toujours plus en amont dans le processus criminel.

L'exemple de l'incrimination pénale d'association de malfaiteurs à but terroriste (AMT) est particulièrement représentatif de cette évolution. Prévue à l'article 421-2-1 du Code pénal, cette infraction, qui revêt une nature délictuelle ou criminelle selon le type de comportement incriminé, constitue la pierre angulaire du dispositif pénal répressif anti-terroriste en droit français. En incriminant le projet criminel dès qu'il est matérialisé par des actes préparatoires, l'association de malfaiteurs terroriste permet au juge d'intervenir très en amont du résultat final recherché, plus tôt même que ne le permet la notion juridique de tentative de l'article 121-5 du Code pénal.

L'avantage de cette approche est évident : il permet d'avancer le seuil de déclenchement de la réponse judiciaire de plusieurs crans, pour l'inscrire dans une action préventive et non plus uniquement réactive. Tous les types de faits préparatoires à un acte terroriste peuvent ainsi être appréhendés pénalement, sans nécessité d'avoir recours à une incrimination spécifique pour chacun (recrutement, entraînement, endoctrinement, fourniture ou acquisition de matériel ou d'armes, fourniture d'assis-

tance logistique, etc.).

La jurisprudence a d'ailleurs démultiplié cet effet en adoptant une conception large du champ d'application de l'infraction d'association de malfaiteurs à but terroriste, en particulier s'agissant de l'élément matériel tenant aux « actes préparatoires ».

Ainsi, le fait pour trois individus de se procurer des billets d'avion pour la Syrie, de rechercher et obtenir des fonds pour financer leur voyage et de se mettre en route par leur pays de destination, suffit à caractériser l'association de malfaiteurs terroriste (CA Paris, 8 avril 2009). De même, constitue une AMT le fait pour un individu d'entretenir des discussions sur internet avec un membre d'AQMI, aux termes desquelles il a accepté le principe de créer une cellule opérationnelle sur le sol européen et discuté de cibles potentielles pour de futures opérations terroristes (Tribunal correctionnel de Paris, 4 mai 2012). Encore, le fait pour un mis en cause de fournir des armes et munitions, un gilet pare-balles et des fonds à un individu « dont il n'ignorait pas sa capacité à commettre des actes en lien avec son idéologie radicale djihadiste », suffit à caractériser l'infraction terroriste, même sans connaissance précise des intentions de cette personne (Cass. crim, 7 oct. 2016).

Il n'est pas non plus nécessaire, pour caractériser l'infraction, d'identifier précisément tous les membres de l'association de malfaiteurs, ni même la fonction ou le rôle précis confié à la personne mise en cause au sein de la structure. Sa seule appartenance au groupe terroriste suffit, dès lors qu'il est démontré qu'il y a adhéré volontairement et avait une connaissance, au moins générale, du but terroriste poursuivi.

En s'inscrivant dans une logique de prévention et d'anticipation de la menace, plutôt que de réaction, le juge a par la même occasion intégré en partie la logique guidant l'action des services de renseignement et fait un pas dans leur direction.

B. L'interpénétration croissante des sphères judiciaire et du renseignement

L'interpénétration entre les sphères de la justice et du renseignement se caractérise par l'entrée de la justice dans le monde du renseignement, et par la mise en place dans les faits d'un embryon de « statut » du renseignement dans la procédure judiciaire.

i. L'entrée du juge dans le monde du renseignement

Les services judiciaires spécialisés

Compte tenu de la particularité de leurs missions, les magistrats affectés aux pôles et juridictions spécialisés ont par nature vocation à entretenir des relations plus privilégiées avec certains services de renseignement. C'est notamment le cas ponctuellement au sein des juridictions interrégionales spécialisées (JIRS). Mais cette communication privilégiée intéresse au premier chef le pôle anti-terroriste, au sein du tribunal de grande instance de Paris, qui dispose, dans les faits, d'une compétence quasi exclusive [4] en matière de terrorisme et qui se trouve, à ce titre, en relation quotidienne avec les services de renseignement, en particulier la Direction générale de la sécurité intérieure (DGSI), qui présente la particularité d'être à la fois un service de renseignement de sécurité et un service de police judiciaire spécialisé.

Cette communication directe entre les magistrats et personnels judiciaires spécialisés et les services du renseignement a d'ailleurs été officiellement consacrée récemment par la loi n° 2017-258 du 28 février 2017 relative à la sécurité publique [5].

Liens avec l'Unité de coordination de la lutte anti-terroriste (UCLAT)

Le ministère de la justice est également représenté, par sa direction des affaires criminelles et des grâces (DACG), aux réunions hebdomadaires organisées par l'UCLAT.

Au cours de ces réunions, les représentants des services de la communauté du renseignement, ainsi que les services associés, partagent les principaux éléments d'actualité en lien avec leurs activités, dans un objectif de bonne coordination.

La présence d'un représentant de la justice - en pratique un magistrat de la DACG - au cours de ces réunions, permet un échange d'informations mutuellement profitable. Le ministère de la Justice y recueille des informations utiles concernant des opérations en cours, mais il peut également apporter aux services de renseignement certaines informations dont ces derniers n'ont pas toujours connaissance, en particulier s'agissant des phases postérieures à l'enquête stricto sensu (audience, ou post-jugement, notamment en cas d'incarcération), sur laquelle

ils ont par nature une visibilité moindre.

La justice dans la communauté du renseignement : le renseignement pénitentiaire

Essentiel à la bonne gestion de la détention, le renseignement pénitentiaire a toujours existé, au moins officieusement. Il suscite aujourd'hui un intérêt renouvelé dans le contexte de la détection des mouvements de repli identitaire et de radicalisation en détention, et plus généralement au soutien des missions de lutte antiterroriste et la répression de la criminalité nationale et transnationale.

Le renseignement pénitentiaire a connu une première reconnaissance institutionnelle au niveau central en 2003, avec la mise en place d'un bureau spécifique (EMS3) au sein de la direction de l'administration pénitentiaire (DAP) du ministère de la justice, coiffant un maillage régional (directions interrégionales) et local (établissements pénitentiaires).

Brièvement supprimé en 2015 [6], le bureau du renseignement pénitentiaire était toutefois rapidement rétabli, après l'adoption de la loi du 3 juin 2016 sur le terrorisme et le crime organisé, qui a officiellement ajouté le renseignement aux missions habituelles de l'administration pénitentiaire [7].

La loi du 28 février 2017 précitée a par ailleurs créé un titre V bis dans le Code de la sécurité intérieure traitant spécialement « du renseignement de sécurité pénitentiaire » (article L855-1CSI).

Désormais, l'administration pénitentiaire fait officiellement partie de la catégorie des « services non spécialisés de renseignement », avec pour mission d'oeuvrer également « à la prévention des évasions et assure[r] la sécurité et le bon ordre des établissements pénitentiaires ou des établissements de santé destinés à recevoir des personnes détenues et participe [r] à la prévention du terrorisme, de la criminalité et de la délinquance organisées ».

Un bureau central du renseignement pénitentiaire est créé au sein de la DAP du ministère de la Justice, avec un projet de renforcement significatif des effectifs. Au niveau interrégional, des cellules, composées d'agents habilitées « secret défense », sont chargées de faire le lien avec les autres structures du renseignement intérieur. Au niveau des établissements eux-mêmes, des officiers habilités spécialement formés et dédiés à cette nouvelle fonction sont en cours de déploiement.

Le rattachement officiel de la justice (à travers l'administration pénitentiaire) à la communauté du renseignement est un enjeu important puisque, à côté des moyens humains, financiers et matériels qu'elle procure, la qualité de « service non spécialisé de renseignement » lui ouvre l'accès, pour l'accomplissement de ses missions, à certaines des techniques spéciales de renseignement limitativement énumérées au titre V du livre VIII du Code de la sécurité intérieure [8] (notamment la sonorisation de lieux, les écoutes téléphoniques, etc.).

ii. L'aménagement de passerelles entre le renseignement et le judiciaire s'agissant de la preuve

Procéduralement, le juge et le renseignement ont longtemps évolué dans des sphères totalement hermétiques, sans réelle interaction.

Comme dans la plupart des pays de droit continental, le renseignement n'a pas en France de statut probatoire particulier. Judiciairement, il n'est utilisé en pratique que pour initier ou orienter une enquête, sous la forme d'un rapport des services joint en procédure après avoir été « blanchi », c'est-à-dire expurgé de toute mention de nature à révéler la source ou la méthode utilisée pour l'obtenir. Compte tenu du caractère souvent très parcellaire des informations ainsi transmises, il revient ensuite aux enquêteurs de les confirmer ou de les infirmer en utilisant les techniques d'enquêtes habituelles. Ce n'est donc pas le renseignement lui-même qui servira de preuve, mais les éléments recueillis dans le cadre de la vérification effectuée en police judiciaire.

Le juge français est d'ailleurs en général tenu totalement à l'écart des questions intéressant l'activité de ces services. Contrairement à son homologue américain [9], anglais ou hollandais, le juge (ou le procureur) français, même spécialisé (sauf rares exceptions, notamment en matière terroriste), ne dispose pas d'une habilitation à connaître des éléments classifiés au titre du secret de la défense nationale, ce qui le prive de facto de l'accès à la majorité de la production des services de renseignement. De plus, les principes essentiels du procès pénal l'empêchent d'en faire état en procédure en l'absence de mécanismes juridiques permettant de garantir la confidentialité des éléments classifiés (principe de l'audience publique [10], principe du contradictoire et d'accès au dossier, etc.).

Rejoignant certains systèmes juridiques, et notamment les États-Unis d'Amérique ou les Pays-Bas, qui ont développé un régime juridique et une doctrine relativement importante concernant la relation fonctionnelle entre les services judiciaires et les services de renseignement, le législateur français a très récemment commencé à s'y intéresser en mettant en place plusieurs réformes aménageant pour la première fois des passerelles, facilitant la communication et les transferts d'information.

Il arrive d'abord que des éléments en possession des services de renseignement, généralement classifiés, apparaissent nécessaires à la manifestation de la vérité dans une enquête judiciaire. Lorsque ces documents ne sont pas spontanément transmis par le service détenteur, le législateur a mis en place un mécanisme spécifique autour d'une autorité administrative, la Commission du Secret de la Défense Nationale (CSDN). Au terme d'une procédure détaillée aux articles L2312-1 et suivants du Code de la défense, la CSDN délivre un avis favorable ou défavorable à la requête en déclassification, qui ne lie pas juridiquement le ministre compétent, mais qui dispose en pratique d'une autorité morale indiscutable puisque les ministres saisis le suivent dans 95% des cas [11]. Une fois déclassifiés, ces éléments peuvent être versés au dossier et seront soumis au principe du contradictoire [12].

Lorsque la découverte d'éléments classifiés se fait de manière incidente, par exemple au cours d'une perquisition judiciaire, la loi a également prévu un mécanisme permettant de saisir ces éléments, puis de les verser en procédure une fois déclassifiés. C'est là aussi la CSDN qui servira d'interface, conformément à l'article 56-4 du Code de procédure pénale.

Réciproquement, la loi du 28 février 2017 relative à la sécurité publique a récemment ouvert la possibilité pour les magistrats du pôle judiciaire anti-terroriste de Paris de communiquer aux services de renseignement, spontanément ou à leur demande, « copie des éléments de toute nature figurant dans ces procédures et nécessaires à l'exercice des missions de ces services en matière de prévention du terrorisme ».

iii. Le développement d'un statut judiciaire protecteur des agents, des sources et des méthodes de renseignement

Parallèlement aux mécanismes créés pour permettre une meilleure circulation de l'information et de la preuve entre la sphère du renseignement et la sphère judiciaire, le législateur français a progressivement adopté une série de mesures visant à protéger spécifiquement les intérêts légitimes des services de renseignement dans le cadre des procédures judiciaires. On observe ainsi progressivement le développement de facto d'un « statut » du renseignement dans la phase judiciaire dont l'enjeu central consiste à permettre l'utilisation des renseignements détenus par les services d'une manière conforme aux principes du procès équitable, sans compromettre la sécurité des agents et la protection des sources et des méthodes.

S'agissant en particulier de l'audition des agents des services de renseignement, la loi est intervenue récemment à plusieurs reprises pour garantir leur anonymat. Ainsi, l'article 656-1 du Code de procédure pénale [13] dispose que lorsque le témoignage d'un agent d'un service de renseignement est requis au cours d'une procédure judiciaire sur des faits dont il aurait eu connaissance lors d'une mission intéressant la défense et la sécurité nationale, son identité réelle ne doit jamais apparaître au cours de la procédure judiciaire. Le cas échéant, son appartenance à l'un de ces services et la réalité de sa mission sont attestées par son autorité hiérarchique. Les questions posées ne doivent avoir ni pour objet ni pour effet de révéler, directement ou indirectement, la véritable identité de cet agent. Les auditions sont reçues dans des conditions permettant la garantie de son anonymat. Par ailleurs, le législateur a prévu, s'il est indiqué par l'autorité hiérarchique que l'audition requise, même effectuée dans les conditions d'anonymat, comporte des risques pour l'agent, ses proches ou son service, que cette audition est faite « dans un lieu assurant l'anonymat et la confidentialité. Ce lieu est choisi par le chef du service et peut être le lieu de service d'affectation de l'agent. » Cet article est tout à fait remarquable en ce qu'il accorde à cette catégorie particulière de témoin un privilège tout à fait exceptionnel en procédure pénale résidant dans la possibilité d'imposer au juge le lieu de son audition.

S'agissant des agents infiltrés, les garanties sont encore plus importantes puisque leur audition est expressément exclue par l'article 706-86 du Code de

procédure pénale. Seul l'officier de police judiciaire sous la responsabilité duquel se déroule l'opération d'infiltration peut ici être entendu en qualité de témoin sur l'opération.

Enfin, toujours pour garantir la protection des agents des services spécialisés agissant dans un cadre judiciaire, et uniquement en matière de lutte contre le terrorisme, la loi n°2006-64 du 23 janvier 2006 a quant à elle prévu la possibilité à l'article 706-24 du Code de procédure pénale, sur autorisation du procureur général près la cour d'appel de Paris, d'identifier les officiers et agents opérant en police judiciaire uniquement par leur numéro d'immatriculation administrative. En effet, habituellement, les actes de procédure doivent comporter les noms et prénoms des officiers de police judiciaire chargés de diligenter l'enquête, ces mentions permettant de vérifier la compétence - notamment territoriale - de l'officier de police judiciaire (OPJ). Dans le cadre de la lutte contre le terrorisme, ces mentions nominatives peuvent cependant présenter des risques pour la sécurité des enquêteurs, en les exposant à d'éventuelles représailles des personnes mises en cause. Les agents concernés peuvent également être autorisés à déposer ou à comparaître comme témoins sous ce même numéro. En pratique, ces dispositions – qui bénéficient en particulier aux OPJ de la Direction général de la sécurité intérieure (DGSI) – ont rapidement été mises en pratique et cette autorisation est aujourd'hui généralisée à toutes les procédures terroristes traitées par les services spécialisés. La révélation de l'identité d'un agent infiltré est sanctionnée d'une peine de cinq ans d'emprisonnement, portée à dix ans si cette révélation a causé la mort de l'enquêteur ou d'un membre de sa famille.

Ces dispositions procédurales spécifiques peuvent par ailleurs être utilement complétées par d'autres mécanismes procéduraux, non spécifiquement mis en place pour les services de renseignement, mais qui peuvent se révéler pertinents dans ce contexte, notamment en cas d'auditions et de confrontations : audition sous X (art. 706-58 et s. CPP), dispositifs techniques permettant l'audition à distance et avec distorsion de la voix (art. 706-61 CPP), dispositif applicable à la protection des « repentis » et à certains témoins[14] (art. 706-63-1 CPP, décret n°2014-346 du 17 mars 2014).

Après une phase d'ignorance réciproque, le juge et le renseignement semblent donc désormais évoluer vers une coopération mutuellement profitable, dans un contexte notamment de recherche de plus grande efficacité opérationnelle en matière de lutte contre le terrorisme. Pour inscrire cette évolution dans le respect des règles de l'État de droit, des mécanismes de contrôle doivent également être mis en place.

II. La reconnaissance d'une nouvelle mission de contrôle par le juge de l'action des services

Parallèlement à la création de ponts procéduraux permettant des interactions opérationnelles réciproquement profitables entre les sphères du renseignement et de la justice, on observe l'émergence d'un type de relation tout à fait nouveau entre le juge et le renseignement s'agissant du contrôle de l'action des services.

A. Le contrôle renforcé du renseignement intérieur

C'est sans doute l'une des évolutions les plus spectaculaires en la matière. La conception prévalant traditionnellement en France excluait en effet en substance toute possibilité de contrôle réel et direct par le juge de l'action des services, ce contrôle étant conçu comme relevant du Parlement (contrôle général de l'action des services et du budget) et de l'exécutif (contrôle et direction de l'activité opérationnelle). La situation a récemment connu un profond bouleversement.

i. Le contrôle indirect de l'action des services : la déclassification

De plus en plus souvent, sous l'impulsion notamment des parties civiles dans les affaires de terrorisme, les magistrats demandent à verser en procédure des éléments détenus par les services de renseignement. Le plus souvent classifiés, ces éléments ne peuvent être communiqués qu'au terme de la procédure de déclassification précédemment évoquée. Lorsque les faits sont commis à l'étranger, notamment sur des zones de conflit difficiles d'accès pour les enquêteurs, ces éléments peuvent d'ailleurs être particulièrement importants. Dans l'affaire concernant la mort en 2011 de deux otages français enlevés par AQMI au Niger, il a ainsi été possible de verser en procédure les enregistrements vidéo de l'intervention des forces spéciales,

dans un contexte de recherche des circonstances exactes ayant conduit à la mort des deux otages. Bien que la communication de tels éléments intervienne uniquement dans un contexte de recherche de la vérité, et non pour contrôler l'action des services, la frontière en pratique apparaît parfois tenue avec un « contrôle » de fait, a posteriori, qui apparaît d'ailleurs discutable à plusieurs égards.

ii. Le contrôle juridictionnel

Mais l'innovation essentielle en la matière résulte de la loi du 24 juillet 2015 relative au renseignement qui a, pour la première fois, donné au juge un véritable pouvoir juridictionnel de contrôle sur l'action des services de renseignement lorsqu'ils ont recours à des mesures de surveillance constituant une ingérence dans la vie privée.

Le législateur a choisi de confier au Conseil d'État, en premier et dernier ressort, par voie d'action ou d'exception, l'ensemble du contentieux de la régularité de la mise en oeuvre des techniques de renseignement.

Ce contrôle juridictionnel peut intervenir à tout moment de la procédure, soit sur saisine de la Commission nationale de contrôle des techniques de renseignement (CNCTR)[15] lorsque le Gouvernement décide de ne pas suivre son avis, ou directement sur saisine de tout justiciable ayant un intérêt direct et personnel qui soupçonnerait la mise en oeuvre à son endroit d'une mesure de surveillance.

Afin de concilier les exigences de la doctrine du renseignement et celles du procès équitable, la procédure suivie devant le Conseil d'État déroge au Code de justice administrative sur plusieurs points essentiels : l'instruction est non contradictoire et couverte par le secret de la défense nationale ; une audience séparée est prévue pour le requérant et pour les services (cette dernière se tenant à huis clos), et la décision est limitée à son dispositif.

Les pouvoirs juridictionnels sont néanmoins réels puisque la haute juridiction peut accéder à l'ensemble des documents et informations détenus par les services, aucun secret ne lui étant opposable[16]. Elle peut, afin de pallier l'impossibilité pour le justiciable de soulever des moyens alors qu'il ne connaît pas la mesure en cause, se saisir de tout moyen, même d'office. Le Conseil d'État dispose des pouvoirs les plus larges d'annulation, d'indemnisation ou d'injonction.

S'il est trop tôt pour tirer un bilan qualitatif de cette importante réforme[17], elle apparaît néanmoins représenter un véritable tournant en la matière, plaçant le juge (administratif) au coeur du contrôle juridictionnel de l'action des services de renseignement.

B. Le contrôle limité du renseignement extérieur

Contrairement au renseignement intérieur, les opérations spéciales des services de renseignement font traditionnellement l'objet d'un encadrement juridique moins développé. La situation semble toutefois évoluer aujourd'hui, avec pour enjeu principal la question de la responsabilité (civile, administrative et surtout pénale) des agents des services de renseignement devant les juridictions françaises[18].

Les opérations du renseignement extérieur se trouvent aujourd'hui beaucoup plus exposées, y compris judiciairement[19]. Les services en ont bien conscience et y voient un élément de fragilisation de leur action. Un certain nombre d'aménagements juridiques sont ainsi intervenus au cours des dernières années, dans le but d'en clarifier le statut juridique.

Le législateur a d'abord inscrit explicitement dans la loi, à l'article L4123-12 II du Code de la défense, que « n'est pas pénalement responsable le militaire qui, dans le respect des règles du droit international et dans le cadre d'une opération mobilisant des capacités militaires, se déroulant à l'extérieur du territoire français ou des eaux territoriales françaises, quels que soient son objet, sa durée ou son ampleur, y compris la libération d'otages, (..) exerce des mesures de coercition ou fait usage de la force armée, ou en donne l'ordre, lorsque cela est nécessaire à l'exercice de sa mission ». Ces dispositions ne valent toutefois que dans un contexte d'opération militaire extérieure officielle, ce qui couvre pas l'ensemble des opérations extérieures menées par les services de renseignement. Un militaire ayant participé une opération extérieure secrète reste donc susceptible, le cas échéant, de voir sa responsabilité juridique pénale et civile engagée devant son juge national.

La loi du 24 juillet 2015 relative au renseignement a également introduit des éléments nouveaux allant dans le sens d'une meilleure protection juridique des agents. Le législateur

a d'abord entendu donner une base législative élargie à la capacité du renseignement extérieur français à mener, y compris à l'étranger, des actions d'entrave face à certains risques ou menaces affectant la sécurité nationale [20].

Surtout, le législateur a manifestement cherché à clarifier la question de la responsabilité pénale des agents impliqués dans des actions clandestines à l'étranger. Le nouvel article L862-2 du Code de la sécurité intérieure dispose désormais, de manière expresse, que les « agents des services spécialisés de renseignement sont pénalement responsables de leurs actes dans les conditions définies au titre II du livre Ier du Code pénal ». Ce faisant, le législateur renvoie au droit commun de la responsabilité pénale et plus particulièrement à l'application de l'article 122-4 du Code pénal, qui prévoit qu'un agent qui accomplit un acte commandé par l'autorité légitime n'engage pas sa responsabilité, sauf lorsque l'acte en question apparaît « manifestement illégal ». Il est toutefois permis de s'interroger sur la portée pratique réelle de cette disposition dans le cas des opérations clandestines des services de renseignement dont le caractère illicite peut parfois apparaître manifeste, au moins au regard de la loi localement applicable.

C'est peut-être la raison pour laquelle le législateur a également introduit l'article L862-1 dans le Code de la sécurité intérieure, accordant à ces mêmes agents un mécanisme de protection proche de celui applicable pour les militaires en opération à l'article 698-2 CPP. S'agissant en effet de « faits commis hors du territoire national, à des fins strictement nécessaires à l'accomplissement d'une mission commandée par ses autorités légitimes, par un agent des services mentionnés à l'article L811-2 », l'article L862-1 CSI prévoit que le procureur de la République ne peut pas engager de poursuites avant d'avoir informé au préalable le ministre concerné (en l'espèce, le ministre de la Défense, s'agissant des opérations de la Direction générale de la sécurité extérieure (DGSE)) et recueilli son avis qui sera versé en procédure si celle-ci est engagée.

Dans ce contexte, un éclaircissement juridique reste souhaitable afin d'éviter de placer le juge national dans une position inconfortable d'arbitre entre les enjeux opérationnels liés à l'action des services de renseignement extérieur et le respect d'un cadre juridique national pas toujours adapté à ces spécificités.

Notes :

1. La portée du secret de l'enquête prévue par le Code de procédure pénale n'est aucunement comparable à la protection légale de la confidentialité de l'action des services de renseignement, notamment à travers la classification des objets et des informations sensibles.
2. Sauf s'agissant du contre-espionnage sur le sol américain, qui était lui-même confié à un service organiquement séparé de la police judiciaire au sein même du FBI.
3. Les réflexions autour de l'articulation entre renseignement et justice, catalysés par la lutte contre le terrorisme, ne se limitent pas à la France ou aux États-Unis, mais concernent aujourd'hui la plupart des États démocratiques. Ils se traduisent par de nombreuses initiatives au niveau international visant à identifier des lignes directrices en la matière autour d'un équilibre satisfaisant entre efficacité répressive et respect des principes de l'État de droit. Voir notamment les recommandations du Forum Global Contre le Terrorisme (GCTF) sur « l'utilisation et la protection du renseignement lors d'enquêtes et de poursuites menées par le secteur de la justice pénale et fondées sur l'Etat de droit » : https://www.thegctf.org/Portals/1/Documents/Framework%20Documents/A/GCTF-Rabat-Good-Practice-6-Recommendations-FRE.pdf
4. Il s'agit aux termes de la loi d'une compétence « concurrente », c'est-à-dire partagée avec les parquets locaux territorialement compétents (article 706-17 CPP). La pratique fait toutefois apparaître un traitement quasi exclusif des affaires terroristes à Paris, à l'exception des contentieux liés aux faits d'apologie qui, pour une bonne administration de la justice, peuvent faire l'objet d'un traitement local, après consultation avec le pôle anti-terroriste de Paris.
5. Article 706-52-2 CPP (procureur de la République de Paris et magistrats instructeurs anti-terroristes) et art. L132-10-1 4° CSI (juges de l'application des peines et services d'insertion et de probation).
6. La Garde des Sceaux considérait en substance que la mission de renseignement n'était pas compatible avec la mission première des agents de l'administration pénitentiaire et s'était opposée à la reconnaissance du renseignement pénitentiaire dans la communauté du renseignement au moment des discussions de la loi renseignement en 2015.
7. Selon des modalités précisées par le décret n° 2017-36 du 16 janvier 2017 relatif à la désignation des services relevant du ministère de la Justice autorisés à recourir aux techniques mentionnées au titre V du livre VIII du Code de la sécurité intérieure, pris en application de l'article L811-4 CSI.
8. Art. L811-4 CSI.
9. Voir notamment le Classified Information Procedures Act (CIPA) de 1980, qui organise, en substance, un mécanisme permettant de faire entrer en procédure des éléments fournis par les services de renseignement, qui peuvent dès lors être utilisés comme des preuves. Cette procédure, très originale, repose sur une négociation entre la partie poursuivante et le juge, en consultation avec la défense, afin de déterminer s'il est nécessaire ou non (au vu des principes fondamentaux du procès tel que les « discovery rules », équivalent pour partie de notre principe du contradictoire) d'introduire en procédure des éléments confidentiels à charge ou à décharge. S'il l'estime nécessaire, le juge peut décider de recourir à des éléments dits « de substitution », c'est-à-dire accepter un document préparé par l'accusation dont sont retirées les mentions et informations non strictement nécessaires à la cause, qui sera versé au dossier en lieu et place du rapport original.
10. La protection des secrets de la défense nationale n'est pas un motif de recours au huis clos à l'audience, sauf le cas très spécifique des infractions en matière militaire en temps de paix (article 698-9 CPP).

11. Voir le Rapport 2016 de la CSDN (portant sur 2013-2015).

12. Par exemple, en novembre 2016, 130 documents de la DGSI et de la DGSE en lien avec les attentats du 13 novembre 2015 étaient notamment déclassifiés et transmis aux magistrats instructeurs en charge du dossier pour y être versés en procédure.

13. Modifié en dernier lieu par la loi n°2016-483 du 20 avril 2016 relative à la déontologie et aux droits et obligations des fonctionnaires.

14. Ce dispositif prévoit notamment la possibilité d'user d'une identité d'emprunt, sur autorisation du président du TGI de Paris.

15. Créée par la loi du 24 juillet 2015, la CNCTR est une autorité administrative indépendante chargée de contrôler l'utilisation des moyens de surveillance par les services de renseignement français. La CNCTR rend des avis sur les demandes de placement sous surveillance d'une personne. La CNCTR est composée de neuf membres (art. L831-1 CSI) : quatre parlementaires, deux membres du Conseil d'État, deux magistrats de la Cour de cassation, ainsi qu'une personnalité qualifiée.

16. Son contrôle est donc plein et entier, contrairement à la situation antérieure (cf. CE Assemblée, 6 novembre 2002, Moon).

17. Une première série d'arrêt a été rendue le 8 février 2017 par la formation spécialisée du Conseil d'État.

18. L'éventuelle responsabilité des agents dans le cadre d'une procédure judiciaire ouverte à l'étranger relèverait de la souveraineté du pays concerné.

19. Voir notamment Vincent Nouzille, Les tueurs de la République, Fayard, 2015.

20. Le nouvel article L.811-2 du Code de la sécurité intérieure dispose que les services spécialisés de renseignement ont notamment pour missions en France et à l'étranger de contribuer « à l'entrave » des « risques et des menaces » susceptibles d'affecter la vie de la Nation.

OUVRAGES RÉCENTS

PARCOURS D'UN JUGE DU SANG CONTAMINÉ...À L'ÉRIKA

AUTEUR : JOSEPH VALANTIN

EDITEUR : SABRES ET LYS

Pour Balzac, le juge d'instruction est l'homme le plus puissant de France. Pour tous, il fait peur et, avec lui, tous les juges. Sans même avoir été choisi par ses concitoyens, ses décisions peuvent froidement détruire des vies. Pourtant, derrière cette apparence d'inhumanité, de fonctionnement froid et insensible, il y a des juges qui doutent, qui pleurent, qui aiment.

L'auteur, magistrat ayant été amené à juger de très nombreuses affaires dont certaines très médiatiques comme celle du sang contaminé et du naufrage de l'Erika, dévoile ici ses émotions, ses regrets, sa tendresse, ses difficultés, ses angoisses, ses erreurs aussi. Il montre aussi les coulisses de ces théâtres de la vie que sont les tribunaux.

Selon lui, pour bien juger, il faut comprendre sans pour autant admettre. Sorti de l'école nationale de la magistrature, Joseph Valantin a d'abord exercé à Morlaix et Brest comme juge d'instruction, avant de présider un tribunal correctionnel à Brest puis Rouen, puis les cours d'assises de la Somme, de l'Aisne et de l'Oise. Nommé conseiller à Paris en 1992 et affecté à une chambre correctionnelle, il a participé, notamment, au jugement de l'affaire dite "du sang contaminé" avant de rejoindre une chambre civile puis commerciale. Revenu au droit pénal en 1997, à la chambre dite de la presse, et affecté en même temps au tribunal des forces armées de Paris, il a été nommé en 2002 à Versailles, pour présider les Cours d'assises des Hauts de Seine et des Yvelines, puis une chambre en partie spécialisée dans les mineurs. En 2008, il revient à Paris pour juger les responsables du naufrage de l'Erika et prend sa retraite aussitôt après.

LES CELLULES DE RENSEIGNEMENT FINANCIER : UN OBJECTIF COMMUN, DES APPROCHES DIFFÉRENTES

GUILLAUME BÈGUE

DOCTEUR EN DROIT, CHARGÉ D'ENSEIGNEMENT, UNIVERSITÉ DE RENNES 1,
MEMBRE DE L'IRJS (INSTITUT DE RECHERCHE JURIDIQUE DE LA SORBONNE)

Les Cellules de renseignement financier (CRF) forment la clé de voûte des politiques de lutte contre le blanchiment de capitaux et le financement du terrorisme. Leur timide apparition dans les années 1990 s'est muée en un positionnement prépondérant puisqu'elles forment aujourd'hui un maillage international tel que souhaité par le GAFI (Groupe d'action financière).

En effet, elles n'ont cessé de connaître un développement croissant tout au long de ces vingt dernières années, avec une accélération notable suite aux attentats de New-York (mandat de lutte contre le financement du terrorisme) et la crise de 2007-2008 (mandat de lutte contre le blanchiment du produit de la fraude fiscale). Réunies sous l'égide du Groupe Egmont, les 152 cellules plus ou moins dotées en ressources financières et humaines qui composent ce réseau international d'échange d'informations dans la lutte globale contre la criminalité financière sont incontournables.

À l'étude du rôle et de la mission des CRF (I), qui sont relativement identiques entre les pays, il pourrait être légitimement déduit que les bases légales et les mécanismes que les législateurs instituent sont similaires. Or, l'analyse comparée des systèmes déclaratifs nationaux soulignant les disparités existantes (II) démontre que c'est loin d'être le cas.

I. Le rôle et la mission des Cellules de renseignement financier

Une fois l'analyse de l'information effectuée et la constitution des dossiers réalisés par une CRF au niveau national, la coopération internationale est l'étape ultime du processus déclaratif.

A. L'analyse de l'information et la constitution de dossiers

Institutionnalisées et reconnues[1], les CRF ont un rôle clé dans le système de prévention de LAB./CFT[2] (lutte contre le blanchiment de capitaux et le financement du terrorisme). Dans l'éventail aujourd'hui élargi de leurs missions[3], elles gardent pour principale fonction de collecter, traiter et enrichir toutes les déclarations émanant des intermédiaires professionnels assujettis[4]. Elles fournissent ainsi des informations qui pourront mener à l'ouverture d'enquêtes et potentiellement aboutir à des poursuites judiciaires, ou qui viennent au soutien d'enquêtes déjà diligentées par les services judiciaires en matière de blanchiment d'argent et de financement des activités terroristes. C'est l'aboutissement de la chaîne de déclaration qui parachève l'affaiblissement du principe de confidentialité.

En pratique, une fois que l'information utile est extraite des déclarations, les experts des cellules vont l'analyser, la classer, et la transformer à des fins de constitution de notes d'information qui seront transmises aux autorités de police ou judiciaires lorsqu'il ressort du dossier une très forte présomption voire, plus rarement, une certitude de blanchiment. Ce qui s'avère difficile est la transformation du soupçon initial en une présomption de blanchiment. Cela implique un examen minutieux des déclarations effectué par les analystes toujours plus nombreux et spécialisés des CRF qui,

grâce à leurs compétences, jugeront de la gravité des opérations financières déclarées et du « potentiel d'exploitation judiciaire » de chaque dossier.

B. La coopération internationale

i. Le Groupe Egmont

Sur le fondement de textes internationaux ou à portée régionale[5], la coopération entre les CRF n'a cessé de croître lors de ces quinze dernières années. La coopération transnationale étant essentielle à une harmonisation de la lutte anti-blanchiment, les CRF échangent des informations entre elles et, sur autorisation, avec les autres autorités chargées de la lutte contre la criminalité en général (ex : services des douanes, administrations fiscales, organismes de sécurité sociale).

La création du Groupe Egmont en 1995 est la concrétisation du besoin d'échanger de l'information dans le cadre de la coopération internationale, entre autres objectifs[6]. La charte de ce groupe opérationnel, dont le secrétariat est basé à Toronto et qui est composé de 150 membres, prévoit, sous condition de réciprocité, d'agrément mutuel et de protection des données échangées, l'échange à titre gracieux d'informations permettant la conduite d'analyses de cas de soupçon de blanchiment de capitaux ou de financement du terrorisme[7]. Ce document décrivant les rôles et responsabilités des membres indique que ceux-ci sont liés par leur adhésion au Groupe. Ils doivent ainsi participer à des groupes de travail régionaux ainsi qu'aux réunions plénières.

ii. La coopération bilatérale

La coopération bilatérale est l'autre moyen utilisé par les CRF pour communiquer entre elles. Allégé des pesanteurs institutionnelles et organisationnelles qu'un groupement multilatéral - fut-il modeste dans son organisation comme le Groupe Egmont - engendre, ce procédé de coopération est très efficace dans l'exercice quotidien des missions des CRF. De nombreux accords bilatéraux de coopération ont donc été signés lors de ces deux dernières décennies[8]. Les CRF du Luxembourg[9], TRACFIN (Traitement du renseignement et action contre circuits financiers clandestins) et la CTIF (Cellule de traitement des informations financières) entretiennent des réseaux développés de CRF avec lesquelles elles ont conclu des accords, ce qui permet de nombreux échanges d'informations dont certaines seront utilisées dans le cadre de procédures judiciaires après accord donné par la CRF expéditrice sur la communication d'informations à des tiers[10]. Dès lors, en sus d'être une aide précieuse aux enquêtes internationales, de telles possibilités d'échanges favorisent la constitution de bases de données qui peuvent être gigantesques (c'est le cas de celles du CANAFE (Centre d'analyse des opérations et déclarations financières du Canada) et du FinCEN (The Financial Crimes Enforcement Network).

II. La comparaison des systèmes déclaratifs nationaux

L'étude des CRF démontre la coexistence de systèmes déclaratifs obéissant à des logiques différentes. Ainsi, entre les systèmes purement déclaratifs et ceux qui privilégient une automaticité des déclarations, il en existe d'autres qui mêlent ces deux caractéristiques.

A. Les systèmes purement déclaratifs : la résistance suisso-luxembourgeoise

Le Luxembourg et la Suisse ont fait le choix de systèmes déclaratifs qui peuvent être qualifiés de « purs ». En effet, ces pays ont institué des obligations de déclarations fondées sur l'intervention humaine, avec toute la subjectivité que cela comporte, et ne prévoient pas de déclarations automatiques fondées sur des critères objectifs légalement énumérés par la loi ou les règlements LAB/CFT. Si les autorités luxembourgeoises et la CRF du Parquet économique et financier de Luxembourg ont pu un temps céder à la tentation d'un système déclaratif tendant vers le refus de la considération de la subjectivité[11], provoquant ainsi une augmentation du nombre des déclarations de doute, l'esprit du système reste similaire à la philosophie du déclarant suisse. Ce dernier, bercé par les longues années d'existence d'un simple droit de communication, a cultivé l'art de ne pas déclarer de simples doutes, mais uniquement des soupçons dont la preuve est rapportée, sauf en cas de « gêne » éprouvée par l'assujetti, sentiment non étayé par des motifs raisonnables et qui peut encore aujourd'hui constituer le motif d'une déclaration au MROS (Bureau de communication en matière de blanchiment d'argent). Les chiffres actuels tirés des rapports annuels de la CRF suisse démontrent que les volumes de déclarations ont augmenté mais restent dans les limites d'une croissance des volumes très modérée et ce, depuis de nombreuses années[12]. Ce système est en définitive l'archétype d'un système de déclaration volontaire « pur ».

B. Les systèmes semi-automatiques : l'axe franco-britannique

i. Les déclarations systématiques

Parallèlement à la déclaration spontanée, il perdure dans certains droits des obligations dites systématiques[13] ou automatiques, autrement dit des procédures qui ne font intervenir que des éléments factuels et en aucun cas une appréciation -subjective ou objective- de la part du professionnel. Force est de constater que le droit français maintient plusieurs cas de déclarations automatiques[14], confirmant ainsi la dualité du système français, « semi-automatique », et non purement volontaire contrairement à ce qui est trop souvent compris.

En premier lieu, l'article L561-15-1I du Code monétaire et financier (COMOFI)[15] prévoit une déclaration automatique des « *éléments d'information relatifs à certaines opérations présentant un risque élevé de blanchiment ou de financement de terrorisme en raison du pays ou du territoire d'origine ou de destination des fonds, de la nature des opérations en cause ou des structures juridiques impliquées dans ces opérations* »,un décret précisant les modalités de transmission[16]. Sont visés les éléments d'information à transmettre en cas de risque élevé relatif au pays ou au territoire d'origine ou de destination des fonds (les pays et des territoires non communicatifs (PTNC) notamment), ainsi qu'au type d'opérations ou des structures juridiques concernées. Dans ce dernier cas, sont bien évidemment visés, entre autres, les *Trusts*, les fondations (*Stichting, Anstalt*) et les fiducies.

Enfin, la traditionnelle obligation de déclaration des informations relatives à des opérations qui seraient particulièrement complexes, ou d'un montant inhabituellement élevé ou ne paraissant pas avoir de justification économique ou d'objet licite, est toujours présente (article L561-15-1 II cumulé avec l'article L561-10-2 du CO.MOFI). Si certains auteurs considèrent, à raison, que dans cette dernière hypothèse « ce n'est pas la déclaration qui est systématique mais l'analyse de la situation »[17], il faut bien admettre que l'étude systématique de ces opérations participe au mouvement d'automatisation.

Soulignons que l'automaticité encadrée relative aux PTNC est une spécificité française qui, à première vue, découle des systèmes de déclaration canadien[18] et américain, notamment. En réalité, ceux-ci se caractérisent par une déclaration dont l'automaticité est fondée sur un seuil, faisant fi de tout autre paramètre tel que la localisation géographique. Par ailleurs, elle n'existe pas nécessairement dans tous les autres ordres juridiques nationaux européens[19].

ii. L'automatisation de la déclaration de soupçon

Quant à la déclaration de soupçon, elle tend vers l'automaticité. Pourtant, « le dispositif français de LAB/CFT. n'est pas un système automatique de déclaration ». Ainsi peut-on lire telle affirmation dans les lignes directrices de l'Autorité de contrôle prudentiel et de résolution (ACPR) relatives aux échanges d'informations au sein d'un groupe ou hors groupe[20]. C'est en réalité une reprise de commentaires inclus dans un document antérieur, publié conjointement par l'ACPR et TRACFIN en 2010[21], mais de manière incomplète. En effet, la phrase initiale poursuit « basé exclusivement sur des critères objectifs définis a priori ».

Est dès lors perceptible la volonté des autorités de persuader les assujettis du caractère non automatique du dispositif français dans une tentative de recadrage qui, à défaut d'être convaincante étant donné les analyses factuelles la contredisant, a au moins le mérite de mentionner ce qu'est supposé demeurer le système français tel que conçu initialement. C'est également *a contrario* la reconnaissance, de l'aveu même des autorités, que l'orientation naturelle du système français de déclaration de soupçon est celle d'un dispositif dont les éléments et les résultats tendent vers une automatisation. Il n'y a pas de meilleure illustration que l'observation des textes, leur interprétation et la jurisprudence de ces dix dernières années pour s'en convaincre.

C'est l'une des conséquences de la disparition de l'appréciation subjective que devrait exercer chaque professionnel assujetti. Elle empêche en effet ces derniers de procéder à l'exercice d'objectivation qui, justement, garantirait au dispositif une meilleure efficacité. Car en réalité, c'est tout l'inverse de l'objectif initialement assigné à la politique de prévention de la criminalité financière qui se produit. L'établissement de critères considérés comme « objectifs » mais qui peuvent être source d'automaticité ne permet pas l'objectivation du soupçon ; sont alors créées les conditions propices à l'automatisation du système. Le dispositif français, à l'origine classé dans la première catégorie, est en réalité

un système semi-automatique qui tend malgré lui vers les systèmes automatiques.

Ce phénomène peut être constaté au Royaume-Uni où le nombre de déclarations annuellement est encore bien plus élevé qu'en France[22]. Nos voisins d'outre-Manche ont recueilli près de 354186 déclarations pour la période octobre 2013 - septembre 2014[23], ce qui équivaut à une activité déclarative dix fois supérieure à celle qui prévaut en France. Le nombre très élevé d'assujettis, la sensibilité de la place londonienne comme premier centre financier mondial et le fait que le soupçon n'a pas à être motivé ni conforté par des éléments objectifs expliquent ces chiffres très élevés.

À ce dernier égard, un point d'achoppement, non sans lien avec la réflexion sur l'insuffisant exercice d'objectivation, a trait à la qualité des déclarations, tel que mentionné précédemment. Plusieurs CRF soulignent ce phénomène de banalisation où la quantité est privilégiée à la qualité. La CRF française[24] mais aussi son homologue britannique[25] en sont l'illustration parfaite. Ce phénomène n'atteint pas cependant la démesure nord-américaine.

C. Les systèmes automatiques nord-américains

Les États-Unis ont élaboré un système LAB/CFT très lourd depuis les menaces terroristes grandissantes pesant sur leur pays[26]. Mais de nombreuses lois anti-blanchiment existaient déjà auparavant[27]. À ce jour, un panel de cinq types de déclaration permettant de conserver la trace des opérations financières est en vigueur, mais uniquement trois d'entre elles intéressent les intermédiaires professionnels : la déclaration de transaction en espèces (elle doit être remplie lorsqu'une institution financière reçoit ou verse plus de 10.000,00 USD en espèces) ; la déclaration d'activité suspecte (elle doit être remplie lorsque tout employé d'assujettis a des raisons de soupçonner un individu de se livrer au blanchiment de fonds, indépendamment du volume de la transaction en question) ; le formulaire fiscal 8300 (il doit être rempli par toute personne participant à une entreprise qui reçoit des paiements en espèces, en échange de biens ou de services, dont la valeur dépasse 10.000,00 USD en une seule transaction ou en une série de transactions connexes)[28].

Nos voisins d'outre-Atlantique se sont donc dotés d'un système de déclaration automatique qui ne laisse que peu de place à l'intervention humaine en comparaison des volumes engendrés par l'obligation de déclaration automatique. Leur CRF, le FinCEN[29], dispose de moyens considérables et traitent des millions de déclarations par an[30]. Plus récente, son homologue canadienne a été développée sur le même modèle organisationnel et avec un objectif premier de traçabilité des fonds[31]. Elle a connu une expansion considérable dans les années 2000, rattrapant le retard que le Canada avait en la matière par rapport aux pays pionniers[32]. À l'instar du système américain, le CANAFE reçoit des millions de déclarations annuellement[33] et confirme la nature des systèmes nord-américains qui suivent une logique différente de celle des systèmes européens.

Conclusion

En dépit de leur différences institutionnelles, les CRF partagent un objectif commun de traitement, d'analyse et d'exploitation de l'information qui leur parvient dorénavant par une multitude de canaux (personnes assujetties aux obligations de prévention du blanchiment et du financement du terrorisme, autorités administratives ou judiciaires). Elles sont appelées à toujours plus de coopération, notamment dans le domaine de la lutte contre le financement du terrorisme. À cet égard, le Groupe Egmont a réaffirmé en 2016 l'importance d'une telle coopération lors d'une réunion intersession ayant débouché sur un engagement collectif de la part de représentants de plus de 100 CRF. Cet engagement inclut en particulier l'amélioration des flux d'information relatifs au financement du terrorisme, le renforcement de la coopération avec le GAFI, la fourniture d'indicateurs relatifs au financement du terrorisme pour contribuer à identifier les activités financières suspectes ou encore l'étude du besoin d'élargissement du champ d'application personnel de l'obligation de déclaration de soupçon. Autant de sujets qui apparaissent cruciaux dans le cadre du volet préventif des politiques de LAB/CFT nationales et régionales, et qui renforcent encore un peu plus le rôle que chaque CRF est appelée à jouer dans le futur.

Notes :

1. Les premières CRF ont été créées au début des années 1990. Au niveau international, plusieurs textes ont imposé avec retard aux États signataires des conventions dans le domaine LAB/CFT et la création de CRF. Le groupe Egmont a, le premier, donné la définition d'une CRF comme un « *organisme national central chargé de recevoir (et s'il y est autorisé, de demander), d'analyser et de communiquer aux autorités pertinentes des renseignements financiers [...] aux fins de lutter contre le blanchiment d'argent* » (voir le site internet : www.egmontgroup.org). L'officialisation de ces termes a été effectuée à travers l'art. 7 (1)(b) de la Convention des Nations-Unis contre la criminalité transnationale du 13 décembre 2000, appelée Convention de Palerme : « *Chaque État Partie : s'assure [...] que son droit interne envisage la création d'un service de renseignements financiers qui fera office de centre national de col-*

lecte, d'analyse et de diffusion d'informations concernant d'éventuelles opérations de blanchiment d'argent », v. le site internet www.un.org. Pendant très longtemps, le GAFI fut silencieux sur la notion de CRF. Les expressions « autorités compétentes » ou « administrations nationales » étaient employées mais aucune référence n'était faite quant à l'organisation souhaitée, le statut, ou le rôle exact que devaient remplir ces institutions. Dans son document consultatif publié en mai 2002, le GAFI fit remarquer que le concept de CRF était déjà défini par le groupe Egmont et qu'il n'était pas nécessaire de répéter cette définition (la recommandation 29 a depuis intégré cet aspect). Au niveau européen, la 4e directive reprend dans son art. 32-1 l'obligation faite à tous les États membres de se doter d'une CRF.

2. Concernant la C.R.F. française, v. H. ROBERT, *TRACFIN, « clé de voûte » de la lutte anti-blanchiment en France*, Revue de Droit bancaire et financier., novembre-décembre 2007, p.17 ; Ch. CUTAJAR, *La cellule Tracfin devient un service à compétence nationale*, JCP éd. Ent., n°9, 1er mars 2007, p.3.

3. Les CRF ont par exemple un rôle de formation et de sensibilisation accru auprès des professionnels assujettis et du grand public. Ce rôle est, depuis le début de son existence, dévolu au CANAFE qui a pour mission d'accroître le niveau de sensibilisation et de compréhension du public à l'égard des questions de blanchiment d'argent, v. le site internet du Gouvernement du Canada : www.gc.ca.

4. Art. L561-23 du COMOFI, art. 22 de la loi belge de 1993 modifiée; pour la Suisse, l'ordonnance sur le bureau de communication en matière de blanchiment d'argent (OBCBA), R.O. 2004 4181 du 25 août 2004 décrit les tâches et les responsabilités du MROS.

5. Art. 2-1 de la décision du Conseil 2000/642/JAI du 17 octobre 2000 relative aux modalités de coopération entre les cellules de renseignement financier des États membres en ce qui concerne l'échange d'informations se lit comme suit : « *une unité nationale centrale qui, aux fins de la lutte contre le blanchiment de capitaux, est chargée de recevoir (et, dans la mesure où elle en a le droit, de demander), d'analyser et de transmettre aux autorités compétentes les informations financières communiquées concernant des avoirs suspects d'être des produits du crime, ou requises par les législations ou réglementations nationales* ».

6. Rendre les CRF.autonomes, améliorer leur efficacité opérationnelle et promouvoir la création de nouvelles CRF.

7. L'art. 3.1 de la charte du groupe Egmont est rédigé comme suit : « *All members foster the widest possible co-operation and exchange of information with other Egmont Group FIUs on the basis of reciprocity or mutual agreement and following the basic rules established in the Principles:*

   1) Free exchange of information for pur poses of analysis at FIU level.

   2) No dissemination or use of the infor mation for any other purpose without prior consent of the providing FIU.

   3) Protection of the confidentiality of the information », v. EGMONT GROUP, *Egmont Group of Financial Intelligence Units Char ter*, 30 octobre 2013, p.8.

8. À titre d'illustration, v. les récents accords entre l'unité française et les CRF de Jersey et Guernesey (mai 2015) suite aux échanges institutionnels croissants à la fin de l'année 2014 entre ces unités, v. TRACFIN, *Rapport annuel d'activité Tracfin*, 2014, p.48.

9. La base légale de la coopération internationale pour la CRF luxembourgeoise est l'art. 26-2 du Code d'instruction criminelle. À la fin 2013, le Luxembourg avait signé 31 accords bilatéraux (l'absence des États-Unis est notable).

10. 22 Contrôle Prudentiel et de T.ar ce n' comprends pas)s financiers clandestins) Qui ne sont cependant pas automatiques, v. le cas de la CR.F. luxembourgeoise qui en 2013 a refusé à 14 reprises la communication d'informations par la CRF étrangère à des tiers lorsque la demande ne vise pas des fins de poursuite de l'infraction de blanchiment ou lorsqu'il persiste un risque de compromettre une instruction en cours à Luxembourg, v. C.R.F. DU PARQUET DE LUXEMBOURG, *op. cit.*, p.28.

11. Principalement sous la pression du GAFI et la crainte du rapport d'évaluation publié en 2010 et qui fut effectivement mauvais, notamment pour les aspects répressifs.

12. Avec même une baisse du nombre de déclarations entre 2011 et 2013, v. M.R.O.S., *Rapport annuel 2014, op. cit*, p.9.

13. JurisClasseur Fiscal, *Modalités de l'obligation de déclaration de soupçon*, Fasc. 670-35 III, 03-2012, 3 novembre 2011.

14. Ce caractère automatique existait déjà par les deuxième et troisième alinéas de l'ancien art. L562-2 du COMOFI, qui prévoyaient une obligation de déclaration relative à des circonstances particulières entourant une opération ou une transaction. Il s'agissait respectivement de la participation de bénéficiaires ou de constituants dont l'identité n'est pas connue *in fine*, ou du cas d'une opération ou d'une transaction qui est effectuée avec un client établi dans un pays considéré comme ne respectant pas les principes établis par l'instance internationale de référence (pays « *noirs GAF.* » à l'époque), cette déclaration automatique étant conditionnée au franchissement d'un seuil.

15. Cette disposition a un champ d'application plus large que l'ancien art. L561-15 IV du COMOFI abrogé par la loi n°2013-672 du 26 juillet 2013 et qui reprenait quasiment mot pour mot la formulation longtemps utilisée pour le cas des clients personne morales, des structures sociétaires ou des relations juridiques pour lesquels l'identification du bénéficiaire effectif n'est pas des plus faciles. Il était rédigé ainsi : « *les personnes mentionnées à l'article L561-2 sont également tenues de déclarer au service mentionné à l'article L561-23 toute opération pour laquelle l'identité du donneur d'ordre ou du bénéficiaire effectif ou du constituant d'un fonds fiduciaire ou de tout autre instrument de gestion d'un patrimoine d'affectation reste douteuse malgré les diligences effectuées conformément à l'article L561-5* ».

16. Art. D 561-31-1 du COMOFI. L'ancienne mouture de l'art. L561-15-1 I avait un champ plus réduit qui visait les « *opérations de transmission de fonds effectuées à partir d'un versement d'espèces ou au moyen de monnaie électronique* »

17. P. MICHAUD, *Tracfin, blanchiment et fraude fiscale : les déclarations de soupçon*, J.C.P. Ent. n°42, 15 octobre 2009, p.18.

18. Pour une étude approfondie du système global canadien de prévention des activités de blanchiment de capitaux et de financement du terrorisme, v. G. BÈGUE, *Le système canadien de lutte contre le recyclage des produits de la criminalité et le financement des activités terroristes*, Lettre Sentinel n°38, Juin-Juillet 2006, p.4.

19. Le droit luxembourgeois est un bon exemple puisqu'il se limite à exiger du professionnel du secteur financier qu'il déclare au procureur d'État, dans le cadre de la lutte contre le financement du terrorisme, « *les transactions dans lesquelles interviennent des personnes figurant sur les listes officielles reprenant des terroristes ou organisations terroristes présumés* » (étonnamment non repris en droit français pendant longtemps). Le règlement CE 1781/2006 est également repris dans les textes de la commission de surveillance du secteur financier (CSSF), une mesure qui relève probablement plus du devoir d'information que d'une volonté interprétative du régulateur. V. *id.*, *Transferts de fonds et prévention du blanchiment de capitaux et du financement du terrorisme bancaire*, Banque et Droit, n°117, Janvier-Février 2008, pp.9-20

20. ACP, *op. cit.*, p.7.

21. ACP et TRASCFIN., *Lignes directrices conjointes de l'Autorité de Contrôle Prudentiel et de TRACF.N sur la déclaration de soupçon*, 21 juin 2010, p.3.

22. Faute de protection juridique suffisante et de latitude laissée aux déclarants.

23. TRACFIN a enregistré 36715 déclarations en 2014, un chiffre en progression de 33,7% par rapport à l'année précédente au cours de laquelle pas moins de 27477 déclarations avaient été reçues. Ce chiffre a doublé entre 2009 (17310 déclarations) et 2014, un minimum de 1500 déclarations supplémentaires chaque année étant comptabilisé depuis 2009, v.TRACFIN, 2014, op. cit., p.9. Le responsable de l'institution ne s'attendait pas à un raz-de-marée déclaratif, mais force est de constater que l'augmentation est bien là, v. J.-B. Carpentier, TRACFIN. ne s'attend pas à un tsunami déclaratif, Revue Banque, n°711, mars 2009, p.51.

24. National crime agency, 2014, op. cit., p.9.

25. « Tracfin déplore de trop nombreuses déclarations tardives, portant sur des faits anciens (souvent consécutifs notamment à un contrôle fiscal en cours) », v. TRACFIN, op. cit., p.7.

26. La CRF britannique fait clairement savoir aux déclarants qu'il faut dorénavant privilégier la qualité à la quantité, v. NATIONAL CRIME AGENCY, op. cit., p.8.

27. Les deux textes fondateurs de ce système sont le Bank Secrecy Act (codifié ainsi : 12 USC 1829b, 12 USC 1951-1959, 31 USC 5311-5314 and 5316-5332, et assorti du règlement d'application 31 CFR Chapter X, préc. 31 C.F.R. Part 103) et le Patriot Act, préc. Il n'existe pas de loi anti-blanchiment unique mais une multitude de textes, certains relatifs au blanchiment en général par les grandes lois citées ci-dessus, et d'autres insérés dans les lois réglementant les différentes professions d'affaires, comme par exemple le Federal Deposit Insurance Act pour les assureurs ou le Securities Exchange Act de 1934 pour les courtiers en valeurs mobilières. Dans chacun de ces textes figurent une ou plusieurs dispositions quant à leur obligation de déclarer des opérations suspectes. Dans tous les cas, le mécanisme de déclaration élaboré aux États-Unis est fondé sur l'automaticité des déclarations.

28. Des dispositions relatives à l'obligation de déclaration figuraient dans le Bank Secrecy Act de 1970. Cette loi relative au secret bancaire ne prévoit pas l'incrimination de l'activité de blanchiment mais oblige les institutions financières à créer et à conserver des traces écrites relatives à divers types d'opérations. Cette base a été étoffée par le vote d'autres lois anti-blanchiment (notamment l'Anti Drug Abuse Act de 1988 ou la loi Annunzio-Wylie de 1992).

29. V. le site internet du U.S. Department of State : www.usinfo.state.gov.

30. Financial Crime Enforcement Network.

31. En 2011, près de 15 millions de déclarations d'espèces ont été effectuées, à comparer aux 1,4 millions de déclarations de soupçon, v. F.i.n.c.e.n., Annual Report, Fiscal Year 2011, p.6.

32. Ibid., p.2.

33. G. BÉgue, op. cit.

34. En 2014, le CANAFE a reçu 20 millions de déclarations, dont 80.000 étaient des déclarations de soupçon, v. CANAFE, Rapport annuel de CANAFE, 2014, pp.5-6.

OUVRAGES RÉCENTS

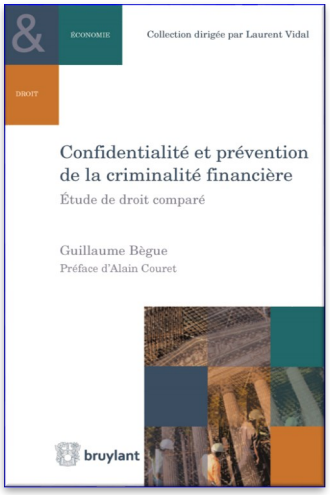
"CONFIDENTIALITÉ ET PRÉVENTION DE LA CRIMINALITÉ FINANCIÈRE"

AUTEUR : G. BÈGUE

EDITEUR : ÉDITIONS BRUYLANT – LARCIER, COLLECTION DROIT ET ECONOMIE

Fruit de quinze ans de travaux de recherches et d'expérience professionnelle, cet ouvrage porte sur les multiples problématiques nées de l'antagonisme entre les éléments constitutifs d'un principe de confidentialité (secret professionnel, protection des données personnelles, devoir de confidentialité, libertés publiques) et les obligations de transparence auxquelles sont assujettis les professionnels du chiffre et du droit (principalement les obligations en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme et celles relatives à la fiscalité (coopération et échange d'informations)).

Cette contribution inédite et très complète revêt une dimension pluridisciplinaire prononcée (aspects juridiques, sociologiques, géopolitiques et économiques). Elle a été rédigée non seulement dans le cadre conceptuel d'une thèse mais aussi et surtout à l'attention de nombreux praticiens. Véritable guide sur la prévention du blanchiment de capitaux et du financement du terrorisme (LAB/CFT), elle réconcilie les obligations de confidentialité aux mesures de transparence imposées au monde bancaire et financier.



Le caractère pratique des nombreux sous-thèmes abordés et la facilité de lecture des analyses et solutions préconisées, tant pour les juristes que les non juristes, devraient répondre aux attentes de nombreux professionnels. Ainsi, les avocats, les sociétés de domiciliation, les gestionnaires de patrimoine indépendants, les notaires ou encore les institutions financières (établissements de crédit, brokers, fonds, établissements de paiement, etc...) au sein desquelles les juristes et surtout les « *Compliance Officers* » exercent leur mission de gestion des risques juridiques et de conformité, seront probablement très intéressés par cet ouvrage.

Par ailleurs, la dimension comparative ravira en particulier les lecteurs de pays francophones dont les législations font l'objet d'une analyse en profondeur, soit le Luxembourg, la France la Suisse et la Belgique. Cet ouvrage pose en outre un éclairage sur certains systèmes de *Common Law* qui sera utile aux professionnels des pays de droit civil dans l'appréhension des problématiques de l'espèce par le monde anglo-saxon. Il apporte enfin, en cette année charnière de transposition de la 4ème directive européenne, de nombreuses clés de décryptage sur l'avenir de la prévention LAB/CFT en Europe.

RAPPORT

COMPTE-RENDU DE LA RÉUNION DE LA COMPAGNIE RÉGIONALE DES COMMISSAIRES AUX COMPTES DE CAEN ET DES PROCUREURS DE LA RÉPUBLIQUE DU RESSORT DE LA COUR D'APPEL DE CAEN

Le 28 avril 2017, s'est tenue au parquet général près la cour d'appel de Caen , la rencontre « traditionnelle » entre la Compagnie régionale des commissaires aux comptes (CRCC) de Caen et les procureurs de la République du ressort de la cour d'appel autour du thème principal de l'obligation de révélation.

Cette rencontre a été l'occasion de revenir sur les dernières modifications du droit national dans le cadre de la mise en conformité avec la réglementation européenne s'agissant, notamment, des modalités d'inscription sur la liste des commissaires aux comptes et sur le processus disciplinaire. Ces modifications marquent une centralisation au niveau national.

Mme Sylvie PETIT-LECLAIR, procureur général, et M. Jean-Max YVER, président de la Compagnie régionale des commissaires aux comptes, ont ouvert la réunion au cours de laquelle plusieurs intervenants se sont succédés pour traiter quatre thématiques.

I. Techniques de la délinquance financière et points de vigilance

Ce thème a donné lieu à l'intervention de M. Didier DUVAL, actuellement responsable de la sécurité financière, la prévention des fraudes et la corruption au sein de la direction de la conformité du groupe Crédit Agricole, invité en sa qualité d'ancien sous-directeur des affaires économiques et financières à la Direction Centrale de la Police Judiciaire (DCPJ).

M.DUVAL a précisé, qu'ayant été commissaire de police en détachement au ministère de la Justice lors du vote de la loi Sapin I relative à la transparence de la vie économique, il a très tôt milité pour une immersion des enquêteurs financiers au sein des services d'enquête chargés de la lutte anti-terroriste. De même, il est un farouche partisan du décloisonnement des services spécialisés dans le cadre d'un secret partagé. Il lui semble primordial de sensibiliser le monde de l'entreprise à son environnement et d'assurer une veille réglementaire dans un cadre très strict et ce, alors même que les poussées normatives sont très fortes - notamment du côté des États-Unis- et lourdes de conséquences.

Il a rappelé que la lutte contre le blanchiment et le financement du terrorisme fait l'objet de la 4ème directive européenne transposable, au plus tard, à la date du 26 juin 2017.

La 3ème directive mise en oeuvre en 2009, a deux conséquences majeures :

- La création de la notion de personne politiquement exposée (s'agissant des infractions de concussion, abus de biens sociaux,... soit d'atteintes à la probité au sens large). Il y a donc obligation d'identifier cette personne politiquement exposée (PPE) : élu national, membre du gouvernement, représentant des établissements publics,.... L'outil anti-blanchiment est

utilisé pour lutter contre la corruption. Il convient également de « surveiller » les PPE étrangères ayant un compte en France.

La 4ème directive directive prévoit l'extension des PPE par la création du PPE dite domestique (dans le cadre du périmètre européen).

- La définition des ayants droit économiques, à savoir les bénéficiaires effectifs d'une entreprise. Comment identifier un acteur physique ayant une activité économique ? Une cartographie est dessinée sur la base de la détention de 25% du capital (en Europe), certains pays fixant ce seuil à 10%.

Il convient de prendre en compte une autre considération tout aussi importante : celle de l'environnement du pays (Justice, services d'enquête, services douaniers…).

Les opérations du « due diligence » sont des vérifications qu'un éventuel acquéreur ou investisseur doit réaliser avant une transaction afin de se faire une idée précise de la situation d'une entreprise. Il faut donc se prémunir contre tout élément négatif d'une opération qui peut être évité -il s'agit d'un devoir élémentaire de précaution- en vérifiant l'honorabilité de tous les acteurs (entrepreneurs, banquiers mais également gestionnaires de fortune).

La loi Sapin II, sur la transparence, la lutte contre la corruption et la modernisation de la vie économique, a pour ambition de porter la législation française au niveau des meilleurs standards européens et internationaux en matière de lutte contre la corruption et de contribuer ainsi à une image positive de la France à l'international.

Dans le volet de la fraude vue de la banque, la lutte contre le blanchiment est un enjeu très fort. Apparue dans la 3ème directive, la lutte contre le blanchiment s'est trouvée « sous les feux des projecteurs » après l'affaire Cahuzac et celle des Panama papers. Il existe une crête très étroite entre optimisation économique et fraude fiscale. Le fait de créer une structure potentiellement illégale n'est pas illégal mais à la condition que l'ayant droit économique déclare cette création à son pays de résidence fiscale.

Les sanctions internationales consistent en un embargo, total ou partiel, ou un gel des avoirs. Les mesures de gel d'avoirs obligent notamment les organismes financiers à geler les avoirs des personnes ou entités désignées dans un règlement européen ou un arrêté. Ces obligations pèsent sur les organismes financiers (banques, organismes d'assurance, transmetteurs de fonds, intermédiaires en financement participatif…). Ces mesures, décidées au niveau international par le Conseil de sécurité des Nations Unies et par l'Union européenne, visent à neutraliser la logistique de l'organisation en cause et la défaillance des services étatiques. Après inventaire des avoirs bancaires de la personne ou de l'organisation concernée, la banque doit figer la situation (il s'agit là d'une obligation de résultat). Aucun flux ne doit plus affecter les comptes. La mesure est valable six mois (renouvelable). Les organismes financiers qui ne respectent pas ce dispositif encourent des pénalités très lourdes.

Les risque est grand pour les entreprises de travailler avec des acteurs sous sanction. Une attention toute particulière doit être portée aux opérations de contournement (recours à des pays « rebonds »). Il convient ainsi de contrôler :

- La devise utilisée. S'il s'agit de dollar, la réglementation des USA est très contraignante ; s'il s'agit de l'euro, le contrôle de la réglementation européenne ou de la législation française doit être effectué. Ce contrôle doit être élargi à la nationalité des acteurs économiques.

- Le flux financier après contrôle du flux marchand. Juridiquement, la banque est propriétaire du compte mis à disposition du client. Aussi, la banque est responsable des flux qui transitent sur ses livres.

- Les opérations bancaires effectuées par les Américains ou des personnes ayant un critère d'américanité. À compter de 50 000 dollars par an, les opérations bancaires doivent faire l'objet d'une déclaration au Trésor américain. Afin de se prémunir, des banques refusent l'ouverture de compte obligeant ainsi la personne à recourir à la procédure de droit au compte (obligation est faite par la Banque de

France).

La corruption crée, au niveau économique, une concurrence déloyale. La recommandation de l'OCDE vise à renforcer la lutte contre la corruption d'agents publics étrangers dans les transactions commerciales internationales.

La loi Sapin II a mis en place de nouveaux dispositifs afin d'assurer l'effectivité et l'efficience des contrôles comptables. En effet, une entreprise corruptrice « n'accepte » jamais la perte que constitue le versement des sommes nécessaires à la corruption. Il y a nécessairement « récupération » de la contre-valeur de la corruption : émission d'une facture pour une prestation fictive ou surfacturation. Le « chemin » emprunté par la facture et les cahiers des charges techniques doivent également faire l'objet de vérification.

La cybercriminalité est largement utilisée dans la commission des fraudes (par le recours au hacking ou via l'ingénierie sociale).

M. DUVAL a terminé son propos en appelant les commissaires aux comptes à faire preuve de pédagogie auprès des entreprises et à les sensibiliser sur les différentes opérations utilisées par les fraudeurs.

II. La réforme européenne de l'audit

M. Simon LUBAIS, ancien président de la CRCC, a ensuite pris la parole.

L'origine et le contexte de la réforme européenne de l'audit

La réforme est née au lendemain de la crise des subprimes aux États-Unis. Trois professions sont concernées : les banquiers, les agents de notation et les auditeurs. La réforme a pour objectif de renforcer la valeur ajoutée de l'audit, de garantir une meilleure indépendance des auditeurs et de concentrer le marché (238 entreprises sont auditées par 130 personnes). La nouvelle réglementation maintient une hétérogénéité évidente de l'audit en Europe.

Les points saillants de la réforme

L'extension en Europe de l'audit adapté dans les PME à la française ; le co-commissariat (spécificité française) acté en Europe ; le maintien du mandat de 6 ans ; deux professionnels ayant exercé la profession de commissaire aux comptes sont désormais membres du H3C (Haut Conseil du Commissariat aux Comptes) ; des normes professionnelles écrites avec le concours paritaire de la profession et un avis -obligatoire- du Conseil national ; la création d'un comité paritaire pour la formation continue ; la limitation des sanctions pécuniaires pour les commissaires aux comptes (personnes physiques) à 25 000 euros au lieu de 1million d'euros prévu par la directive ; la limitation des sanctions pécuniaires pour les collaborateurs à 50 000 euros pour les seules infractions relatives à l'indépendance ; pas de responsabilité de la gouvernance des entreprises pour les mandats non entités d'intérêt public (EIP) ; trois délégations de plein droit du H3C à la Compagnie nationale des commissaires aux comptes expressément prévues en matière de formation, d'inscription et de contrôle d'activité dans les non EIP.

On note une disparité du périmètre des entreprisse d'intérêt public, de même que la rotation des règles des cabinets d'audit.

Les services autres que la certification des comptes

- Les services interdits : élaboration des comptes, conseil juridique, tenue du secrétariat juridique, externalisation de services supports à l'entreprise, commissariat aux apports et aux fusions, manipulation et séquestre de fonds pour le compte de l'entreprise.
- Les services autorisés : tout ce qui n'est pas strictement interdit est présumé être autorisé. Ceci s'accompagne, corrélativement, du renforcement de la responsabilité professionnelle. Il existe un processus d'autorisation préalable.

Le rapport d'audit

Il existe une trame du rapport d'audit commune pour les rapports EIP et non EIP. Ce rapport contient une prise de position sur les risques et sur la mise en place des process de contrôle et un focus sur la continuité d'exploitation. Cette dernière appréciation doit être justifiée pour les EIP.

Pour les EIP et les sociétés de financement, pour les quelles un comité d'audit est obligatoire, le commissaire aux comptes doit remette un rapport complémentaire.

Le renforcement des compétences et des pouvoirs du H3C

Le H3C a la responsabilité finale de la supervision de l'agrément et de l'enregistrement des contrôleurs légaux, de l'adoption des normes relatives à la déontologie et au contrôle interne de qualité des cabinets d'audit et des activités d'audit, de la formation continue, des systèmes d'assurance qualité, des systèmes d'enquête et des systèmes administratifs en matière disciplinaire.

Le H3C définit le cadre et les orientations des contrôles ; il diligente des enquêtes portant sur les manquements aux dispositions du Titre II du Livre VIII du Code de commerce et à celles du règlement ; il prononce des sanctions ; il statue, comme instance d'appel, sur les décisions prises par les commissions régionales en matière de contentieux des honoraires ; il coopère avec les autorités d'autres États exerçant des compétences analogues et les autorités de l'Union européenne chargées de la supervision des EIP, les banques centrales, le système européen de banques centrales, la Banque centrale européenne, et le Comité européen du risque systémique ; il suit l'évolution du marché du contrôle légal des comptes des EIP et il élabore un rapport à la Commission européenne.

Le H3C est composé de 14 membres : quatre magistrats dont un membre de la Cour de cassation, président du Haut conseil, deux magistrats de l'ordre judiciaire et un magistrat de la Cour des comptes , le président de l'Autorité des marchés financiers (AMF) ou son représentant, le président de l'Autorité de contrôle prudentiel et de résolution (ACPR) ou son représentant, le directeur général du Trésor ou son représentant, un professeur des universités spécialisé en matière juridique, économique ou financière, quatre personnes qualifiées en matière économique et financière choisies notamment pour leur compétence dans le domaine des offres au public et des sociétés dont les titres sont admis aux négociations sur un marché réglementé, deux personnes ayant exercé la profession de commissaire aux comptes.

Une commission composée à parité des membres du collège et de commissaires aux comptes est placée auprès du H3C afin d'élaborer les projets des normes.

Auparavant, l'inscription des commissaires aux comptes intervenait au niveau régional. Dorénavant, si l'instruction du dossier est effectuée au niveau régional, la décision d'inscription est prise au niveau national.

Le H3C a la possibilité de sanctionner les administrateurs pour leurs manquements : 250 000 euros pour les personnes physiques ; une sanction pécuniaire n'excédant pas la plus élevée des sommes suivantes : 1 million ou, lorsque la faute intervient dans le cadre d'une mission de certification, la moyenne annuelle des honoraires facturés au titre de l'exercice durant lequel la faute a été commise ou des deux exercices précédant celui-ci, pour les personnes morales.

Les règles relatives à la gouvernance des cabinets sont fixées par l'article L822-3-1 du Code du commerce.

La réforme de l'audit fait l'objet d'un site dédié : www.cncc.fr/reformeeuropeenne-audit

III. Les relations dirigeant l'entreprise/commissaire aux comptes

Ce thème a été abordé par M. Christophe CHARENTON, membre de la CRCC.

Le premier contact avec l'entreprise

La certification est une opération consistant à apporter une assurance aux tiers sur la qualité des comptes sans porter de jugement ni sur la gestion, ni sur les objectifs, ni sur les stratégies de l'entreprise. Cette opération répond à des normes professionnelles, un Code de déontologie, une documentation et la doctrine. Elle nécessite un contact régulier avec la direction de l'entreprise et l'organisation de réunions lors de étapes clés de la mission. Le commissaire aux comptes doit savoir établir un lien de confiance avec la direction de l'entreprise.

Les points d'attention de la mission

- La proposition de mission est suivie, en cas d'acceptation, d'une lettre de mission, qui fixe les modalités et les conditions de l'intervention du commissaire aux comptes.
- La base barème est le nombre « normal » d'heures de travail du commissaire

aux comptes. Le nombre d'heures peut être adapté en fonction de la complexité de la société, de la nature de son activité, de la présence ou non d'un expert comptable, ...

- La phase préliminaire comporte une mission permanente (contacts informels, identification des risques inhérents,...) et une intervention préliminaire avant la clôture des comptes (inventaire physique, point d'activité, contrôle interne,...).
- La mission finale : réunion de synthèse, échange sur les résultats, clarification des éventuels éléments identifiés, présentation des recommandations.

Le « travail » du commissaire aux comptes doit favoriser les échanges et la discussion en toute transparence, mettre en place des réunions d'échange et d'écoute sans imposer uniquement un monologue énumérant ses conclusions.

IV. La procédure d'alerte

Concernant ce dernier thème, M. Jean-Max YVER, président de la CRCC, a exposé que la procédure d'alerte intervient souvent pour « limiter la casse » visant des faits ou des situations de nature à compromettre la continuité de l'exploitation. L'objectif est d'anticiper, de détecter les incidents le plus tôt possible et de prévoir des solutions.

Les critères de déclenchement

- Lors de l'examen des comptes annuels ou d'une situation comptable intermédiaire (capitaux propres négatifs, fonds de roulement très insuffisant, ...).
- Lors d'entretiens avec les dirigeants ou les services comptables et lors de l'examen des prévisions communiquées (impossibilité de renouveler, à leur échéance, les crédits indispensables ou d'obtenir des financements supplémentaires nécessaires, pertes de marchés importants,...).
- À l'occasion d'évènements particuliers (destruction de l'outil de production, difficultés politiques sérieuses dans le pays des clients ou des fournisseurs importants, changements de lois ou projets de loi défavorables,...).
- Lors de modification de la stratégie propre à la société ou définie par le groupe (abandon de la politique habituelle de distribution des dividendes ou dividendes distribuées malgré d'importants résultats déficitaires, absorption d'une filiale en difficulté, ...).

Le commissaire aux comptes doit rechercher une vision constructive de l'alerte, faire preuve de pédagogie, rappeler la gradation de la procédure (la première phase est confidentielle dans les SA) ; informer le président du tribunal de commerce ou le président du tribunal de grande instance (deuxième phase dans les SA) et expliquer la finalité de la procédure aux dirigeants.

Les diligences

- Demander des explications au dirigeant et éventuellement aux organes d'administration.
- Respecter scrupuleusement les délais de la procédure.
- Apprécier les réponses et mettre en oeuvre les diligences complémentaires.
- Documenter les décisions prises et leur motivation.
- Informer le président du tribunal de commerce ou du tribunal de grande instance.
- Rédiger le rapport spécial d'alerte.

© Toute reproduction ou utilisation des articles de la revue du *GRASCO* est interdite sans l'autorisation préalable du *GRASCO* et ne peut être effectuée qu'en vue de l'utilisation qui aura été acceptée par le GRASCO

La Revue du GRASCO doit être citée de la manière suivante : L.R.D.G., année, n° xx, p. xxx

LA LUTTE CONTRE LA CRIMINALITÉ FINANCIÈRE : QUEL RÔLE POUR L'UNITÉ MAROCAINE DE TRAITEMENT DU RENSEIGNEMENT FINANCIER ?

IHSAN EL HASSANI

PROFESSEURE ASSISTANTE À LA FACULTÉ DES SCIENCES JURIDIQUES ÉCONOMIQUES ET SOCIALES DE CASABLANCA (MAROC)

Longtemps méconnu des différents systèmes pénaux, le phénomène du blanchiment de capitaux n'a commencé à être incriminé qu'à partir des années 1980. Au Maroc, cette délinquance financière a été règlementée par le Code pénal marocain dans son article 574-1 depuis 2007. Cependant, l'impuissance des milieux judiciaires, à eux seuls, à combattre une criminalité plus organisée amenait à s'interroger sur de nouveaux moyens de lutte visant à priver les criminels de leur principale motivation.

C'est dans ce contexte que le Groupe d'action financière (GAFI), créé en 1989, s'est fixé pour objectif d'élaborer des normes devant être observées par la communauté internationale en matière de lutte contre le blanchiment de capitaux, le financement du terrorisme et les autres menaces liées à l'intégrité du système financier international.

Plusieurs organismes régionaux de type GAFI, dont le Groupe d'Action Financière pour la région du Moyen- Orient et de l'Afrique du Nord (GAFIMOAN), ont été par la suite créés dans le but d'adapter la législation des pays membres aux standards internationaux, et aux dispositions édictées en la matière par l'Organisation des Nations Unies.

Le corpus législatif national de lutte contre le blanchiment de capitaux et le financement de terrorisme s'est constitué à partir de 2003 avec l'adoption de la loi 03-03 antiterroriste et a évolué progressivement pour converger vers les normes internationales, à travers l'adoption de la loi 43-05 de 2007 relative au blanchiment de capitaux qui a créé l'Unité de Traitement du Renseignement Financier (UTRF). Cette loi est actuellement en cours de révision pour capitaliser l'expérience acquise depuis 2009 et adapter la législation nationale aux nouvelles recommandations du GAFI en la matière.

Cet article traite les différents aspects de traitement de l'information financière par l'Unité marocaine de Traitement du Renseignement Financier notamment à travers une esquisse d'une étude comparative à l'effet de situer cette institution marocaine par rapport à ses homologues étrangers. L'analyse portera sur les thèmes suivants : la typologie choisie par l'Unité pour accomplir ses missions et la présentation de ses attributions et son fonctionnement (I) ; les conditions de traitement de l'information liée aux déclarations de soupçon et aux obligations des personnes assujetties par l'Unité (II) ; l'évolution des échanges de renseignements financiers entre l'Unité et les cellules homologues étrangères (III) ; quelques pistes de réflexion et de propositions pour rendre le dispositif national plus efficace dans le fastidieux travail de lutte contre le phénomène du blanchiment de capitaux (IV).

I. L'Unité marocaine de Traitement du Renseignement Financier

A. Les types de cellules de renseignement à caractère financier (CRF)

Les CRF peuvent revêtir diverses formes, variables selon le choix des pays. Dans la pratique, trois

catégories de modèles d'Unités prédominent : administratif, policier et judiciaire. Il convient toutefois de préciser que certains pays optent pour des CRF mixtes ou hybrides qui incorporent des caractéristiques de deux ou trois des types de cellules précités.

i. Les CRF à caractère administratif

Le rattachement administratif de ces CRF varie d'un pays à un autre. Néanmoins, le système le plus fréquent consiste à installer la CRF au sein du ministère des Finances (cas de la France, du Sénégal, de la Slovénie, des États-Unis, du Canada, de l'Espagne, de la Grèce, de la Turquie et du Mexique par exemple), ou au sein de la banque centrale comme la Corée, ou placée sous l'égide des ministères des Finances et de la Justice (la Belgique).

La préférence aux cellules de type administratif par rapport aux autres services se justifie par divers motifs. Les CRF ont souvent plus de facilités pour consulter les entités notifiant les renseignements, et elles peuvent participer directement à la règlementation et la surveillance du secteur financier, disposant à ce titre de données confidentielles susceptibles de nourrir leur analyse. Les cellules de ce type ont également la possibilité de travailler plus étroitement avec des services connexes tels que ceux de l'administration fiscale. De l'avis des pays concernés, elles jouent un rôle d'interface entre le secteur financier et les autres secteurs soumis à l'obligation de déclaration et les autorités répressives chargées de l'application de la loi. De même, les institutions financières hésitent moins à révéler des informations si elles savent que leur diffusion sera limitée aux cas de blanchiment de capitaux et au financement du terrorisme (BC/FT) et qu'elle sera fonction de l'analyse propre de la CRF. Néanmoins, un retard peut se produire dans l'application de mesures répressives sur la base des révélations financières : gel d'une opération suspecte ou arrestation d'un suspect, par exemple. Pour obtenir des éléments de preuve, la cellule ne possède généralement pas les compétences légales étendues dont disposent les organismes de poursuite pénale et les autorités judiciaires.

ii. Les CRF de type policier

La CRF, dans un tel système, est proche des autres autorités d'application de la loi (ministères de l'Intérieur ou de la Sécurité), et bénéficie de leur savoir-faire et de leurs sources d'informations. En échange, les organismes de poursuite pénale peuvent facilement avoir accès aux informations reçues par la CRF et peuvent les utiliser dans le cadre de toute enquête, ce qui augmente son utilité. Les informations peuvent être échangées en recourant aux vastes réseaux nationaux et internationaux d'échange d'informations sur la criminalité (comme Interpol). Ce type de cellule est généralement plus axé sur les enquêtes que sur les mesures de prévention.

Dans ce modèle, la cellule n'est pas un interlocuteur naturel des institutions financières ; la confiance réciproque doit être instaurée. Les institutions déclarantes peuvent hésiter à révéler des informations aux forces de l'ordre si elles savent que ces informations peuvent être utilisées dans le cadre d'une enquête sur tout délit (et pas uniquement sur le blanchiment de capitaux et sur le financement du terrorisme). De même, les institutions déclarantes peuvent être peu enclines à révéler aux forces de l'ordre des informations sur des opérations qui sont simplement suspectes. Parmi les pays qui ont opté pour ce type de CRF on peut citer l'Allemagne, l'Autriche, l'Estonie, la Hongrie, l'Irlande, l'Islande, le Royaume-Uni, la Slovaquie et le Suède.

iii. Les CRF de type judiciaire

Ce type de CRF est créé au sein du pouvoir judiciaire de l'État et relève souvent de l'autorité du parquet (cas du Luxembourg, de Chypre et de l'Australie). Les déclarations d'activités financières suspectes sont généralement reçues par le parquet, qui peut ouvrir une enquête si le soupçon est confirmé. Ce modèle dote la cellule de pouvoirs judiciaires, comme saisir des fonds, bloquer des comptes, mener des interrogatoires, détenir des suspects et procéder à des perquisitions qui doivent être exercées sans retard. Ce type de cellule peut trouver des difficultés à échanger des informations avec des CRF d'un autre type.

iv. Les CRF à caractère hybride

Parmi les États qui ont créé des CRF hybrides, on peut citer le Danemark, Jersey, Guernesey et la Norvège. Ce type de système hybride comprend les CRF qui comportent diverses combinaisons des options décrites ci-dessus. Ce

modèle tente de réunir les avantages de tous les modèles cités. Certaines CRF combinent les caractéristiques des CRF de types administratif et policier. Pour certains pays, ce type résulte de la fusion de deux organismes qui étaient chargés de la lutte contre le blanchiment de capitaux.

v. Le type de CRF choisi au Maroc

Le Maroc, convaincu des avantages du modèle administratif, a décidé de choisir et de placer l'UTRF en dehors du système policier. Ce choix va de pair avec la décision de limiter les compétences de l'Unité à la réception, l'analyse et la diffusion des déclarations d'opérations suspectes et de ne pas lui conférer les pouvoirs d'enquête ou de poursuite.

En créant une autorité de type administrative qui joue le rôle d'interface entre le monde financier et le monde judiciaire, les autorités peuvent obtenir plus facilement les renseignements des institutions déclarantes, souvent conscientes des inconvénients, vis-à-vis de leurs clients, d'avoir des liens institutionnalisés directs avec des organismes de police. Le secteur bancaire donne souvent la préférence aux CRF de type administratif. Pour les personnes assujetties, c'est-à-dire les personnes déclarant toutes opérations complexes et inhabituelles, l'Unité est un interlocuteur neutre technique et spécialisé.

B. Les missions de l'Unité marocaine de Traitement du Renseignement Financier

La principale mission de l'UTRF est de contribuer à protéger l'intégrité de l'économie et du système financier à travers la lutte contre le LCB/FT. Ses fonctions opérationnelles englobent le processus de collecte, de traitement, d'enrichissement et de signalement aux autorités judiciaires le cas échéant, des renseignements et informations qui lui parviennent des personnes assujetties, des administrations partenaires et des cellules de renseignement financier homologues.

Le rôle de l'Unité consiste donc à recueillir, analyser et enrichir les déclarations émises par les personnes assujetties. Elle est donc représentée comme un service d'enquête administrative dont l'action s'inscrit en amont de la phase judiciaire. Afin de procéder à des recoupements d'informations financières sur les opérations déclarées, l'Unité dispose de différents pouvoirs strictement encadrés par la loi 43-05 : le droit de communication, le droit d'opposition à l'exécution de transactions suspectes et le droit d'échange d'informations avec les Unités ayant une compétence similaire. Elle est également chargée, en tant qu'autorité de supervision et de contrôle, de donner son avis sur le contenu des mesures de prévention du blanchiment de capitaux et de proposer au Gouvernement tout projet de réforme législative, règlementaire ou administrative en la matière.

C. La composition de l'Unité marocaine de Traitement du Renseignement Financier

Prévue par l'article 14 de la loi n°43-05 relative à la lutte contre le BC/FT, l'UTRF a été créée par le décret du 24 décembre 2008[1] et installée par le Premier ministre le 10 avril 2009.

Le fonctionnement de cette instance rattachée au chef du gouvernement est défini selon les articles 6 et 7 du décret 2008. L'Unité est composée d'un président et de 13 membres représentant les départements et organismes chargés de la LCB/FT (ministère chargé des finances, ministère de la Justice, ministère de l'Intérieur, Bank Al-Maghrib, Direction générale de la sûreté nationale, État-Major de la gendarmerie royale, administration des douanes et impôts indirects, Conseil déontologique des valeurs mobilières et Office des changes). Le président de l'UTRF est nommé par le chef du gouvernement sur proposition du ministre de la Justice, du ministre de l'Intérieur et du ministre chargé des finances, pour une durée de quatre ans renouvelable.

Le secrétariat de l'UTRF est assuré par son Secrétaire général. Les membres de l'Unité sont nommés par les administrations ou organismes dont ils relèvent. Son Secrétaire général, qui est placé sous l'autorité du président de l'Unité, est nommé par le chef du gouvernement.

L'UTRF exerce ses attributions qui lui sont dévolues par la loi 43-05 précitée à travers des décisions ou des directives qui sont publiées au bulletin officiel.

II. Le renseignement financier au niveau national

La loi n° 43-05 soumet les personnes assujetties à l'obligation de déclarer à l'Unité les opérations suspectées d'être liées au blanchiment de capitaux tel que défini par la loi. De même, elle dote l'Unité d'un droit de communication de l'information qu'elle peut exercer auprès des personnes assujetties et des administrations, ce qui lui permet

d'enrichir sa base de données et de disposer des éléments nécessaires à l'analyse des déclarations qu'elle reçoit.

A. La déclaration de soupçon (DS)

i. Les modalités de la déclaration de soupçon

Chaque personne assujettie désigne les personnes assurant la liaison avec l'Unité. Ces personnes accréditées auprès de l'Unité sont seules habilitées à communiquer les informations relatives aux déclarations de soupçon. Ces déclarations sont transmises conformément au protocole d'échange d'informations entre l'Unité et les différentes personnes assujetties[2]. La déclaration de soupçon porte sur toute somme, opération ou toute tentative de réalisation d'opérations par des clients habituels et occasionnels pour lesquelles les personnes assujetties soupçonnent ou ont une bonne raison de soupçonner d'être liées au blanchiment de capitaux, à une ou plusieurs de ses infractions sous-jacentes[3] ou au financement du terrorisme. Elle porte également sur toute opération dont l'identité du donneur d'ordre ou de bénéficiaire est douteuse. Ces déclarations sont produites par les personnes assujetties qui sont tenues de mettre en place un dispositif interne de vigilance renforcé. La déclaration de soupçon est communiquée à l'Unité soit via son système d'information UTRF Net, soit par un autre moyen convenu avec les services de l'Unité.

En application de la loi n° 43-05, les autorités de supervision et de contrôle veillent à l'application par les personnes assujetties, placées sous leur autorité, des nouvelles dispositions législatives en matière de lutte contre le BC/FT.

À cet égard, il y a lieu de préciser qu'en cas de constatation par l'Unité d'un défaut grave de vigilance ou de carence dans le dispositif interne de contrôle d'une personne assujettie, elle saisit l'autorité investie du pouvoir de contrôle et de sanction de ladite personne qui prononce alors des sanctions à son encontre, sur la base de la législation qui lui est applicable (sanctions administratives). De plus, une sanction pécuniaire de 100 000 Dh à 500 000 Dh peut être infligée à toute personne assujettie qui a manqué à ses obligations de vigilance, de veille interne et de déclaration de soupçon ; elle est prononcée par l'autorité de supervision et de contrôle de ladite personne ou, à défaut, par l'Unité elle-même. Enfin, les dirigeants ou agents des personnes assujetties qui ont porté à la connaissance de la personne objet d'une déclaration de soupçon, soit la déclaration de soupçon dont elle a fait l'objet, soit des renseignements sur les suites réservées à cette déclaration, peuvent aussi s'exposer à des sanctions pénales[4].

ii. L'évolution de la déclaration de soupçon par catégorie de personnes assujetties

Depuis la réception de la première DS en octobre 2009 et jusqu'à fin décembre 2014, le nombre de DS reçues par l'Unité s'élève à un total de 870 DS dont 860 déclarations liées au blanchiment de capitaux et 10 déclarations relatives au financement de terrorisme. Le tableau ci-dessous illustre l'évolution des DS reçues par l'Unité entre 2009 et 2014 par catégorie de personnes assujetties.[5]

Nombre de DS par catégorie de personne assujettie	2009	2010	2011	2012	2013	2014	Total	%
Banques	11	66	97	160	189	261	784	90%
Sociétés de transfert de fonds	-	4	5	7	19	39	74	9%
Casinos	-	-	-	-	5	-	5	-1%
Compagnies d'assurance	-	-	-	-	-	3	3	-1%
Notaires	-	-	-	2	-	-	2	-1%
Sociétés de financement	-	-		-	-	1	1	-1%
Total de DS	11	70	102	169	213	305	870	
DS/BLC	11	68	102	168	210	301	860	99%
DS/FT	-	2	-	1	3	4	10	1%

À la lecture de ce tableau, la répartition du nombre des DS par catégorie de personne assujettie illustre la prédominance des banques qui ont enregistré un taux de 90%. Les banques, dont le dispositif prudentiel est imposé par Bank Al- Maghrib, se placent en tête des dénonciateurs car elles sont la principale cible des blanchisseurs de capitaux. Cette évolution s'explique par l'importance des opérations financières au sein des banques, la mise en place par ces dernières des dispositifs internes de vigilance renforcés, l'intégration de la gestion des risques dans le système d'information et le contrôle et la supervision de Bank Al- Maghrib. À cet effet, et dans le cadre de l'exercice de ses contrôles, Bank Al-Maghrib a infligé des sanctions à deux banques implantées en Afrique subsaharienne, la première a été sanctionnée pour un retard de mise en oeuvre des recommandations de Bank Al-Maghrib en matière d'obligations de vigilance et de mesures prudentielles, alors que la seconde l'a été à cause d'une lacune dans le dispositif de contrôle interne[6].

Ce n'est qu'à partir de l'année 2012 que l'assiette des déclarants a été élargie aux notaires, casinos, compagnies d'assurance et sociétés de financement. Malgré l'adoption par l'Unité de la Décision n° D.5/2012 du 16 novembre 2012 relative aux obligations incombant aux personnes assujetties soumises à son contrôle et aux modalités de ce contrôle, certains déclarants relevant du secteur non financier comme les intermédiaires immobiliers, les négociants en pierres et métaux précieux, les experts comptables, les conseillers fiscaux, les établissements de jeux de hasard, n'ont communiqué aucune DS à l'Unité. De même, les déclarations effectuées par les casinos, les notaires, les compagnies d'assurance et les sociétés de financement restent très timides par rapport à leur nombre.

Cette absence ou insuffisance de DS est-elle due au manque de sensibilisation de certaines personnes assujetties, à la formation de leurs personnels, à leurs réticences ou à la déficience de leurs systèmes d'information ?

iii. Le droit d'opposition

Certains pays confèrent à la CRF le pouvoir de bloquer pendant un temps limité l'opération qui a fait l'objet de la déclaration. Pendant ce délai, la CRF peut analyser l'opération et si, après analyse, elle conclut que l'opération est effectivement liée à une activité criminelle, elle peut transmettre le dossier aux autorités de poursuite pénale compétentes pour geler pendant une période plus longue l'opération et les comptes bancaires y afférents. Dans quelques cas, la CRF a un pouvoir plus large lui permettant de geler la totalité d'un compte bancaire, voire de saisir les avoirs. Il convient de noter que le pouvoir de la CRF de bloquer les opérations est inhabituel en ce sens que, dans la plupart des systèmes juridiques, cette mesure ne peut être prise que sur ordre d'un tribunal.

En vertu des pouvoirs qui lui sont conférés par la loi 43-05, l'UTRF, à l'instar des autres CRF, elle a la possibilité d'opposer l'exécution de toute opération faisant l'objet d'une DS. L'exécution de l'opération est reportée pour un délai de deux jours ouvrables à compter de la date de réception de ladite déclaration par l'Unité.

Sur demande de l'Unité, le président du tribunal compétent peut, après présentation des conclusions du parquet, proroger le délai d'opposition de quinze jours au maximum, à compter de la date d'expiration du délai de deux jours ouvrables précité. Si après le délai d'opposition de deux jours la personne assujettie ne reçoit pas de décision de proroger ledit délai, elle peut exécuter l'opération.

L'Unité a émis 5 décisions d'opposition durant la période 2009-2014. Pour l'une d'elle émise en 2013, l'Unité a obtenu une prorogation de quinze jours de la part du président du tribunal de première instance de Rabat. Au cours de l'année 2014, aucune décision d'opposition n'a été émise par l'Unité.

iv. Les éléments générateurs du soupçon

Les principaux éléments qui ont généré le soupçon de blanchiment sont : des versements de fortes sommes en espèces ou des retraits qui ne correspondent pas au profil socioprofessionnel du déposant ; des tentatives de rapatriement de grosses sommes d'argent basées sur des documents douteux ; des versements en devises et billets en dirhams sur différents comptes bancaires ; des transferts de fonds vers des pays à haut risque ; des tentatives répétées de réceptions de virements frauduleux ; des comptes dormants réactivés à travers des versements en espèces d'origine douteuse ; des opérations effectuées dans des conditions inhabituelles faisant intervenir des montages juridiques et financiers complexes ; des changements brusques dans

le mode de fonctionnement du compte.

B. L'analyse et l'enrichissement des informations reçues

Lorsque l'Unité reçoit les déclarations de soupçon, elle procède à leur analyse pour vérifier la véracité et le poids des renseignements qu'elles contiennent. Pour les aider dans cette tâche, les analystes réalisent des actes d'investigations au moyen de bases de données. Deux niveaux d'analyse peuvent être distingués dans le processus de traitement d'une déclaration de soupçon :

- Le premier niveau d'analyse de l'information reçue vise à déterminer les éléments d'environnement des personnes déclarées. Les bases ouvertes sont ainsi largement consultées. D'autres outils sont également sollicités comme l'exercice de droit de communication auprès des administrations susceptibles d'avoir des informations sur les personnes auteurs d'opérations soupçonnées (administrations de l'État, les établissements publics et toute autre personne chargée d'une mission de service public). Lorsque les informations reçues développent des éléments transnationaux, les homologues étrangers de l'Unité sont également sollicités. Ce premier niveau d'analyse doit permettre d'orienter l'information. L'orientation est l'action visant à décider des modalités de traitement d'une information. Elle peut déboucher soit sur une enquête, soit sur une mise en attente lorsque l'information semble potentiellement inexploitable, soit sur la levée du doute. Elle peut, néanmoins, au regard de nouvelles informations ultérieurement reçues par l'Unité, être réactivée. En effet, l'Unité est susceptible de réactiver les informations reçues au titre des années antérieures (dans la limite de dix ans).

- Le second niveau d'analyse consiste à mener des investigations approfondies aboutissant à traiter le dossier sur une plus longue période. Il peut être nécessaire d'approfondir les recherches par la demande des relevés de comptes bancaires. Les dossiers relatifs aux déclarations de soupçon et aux données individuelles sont traités par les services de l'Unité qui sont tenus au secret professionnel.

i. Le droit de communication de l'UTRF

La loi n° 43-05 permet à l'Unité de solliciter les personnes assujetties et ses partenaires pour lui communiquer les informations requises afin d'enrichir les dossiers objet de l'analyse. Sont sollicités à cet effet les administrations et les organismes publics dont figurent la police et les autorités judiciaires, qui jouent un rôle de premier plan dans l'application de la loi, mais aussi, les services des douanes et les autorités de réglementation financière, lesquels recueillent et détiennent dans le cadre de leurs activités normales des renseignements importants sur les personnes physiques et morales et les transactions financières.

Le tableau suivant présente l'évolution du nombre des demandes d'informations adressées par l'Unité aux personnes assujetties, administrations, établissements publics et personnes physiques ou morales de droit public ou privé[7].

L'analyse des taux de réponse durant la période allant de 2009 à 2011 permet de constater que les personnes assujetties enregistrent globalement un taux de réponse avoisinant les 100%. Quant aux personnes de droit public ou privé visées à l'article 22 de la loi n° 43-05, l'Unité a continué à développer les relations de coopération notamment avec les administrations membres en vue de renforcer leur contribution à l'enrichissement des dossiers traités et de sa base de données.

Entre 2012 et 2013, Les DI envoyées aux personnes assujetties ont enregistré une baisse de 10% pour s'établir à 1543 DI en 2013 contre 1714 DI en 2012. Ceci résulte selon le rapport annuel de l'UTRF de 2013 de l'amélioration de la qualité des informations communiquées à l'Unité par certaines personnes assujetties lors de la transmission des DS et des efforts récurrents de l'UTRF pour les sensibiliser, les accompagner et les inciter à améliorer leur rendement.

Entre 2013 et 2014, les DI reçues des personnes assujetties ont enregistré une forte augmentation. Cette progression s'explique par l'évolution des DS et des demandes reçues par l'Unité dans le cadre de la coopération internationale.

ii. Les communications spontanées

Contrairement aux déclarations de

Demandes d'information (DI)	2009 à 2011	2012	2013	2014
DI envoyées aux personnes assujetties	1972	1714	1543	4914
DI envoyées aux partenaires	_	1438	1538	2465

soupçon, la communication spontanée (CS) ne peut à elle seule justifier l'ouverture d'une enquête par l'Unité. Les données issues des CS alimentent une base documentaire et ont uniquement vocation à enrichir les investigations en cours. En application des dispositions de l'article 22 de la loi n° 43-05, l'Unité reçoit des notes d'informations sous forme de communication spontanée en provenance de ses partenaires. Ces derniers doivent informer l'Unité des infractions aux dispositions de ladite loi qu'ils ont constatées à l'occasion de l'exercice de leurs missions. Dans ce cadre, entre 2011 et 2014, l'Unité a reçu de ses partenaires des CS réparties comme suit[8] :

Nombre de CS par origine	2009	2010	2011	2012	2013	2014	Total depuis 2009
Office des Changes	-	-	2	1	7	-	10
Administration des Douanes et Impôts Indirects	-	-	2	-	1	5	8
Bank Al- Maghrib			-	-	1	4	5
Centre Monétique Interbancaire	-		-	-	1		1
Instance Centrale de Prévention de la Corruption	-	-	-	1		-	1
Total des CS	-	-	4	2	10	9	25

C. La diffusion de l'information

Les renseignements recueillis par l'Unité dans le cadre de ses missions sont confidentiels et ne peuvent être utilisés à d'autres fins que celles prévues par le dispositif de lutte contre le BC/FT. Toutefois, l'Unité est habilitée à communiquer les documents et renseignements recueillis aux autorités compétentes en vue d'accomplir le travail de lutte contre la criminalité financière, à l'exception de la déclaration de soupçon. L'Unité peut partager des renseignements financiers et des informations connexes avec les autorités étrangères. L'aptitude de l'Unité à partager les informations valables influe non seulement sur l'efficacité du régime de LBC/FT interne du pays, mais aussi sur sa capacité de coopération à l'échelle internationale.

i. Les transmissions à la justice

Le choix de l'autorité qui reçoit les informations dépend du système juridique du pays concerné. Dans certains systèmes, les informations sont transmises à la police afin que celle-ci procède aux enquêtes qui débouchent sur un dossier prêt à être transmis au parquet aux fins de poursuites. Dans d'autres systèmes, le dossier est transmis directement au parquet, qui ordonne, le cas échéant, des enquêtes complémentaires et, si les preuves sont suffisantes, entame les poursuites.

En ce qui concerne le système marocain, les dossiers d'informations traités par l'UTRF sont transmis au procureur général du Roi près la Cour d'appel de Rabat quand il s'agit de présomptions de financement du terrorisme et au procureur du Roi près tribunal de première instance de Rabat en cas de blanchiment de capitaux.

De 2011 à 2014, l'Unité a transmis 41dossiers au parquet. Entre 2009 et 2010 aucune transmission n'a été effectuée. Ceci s'explique par le fait que, d'une part, 2009 coïncide avec la création de l'UTRF et, d'autre part, l'année d'après, 70 signalements sont formulés uniquement par les banques et les sociétés de transfert de fonds. Le tableau suivant illustre l'évolution des transmissions au Procureur de Roi.

En vertu des dispositions de la

	2011	2012	2013	2014	Total
Transmissions de l'Unité au Procureur de Roi	5	9	11	16	41

Source : Rapports annuels de l'UTRF 2011-2014

loi 43-05, le procureur du Roi notifie à l'Unité les décisions définitives prononcées dans les affaires dont il a été saisi. De même, il peut ordonner au cours de la phase d'enquête pour une durée qui ne peut excéder un mois renouvelable une fois : le gel par l'interdiction temporaire du transfert, de la conversion, de la disposition ou du mouvement des biens ; la désignation d'une institution ou d'un organisme privé aux fins d'assurer temporairement la garde ou le contrôle des biens. Le procureur du Roi ou le juge d'instruction peuvent également ordonner la saisie des biens appartenant à des personnes physiques ou morales suspectées d'être impliquées avec des individus, des organisations ou activités en rapport avec les infractions de blanchiment de capitaux, même si celles-ci ne sont pas commises sur le territoire national.

ii. Les infractions sous-jacentes retenues par l'UTRF

En 2014, les principaux faits délictueux retenus par l'Unité après analyse sont : le détournement de fonds par l'utilisation de virements frauduleux ; l'introduction dans le circuit bancaire de fonds liés au trafic de stupéfiants et au trafic de cigarettes de contrebande ; la manipulation de montants importants en espèces et création de sociétés dont certaines ne sont pas en activité ; l'utilisation de documents douteux et les déclarations mensongères concernant la profession exercée ; l'utilisation de documents falsifiés pour l'encaissement de mandats internationaux ; les virements frauduleux au profit de comptes de sociétés sans activité ; l'utilisation de cartes prépayées pour la collecte d'argent ; l'utilisation de prête-noms par une personne ayant un profil financier douteux.

iii. Les activités relatives au gel des biens

Dans le cadre du respect des résolutions des instances internationales habilitées relatives au gel des biens pour infraction de terrorisme, l'Unité procède régulièrement à l'actualisation des listes des personnes désignées par les comités du Conseil de sécurité des Nations Unies (CSNU) pour infraction de terrorisme et les communique via son site web officiel aux personnes chargées de l'exécution de gel pour s'assurer que les personnes et les entités qui figurent sur les listes ne détiennent pas des biens. Dans ce cadre, l'Unité a adopté en 2013 la décision n°6 relative au gel des biens pour infraction de terrorisme qui remplace et annule la décision du 27 avril 2011[9]. Parallèlement, le nombre des demandes d'informations envoyées en 2014 dans le cadre du traitement des listes du Conseil de sécurité a atteint 1.242 dossiers contre 780 en 2013 et 377 en 2012.

Par cette décision n°6, l'Unité fixe les modalités de mise en oeuvre des mesures de gel des biens appartenant aux personnes visées par les résolutions du CSNU. Cette décision transpose les obligations qui découlent des résolutions du CSNU, notamment l'obligation de geler, sans délai et sans notification préalable, les fonds et autres biens des personnes et entités visées par les listes du CSNU et la suspension de toute transaction à laquelle elles font parties. Elle décrit également les conditions liées à la levée du gel des biens.

III. Le traitement du renseignement financier au niveau international

A. Le Groupe Egmont

Le Groupe Egmont est un forum international des CRF créé en 1995 en vue d'établir les normes de fonctionnement des CRF et des échanges d'informations entre elles dans le domaine de la lutte contre le blanchiment de capitaux et de promouvoir la coopération entre ses membres. Les échanges d'informations avec les Unités similaires s'effectuent sur la base des principes convenus notamment en matière de réciprocité, de confidentialité et de sécurité des échanges des données. Ces principes constituent les standards internationaux en matière de coopération internationale en la matière.

Le Maroc a adhéré au Groupe Egmont le 13 juillet 2011. Une telle adhésion, qui répond à l'une des recommandations principales du GAFI, constitue une étape importante dans le renforcement du dispositif national de lutte contre le blanchiment de capitaux et marque une nouvelle avancée dans la contribution du Maroc à l'effort de la communauté internationale en la matière. Le Maroc devient ainsi le 1er pays de l'Afrique du Nord et le 9ème pays du continent africain à intégrer ce forum international.

Les informations échangées entre l'UTRF et les CRF membres du

Groupe Egmont se font via le système ESW. C'est un système d'échange sécurisé permettant à toute CRF de solliciter et de répondre aux demandes de renseignements des autres CRF dans des délais rapides. Pour les CRF non membres au Groupe, l'Unité utilise d'autres moyens de communication et les invite à s'inscrire au système sécurisé "UTRF Net" et à l'utiliser lors des échanges d'informations.

B. L'évolution des échanges de renseignements avec les cellules étrangères

L'UTRF, conformément aux articles 24 et 34 de la loi n°43-05, peut échanger avec ses homologues étrangers des renseignements financiers liés à la LBC/FT. Ces échanges peuvent être effectués sur la base du principe de réciprocité ou par le biais des protocoles d'entente (Mémorandums d'Entente) conclus avec des cellules homologues.

De 2009 jusqu'à fin 2014, L'UTRF a, dans le cadre de l'analyse de soupçon de blanchiment ou de financement du terrorisme, adressé 58 demandes de renseignement financier (DRF) à ses homologues étrangers contre 344 DRF reçues des CRF étrangères.

Le tableau suivant illustre l'évolution des échanges de renseignements avec les principaux partenaires de l'Unité[10] entre 2009 et 2014.

i. Les demandes de renseignements reçues des CRF étrangères

Entre 2011 et 2012, l'évolution du nombre des DRF reçues de l'étranger a été significative enregistrant un taux de progression de l'ordre de 66%. Les DR reçues émanent de 14 CRF étrangères. Plus de 85% des DRF proviennent des principaux pays européens partenaires du Maroc. Les autres demandes de renseignements émanent des pays de la région du Moyen-Orient et de l'Afrique du Nord, ainsi que d'autres pays partenaires. Le délai de réponse aux demandes de l'étranger est variable en fonction de l'urgence, de la complexité de l'affaire et de l'analyse à accomplir.

L'analyse des demandes de renseignements reçues des différentes CRF étrangers a montré que ces demandes sont motivées par les indices suivants : versements en espèces à l'étranger et transfert vers le Maroc ou pays voisin en inadéquation avec le profil de l'émetteur ; transfert de sommes d'argent vers le Maroc effectué par des personnes connues à l'international pour infractions diverses ; réalisation à l'étranger de transactions financières non justifiées par des personnes résidentes au Maroc.

ii. Les demandes de renseignements émises par l'Unité

Ce sont les pays européens qui demeurent en tête des CRF destinatrices des DR, suivis des pays de l'Afrique du Nord et de la région du Moyen-Orient. Le délai et la qualité des réponses aux demandes de la CRF varient sensiblement en fonction des pays concernés et du pouvoir des CRF étrangères à rechercher des informations. À noter qu'en 2014, les échanges de renseignements ont eu lieu principalement avec les CRF européennes avec un taux avoisinant 86% contre 91% en 2013, ce qui explique l'ouverture de l'Unité vers d'autres continents.

iii. Les communications spontanées reçues des cellules homologues

Afin de dynamiser la coopération internationale entre ses membres, le groupe Egmont encourage la communication spontanée de renseignements entre CRF. Dans ce cadre, et lors du traitement d'un dossier réalisé par une cellule, celle-ci peut considérer que les informations en sa possession sont susceptibles d'intéresser une CRF homologue et juger par conséquent qu'il est opportun de les lui adresser sans contrepartie. La CRF émettrice peut notifier, lors de cet envoi, à la CRF destinatrice de la CS qu'elle n'est pas en attente d'un retour d'informations de la part de cette dernière. L'Unité réserve aux demandes de renseignements et aux communications spontanées, dans le cadre de la coopération internationale, un traitement analogue aux déclarations

DRF	2009	2010	2011	2012	2013	2014	Total depuis 2009
DRF reçues des CRF	1	23	60	100	82	78	344
DRF émises / l'Unité	-	-	8	20	11	19	58
Communications spontanées (CS) reçues des CRF	-	-	-	-	4	6	10
Total des DRF	1	23	68	120	97	103	412

de soupçon en ce qui concerne l'enrichissement et l'analyse ainsi qu'une éventuelle transmission au parquet, avec l'accord de la CRF homologue émettrice.

C. La demande d'informations à une CRF

Une demande d'informations adressée à une CRF passe par quatre étapes :

- Étape 1 : une CRF étrangère formule une demande d'informations financières pour étayer son enquête sur une affaire de BC/FT ou autres délits connexes.

- Étape 2 : la CRF sollicitée détermine si la demande répond aux conditions légales, opérationnelles et stratégiques. Dans l'affirmative, la CRF recherche dans ses bases de données ou ses dossiers des informations correspondant à la demande.

- Étape 3 : le cas échéant, la CRF demande des informations à d'autres organismes publics et aux institutions financières en vue de répondre à la demande.

- Étape 4 : la CRF analyse les informations et établit un rapport à partager avec la CRF qui a introduit la demande et fixe les conditions auxquelles cette CRF peut utiliser et diffuser les informations contenues dans le rapport.

D. La coopération bilatérale

La capacité d'une CRF à échanger les informations avec ses homologues étrangers et sa volonté de coopérer à l'international sont des éléments fondamentaux pour l'appréciation de son opérationnalité et de sa conformité aux normes internationales. L'Unité marocaine a signé, depuis sa création en 2009, 17 accords de coopération (Mémorandum Of Understanding-MOU) avec des CRF homologues élaborés sur la base des principes du Groupe Egmont et des dispositions légales et règlementaires en vigueur, notamment l'article 24 de la loi n°43-05, le règlement intérieur et les procédures de l'Unité. Des accords de coopérations ont ainsi été signés en[11] :

- 2010, avec Anti-Money Laundering and Suspicious Cases Uni (AMLSCU) des Émirats arabes unis, la Cellule de Traitement des Informations Financières (CTIF) de Belgique, le Traitement du Renseignement et Action contre les Circuits Financiers clandestins (TRACFIN) de France ;

- 2011, avec la Cellule de Traitement du Renseignement Financier (CTRF) d'Algérie, la Commission Tunisienne des Analyses Financières (CTAF) de Tunisie ;

- 2012, avec la Cellule Nationale de Traitement des Informations Financières (CENTIF) de Burkina Faso, la Cellule Nationale de Traitement des Informations Financières (CENTIF-CI) de Côte d'Ivoire, la Cellule Nationale de Traitement des Informations Financières (CENTIF) du Togo, Anti Money Laundering & Counter Terrorist Financing Unit de Jordanie, l'Égyptian Money Laundering Combating Unit (EMLCU) d'Égypte, la Cellule Nationale de Traitement des Informations financières (CENTIF) du Bénin, l'Agence Nationale d'Investigation Financière (ANIF) du Gabon, la Cellule Nationale de Traitement des Informations Financières (CENTIF) du Niger ;

- 2013, avec Main Financial information Unit For Combating Money Laundering de Libye, Financial Crimes Investigation Board (MASAK) de Turquie, la Cellule Nationale des Renseignements Financiers (CENAREF) du Congo ;

- 2014, avec Bangladesh Financial Intelligence Unit (BFIU) du Bangladesh ;

- 2015, avec la Cellule de Renseignement Financier (Financial Follow- UP Unit) de l'État de Palestine ;

- 2016, avec le Service d'Information et de Contrôle sur les Circuits Financiers de Monaco.

À noter que les échanges avec les CRF de France et de Belgique, sur la base de la réciprocité, avaient commencé avant même la signature des accords de coopération en 2010. En vertu du même principe, l'Unité a procédé à des échanges d'informations avec les CRF des Pays-Bas, du Liban et du Sultanat d'Oman.

E. Les pratiques comparées des CRF concernant l'infraction fiscale

Les infractions fiscales sont souvent intrinsèquement liées à d'autres infractions financières, car les criminels ne déclarent pas leurs revenus issus d'activités illicites. À l'inverse, ils peuvent majorer leur revenu déclaré afin de blanchir les produits de la criminalité. Le GAFI a explicitement reconnu les liens entre infractions fiscales et blanchiment de capitaux en inscrivant ces infractions sur la liste des infractions préalables désignées aux fins du blanchiment de capitaux.

L'analyse des infractions sous-jacentes retenues par l'UTRF révèle l'inexistence de la fraude fiscale comme infraction principale qui peut servir au financement d'activités illicites. La loi 43-05 s'applique à 7 types d'infractions qui sont étendues par la loi 13-10 à 16 autres infractions liées au BC/FT. Une partie des déclarations de soupçon échappe donc aux personnes assujetties vu l'ab-

sence de cette infraction sous-jacente.

S'agissant des enquêtes relatives aux infractions à caractère fiscal, chaque pays opte pour l'une des quatre pratiques suivantes :

- L'administration fiscale est chargée de diriger et de mener les enquêtes. Les pays qui appliquent cette pratique sont : L'Afrique du Sud, l'Allemagne, l'Australie, le Canada, la Corée, les États-Unis, la Grèce, l'Inde, l'Irlande, la Nouvelle-Zélande, le Royaume-Uni et la Suisse.

- L'administration fiscale conduit les enquêtes, mais, sous la direction du ministère public. C'est le cas en Autriche, au Chili, en Espagne, aux États-Unis, aux Pays-Bas, au Portugal et en Suède. En Espagne, les enquêtes sont actuellement dirigées par un juge d'instruction.

- Un organisme fiscal spécialisé, placé sous la tutelle du ministère des Finances mais ne relevant pas de l'administration fiscale, est chargé de réaliser l'enquête. C'est le cas en Turquie, en Grèce et en Islande.

- La responsabilité d'enquête incombe à la police ou au ministère public (procureur). La Belgique, le Danemark, la Finlande, la France, le Japon, le Luxembourg, le Mexique, la Norvège, la République slovaque, la République tchèque et la Slovénie adoptent cette pratique.

Il est intéressant de souligner qu'en Italie, la législation autorise à la CRF italienne de bénéficier d'un accès direct au registre des comptes et dépôts tenu par l'administration fiscale (droit de consultation), qui contient des informations sur les comptes et les transactions financières effectuées par des intermédiaires financiers. Ces renseignements sont extrêmement utiles pour la cellule. Ils sont utilisés pour analyser les déclarations de transactions suspectes, améliorer la coopération internationale en échangeant des renseignements avec d'autres cellules à l'étranger. La cellule italienne coopère étroitement avec la *Guardia di Finanza* (Gardes des Finances)[12] et lui transmet des déclarations de transactions suspectes pour enquête dans les cas présumés de blanchiment de capitaux ou de fraude fiscale. L'Italie ne relève d'aucune des quatre pratiques décrites ci-dessus.

Après avoir passé en revue les exemples de pratiques présentés ci-dessus, il semble que l'UTRF peut adopter et adapter des pratiques similaires en tenant compte de ses besoins, de son cadre juridique et de ses expériences spécifiques ou envisager d'autres modèles pouvant procurer des avantages comparables comme le modèle italien.

De même, l'UTRF et les organismes publics qui participent à la lutte contre la délinquance financière, doivent adopter une approche gouvernementale intégrée pour lutter contre la criminalité financière. Autrement dit, les différents organismes ne peuvent pas agir isolément les uns des autres. Chacun de ces organismes est susceptible de détenir des informations opérationnelles et stratégiques intéressant les activités de lutte contre la délinquance financière menées par les autres. On entend par informations opérationnelles celles afférentes à des affaires et enquêtes données. Les informations stratégiques ont trait à des risques et menaces allant au-delà d'un dossier particulier.

IV. Les pistes d'amélioration

L'efficacité du dispositif de LBC/FT, la réussite de la mission de l'Unité ainsi que l'amélioration de sa capacité à l'échelle internationale sont tributaires de la réalisation de certains éléments. Voici quelques pistes d'amélioration possible :

- Le dispositif de LBC/FT doit être conforme aux nouvelles normes du GAFI en matière de lutte contre le blanchiment de capitaux, ce qui nécessite de nouveaux amendements législatifs et le lancement d'importants chantiers relatifs à l'étude des risques de blanchiment de capitaux, le renforcement de la coopération entre les institutions nationales concernées et à la consolidation des structures et des pouvoirs de l'Unité.

- Les organismes concernés par LCB/FT, les personnes assujetties et les autorités judiciaires doivent améliorer leur propre efficacité et coopérer entre eux pour former un tout performant.

- La coopération interinstitutionnelle peut perfectionner l'intégrité et la gouvernance des transactions financières en renforçant la capacité des pays à lutter contre les infractions financières. Une coopération interinstitutionnelle nationale et internationale efficace est la seule parade viable face à des criminels qui agissent dans un environnement financier complexe qui transcende les frontières.

- La participation active des institutions financières doit être renforcée en les incitant à communiquer davantage les informations financières à l'Unité.

- Une politique plus volontariste doit être mise en place pour mener une lutte acharnée contre cette délinquance financière à travers la lutte contre la corruption, le trafic des stupéfiants et

d'autres délits graves.

- Face au faible taux de bancarisation de la population au Maroc, il faut imaginer d'autres mécanismes pour détecter le blanchiment du produit de la délinquance afin de contrôler les secteurs où beaucoup de transactions se font en liquide, comme l'immobilier ou le commerce des métaux précieux.

- L'UTRF, autorité de supervision et de contrôle de certaines personnes assujetties[15] qui ne relèvent d'aucune autorité de contrôle d'après la loi 13-10 de 2011 comme les gérants de casinos, les agents immobiliers, les comptables externes, les conseillers fiscaux et les négociants en pierres et métaux précieux, doit être dotée d'une large compétence lui permettant de surveiller le respect de l'obligation de déclaration et des autres obligations préventives par toutes les personnes assujetties par la loi, qu'elles soient ou non soumises à une surveillance prudentielle. Elle peut s'inspirer notamment de l'expérience de l'Australie, du Canada et de l'Espagne, par exemple. L'avantage de ce système est que le savoir-faire en matière de LBC/FT est concentré entre les mains d'un organisme de surveillance unique, ce qui peut améliorer son efficacité.

- La consolidation du rôle préventif de l'UTRF dans le domaine de la lutte contre le blanchiment de capitaux, doit être affirmée à travers les sessions de formation et l'intensification des campagnes de sensibilisation des personnes assujetties relevant du secteur non financier sur leurs obligations légales et règlementaires en la matière.

- L'Unité, pour accomplir ses missions et jouer pleinement son rôle de LBC/FT est appelée à accroître le nombre de ses cadres.

- Les missions de contrôle sur les établissements bancaires, succursales et leurs filiales installés aussi bien au Maroc qu'à l'étranger en vue de sanctionner tout manquement au respect des dispositions de la loi doivent être renforcées et généralisées. En France par exemple, l'autorité française de tutelle a sanctionné, en décembre 2013, une filiale d'une banque marocaine à une amende d'un million d'euros. Cette sanction est justifiée par le non-respect des procédures de surveillance et d'alerte notamment celles prévues pour les personnes politiquement exposées[13], par des manquements aux obligations déclaratives ou de vigilance et par l'analyse à tort de certaines relations d'affaires comme les clients occasionnels[14].

- La coopération internationale par l'échange d'expériences et de renseignements financiers avec d'autres CRF doit être fortement développée. Cette coopération plus étendue permet à l'Unité d'élargir sa base de données, d'améliorer la qualité de ses analyses et de renforcer l'efficacité et la crédibilité de l'ensemble du dispositif de lutte contre le blanchiment d'argent. De même, cette coopération approfondie a pour objectif de couper le chemin aux blanchisseurs vers le paradis bancaire ou le paradis fiscal.

Notes :

1. Décret n° 2-08-572du 24 décembre 2008 portant création de l'Unité de Traitement du Renseignement Financier (UTRF), Bulletin officiel du 15 janvier 2009.
2. Voir Décision de l'UTRF n°4 du 24 novembre 2011 relative à la déclaration de soupçon et à la communication d'informations à l'Unité.
3. La loi 43-05 s'applique à 7 types d'infractions que sont le trafic de stupéfiants et des matières psychotropes ; le trafic d'êtres humains ; le trafic d'immigrants ; le trafic illicite d'armes et de munitions ; la corruption, la concussion, le trafic d'influence et le détournement de biens publics et privés ; les infractions de terrorisme et, enfin, la contrefaçon ou la falsification des monnaies, d'effets publics ou d'autres moyens de paiement. La loi 13-10 étend le blanchiment à 16 autres infractions, dont l'appartenance à une bande terroriste, l'exploitation sexuelle, l'escroquerie, les infractions commises à l'encontre de l'environnement, la contrebande et la fraude sur les marchandises et les produits alimentaires. Pour en savoir plus voir art. 574.2 du Code pénal marocain.
4. Voir les articles 28 et 30 de la loi relative à la lutte contre le BC/FT. Version consolidée en date de 3 mai 2013.
5. Voir les rapports annuels de l'UTRF de 2010- 2011-2013-2014.
6. La tribune : « Supervision Transfrontalière, BAM Veille au Grain », publié par LNTech le 05/08/2015. Idem, voir le rapport de l'exercice 2013 de Bank Al- Maghrib page 150.
7. Voir les rapports annuels de l'UTRF 2011- 2013 et 2014.
8. Voir les rapports de L'UTRF 2013 et 2014.
9. Voir Décision de l'UTRF D6/ 2013 relative au gel des biens pour infraction de terrorisme.
10. Voir les rapports annuels de l'UTRF 2011-2012- 2013 et 2014.
11. Rapports annuels de l'UTRF : 2010, 2011,2012, 2013 et 2014.
12. La Garde des Finances (en italien Guardia di Finanza) est la police douanière et financière italienne. Ses principales attributions sont les contrôles douaniers et la lutte contre la fraude, la contrebande, le trafic international de drogue, l'immigration clandestine, la contrefaçon, le blanchiment d'argent.
13. Toute personne marocaine ou étrangère exerçant ou ayant exercé des fonctions publiques au Maroc ou à l'étranger, ou au sein de, ou pour le compte d'une organisation internationale, ainsi que les membres de sa famille et ses associés qu'ils soient de nationalité marocaine ou étrangère.
14. Banque Chaâbi du Maroc Procédure n°2012-08 « Blâme et sanction pécuniaire de 1 million d'euros » décembre 2013.
15. Voir la Directive Générale n° DG.1/2014 destinée aux personnes et aux professions soumises à la supervision et au contrôle de l'UTRF en matière de LBC/FT.

le cnam

Conservatoire national
des arts et métiers

POLE SECURITE-DEFENSE
CHAIRE DE CRIMINOLOGIE

A NOTER DANS VOS AGENDAS - *SAVE THE DATE*

19 SEPTEMBRE 2017 – DE 09.00 A 13.00

CNAM, 292 RUE SAINT MARTIN PARIS

FACE AUX MENACES - DECELER, ANALYSER, FORMER

PRESENTATION DES FORMATIONS ET PARCOURS

Interventions des professeurs et enseignants du Master de Criminologie, des licences professionnelles, des formations qualifiantes du CNAM et des partenaires du pôle (Ministères de l'intérieur et de la défense, directions et services spécialisés).

Réservation obligatoire à : cnamsecdef@cnam.fr