LA REVUE DU
GRASCO

www.grasco.eu
www.larevuedugrasco.eu

N°21— Décembre 2017

Parution trimestrielle Gratuite
ISSN 2272-981X

EDITORIAL

CHANTAL CUTAJAR

DIRECTRICE DU GRASCO

La lutte contre la corruption transnationale, un enjeu de souveraineté économique pour la France.

Plusieurs enquêtes diligentées par la justice américaine sur le fondement du Foreign Corrupt Practices Act (FCPA) d'application extraterritoriale depuis 1998 concernent plusieurs fleurons de l'économie française dont certains se sont vus infliger des amendes colossales. Cependant, au nom de la nécessité évidente de lutter contre la corruption et du respect du droit, force est de constater que des considérations stratégiques et opportunistes sous-tendent le choix, par les autorités américaines, de diligenter ou non des enquêtes et de sanctionner des entreprises notamment françaises.

C'est ainsi que certaines d'entre elles, considérablement affaiblies par les sanctions financières sont ensuite contraintes de passer sous contrôle de groupes américains. Tel fût notamment le cas d'Alstom dont la branche énergie, représentant les trois quarts de l'activité du groupe a été reprise en 2015 par General Electric ou encore Alcatel, contrainte de fusionner avec l'entreprise américaine Lucent en 2006, qui en prit progressivement le contrôle.

C'est dans ce contexte que la loi Sapin II est intervenue pour imposer aux grandes entreprises françaises de se doter de dispositifs de conformité destinés à prévenir la corruption et a confié le contrôle du respect des obligations légales à la nouvelle Agence Française Anticorruption (AFA) dont la mission est d'aider les organismes assujettis à prévenir et à détecter les faits d'atteintes à la probité. En cas de manquement constaté et après avoir reçu les éventuelles observations de l'entité contrôlée jointes au rapport de contrôle, le directeur de l'AFA peut saisir la commission des sanctions afin que soit enjoint à l'entité contrôlée et à ses représentants d'adapter les procédures de conformité internes destinées à la prévention et à la détection des faits de corruption ou de trafic d'influence ou qu'il leur soit infligé une sanction pécuniaire.

Il n'est cependant pas certain que ce dispositif dissuadera les autorités américaines de continuer à mettre en oeuvre le FCPA. Ni la loi de blocage ni le principe non bis in idem ne paraissent de nature à venir à bout de la volonté hégémonique des Etats-Unis d'imposer le système juridique américain au moyen de l'extraterritorialité de son droit, notamment en matière de lutte contre la corruption.

Ceci explique sans doute que le Ministère de l'économie et des finances ait souhaité confié au service de l'information stratégique et de la sécurité économique (Sisse) le soin d'auditionner 200 groupes et Entreprises de tailles

SOMMAIRE

EDITO 1

INTERVIEW :

CHRISTINE GUÉGUEN, PRÉSIDENTE DU HAUT CONSEIL DU COMMISSARIAT AUX COMPTES 4

CONSTATS ET PRECONISATIONS:

LE RÔLE D'UN SYSTÈME NATIONAL D'INTÉGRITÉ DANS LA RÉDUCTION DE LA CORRUPTION, PAR JEANNE DOMINJON 9

DOCTRINE SCIENCES CRIMINELLES :

LA BELGIQUE : TERRE D'IMPUNITÉ POUR LES DÉLINQUANTS FINANCIERS ?, PAR MICHEL CLAISE 17

LES TROIS DYNAMIQUES DE L'ACTION DE L'UNION EUROPÉENNE DANS LA LUTTE CONTRE LE BLANCHIMENT D'ARGENT CRIMINEL ET LE FINANCEMENT DU TERRORISME, PAR PIERRE BERTHELET 23

DOCTRINE JURIDIQUE :

LES OBJETS CONNECTÉS, OPPORTUNITÉS ET DÉFIS POUR LA SÉCURITÉ ET LE DROIT, PAR MYRIAM QUÉMÉNER ET ADEL JOMNI 31

LA LOI N° 2017-1510 DU 30 OCTOBRE 2017 RENFORÇANT LA SÉCURITÉ INTÉRIEURE ET LA LUTTE CONTRE LE TERRORISME EST-ELLE CONFORME À LA CONSTITUTION ?, PAR DOROTHÉE GOETZ 40

REGARDONS AILLEURS :

L'OBTENTION DE LA « PREUVE ÉLECTRONIQUE » AUX ÉTATS-UNIS : UN POSSIBLE RÊVE ?, PAR MARIE-LAURENCE NAVARRI. 48

intermédiaires français sur leurs procédures antifraude et anti-corruption de façon confidentielle. Le service aurait été « sollicité par plusieurs groupes inquiets du risque d'être exposé à des juridictions étrangères et soucieux d'améliorer leurs procédures ».

Le Sisse a notamment reçu pour mission d'élaborer des standards de conformité s'appliquant aux entreprises en matière de relations financières avec l'étranger, de lutte contre les fraudes aux entreprises et contre la corruption et de responsabilité sociale et environnementale.

Dans son Flash n° 37 de novembre 2017 consacré à l'ingérence économique, le service évoque ainsi des actions d'ingérence économique dont les sociétés françaises sont régulièrement victimes et cite l'exemple « d'une multinationale française ayant connu une forte dévalorisation boursière après avoir été mise en cause dans une affaire de corruption, les investisseurs s'inquiétant des conséquences d'une possible enquête judiciaire. Pour contrer ces accusations, la société tricolore a rapidement publié un communiqué de presse, assurant collaborer avec les autorités judiciaires compétentes et indiquant avoir mis en place, au sein de ses différentes filiales, des procédures de contrôle afin de détecter et d'empêcher toutes les actions qui pourraient enfreindre la loi ».

Le ministère a confié de façon paradoxale la mission d'audit de 200 entreprises françaises à FTI Consulting, dont le siège social est à Washington DC.

Cette procédure, en effet interpelle à deux égards :

Tout d'abord, se pose la question de l'articulation de cette mission d'audit avec la mission confiée par le législateur à l'AFA dont l'intervention vise justement à améliorer les procédures de conformité et à sanctionner les manquements aux obligations légales de conformité.

Ensuite le choix de TCI consulting pour réaliser l'audit de 200 entreprises françaises surprend lorsque l'on sait que cette société a son siège à Washington DC et que les cabinets d'audit américains sont tenus de communiquer aux autorités toute opération susceptible de contrevenir à l'intérêt national qu'elles pourraient découvrir au cours de leurs missions.

La lutte contre la corruption transnationale nécessite la mise en oeuvre d'une stratégie globale dont le renseignement et l'intelligence économique doivent être partie prenante notamment pour contrecarrer son instrumentalisation par les Etats-Unis dans le but d'asseoir sa souveraineté économique et juridique. Mais cet angle d'attaque ne saurait constituer un pôle indépendant de la stratégie globale parce que ce n'est pas de cette manière que nous protègerons les entreprises françaises contre les procédures américaines. C'est en France, à l'AFA, de procéder aux contrôles dans des conditions de transparence et de respects des droits fondamentaux que la « Charte des droits et devoirs des parties prenantes au contrôle » qui vient d'être publiée, énonce clairement.

L'AFA doit ainsi contrôler non seulement la mise en place d'un dispositif de prévention et de détection de la corruption et du trafic d'influence mais également et la qualité des dispositifs de conformité mis en oeuvre. Si la Charte précise qu'elle n'a pas vocation à décrire avec exhaustivité le dispositif de contrôle, mais que « le respect des principes et comportements qu'elle décrit par toutes les personnes participant aux opérations de contrôle, contribue à un déroulement satisfaisant de ceux-ci tout en préservant les droits et devoirs de chacun ». Elle envisage ainsi dans cinq parties le dispositif de contrôle des assujettis, l'organisation des contrôles, la Commission des sanctions, les droits et devoirs des parties prenantes au contrôle des entités contrôlées et aux principes de bonne conduite du contrôle.

La montée en puissance de l'AFA et l'efficacité de la Commission des sanctions constituent le meilleur rempart contre l'instrumentalisation de la lutte contre la corruption transnationale. Il faudrait pour cela changer de paradigme et renoncer définitivement à considérer la corruption dans les affaires internationales comme un mal nécessaire mais plutôt envisager sa lutte comme un impératif catégorique et ainsi, grâce à une prévention réelle, effective, inscrite dans la culture de l'entreprise et dans l'ADN des hommes et des femmes qui la compose, avec un caractère pérenne construire un bouclier solide et respecté contre les tentatives d'instrumentalisation de la lutte contre la corruption à d'autres fin moins nobles.

Notes :

1. Rapport d'information déposé par la Commission des affaires étrangères et la commission des finances en conclusion des travaux d'une mission d'information constituée le 3 février 2016 sur l'extraterritorialité de la législation américaine », Assemblée nationale, Paris, 5 octobre 2016
2. Loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique
3. Corruption, trafic d'influence, concussion, prise illégale d'intérêt, détournement de fonds publics et favoritisme
4. Le Sisse est un service à compétence nationale au sein de la Direction générale des entreprises du ministère en charge de l'économie
5. Anne DRIF, Corruption : Bercy veut renforcer la sécurité des entreprises françaises in Les Echos du 18 novembre 2017, https://www.google.com/search?q=SISSE&ie=utf-8&oe=utf-8&client=firefox-b-ab
6. https://www.entreprises.gouv.fr/information-strategique-sisse
7. https://www.economie.gouv.fr/afa/controles-lafa-consultez-charte

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

CHRISTINE GUÉGUEN, PRÉSIDENTE DU HAUT CONSEIL DU COMMISSARIAT AUX COMPTES

PROPOS RECUEILLIS PAR JOCELYNE KAN

L.R.D.G. : Quelles sont les nouvelles missions du Haut Conseil du commissariat aux comptes (H3C) depuis l'entrée en vigueur de la réforme européenne de l'audit ?

Autorité publique indépendante dotée de la personnalité morale, le Haut Conseil du commissariat aux comptes (H3C) est l'autorité de régulation de la profession de commissaire aux comptes en France.

En 2016, l'entrée en vigueur de l'ordonnance n° 2016-315 du 17 mars 2016 qui a mis le droit français en conformité avec le droit de l'Union européenne en transposant la directive 2014/56/UE, a modifié les missions et compétences du H3C.

Outre ses attributions antérieures relatives notamment à la réalisation des contrôles de l'activité des professionnels, le régulateur est désormais chargé de l'inscription des commissaires aux comptes, de toutes les modifications affectant la liste des inscrits dont il assure la tenue, de la supervision de leur formation continue, et de l'adoption de toutes les normes applicables à la profession. Enfin, il a acquis des pouvoirs d'enquête et il peut prononcer directement des sanctions, y compris pécuniaires.

Toutes les missions du Haut conseil sont définies à l'article L. 821-1 du Code de commerce :

- Il procède à l'inscription des commissaires aux comptes et des contrôleurs de pays tiers. Il tient les listes prévues à cet effet. En application de l'article L.822-1 du Code de commerce, « *les fonctions de commissaire aux comptes sont exercées par des personnes physiques ou des sociétés inscrites sur une liste établie par le Haut conseil du commissariat aux comptes, dans les conditions prévues aux articles L.822-1-1 à L. 822-1-4* ».
- Il adopte les normes relatives à la déontologie des commissaires aux comptes, au contrôle interne de qualité et à l'exercice professionnel. Ces normes guident et sécurisent la démarche du commissaire aux comptes. Une commission composée à parité de membres du Collège du H3C et de commissaires aux comptes est placée auprès du Haut conseil afin d'élaborer les projets de normes avant leur adoption par le H3C puis leur homologation par le garde des Sceaux.
- Il définit les orientations générales et les différents domaines sur lesquels l'obligation de formation continue des commissaires aux comptes peut porter. Il veille au respect des obligations des commissaires aux comptes dans ce domaine.
- Composé du Président et de deux membres du Collège du Haut conseil, le « bureau » accorde aux

commissaires aux comptes certaines dérogations à l'application des textes relatifs à la rotation des cabinets et la réalisation de missions autres que la certification des comptes. Il définit le cadre et les orientations des contrôles auxquels sont soumis les commissaires aux comptes. Il en supervise la réalisation et peut émettre des recommandations dans le cadre de leur suivi. Il réalise lui-même les contrôles des commissaires aux comptes détenant des mandats auprès d'entité d'intérêt public (EIP) grâce à des contrôleurs salariés du Haut conseil, et il supervise les contrôles réalisés sur délégation par les instances professionnelles auprès des commissaires aux comptes ne détenant pas de mandats auprès d'EIP. Les contrôles ont pour objet de s'assurer du bon exercice du commissariat aux comptes. Ils permettent de vérifier la conformité de l'exercice du commissariat aux comptes à la réglementation et d'apprécier la qualité des audits effectués par les professionnels. En cas de manquement, les contrôles peuvent conduire à l'émission de recommandations ou à la saisine du rapporteur général du Haut conseil, en vue de l'ouverture éventuelle d'une procédure disciplinaire.

– Il diligente des enquêtes. Un service d'enquêtes avec à sa tête un rapporteur général est chargé de procéder aux enquêtes préalables à l'ouverture éventuelle de procédures de sanction. Le rapporteur général est saisi de tout fait susceptible de justifier l'engagement d'une procédure de sanction par les personnes habilitées à le faire et peut également se saisir des signalements dont il est destinataire. Il peut désigner des enquêteurs pour l'assister dans les enquêtes ouvertes et faire appel à des experts, commissaires aux comptes. Il établit un rapport d'enquête qu'il adresse à la formation du Collège du Haut conseil statuant sur les cas individuels[1] qui peut décider d'ouvrir une procédure de sanction. Le rapporteur général peut également diligenter des enquêtes pour répondre aux demandes d'assistance des autorités des États membres de l'Union européenne exerçant des compétences analogues aux siennes et autoriser les agents de ces autorités à assister aux actes d'enquête. Sous réserve de réciprocité et à la condition que l'autorité concernée soit soumise au secret professionnel avec les mêmes garanties qu'en France, il peut aussi être amené à répondre aux demandes de coopération des autorités des États non-membres de l'Union européenne exerçant des compétences analogues aux siennes.

L'article 30 de la directive n° 2014/56/UE requiert que les États membres mettent en place des systèmes efficaces d'enquêtes et de sanctions pour détecter, corriger et prévenir une exécution inadéquate du contrôle légal des comptes. Ce pouvoir de sanction est exercé par la formation restreinte du Haut conseil ou les commissions régionales de discipline après que le Collège du Haut conseil dans sa formation poursuivante (i.e. hors les membres de la formation restreinte), dite « formation statuant sur les cas individuels » a décidé d'ouvrir une procédure de sanction. Le Code de commerce définit la procédure ainsi que les personnes qui peuvent être sanctionnées, la nature des sanctions et le plafond des sanctions pécuniaires. Peuvent être mis en cause : les commissaires aux comptes, les associés et salariés du commissaire aux comptes, toute autre personne participant à la mission de certification des comptes, ainsi que leurs proches, les entités soumises à l'obligation de certification de leurs comptes et les membres de leurs organes de directions.

– Il est l'instance d'appel des décisions prises par les commissions régionales de discipline en matière de contentieux des honoraires.

– Il coopère avec ses homologues dans le cadre européen et dans le cadre international, ainsi qu'avec les instances européennes de surveillance prudentielle. Il est membre des coordinations européenne et internationale qui conduisent une démarche harmonisée de la régulation de l'audit. Il s'implique également dans les processus de consultation et de dialogue mis en place entre les normalisateurs mondiaux et les organisations de coopération des régulateurs d'audit.

– Le règlement (UE) n° 537/2014 du 16 avril 2014 comporte des exigences spécifiques applicables au contrôle légal des comptes des entités d'intérêt public. Son article 27 instaure un suivi de la qualité et de la

compétitivité du marché de la fourniture de services de contrôle légal des comptes à ces entités par les autorités de régulation de l'audit de l'Union européenne.

En application du II de l'article L. 821-1 du Code de commerce, le Haut conseil peut déléguer à la Compagnie nationale des commissaires aux comptes (CNCC) la réalisation des missions suivantes : l'inscription des commissaires aux comptes et la tenue de la liste des inscrits, le suivi du respect des obligations de formation continue des commissaires aux comptes, les contrôles visant des cabinets ne détenant pas de mandat d'entité d'intérêt public.

L.R.D.G. : Comment s'articule l'architecture institutionnelle du commissariat aux comptes : H3C, Compagnie nationale des commissaires aux comptes, compagnies régionales des commissaires aux comptes ?

La Compagnie nationale des commissaires aux comptes (CNCC), établissement d'utilité publique doté de la personnalité morale, concourt au bon exercice de la profession, à sa surveillance ainsi qu'à la défense de l'honneur et de l'indépendance de ses membres. Dans chaque ressort de cour d'appel, il est en outre institué une compagnie régionale des commissaires aux comptes (CRCC), également dotée de la personnalité morale. Avant la création du H3C, la CNCC et les CRCC remplissaient certaines missions aujourd'hui confiées au régulateur telle que le contrôle d'activité.

La réforme européenne de l'audit, en vigueur depuis le 17 juin 2016, a renforcé la supervision publique de l'audit en confiant aux autorités en charge de la régulation et de la supervision des commissaires aux comptes de nouvelles missions : l'inscription des commissaires aux comptes, la supervision de leur formation continue, l'élaboration et l'adoption des normes applicables à la profession sont désormais sous la responsabilité finale du Haut conseil.

Le législateur a néanmoins voulu conserver un équilibre institutionnel en prévoyant que le Haut conseil puisse déléguer l'exercice de certaines de ses compétences à la CNCC dans le cadre d'une convention de délégation homologuée par le garde des Sceaux. Peuvent ainsi être délégués à la CNCC l'inscription des commissaires aux comptes et la tenue de la liste des inscrits, le suivi du respect de leurs obligations de formation continue, et les contrôles d'activité visant des cabinets ne détenant pas de mandat auprès d'EIP. Le règlement européen interdit en revanche au Haut conseil de déléguer les contrôles des commissaires aux comptes qui interviennent auprès des EIP.

Le législateur n'ayant pas prévu de possibilité de délégation des missions du H3C directement aux CRCC ou la possibilité d'une subdélégation, les CRCC assistent la CNCC dans la réalisation des missions déléguées sans cependant pouvoir lui être substituée.

Trois conventions de délégation ont ainsi été conclues entre le Haut conseil et la Compagnie nationale des commissaires aux comptes (CNCC) le 12 avril 2017. Elles ont été homologuées par trois arrêtés du garde des Sceaux, ministre de la justice, le 25 avril 2017 (inscription des commissaires aux comptes et tenue de la liste des inscrits, contrôles visant des cabinets ne détenant pas de mandat d'entité d'intérêt public) et le 3 mai 2017 (suivi du respect de la formation continue des commissaires aux comptes). Ces conventions fixent les conditions de délégation.

Il convient d'ajouter que l'ordonnance n° 2016-315 du 17 mars 2016 prévoit par ailleurs que les projets de normes seront élaborés par une commission placée auprès du Haut conseil et composée à parité de membres du Collège du Haut conseil et de commissaires aux comptes. Le nombre et les modalités de désignation des membres de cette commission ainsi que les règles relatives à son organisation et à son fonctionnement sont fixés par le règlement intérieur du H3C qui dispose que les commissaires aux comptes qui y siègent sont désignés par la CNCC. Les normes sont ensuite adoptées par le Haut conseil mais après avis de la CNCC, et sont homologuées par arrêté du garde des Sceaux.

Des groupes de travail ont également été mis en place afin de favoriser le dialogue entre le régulateur et les professionnels par l'intermédiaire de leurs instances professionnelles. Le Collège du H3C a ainsi approuvé le 14 avril 2016 le principe de la création d'un groupe de réflexion pour préparer les décisions relatives aux orientations générales qui seront prises par le Collège du H3C en matière de formation continue des commissaires aux comptes.

Enfin, un groupe de contact H3C / CNCC, créé avant la ré-

forme pour préparer les changements induits par celle-ci, poursuit ses travaux sur la lecture des nouveaux textes réglementant l'exercice de la profession, issus de la réforme de l'audit qui posent des difficultés d'interprétation. Ce groupe permet au Collège du H3C de prendre position sur certaines difficultés identifiées et d'apporter ainsi tout éclairage utile aux personnes intéressées.

L.R.D.G. : Quelles sont les faiblesses dans les certifications des comptes les plus souvent observées par le H3C ?

Les contrôles constituent un élément clef du système de supervision publique des commissaires aux comptes et des cabinets. Ils ont pour objectif de s'assurer de la qualité des audits effectués. Pour atteindre cet objectif, les contrôleurs doivent vérifier, d'une part, l'adéquation de l'opinion émise sur les comptes au regard des diligences réalisées, ainsi que la conformité de ces dernières à la réglementation en vigueur, et, d'autre part, la pertinence et l'efficacité du système interne de contrôle qualité mis en place au sein des cabinets d'audit.

Il convient à cet égard de préciser que lorsque des défaillances dans l'exécution des diligences d'audit requises pour un mandat donné sont constatées, il ne peut en être déduit que les états financiers de l'entité concernée sont forcément erronés. Ces défaillances révèlent cependant, en tout état de cause, que la certification des comptes n'est pas étayée ou pas suffisamment étayée par les diligences réalisées, ce qui ne permet pas d'avoir l'assurance raisonnable que les états financiers audités ne comportent pas d'anomalies ou d'erreurs significatives.

Le Haut conseil constate que le nombre de mandats présentant des défaillances relatives aux diligences réalisées, qui ont un impact sur l'opinion émise sur les comptes audités, demeure trop important.

Les défaillances les plus fréquemment identifiées au sein des cabinets EIP et non EIP concernent :

- l'approche d'audit au regard de l'évaluation des éléments pertinents du contrôle interne et des systèmes d'information des entités auditées ;
- l'exercice collégial du co-commissariat aux comptes au regard de la répartition des travaux, la concertation sur l'approche d'audit et l'examen critique des diligences réalisées par le co-commissaire aux comptes ;
- le respect des obligations de formation des commissaires aux comptes.

Toutefois, le H3C a parallèlement relevé que les actions correctrices demandées à l'occasion de contrôles antérieurs avaient bien été mises en oeuvre, et que le système de contrôle qualité interne des cabinets s'améliorait.

L.R.D.G. : Quel est le rôle du H3C dans le cadre de sa mission de surveillance du commissariat aux comptes dans la lutte contre la corruption, les fraudes, et quel est le rôle du H3C spécialement en matière de lutte contre le blanchiment et le financement du terrorisme ? Comment est organisé le contrôle des commissaires aux comptes en cette matière ?

Une norme d'exercice professionnel spécifique définit les procédures d'audit que doit mettre en oeuvre le commissaire aux comptes pour identifier et évaluer le risque d'anomalies significatives résultant de fraudes dans les comptes et adapter ses travaux en réponse à cette évaluation.

Rappelons que dans le cadre de sa mission, le commissaire aux comptes n'a pas l'obligation de détecter systématiquement les fraudes existantes, mais qu'il doit identifier le risque d'anomalies significatives dans les comptes résultant d'erreurs ou de fraudes. Lorsque le commissaire aux comptes a identifié une fraude ou a obtenu des informations sur la possibilité d'une telle fraude, il en informe les organes de direction. Lorsque les comptes comportent des anomalies significatives résultant de fraudes susceptibles de recevoir une qualification pénale, le commissaire aux comptes doit révéler les faits au procureur de la République.

De la même manière, dans le cadre de la lutte contre le blanchiment de capitaux et le financement des activités terroristes et, en application de l'article L. 823-12 du Code de commerce, les commissaires aux comptes mettent en oeuvre les obligations relatives à la lutte contre le blanchiment des capitaux et le financement du terrorisme définies aux sections 2 à 7 du chapitre Ier du titre VI du livre V du Code monétaire et financier.

Une norme d'exercice professionnel est consacrée aux diligences du commissaire aux comptes relatives à la vigilance à

l'égard de l'identification de l'entité et du bénéficiaire effectif ; la vigilance à l'égard des opérations réalisées par l'entité et à la déclaration à faire à Tracfin. Elle définit, en outre, les liens éventuels entre la déclaration devant être faite à Tracfin et la révélation des faits délictueux au procureur de la République.

Lors des contrôles d'activité menés auprès des cabinets, le Haut conseil s'assure du bon exercice du commissariat aux comptes. Il vérifie ainsi la conformité de cet exercice et apprécie la qualité des audits effectués par les professionnels. En 2016, le Haut conseil a de nouveau relevé des défaillances liées à la mise en oeuvre des diligences relatives à la fraude et au blanchiment.

Rappelons qu'en cas de manquement, les contrôles peuvent conduire à l'émission de recommandations ou à la saisine du rapporteur général du Haut conseil, en vue de l'ouverture éventuelle d'une procédure disciplinaire.

Dans ce cadre, en cas de constatation de faits susceptibles d'être liés au blanchiment de capitaux ou au financement du terrorisme, le rapporteur général en informe Tracfin.

L.R.D.G. : Dans son rapport d'activité 2016, Tracfin appelle à davantage exploiter le potentiel de signalement, note des progrès dans la qualité des déclarations mais réitère ses critiques quant au défaut trop fréquent des pièces jointes, pourtant détenues par les professionnels, tels que les documents comptables ou les extraits K-bis. Quelles mesures pensez-vous prendre pour y répondre dans la perspective de l'évaluation de la France par le Groupe d'action financière (GAFI) ?

La recommandation n°1 du GAFI et l'article 7 de la directive (UE) 2015/849 du Parlement européen et du Conseil du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme requièrent l'élaboration d'une analyse nationale des risques en matière de lutte anti-blanchiment et contre le financement du terrorisme.

En application de l'article D. 561-51 du Code monétaire et financier, le Conseil d'orientation de la lutte contre le blanchiment de capitaux et le financement du terrorisme doit élaborer et mettre à jour régulièrement « un document de synthèse sur la menace de blanchiment de capitaux et de financement du terrorisme ». À ce titre, le Conseil d'orientation de la lutte contre le blanchiment de capitaux et le financement du terrorisme (COLB) a été chargé par le ministre des Finances et des Comptes publics d'élaborer l'analyse nationale des risques telle que requise par la directive précitée. Afin d'aider le COLB dans cette analyse, le Haut conseil et la CNCC ont établi un questionnaire à l'attention des commissaires aux comptes afin notamment :

- d'évaluer le niveau de connaissance des dispositions applicables à la profession de commissaires aux comptes en matière de lutte contre le blanchiment de capitaux ou le financement du terrorisme,
- de définir une classification des risques de blanchiment des capitaux et de financement du terrorisme,
- d'évaluer l'effectivité des procédures de contrôle interne relatives à la lutte anti-blanchiment/Financement du terrorisme (LAB-FT) mises en place par les commissaires aux comptes,
- d'évaluer le niveau de formation des professionnels.

Un rapport de synthèse des réponses reçues a été adressé au COLB.

Concernant plus particulièrement les constats et recommandations de Tracfin concernant les déclarations des professionnels du chiffre, le nombre de signalements émis par les commissaires aux comptes est en hausse de 50% entre 2015 et 2016.

Enfin, des travaux seront prochainement engagés afin de définir des Lignes directrices conjointes au Haut conseil et à Tracfin sur les obligations de déclaration et d'information auprès de cet organisme. Elles auront pour objet de préciser les attentes de la cellule de renseignement financier comme celles du régulateur concernant les obligations de déclaration et d'information à Tracfin.

Notes :

1. Cette formation spécialisée du Collège est composée de membres du Collège qui ne siègent pas au sein de la formation de jugement dite formation restreinte.

LE RÔLE D'UN SYSTÈME NATIONAL D'INTÉGRITÉ DANS LA RÉDUCTION DE LA CORRUPTION

JEANNE DOMINJON

CHARGÉE D'ÉTUDES ET PARTENARIATS À LA HAUTE AUTORITÉ POUR LA TRANSPARENCE DE LA VIE PUBLIQUE (HATVP)

Deux mille milliards de dollars de pots-de-vin[1] versés chaque année dans le monde : le coût de la corruption

apparaît comme exorbitant pour la société, engloutissant a *minima* 2,6%[2] de la richesse mondiale annuelle. Ce chiffre ne rend pas compte de l'ensemble des répercussions, la corruption pouvant affecter divers facteurs de la production de richesse (la qualité des services publics, la stabilité du cadre macroéconomique, l'intensité de la concurrence, etc.) et créer ainsi des manques à gagner importants. Ces conséquences sont particulièrement difficiles à évaluer. Le service de recherche du Parlement européen s'est emparé du sujet, montrant que les pays du vieux continent ne sont pas épargnés par ce phénomène. Son étude[3] estime que le coût de la corruption pourrait s'élever jusqu'à 990 milliards d'euros chaque année (perspective la plus pessimiste), soit 6,3% du produit intérieur brut des 28 États membres de l'Union.

Les premières personnes à pâtir de la corruption sont les plus démunies. L'argent public détourné par les différentes pratiques de corruption est une richesse qui n'est pas utilisée dans les services publics (santé, éducation…), dont les personnes ayant le moins de ressources sont les plus dépendantes. L'urgence à agir pour réduire la corruption est manifeste, et d'ailleurs soulignée par les institutions internationales depuis le début des années 1990. Ces dernières exercent depuis lors une influence importante sur les évolutions du droit pénal français[4] dans ce domaine. Le Code pénal français distingue la corruption en tant que telle depuis 1791, l'infraction était auparavant confondue avec la concussion[5].

Le droit pénal de la corruption est fondé sur une « *distinction cardinale* »[6] entre corruption passive et active. *La corruption est en effet une infraction duale, qui nécessite un corrompu et un corrupteur : « La corruption passive est le fait pour un agent compétent de se laisser acheter pour accomplir ou ne pas accomplir un acte de sa fonction. La corruption active est le fait pour une personne de rémunérer l'accomplissement ou le non-accomplissement d'un tel acte par l'agent compétent.*»[7] Malgré un arsenal pénal complet réprimant tout type d'acte de corruption, du trafic d'influence[8] à la corruption de l'organisateur d'une manifestation sportive[9] en passant par l'entrave à la justice[10], les français continuent à estimer que le pays est plutôt corrompu. La France n'obtient que 69/100 dans le dernier indice[11] de perception de la corruption élaboré par Transparency international, se classant au 23ème rang mondial. De plus, nos concitoyens ont le sentiment que 75% des responsables politiques sont corrompus, une tendance stable depuis 2014[12]. Si l'instauration d'une législation répressive

complète est indispensable, elle est insuffisante pour réduire la corruption de manière structurelle.

Phénomène complexe, protéiforme, la corruption appelle une réponse holistique. Pour la réduire, un ensemble de politiques publiques et d'outils sont à la disposition des décideurs publics. La combinaison de ces réponses, des différentes approches développées par les pays dessine peu à peu un cadre national d'intégrité, spécifique à chaque pays. Le développement d'un cadre national d'intégrité englobe la répression pénale, qui est l'une des multiples facettes d'une politique anticorruption efficace, et donne les clefs pour construire une société où la corruption serait la plus réduite possible. Revenir sur les théories successives des systèmes nationaux d'intégrité (I) permet d'esquisser une première analyse de la situation française au regard de ce cadre de réflexion (II).

I. L'émergence d'un cadre conceptuel : les théories des systèmes nationaux d'intégrité

Les premiers à évoquer les différentes actions de prévention ou de lutte contre la corruption comme un ensemble cohérent, à essayer d'avoir une approche globale de la réduction de la corruption, ont été les associations et les institutions internationales pourvoyeuses de recommandations concrètes pour les décisionnaires politiques. L'objectif d'une théorisation de la lutte contre la corruption était d'ordre pratique : obtenir l'adoption de mesures efficaces afin de la réduire.

A. D'approches prescriptives…

Pionnier du militantisme anticorruption, Jérémy Pope a également été un des premiers à penser un cadre global de lutte contre la corruption. Dès 1996, le membre fondateur de Transparency international, premier directeur général de l'association fondée en 1993, élabore la théorie du temple d'intégrité. Ce temple est construit sur deux fondements et comporte un ensemble des piliers. Filant la métaphore du temple grec, J. Pope expliquait que le fronton ne pouvait tenir que si l'ensemble des colonnes étaient d'une même hauteur et présentait la même robustesse. Le soubassement du temple d'intégrité est composé de deux blocs : la prise de conscience par le public et les valeurs démocratiques. Sur ces fondations peuvent s'élever les piliers suivants : la volonté politique de lutter contre la corruption ; un Parlement actif couplé à une instance indépendante de contrôle des comptes publics ; un système judiciaire indépendant ; une fonction publique intègre. Sur cette base, Transparency international a élaboré son guide pratique publié en 2000 (*the TI source book*), militant en faveur d'un système national d'intégrité et détaillant 12 piliers institutionnels. Ce guide est conçu pour accompagner les décideurs publics qui souhaitent mettre en place un système national d'intégrité, avec une approche concrète, faisant état des bonnes pratiques.

Ce plaidoyer en faveur d'une approche globale de la lutte contre la corruption a rencontré un écho favorable auprès des institutions internationales puisque dès 1998, l'Organisation de coopération et de développement économiques (OCDE) élabore des recommandations pour l'intégrité, qui englobent des mesures de lutte contre la corruption. Cette recommandation[13] a d'ailleurs été renouvelée en début d'année, le Conseil de l'OCDE rappelant que « *l'intégrité constitue l'un des piliers des structures politiques, économiques et sociales, et qu'elle est donc essentielle au bien-être économique et social et à la prospérité des individus et des sociétés dans leur ensemble* ».

B. … à l'élaboration de théories englobantes

Si les premières approches théoriques des systèmes nationaux d'intégrité visaient explicitement à émettre des recommandations concrètes pour adopter des politiques de prévention ou de lutte contre la corruption, cette vision a ensuite retenue l'attention de chercheurs, en particulier de politistes ou d'économistes. En 2008, des chercheurs australiens[14] décrivent le système national d'intégrité sur le modèle d'un nid d'oiseau. Les différents liens entre les institutions forment les brindilles inextricables du nid d'oiseau, si bien qu'il est impossible de déterminer précisément quelle action ou quelle institution permet au nid de tenir. L'ensemble des institutions d'un pays peuvent participer au nid, à la fois celles dont la mission est de promouvoir l'intégrité (« core integrity institutions »), qui agissent d'abord sur le secteur public, mais également

celles dont ce n'est pas le principal objectif mais qui instaurent des standards internes afin de promouvoir l'intégrité (« distributed integrity institutions »). Pour ces auteurs, la difficulté de la métaphore du temple est que si l'un des piliers est faible, l'ensemble s'effondre. Pour eux, un système national d'intégrité n'a pas cette caractéristique, car c'est plutôt un ensemble de liens et d'actions, qui isolément sont fragiles, mais qui une fois accumulées sont extrêmement difficile à dénouer.

En 2013, Frédérique Six et Alan Lawton[15] estiment que les approches prescriptives et les autres théories élaborées au début des années 2000, assez descriptives, ne sont pas pertinentes pour conceptualiser un système national d'intégrité car elles ne sont pas dynamiques. C'est pourquoi les deux anglo-saxons esquissent une approche « configurationnelle » des systèmes d'intégrité. L'idée principale est qu'en fonction des différents pays, les systèmes nationaux d'intégrité suivent des trajectoires différentes, se structurent autour d'éléments distincts, mais peuvent néanmoins atteindre un même niveau d'efficacité. Les catégories d'éléments d'un système national d'intégrité sont communes à tous : « *des politiques, des pratiques, des institutions et des gardiens de l'intégrité* », mais leur développement et leur configuration dépend des histoires institutionnelles et culturelles de chaque pays. Ainsi, des pays accusant un faible niveau de corruption n'ont pas besoin des mêmes institutions qu'un pays avec un niveau plus important de corruption pour parvenir à une même efficacité du système d'intégrité. Les auteurs proposent d'évaluer l'efficacité des configurations des systèmes nationaux d'intégrité. Pour cela, ils listent six composantes et analysent, à l'aide de la théorie des ensembles flous, les configurations qui permettent d'obtenir des systèmes d'intégrité efficaces. Cette théorie mathématique cherche à représenter l'imprécision dans la définition de certaines catégories afin de pouvoir élaborer un raisonnement logique malgré le caractère flou des objets étudiés. Les auteurs précisent : « *Dans la théorie des ensembles, les cas sont analysés pour leur appartenance à différents ensembles. Par exemple, un cas, un pays, peut faire partie de l'ensemble des États membres de l'UE, ou pas. Un cas peut aussi être considéré comme faisant partie de l'ensemble des nations démocratiques, ou pas. [...]Les ensembles flous permettent une plus grande variation dans l'appartenance à des ensembles. La théorie des ensembles flous est particulièrement appropriée dans les domaines présentant une complexité causale. Il existe plusieurs combinaisons de conditions qui mènent à l'apparition d'une issue donnée et une condition donnée peut mener à différentes issues, en fonction du contexte social* ». Dans cette étude, ils retiennent seize configurations sur les soixante-quatre possibles, en éliminant celles qui sont très improbables en théorie ou en pratique.

Dans ce tableau, seules quatre configurations assurent une intégrité élevée, et le résultat est incertain pour cinq d'entre elles. Il est à noter que cette approche configurationnelle et cette proposition d'évaluation d'un système national d'intégrité reste à un niveau très théorique puisque les informations nécessaires pour mener à bien l'évaluation sont rarement disponibles dans la réalité.

L'ensemble des théories évoquées ci-dessus, prescriptives, descriptives ou dynamiques, s'accordent sur un point : l'élaboration d'un cadre national d'intégrité inclut l'intériorisation de valeurs par la société, qui mène à une intolérance à la corruption. En d'autres termes, le développement d'un cadre national d'intégrité solide passe par le développement d'une culture de l'intégrité. Cette culture constitue d'ailleurs le deuxième

Configurations possibles	Composante I Politiques basées sur des valeurs	Composante II Organismes de surveillance indépendants	Composante III Médias indépendants	Composante IV Absence de logique corrompue	Résultat Intégrité élevée
A	Oui	Oui	Oui	Oui	Oui
B	Oui	Oui	Oui	Non	?
C	Oui	Oui	Non	Non	?
D	Oui	Oui	Non	Oui	Non
E	Oui	Non	Oui	Oui	Non

Extrait du tableau présentant les résultats de l'étude[16]

pilier de la recommandation récente de l'OCDE. Les valeurs associées à cette culture sont très larges, puisqu'elles recouvrent, selon les auteurs, un ensemble des valeurs associées à la démocratie : l'attachement à la liberté des médias, le développement du sens de l'intérêt général pour les agents publics... La dimension morale de la culture de l'intégrité prônée n'est pas sans rappeler la vertu des citoyens érigée en principe démocratique par Montesquieu[17].

C. Vers l'élaboration de normes adaptées aux enjeux anticorruption

La réglementation est l'un des outils principaux pour lutter contre la corruption. La littérature scientifique s'est penchée sur la spécificité des normes anticorruption, soulignant qu'un délicat équilibre devait être trouvé entre incitations et interdictions.

Pour la chercheuse Maria de Benedetto[18], une réglementation inadaptée peut concourir à l'augmentation des actes de corruption. Elle décrit trois mécanismes de corruption : ne pas se conformer à un devoir pour éviter un coût ; obtenir un bénéfice qui n'est pas dû ; obtenir une régulation qui favorise certains intérêts. Ces trois processus sont possibles et mêmes favorisés lorsque la réglementation est instable, peu claire ou surabondante. L'inflation législative que l'on constate dans un certain nombre de pays européens engendre une bureaucratisation plus importante. Les fonctionnaires deviennent alors les seuls à connaître et interpréter les normes, ce qui ouvre des possibilités plus larges de les corrompre. En effet, il est moins coûteux pour un acteur soumis à la réglementation (autorisation d'entrée sur un marché etc.) de payer un agent public pour y échapper que de se conformer aux multiples exigences, dont la compréhension nécessite l'embauche d'onéreux consultants spécialisés. Une production élevée de normes crée également de nombreuses opportunités de lobbying, que l'auteure relie, en raison du risque de détournement de la décision vers des intérêts privés, à la corruption. Une fois encore, il est moins coûteux pour les acteurs d'influencer les décideurs publics pour obtenir une réglementation favorable que de se conformer ensuite à des règles complexes. Cette vision de la corruption s'appuie sur la théorie de l'agent économique, qui comme un agent rationnel, effectue au moment de prendre une décision un calcul coût-bénéfice personnel. L'adaptation de ce calcul à la corruption a ainsi été écrite par Gary Becker : « *la décision individuelle sur se conformer ou pas est le résultat d'un raisonnement économique qui connecte le coût de la conformité, la taille de la sanction et le risque d'encourir la sanction* »[19].

Pour Maria de Benedetto, les législations anticorruption actuelles ne font pas de l'intégrité un comportement rentable, ce qui explique qu'elles ne soient pas respectées. Il faut donc repenser les normes. Deux pistes permettraient d'obtenir des normes anticorruption efficaces. Pour le stock, la simplification (voire la suppression) d'un grand nombre de réglementations réduirait d'autant le coût de la mise en conformité et le pouvoir arbitraire supposé des agents publics. Pour le flux, l'auteur propose d'instaurer une étude d'impact spécifique sur la corruption avant l'adoption d'une loi. Trois facteurs permettent d'évaluer l'effet sur des comportements déviants : quel coût de mise en conformité pour les acteurs concernés ; quel risque de contrôle et de sanctions (toujours conserver une part de contrôle aléatoire) ; quelle adaptation des sanctions (pas forcément économiques) aux transgressions.

Cette approche par la rationalité de l'agent est largement pondérée par les derniers développements des sciences cognitives et comportementales qui soulignent d'autres déterminants de l'action : la sensibilité à l'environnement, à l'avis des pairs, à la moralité etc. Nicoletta Rangone[20] retient trois éléments en particulier pour analyser les choix comportementaux face à la corruption : la façon dont l'information est présentée ; la tendance à se conformer au choix des pairs (et donc au niveau environnant d'intégrité) ; la capacité limitée des individus à évaluer les risques et probabilités. Pour établir des normes anticorruption efficaces, il faut prendre en compte ces trois tendances. L' auteure en déduit deux lignes directrices pour établir la réglementation anticorruption : une législation claire et stable (elle reprend ici l'argument du risque de corruption lié au pouvoir discrétionnaire de l'administration) ; mais également le besoin d'une régulation spécifique anticorruption qui manie à la fois des incitations et des

interdictions. Par exemple, elle préconise l'élaboration d'une réglementation spécifique pour les lanceurs d'alerte, qui prenne en compte l'apport des sciences cognitives. La rémunération du lanceur d'alerte (incitation) peut nuire à l'objectif. En effet, contrairement à ce que laisserait penser la théorie de l'agent rationnel, la rémunération du lanceur d'alerte réduit la dimension morale de l'acte, et peut donc être « désincitative », la première motivation de l'individu étant éthique en l'espèce. En revanche, la reconnaissance par ses pairs de son acte (lié à une culture positive autour de l'alerte) incite l'agent à lancer une alerte.

Ainsi, le besoin d'une approche holistique de la prévention et de la lutte contre la corruption fait aujourd'hui largement consensus, tant auprès des militants que des institutions internationales ou des chercheurs. Les diverses approches des systèmes nationaux d'intégrité ont des fondements théoriques différents, mais certains outils se diffusent auprès des décideurs publics, comme la transparence ou l'encadrement du lobbying. Depuis les lois pour la transparence de la vie publique d'octobre 2013, la France a connu un foisonnement normatif dans ce domaine, posant les bases de son propre système national d'intégrité.

II. Le cadre national d'intégrité englobe la lutte contre la corruption : une évaluation partielle de la situation française

Pas moins de six textes législatifs relatifs à la transparence, la déontologie ou la lutte contre la corruption ont été adoptés au cours de la XIVème mandature, instituant quelques nouveautés majeures, comme la Haute Autorité pour la transparence de la vie publique (HATVP), des référents déontologues locaux, ou bien encore l'Agence française anti-corruption (AFA). Dans quelle mesure ce nouveau cadre législatif constitue un système national d'intégrité au sens des théories présentées ci-dessus ? Cet article ne prétend pas mener une évaluation exhaustive de la situation française, mais montrer quelques liens entre les outils théoriques développés et les choix des décideurs publics français.

A. Les outils pour les plus hauts responsables publics

Le législateur français s'est tout d'abord attaché, avec les lois de 2013, à promouvoir l'intégrité des plus hauts décideurs publics. Par les responsabilités liées à leurs fonctions, ils ont un devoir d'exemplarité. Afin non seulement de garantir leur intégrité, par des mécanismes de contrôle, mais également de la donner à voir aux citoyens, par des mécanismes de transparence, la HATVP a été créée début 2014. Autorité administrative indépendante, elle est chargée en premier lieu du contrôle des déclarations de patrimoine et d'intérêts des 15800 plus hauts responsables publics du pays, qui sont répartis en deux grandes catégories : les responsables politiques, notamment les parlementaires, les membres du Gouvernement et grands élus locaux ; les responsables publics non élus, c'est-à-dire certains hauts fonctionnaires, par exemple les emplois à la décision du Gouvernement, les responsables des entreprises publiques, les présidents et membres des autorités administratives indépendantes.

Pour effectuer le contrôle du caractère exact, sincère et exhaustif des déclarations de patrimoine, la HATVP dispose de moyens humains, juridiques et techniques qui en font à certains égards un service d'enquête administratif. Si le contrôle des déclarations de patrimoine a pour objectif la détection d'enrichissement illicite ou d'autres infractions, celui des déclarations d'intérêts est d'une nature différente. La HATVP détecte les situations de conflit d'intérêts et, en dialogue avec le déclarant, fait des recommandations pour mettre fin à ces situations. À ces missions premières s'ajoutent deux autres compétences : la régulation du lobbying et, plus généralement, la promotion de la transparence de la vie publique.

Le statut d'autorité administrative indépendante permet de faire entrer la HATVP dans la catégorie des gardiens de l'intégrité, au sens de la théorie configurationnelle, puisqu'elle est un contrôleur externe aux institutions politiques et à l'administration. Elle semble également être une « core integrity institution » au sens de la théorie du nid d'oiseau, sa mission principale étant de veiller à l'intégrité des responsables publics. De plus, elle a tissé des liens importants avec d'autres institutions, que ce soit l'institution judiciaire, via les transmissions de dossiers au par-

quet pour les cas d'infractions détectées, les juridictions financières, l'administration fiscale, etc.

La mission de promotion de la transparence de la vie publique s'inscrit parfaitement dans le développement d'un système national d'intégrité, la transparence étant un outil défendu par l'ensemble des théoriciens. Augusti Cerrillo-i-Martinez identifie trois niveaux de transparence[21], chacun jouant un rôle dans la prévention de la corruption. Pour l'auteur, la transparence est la base de toute bonne gouvernance et un outil pertinent de prévention de la corruption. Le premier niveau est la transparence passive, c'est-à-dire le fait pour l'administration publique de délivrer les documents publics aux citoyens lorsque ces derniers en font la demande. Ce premier niveau est institué en France par la loi du 17 juillet 1978 qui a notamment créée la Commission d'accès aux documents administratifs. Le second niveau est la transparence active, qui consiste pour les administrations à publier d'elles-mêmes des documents administratifs et des informations intéressants le public. La HATVP s'inscrit dans ce niveau de transparence par la publication sur son site internet des déclarations (déclarations de patrimoine et d'intérêts des ministres ; déclarations d'intérêts des élus locaux et parlementaires). Le troisième niveau de transparence est collaboratif, et consiste à rendre possible la réutilisation des informations publiées par les citoyens. Pour atteindre ce niveau, plusieurs conditions doivent être remplies, en particulier la gratuité et la facilité de l'accès, par la publication dans un format ouvert et réutilisable (open data). Depuis le mois d'août 2017, la HATVP publie en open data les déclarations, permettant ainsi leur libre réutilisation. Les autres administrations françaises s'orientent également vers ce niveau de transparence. En effet la loi pour une République numérique rend obligatoire pour l'ensemble des collectivités territoriales de plus de 3500 habitants la publication en open data de leurs bases de données à partir de 2018. Ce passage à l'open data par défaut représente une véritable révolution.

Pour Augusti Cerrillo-y-Martinez, le potentiel anticorruption de la transparence est considérable. Néanmoins, pour pouvoir se révéler, d'autres facteurs sont essentiels, comme un système judicaire capable de condamner les corrompus, des médias libres, une sensibilisation des citoyens à l'usage anticorruption qui peut être fait des documents libérés, etc. Il est probable que plusieurs années de pratique de la transparence soient nécessaires pour établir une causalité avec la réduction de la corruption. À ce jour, il n'y a pas de corrélation démontrée empiriquement, mais l'auteur l'explique par la jeunesse des législations promouvant la transparence, et leur caractère souvent inabouti.

B. L'extension à l'ensemble des responsables publics

Si le législateur français a commencé par instaurer des règles en faveur de l'intégrité des plus hauts responsables publics, il a étendu divers mécanismes de prévention des conflits d'intérêts et de développement de la déontologie à l'ensemble des agents publics.

L'outil pratique de la prévention des conflits d'intérêts, la déclaration d'intérêts, a ainsi été étendu à l'ensemble des magistrats, administratifs, financiers, et judiciaires, accompagné d'un entretien déontologique. Si le modèle de la déclaration d'intérêts des magistrats s'inspire largement de celle conçue pour la HATVP, elle reste un outil interne aux juridictions, afin de garantir l'indépendance de la justice. L'entretien déontologique peut également devenir un moment de conseil déontologique, particulièrement personnalisé. Cette dimension du conseil et de l'accompagnement des responsables publics est également très présente dans les missions de la HATVP, qui peut être saisie de demande d'avis par ses déclarants ou par des institutions dirigées par ses déclarants. Si les avis de la Haute Autorité relatif à des situations personnelles restent confidentiels la saisine d'une institution indépendante, externe à l'organisation dans laquelle le déclarant exerce ses fonctions, constitue une extériorisation du conseil déontologique.

La loi du 20 avril 2016 relative à la déontologie et aux droits et obligations des fonctionnaires a quant à elle renforcé les obligations déontologiques des agents publics. Cela s'est accompagné de la création d'un nouveau droit : celui de bénéficier d'un conseil déontologique. Ce droit sera notamment exercé en fai-

sant appel au nouveau référent déontologue qui doit être nommé dans chaque administration. Le décret du 10 avril 2017 relatif au référent déontologue dans la fonction publique laisse aux administrations une grande latitude pour choisir la forme de ce déontologue (personne seule, comité etc.) et de son activité. Cette marge de manoeuvre laisse aux collectivités locales la possibilité d'adapter la fonction à leurs besoins spécifiques. De nombreuses attentes et espoirs pèsent sur ce nouveau référent déontologue qui est l'un des maillons de diffusion d'une culture de l'intégrité à tous les niveaux de l'action publique.

C. Une première prise en compte du secteur privé

Un système national d'intégrité ne se limite pas à des règles encadrant le secteur public, bien qu'elles soient souvent premières. La loi du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, dite Sapin II, étend les mécanismes de transparence et de prévention de la corruption au secteur privé.

L'une des avancées majeures apportées par ce texte est la création d'un répertoire numérique des représentants d'intérêts, c'est-à-dire des lobbyistes, confié à la HATVP. Comme le souligne Maria de Benedetto, l'encadrement des pratiques de lobbying est une étape majeure dans la prévention de la corruption. Pour Enrico Carloni[22], la complexité de cet encadrement réside dans le fait que les lobbies sont à la fois des éléments utiles à un fonctionnement fluide des institutions démocratiques, tout en portant en eux la possibilité permanente de fausser la décision publique en la faisant basculer en faveur d'intérêts privés. Pour l'auteur, la prise en compte tardive de la représentation d'intérêts par les décideurs publics vient notamment du fait que reconnaître la capacité d'influence des lobbies (qui justifie de les encadrer) serait reconnaître la part d'opacité de la prise de décision publique. Se laisser influencer par des représentants d'intérêts serait une trahison par le responsable politique, ou administratif, de l'intérêt général, et donc de sa mission première.

L'encadrement du lobbying a pour conséquence de légitimer cette profession, et reconnaît notamment son apport en termes d'expertise auprès des décideurs publics. Cette reconnaissance même permet d'instaurer des règles de transparence et des obligations déontologiques pour les lobbyistes. La vivacité des débats parlementaires sur la définition du champ des représentants d'intérêts lors de l'examen du projet de loi Sapin II montre que la vision des lobbies est encore loin d'être apaisée.

La loi française a entériné un dispositif très large, comportant les trois éléments pointés par Enrico Carloni. Tout d'abord, elle reconnaît la profession par une définition du représentant d'intérêts (définition très englobante, pouvant concerner des personnes morale ou physique, ayant le lobbying pour activité principale ou régulière). Ensuite, elle instaure des obligations déontologiques pour les représentants d'intérêts (listées à l'article 18-5 de la loi n° 2013-907 du 11 octobre 2013 relative à la transparence de la vie publique). Enfin, elle crée de la transparence sur cette activité via un registre numérique. Les représentants d'intérêts doivent notamment déclarer sur ce registre l'identité de leurs dirigeants et des personnes chargées des activités de représentation d'intérêts ainsi que le champ de ces activités. Ces éléments sont rendus publics sur le site de la HATVP. Mais l'effort de transparence demandé aux lobbies est plus grand que cette simple inscription, puisqu'à partir de 2018, les représentants d'intérêts devront rendre à la HATVP des rapports d'activité annuels retraçant les actions de lobbying effectuées au cours de l'année et les dépenses afférentes, qui seront disponibles en open data sur le site internet de la Haute Autorité.

Le second apport de la loi Sapin II au cadre national d'intégrité français est l'obligation nouvelle pour les entreprises privées ou publiques et les administrations de se doter d'un dispositif de prévention de la corruption. Les entreprises de plus de 500 salariés et dont le chiffre d'affaires est supérieur à 100 millions d'euros doivent ainsi établir un code de conduite, un dispositif d'alerte interne, une cartographie des risques etc. L'agence française anticorruption est chargée du contrôle de l'efficience des dispositifs, ainsi que d'une mission d'accompagnement de ces acteurs.

La lutte contre la corruption,

enjeu majeur, ne se résume pas à la répression des atteintes à la probité mais suppose le développement d'un véritable système national d'intégrité. Les différents outils de construction d'un tel système que sont la transparence, les règlementations adaptées, la prévention des conflits d'intérêts, le développement d'une culture de l'intégrité, se renforcent les uns les autres et construisent peu à peu un ensemble efficace pour réduire la corruption.

Le législateur français semble depuis quelques années être entré dans cette approche globale de la corruption et de l'intégrité publique, en développant ces différents outils, tout d'abord pour les plus hauts responsables publics français, puis en les étendant à l'ensemble du secteur public, et enfin en les appliquant au secteur privé. L'aspect très récent des législations françaises ne permet pas aujourd'hui d'en dresser le bilan, mais nul doute que les institutions internationales ou les politistes s'appliqueront à évaluer ces nouvelles normes et pratiques au regard de l'objectif fondamental de réduction de la corruption.

Notes :

1 Selon une estimation du fonds monétaire international : Corruption: Costs and Mitigating Strategies, prepared by a Staff Team from the Fiscal Affairs Department and the Legal Department, mars 2016.

2 PIB mondial : environ 75,54 mille milliards de dollars en 2016 d'après la banque mondiale.

3 The Cost of Non-Europe in the area of Organised Crime and Corruption. Annex II- The Cost of Non-Europe in the Area of Corruption. Research paper by RAND Europe, mars 2016.

4 Rapport n° 51 (2007-2008) de M. Hugues PORTELLI, fait au nom de la commission des lois du Sénat, déposé le 24 octobre 2007 sur le projet de loi relatif à la lutte contre la corruption.

5 Corruption et trafic d'influence, Chapitre 1, §8, Wilfrid JEANDIDIER, Répertoire de droit pénal et de procédure pénale, Dalloz, avril 2014.

6 Ibid.

7 Corruption, fiche Dalloz, septembre 2017.

8 Article 432-11 du Code pénal.

9 Article 445-2-1 du Code pénal.

10 Article 434-9-1 du Code pénal.

11 https://www.transparency.org/news/feature/corruption_perceptions_index_2016

12 Baromètre de la confiance en politique du Cevipof, décembre 2016.

13 http://acts.oecd.org/Instruments/ShowInstrumentView.aspx?InstrumentID=353&Lang=fr&Book=False

14 Promoting Integrity: Assessing and Improving Public Institutions. Head, B.W., Brown, A.J., and Connors, C., (eds) 2008. Aldershot UK: Ashgate.

15 Frédérique Six, Alan Lawton« Pour une théorie sur les systèmes d'intégrité : une approche configurationnelle », Revue Internationale des Sciences Administratives, 2013/4 (Vol. 79), p. 687-708.

16 Ibid.

17 De l'Esprit des Lois, Chapitre 3 : Du principe de la démocratie. Montesquieu, 1748.

18 Preventing corruption and promoting good government and public integrity, Chapitre 3: Understanding and preventing corruption : a regulatory approach, M. de Benedetto, ed. Bruylant, avril 2017.

19 Crime and punishment : an economic approach, The Journal of political economy, 76, G. S. Becker, 1968.

20 Preventing corruption and promoting good government and public integrity, Chapitre 4 : A behavioural approach to administrative corruption prevention, N. Rangone, ed. Bruylant, avril 2017.

21 Preventing corruption and promoting good government and public integrity, Chapitre 1 : Public transparency as a tool to prevent corruption in public administration, A. Cerrillo-i-Martinez, ed. Bruylant, avril 2017.

22 Preventing corruption and promoting good government and public integrity, Chapitre 8 : Lobby regulation to prevent corruption, E. Carloni, ed. Bruylant, avril 2017.

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

LA BELGIQUE : TERRE D'IMPUNITÉ POUR LES DÉLINQUANTS FINANCIERS ?

MICHEL CLAISE

MAGISTRAT, JUGE D'INSTRUCTION AU TRIBUNAL
DE PREMIÈRE INSTANCE DE BRUXELLES (BELGIQUE)

Il m'est demandé de dresser un état des lieux du cadre institutionnel belge affecté à la lutte contre la criminalité financière et le titre de cette intervention laisse présager une difficile conclusion. Pourtant, l'enjeu est de taille car il remet en question l'équilibre même de nos démocraties. Un phénomène criminel tant de fois été décrit, dénoncé par des professionnels laissés pour compte par les dirigeants politiques des Nations. Je propose dans un premier temps une approche générale de ce phénomène afin de mettre en évidence toute l'importance de sa prise en considération par le pouvoir politique.

I. L'ampleur du phénomène de la criminalité financière

Le 1er octobre 1996, sept magistrats anti-corruption européens (Bernard Bertossa, Edmondo Bruti Liberati, Gherardo Colombo, Benoît Dejemeppe, Baltasar Garzon Real, Carlos Jimenez Villarejo, Renaud Van Ruymbeke) se réunissaient pour lancer « l'appel de Genève », une mise en garde de la société sur l'importance de la criminalité financière qui s'est emparée de l'économie et de la finance dans des proportions inquiétantes, de l'impact de ce phénomène dans les démocraties, et de la réticence des dirigeants à vouloir la combattre. Et de plaider pour la création d'un espace judiciaire européen qui permettrait une lutte décente et cohérente contre ce cancer mondial.

21 ans plus tard, où en sommes-nous ? Le monde politique a- t-il pris ces magistrats au sérieux, en favorisant une répression indispensable et en débloquant les moyens adéquats pour l'exercer ? Le monde financier a-t-il renoncé au culte du dieu Profit, pour lui préférer l'éthique ? Les citoyens ont-ils désormais conscience des dégâts commis par ces criminels qui déstabilisent notre système économique et social ?

Les institutions européennes ont procédé à une analyse chiffrée de haute qualité sur l'importance du phénomène criminel en Europe et dans le monde. C'est la « Résolution du Parlement européen du 23 octobre 2013 sur la criminalité organisée, la corruption et le blanchiment de capitaux: recommandations sur des actions et des initiatives à entreprendre (rapport final) (2013/2107(INI)) »

Ce texte devrait être le credo de tout gouvernement qui prétend défendre un idéal démocratique.

Pour appuyer ses conclusions, la Résolution développe les chiffres de la criminalité par type d'infraction.

Ainsi, les organisations criminelles internationales actives dans l'Union européenne seraient au nombre de 3 600 et 70 % d'entre elles auraient une composition et un rayon d'action géographiquement hétérogènes, tandis que plus de 30 % auraient une vocation polycriminelle. Par an, au sein de l'Union européenne, la traite des êtres humains représenterait des profits qui atteindraient 25 milliards d'euros, le trafic d'espèces sauvages de 18 à 26 milliards, le trafic illégal de cigarettes 10 milliards, les médicaments contrefaits vendus sur internet 3 millions. Le trafic d'armes légères dans le monde et par an se situe entre 130 et 250 millions d'euros ; plus de 10 millions d'armes circuleraient.

La cybercriminalité entraîne des pertes annuelles évaluées à 290 milliards d'euros.

D'autres institutions internationales développent cette analyse. Selon la Banque mondiale, la corruption représente 5 % du PIB mondial (2 600 milliards de dollars US), plus de 1 000 milliards de dollars étant versés chaque année en pots-de-vin. La corruption majore de 10 % le coût total de l'activité des entreprises dans le monde et de 25 % celui des marchés publics dans les pays en voie de développement.

Le blanchiment d'argent est, à son tour, non seulement lié aux activités typiques de la criminalité organisée, mais également à la corruption, à la fraude fiscale et à l'évasion fiscale. La fraude fiscale, l'évasion fiscale, l'évitement fiscal et la planification fiscale agressive engendrent chaque année, dans l'Union européenne, une perte de recettes fiscales potentielles estimée à 1 000 milliards d'euros, soit un coût annuel d'environ 2 000 euros pour chaque citoyen européen.

Selon les estimations de la Commission, 193 milliards d'euros de recettes de TVA (soit 1,5 % du PIB) ont été détournés en 2011 du fait du non-respect des règles ou pour cause de non-recouvrement.

La situation est catastrophique et le Parlement européen, tout en stigmatisant les faiblesses des États membres et de leurs systèmes administratif et judiciaire, invite ceux-ci à prendre des mesures drastiques adéquates afin de lutter contre le phénomène.

Ces chiffres sont confirmés par le Fonds monétaire international qui évalue le volume annuel des opérations de blanchiment dans le monde, ce qui correspond en moyenne de 2% à 5% du PIB mondial, ou encore à une somme comprise entre 1 000 et 3 000 milliards de dollars US. Parmi les infractions les plus rémunératrices, le trafic de stupéfiants représenterait 34% de l'argent blanchi, la fraude douanière 19% et les autres activités criminelles telles que la corruption, le vol, le trafic d'êtres humains, le trafic d'organes, etc ... à 46%. Le Programme des Nations Unies pour le contrôle international des drogues (PNUCID) estime que le trafic illicite des drogues produit chaque année environ 400 milliards de dollars de profit par la vente au détail, soit près du double du revenu de l'industrie pharmaceutique mondiale ou 10 fois environ le montant total de l'aide publique au développement.

La déstabilisation se fait plus forte suite à la crise financière. Il faut l'admettre désormais : cela fait quelques décennies que le pouvoir du monde financier, licite comme illicite, a supplanté celui des gouvernements. La crise des subprimes en est à la fois le triste exemple par sa survenance et la preuve flagrante par ce qui s'en est suivi. Quel carnage social que celui qui fit suite à l'effondrement de la pyramide factice des produits immobiliers surévalués « made in USA » ! Et le chantage qui s'en suivit : à défaut de soutenir les banques, seuls responsables de cette situation, et malgré leurs erreurs et leurs man oeuvres dolosives pour s'en sortir, soit en refilant à d'autres banques leurs produits malsains, soit en faisant croire à leurs clients qu'il y avait de « bonnes affaires » à réaliser, sachant qu'il n'en était plus rien, leurs dirigeants brandirent aux ministres des pays aisés l'épouvantail de leur faillite et brossé le tableau mortifère d'une crise sociale sans précédent qui en découlerait. Que firent les politiques ? Céder !

La dérive financière s'accompagne en outre de l'explosion de sa criminalité et des terribles conséquences qui en découlent : pénétration sournoise de l'argent sale dans le flux mondial de la circulation des capitaux, prise de possession des rennes de l'économie par les entreprises mafieuses, domination des certaines Nations par les effets de la corruption et collusion volontaire entre les entreprises licites et ces entreprises pirates dans l'unique but de « faire des affaires ». Comme si le néolibéralisme avait décidé de fermer les yeux, d'ignorer ces phénomènes, et de laisser se consommer ce mariage honteux. En s'imaginant peut-être que l'argent sale est la solution du sortir de la crise.

Ces deux phénomènes s'entrecroisent donc, liés malheureusement par de mêmes intérêts. Alors se pose cette terrible question : est-ce que lutter contre cette hydre ne serait qu'un combat perdu d'avance, tant les armes sont inégales ?

II. Les réactions des pouvoirs publics face au phénomène de la criminalité financière

Dans cette lutte qui oppose les criminels financiers à ceux qui ont encore la foi dans la possibilité de les combattre, la victoire est loin d'être acquise à ces derniers.

La question de la réaction sociale face au phénomène de la criminalité financière est cruciale car l'intensité de cette réaction pourrait dicter de nouveaux comportements aux mondes politique et judiciaire. Dans un ouvrage intitulé « Sociologie des élites délinquantes » paru aux éditions Armand Collin, Pierre

Lascoumes (directeur de recherche CRNS) et Carla Nagels (professeur de criminologie) consacrent une partie importante de leur réflexion aux ambiguïtés de la réaction sociale face à la criminalité en col blanc et à la corruption politique. Se basant sur des études outre-Atlantique et plus particulièrement sur une recherche menée aux États-Unis en 1984 et portant sur un échantillon représentatif de 60 000 personnes (travail mené dans le cadre de la National Survey of crime severity), les auteurs analysent les chiffres et tirent des conclusions personnelles. « On peut retenir que la gravité attribuée par la population à des faits de délinquance économique, financière et d'atteinte à la probité publique repose sur des normes de jugements proches de celles utilisées pour les autres formes de transgression : plus il existe un dommage tangible et important (à plus forte raison s'il y a atteinte à une personne) plus la gravité sera élevée. À l'inverse, les transgressions aux faibles impacts (surtout économiques) ou aux conséquences abstraites (fraude fiscale) se voient toujours attribuer une faible gravité ».

Il n'est pas contestable que l'impact de la criminalité financière sur notre société actuelle est comparable à celui du Titanic lorsqu'il heurta l'iceberg. Dans un premier temps, les passagers ne s'étaient pas rendu compte du drame qui se préparait, tandis que l'équipage refusait d'y croire.

Le caractère passif du citoyen face au phénomène peut avoir plusieurs explications, dont l'absence de personnalisation des victimes, comme le souligne les auteurs précédemment cités, ce qui empêche toute empathie à l'égard de celles-ci.

Une autre explication trouve sans doute sa source dans la complexité de ce type de criminalité : les infractions reposent sur des mécanismes subtils, des scénarios alambiqués. Pour comprendre un carrousel à la TVA, il faut prendre le temps d'étudier les schémas internationaux de transferts de marchandises et de fonds. Une activité frauduleuse particulièrement lucrative qui, parfois, suscite chez certains aussi une forme d'admiration pour ces criminels qui détournent plusieurs millions d'euros en fraudant si facilement la victime virtuelle qu'est l'État, sans verser une goutte de sang, alors que les agressions dans les rues prolifèrent. Alors, comment faire pour sortir le citoyen de cette indifférence parfois condescendante ?

Tant les grandes affaires que les structures mises en place pour pratiquer la fraude au plus haut niveau ne peuvent être connues et comprises par les citoyens que par le travail de la presse : des journalistes formés et indépendants qui relayent le déroulement des grands procès commentent les arguments développés par le parquet et la réponse de la défense, s'interrogent sur les dérives judiciaires, comme les délais incroyablement longs pour traiter un dossier jusqu'au bout, dénoncent les pratiques frauduleuses qui se développent dans notre société avec un parfum insupportable d'apparente impunité.

Récemment, c'est bien toutefois dans la dénonciation des pratiques frauduleuses internationales que la presse s'est étonnamment illustrée.

Première salve tirée en avril 2013 : **l'Offshore Leaks**. Après un travail d'enquête de plusieurs années, l'International Consortium of Investigative Journalists, a dévoilé des fuites immenses de capitaux vers les paradis fiscaux par des personnalités politiques du monde entier, dont la femme du vice-premier ministre du gouvernement russe, Robert Mugabe, l'ancien trésorier de campagne de François Hollande et de nombreux hommes d'affaires (pas moins de 130 en France et une centaine en Belgique).

La deuxième salve est tirée par les mêmes médias en janvier 2014 : **Lux Leaks 1 et 2.** Les révélations portent cette fois sur la fiscalité du Luxembourg qui permet des accords fiscaux avec des entreprises, appelés «tax rulings». Les 548 noms dévoilés ne sont que la partie émergée de l'iceberg : il s'agit d'un système bien rodé qui consiste à favoriser l'installation du client sur le territoire luxembourgeois, moyennent une pratique d'évitement fiscal. Mais il faut néanmoins souligner que la pratique, contestable éthiquement, n'est en rien illégale.

Troisième salve : **Swiss Leaks**. Février 2015, des journalistes encore dénoncent les pratiques d'une banque suisse qui consistent à favoriser l'évasion fiscale et la dissimulation des fonds par sociétés écrans interposées. De nombreuses personnalités du monde politique, des affaires, du spectacle. Ils sont tous clients de la banque.

Quatrième salve : **Panama papers**. Avril 2016, le même consortium dévoile 214 000 sociétés off shore constituées par un cabinet d'avocats panaméens, Mossack Fonseca, et derrière les structures fictives, les bénéficiaires économiques. Le parlement européen constitua une commission d'enquête dont les conclusions furent plus que décevantes en termes d'action.

La cinquième salve, toute récente, **Paradise papers**, n'entraîna aucune modification des comportements politiques.

Mais que reste-t-il comme réactions, dans la population, après que ces scandales aient éclaté ? Les Offshore Leaks, Lux Leaks et Swiss Leaks, Panama papers et Paradise papers n'ont-ils été que des feux d'artifice dans le ciel sombre de notre société en crise ? Après le bouquet final, il faut bien constater le retour des ténèbres et du silence pesant de l'indifférence.

Et la Belgique, dans tout cela ? A part quelques cris d'indignations, aucune action politique n'a été mise en place suite aux « leaks » qui animèrent un temps restreint le paysage journalistique. À une exception : après les Panama papers, une commission parlementaire d'enquête fut mise sur pied. Il faut préciser que cette nouvelle vague de révélations était concomitante avec le dévoilement de plusieurs scandales politiques internes. Les citoyens se montrèrent plus fermes, exigeant explications et réactions. Les conclusions récentes de la commission sont le fruit d'un compromis politique: les professionnels experts ayant participé aux travaux n'ont pu que constater une faiblesse réelle dans les moyens suggérés destinés à lancer une vraie politique de lutte contre ce type de criminalité.

Alors vient la difficile constatation que le manque de moyens en termes de budget décidé par le politique s'accroit, et que la lutte contre la criminalité financière est reléguée dans les soupentes des préoccupations des dirigeants.

En voici une description sommaire.

La magistrature

Le parquet dispose d'un pouvoir absolu quant au sort des affaires dont il a la charge. Cette immense responsabilité est d'autant plus sensible qu'il y va dans l'aboutissement de sa mission de la crédibilité de la justice aux yeux du citoyen. La société attend qu'une juste répression soit organisée tant à l'égard des auteurs des petits délits commis dans les rues que des grands crimes et que les victimes puissent à la fois faire valoir leurs droits à être entendues et à être indemnisées. Mais voilà, les chiffres sont terribles. Des dizaines de milliers de dossiers sont classés sans suite (20 000 rien que dans l'arrondissement judiciaire de Bruxelles, soit environ 60% des dossiers) alors même que parfois les auteurs des délits et les victimes sont connus.

La répression financière n'échappe pas à ce difficile constat. Les substituts spécialisés sont en sous-effectifs au regard du nombre des affaires qui s'entassent dans leurs armoires. Cet encombrement entraîne plusieurs conséquences : retard dans le traitement des dossiers qui finissent par aboutir à la prescription, abandon systématique des poursuites. Et classement sans suite sans être examinés de plus de 90% des dossiers de déclarations de suspicions transmis par la Cellule de traitement des informations financières (Tracfin belge).

Quant aux juges du fond, trop peu nombreux, surtout près les Cours d'appel, leurs chambres engorgées se spécialisent dans les arrêts de prescription ou de dépassement du délai raisonnable.

Les policiers fédéraux

Les policiers fédéraux sont chargés d'exécuter les enquêtes confiées par le parquet ou les juges d'instruction. En matière financière, ces professionnels reçoivent une formation spécifique préalable à leur affectation à une section spécialisée. À Bruxelles, ils se répartissent en deux sections (DR4 et DR5) ayant chacune leurs activités spécifiques (blanchiment, banques, TVA, faillites…).

La police fédérale, tous services confondus, est une machine bien huilée mais qui connaît aujourd'hui d'inquiétants grippages. Comme le secteur de la Justice, l'appareil policier souffre de ces mêmes problèmes que sont la réduction des budgets et l'augmentation du nombre d'enquêtes. Notre société est confrontée à un accroissement sans précédent de la criminalité, causé par une multitude de facteurs, comme la perméabilité des frontières qui fait exploser les marchés illicites en tout genre : trafic de stupéfiants, d'armes, d'êtres humains… On peut coter également les effets de la crise financière et l'augmentation de la pauvreté qui en résulte, le développement des techniques criminelles comme la cybercriminalité, l'effroyable ascension du phénomène du terrorisme : il y aurait près de 600 combattants belges partis en Syrie rejoindre l'État Islamique, ce qui signifie autant de dossiers entre les mains des magistrats et des policiers, sans compter la gestion de la sécurité des citoyens suite aux attentats, etc… Les budgets alloués à la police fédérale s'avèrent insuffisants pour faire face à ce maelstrom, c'est un fait ! La lutte contre la criminalité financière n'échappe pas à ce constat. Les sections spécialisées voient leur nombre de personnel se réduire au point qu'il arrive que le directeur judicaire chargé de désigner les enquêteurs à la demande d'un magistrat lui réponde qu'il ne peut faire suite à

cette demande par manque d'effectifs. Une situation regrettable, vu l'immense qualité des policiers qui ne demandent qu'à transmettre leur expérience à des équipes nouvelles.

Mais le manque de moyens n'explique pas tout, face à certains dérèglements au sein du corps policier chargé de la lutte contre la criminalité financière. Ainsi le sort tout récent réservé à la section de la police fédérale dénommée « Direction de la lutte contre la criminalité économique et financière », subdivisée en sous-sections spécialisées, telles que l'Office central pour lé répression de la corruption (OCRC), le Federal Computer crime unit (FCCU), et l'Office central de lutte contre la délinquance économique et financière organisée (OCDEFO). La création de ces services centralisés poursuivait plusieurs objectifs, dont une action efficace en termes de collaboration avec les autorités judiciaires et policières des autres pays dans le cadre des enquêtes ayant des incidences internationales. Ainsi le FCCU, composé tant d'informaticiens pointus que de policiers fédéraux rompus aux enquêtes, a mené avec une incroyable réussite, des enquêtes dans plusieurs dossiers de hacking bancaire, c'est -à-dire de piratage des systèmes informatiques de banques, de sociétés privées et publiques et de particuliers en vue de détourner les montants déposés sur les comptes, en collaboration avec les pays européens, Europol et Eurojust. On annonce, via le Service public fédéral (SPF) de l'Intérieur, que ce service va être purement et simplement supprimé.

Il en est de même pour l'OCDEFO. Cet Office centralisé, créé le 9 juin 1993, a un champ d'action particulièrement large en matière de lutte contre la criminalité financière : blanchiment d'argent, délits fiscaux graves et organisés comme les carrousels à la TVA, certaines infractions en matière boursière, fraude au détriment de l'Union européenne... Aux policiers spécialisés s'ajoutent 14 agents fiscaux qui, durant leur affectation à ce service, reçoivent le statut d'officier de police judiciaire. Les dossiers qui leurs sont confiés en termes d'enquêtes touchent non seulement à des phénomènes criminels de très grande ampleur et à caractère international, mais également d'une nature particulièrement complexe. La complémentarité des services policiers et fiscaux constitue une plus-value exceptionnelle, entraînant depuis la création de l'Office des résultats spectaculaires, au point de lui conférer une réputation qui a dépassé nos frontières. Outre la résolution de grandes enquêtes internationales, dont les polices des autres pays ont largement profité, notamment en matière de lutte contre le carrousel TVA, certains policiers et agents fiscaux de ce service sont devenus formateurs internationaux, notamment à La Haye et en France, dispensant des cours aux fonctionnaires, policiers et magistrats européens, sans compter leur présence dans les projets de création d'institutions internationales qui seront chargées de la lutte contre les phénomènes de la fraude et du blanchiment d'argent.

Mais cette capacité exceptionnelle d'enquête n'est pas la seule qualité qui met en avant l'importance du maintien de l'OCDEFO. La détection des grandes fraudes fiscales et sociales relève également de la compétence de ce service, par les contacts organisés avec les administrations qui permettent la seule prévention immédiate existante à ce jour. La mise au point d'un contrôle automatisé mensuel du dépôt des déclarations TVA des 600 000 sociétés belges a permis une réduction spectaculaire de la fraude de type carrousel. En 2001, l'évaluation du manque à gagner pour le Trésor dû au détournement frauduleux dès règles en matière de TVA était de 1,1 milliard d'euros. Toutefois, grâce au système préventif de détection, cette évaluation a pu être revue à la baisse au fil des ans, jusqu'à atteindre le chiffre de 40,64 millions d'euros en 2014.

Alors, une question lancinante se pose : pourquoi l'actuel gouvernement via le ministre de l'Intérieur, souhaite-t-il casser cet outil exceptionnel, renvoyer les agents fiscaux dans les administrations, dispatcher les policiers spécialisés dans les arrondissements de provinces, sans garantie d'affectation à un service de lutte contre la criminalité financière, perdre la capacité de réaction immédiate dans les phénomènes criminels détectés et ainsi relancer les chiffres de la criminalité vers le haut et voir disparaître l'efficacité dans la collaboration internationale nécessaire pour contrer les grandes fraudes? À une question parlementaire sur le sujet, le ministre répond en invoquant une « optimalisation » des services de police. Mais laquelle ? Certains observateurs avancent une raison communautaire à l'origine de la décision à savoir la volonté gouvernementale de poursuivre à tout crin la régionalisation du pays, ce qui implique la suppression de tout organe centralisé.

Les experts

Certaines enquêtes nécessitent la désignation de professionnels indépendants : experts-comptables,

traducteurs-interprètes, architectes... qui assistent les magistrats par leur compétence spécifique. Une fois de plus, la réduction des budgets retarde le payement des états de frais et honoraires de ces auxiliaires de justice, de manière telle que pas mal d'entre eux hésitent à travailler encore pour la Justice.

La liste est encore longue : ainsi les magistrats avancent-ils de leur poche les frais de voyage dans l'exécution des commissions rogatoires.

Après avoir constaté l'immensité du phénomène mondial et ses conséquences pour les Nations démocratiques, une question se pose: pourquoi tant de laxisme dans le combat qui devrait être mené contre les criminels financiers ? L'indifférence citoyenne, la complexité de la matière, la volonté politique de ne pas porter atteinte à certaines entreprises qui pourraient être impliquées dans des pratiques illicites, proches du pouvoir ? Comme si les professionnels spécialisés dans ce combat étaient craints, à défaut d'être crus... Même si certains dossiers parfois aboutissent, notamment par le biais de la transaction pénale, qui permet aux nantis de s'offrir une virginité judiciaire, parfois à trop bas prix eu égard au profit illicite tiré de l'infraction, ou par miracle dans le circuit judiciaire traditionnel, leur nombre est tellement dérisoire eu égard à la proportion du phénomène global. Et comme dit le proverbe africain qui correspond si bien à ce type de délinquance : « Le voleur, c'est celui qui est pris ».

OUVRAGES RÉCENTS

LES MAGISTRATS SUR LE DIVAN

AUTEUR : DOMINIQUE VERDEILHAN

EDITEUR : ÉDITION DU ROCHER

Résumé

Marc Trévidic, Laurence Vichnievsky, François Molins, Renaud Van Ruymbeke, Jean-Claude Marin, Philippe Courroye, Éliane Houlette et bien d'autres... Plus de 80 magistrats, se confient pour la première fois. Présidents de cour d'Assise, procureurs, juges d'instruction, juges des enfants, ils révèlent ce qu'ils n'ont jamais osé évoquer : leurs angoisses, leurs souvenirs souvent traumatisants, leur détresse. Ils sont marqués, parfois de manière indélébile, par des affaires plus ou moins retentissantes : les attentats de Paris, le crash de la Germanwings, les crimes de Michel Fourniret ou de Pierre Chanal, la mort d'Ilan

Halimi ou du petit Grégory, mais aussi par les dossier Elf ou Chirac. Comment faire face chaque jour aux scènes de crimes, aux autopsies, aux catastrophes aériennes, aux attentats ? Ils se sont tus, niant leurs émotions, mais la robe n'est pas une carapace. On ne sort pas indemnes de la justice, les magistrats non plus. Dominique Verdeilhan a su mettre sur le divan ces hommes et ces femmes, leur permettant de se livrer dans des témoignages bouleversants, touchants, édifiants, qui apportent un autre regard sur la justice et ceux qui la rendent.Vous sortirez différents de la lecture de ce livre. Dominique Verdeilhan est journaliste, chroniqueur judiciaire sur France 2 et Franceinfo:. Il couvre les grandes affaires judiciaires depuis plus de 25 ans.

LES TROIS DYNAMIQUES DE L'ACTION DE L'UNION EUROPÉENNE DANS LA LUTTE CONTRE LE BLANCHIMENT D'ARGENT CRIMINEL ET LE FINANCEMENT DU TERRORISME

PIERRE BERTHELET

DOCTEUR EN DROIT ET CHERCHEUR POST-DOCTORAL
À L'UNIVERSITÉ LAVAL (QUÉBEC)

Le blanchiment d'argent criminel et le financement du terrorisme constituent une préoccupation de premier plan pour l'Union européenne. Un rapport, mentionné dans une proposition de directive présentée le 21 décembre 2016, visant à lutter contre le blanchiment de capitaux au moyen du droit pénal, évalue à 110 milliards d'euros le montant des activités criminelles au sein de l'Union européenne[1]. Cette même proposition rappelle que d'après les Nations Unies, le montant total des produits du crime à l'échelle mondiale s'élevait, en 2009, à près de 1.800 billions (mille milliards) d'euros. Face à cela, l'Union européenne s'est dotée d'un ensemble d'instruments juridiques, toujours plus nombreux et perfectionnés.

Le blanchiment d'argent criminel et le financement du terrorisme sont des phénomènes distincts. Mais, il existe un couplage de leur lutte respective qui se caractérise par la combinaison des instruments adoptés : les outils de lutte contre le blanchiment d'argent criminel (LBC) participent à celle réalisée contre le financement du terrorisme (FT). L'idée qui préside à cette stratégie de jonction de deux phénomènes distincts est de ne pas dupliquer l'action menée par la mise en place d'instruments qui pourraient se chevaucher et se faire concurrence. Toutefois, il importe de noter que « *l'accent mis sur la problématique des "finances terroristes" tend à reconfigurer le champ de l'anti-blanchiment* »[2]. La LBC et celle contre le financement du terrorisme fonctionnent de manière interactive. Les avancées dans un domaine bénéficient à l'autre, de par ce processus d'interdépendance.

De plus, il convient de souligner, dans ces deux phénomènes, l'introduction de la logique gestionnaire du risque (par exemple dans la définition des secteurs de l'économie vulnérable au risque de blanchiment d'argent criminel, au financement du terrorisme ou aux « pays tiers à haut risque »). Cette approche par le risque tend à supplanter l'approche légaliste traditionnelle : plutôt que de définir un ensemble précis de normes applicables, par exemple, à chaque transaction financière, l'approche fondée sur les risques se veut plus flexible, en distinguant chacune de ces transactions selon leur degré de risque au blanchiment de capitaux et de financement du terrorisme[3]. Une telle logique gestionnaire se retrouve également dans la stratégie de sécurité intérieure, qui constitue l'agenda institutionnel au sein duquel est mis en oeuvre la LBC/FT.

Enfin, il faut mentionner la dynamique, qui est, au demeurant, bien connue des juristes, du néo-fonctionnalisme. Cette théorie de

l'intégration a été remis en cause comme schéma explicatif de la construction européenne au cours des années 1990, elle a été actualisée et adaptée de manière à conserver sa pertinence[4]. Il s'agit plus exactement d'une théorie d'après laquelle la définition d'un objectif génère celle des moyens. Quant aux coopérations concrètes menées, qui visent à répondre aux buts fixés, elles provoquent un effet d'entraînement, c'est-à-dire l'émergence de nouvelles coopérations et le renforcement de celles existantes, ainsi qu'une réduction corrélative du champ de la souveraineté nationale[5]. Le droit européen en matière de LBC/FT se caractérise par des transferts progressifs de compétence en faveur de l'Union, qui découle d'un objectif général, à savoir approfondir le marché intérieur, et des objectifs secondaires, notamment protéger ce marché d'une criminalité qui s'est transnationalisée. Produit dérivé du fonctionnalisme, le néo-fonctionnalisme insiste sur les nécessités comme moteur d'une intégration autonome. Or, ces nécessités, qui font émerger une volonté institutionnelle aux fins de poursuite de la construction européenne, sont, dans le domaine de la LBC/FT, liées à la gravité du danger, qu'il s'agisse du danger criminel ou du danger terroriste. Un auteur note à ce propos que « *la menace est grave et pressante, mais les moyens d'y faire face paraissent dérisoires. L'argent de l'hyperterrorisme circule discrètement (et donc librement) partout dans le monde entier. Sa destination est connue, mais il s'agit bien là de la seule certitude ; par contre, on ne sait pas vraiment d'où il vient et à peine où il passe* »[6]. Les impératifs de contrer ce phénomène requièrent une intervention de l'Union qui se caractérise par un droit toujours plus dense, composés d'instruments juridiques contraignants finissant par piéger progressivement les souverainetés nationales.

L'objectif de cet article n'est pas de décrire le contenu de chacune des normes du droit positif, ni même de retracer fidèlement et dans tous les détails l'histoire de l'action de l'Union sur le plan du droit, dans le domaine de la lutte contre le blanchiment d'argent sale et le financement du terrorisme mais de tenter de dégager une logique globale de cette action. Observer la lutte entreprise dans le temps long permet d'identifier trois dynamiques complémentaires au niveau de l'Union européenne : la dynamique de l'association (I), la dynamique de la gestion (II), la dynamique intégrative (III).

I. Une dynamique d'association : du blanchiment d'argent criminel au financement du terrorisme

Le blanchiment d'argent criminel est un phénomène étroitement lié avec l'activité des organisations criminelles désireuses de bénéficier des produits de leur activité criminelle tout en en effaçant les traces. La Commission indique, dans une communication de 2008, que « *les organisations criminelles constituent des réseaux internationaux à grande échelle et tirent des profits substantiels de leurs diverses activités. Ces profits sont ensuite blanchis et réinjectés dans l'économie légale. L'efficacité des dispositifs nationaux de lutte contre le blanchiment de capitaux et la coopération internationale en la matière revêtent une importance cruciale* »[7]. La LBC est alors un moyen de faire en sorte que, pour reprendre l'intitulé de cette communication, « le crime ne paie pas » (A). La dynamique LBC/FT tient, quant à elle, au fait que le blanchiment d'argent criminel et le financement du terrorisme sont appréhendés conjointement (B).

A. La LBC comme moyen de faire en sorte que « le crime ne paie pas »

L'affirmation semble désormais une évidence : le blanchiment d'argent est corrélé à l'activité des organisations criminelles désireuses de réinvestir dans l'économie légale des fonds d'origine illégale. Le blanchiment d'argent est étroitement imbriqué à la criminalité organisée, celle-ci ayant besoin de techniques complexes de dissimulation de l'argent de ses activités criminelles, aux fins de réinjection dans l'économie légale. En effet, « *le commerce illégal de stupéfiants, une fois dépassée la connotation mercantiliste initiale, prend, à travers le blanchiment, le statut de composante de la catégorie plus large de crime organisé* »[8]. Le lien

entre blanchiment et criminalité organisée est d'ailleurs consacré par la première directive anti-blanchiment le 10 juin 1991 soulignant le fait que « *le blanchiment de capitaux a une influence évidente sur le développement du crime organisé en général et du trafic de stupéfiants en particulier* »[9].

Un consensus a été dégagé dans les années 1990 et 2000 parmi les institutions européennes autour du thème de la lutte contre la criminalité organisée, le blanchiment d'argent et la criminalité économique[10]. La lutte contre la délinquance financière constitue à ce propos un concept générique destiné à englober la criminalité organisée transnationale, la criminalité grave et d'autres formes de criminalité en col blanc à travers différents procédés : incrimination, dépistage et confiscation notamment. La Commission constate, dans sa communication du 2 juin 2005 sur l'élaboration d'un concept stratégique, que « *c'est l'appât du gain qui est le moteur de la criminalité organisée. L'élimination de toute possibilité de blanchir les produits du crime et de financer des activités criminelles porterait sérieusement atteinte à la motivation et aux moyens des groupes criminels organisés* »[11]. Le Conseil fait la même observation l'année suivante. Il indique, en effet, que « *le moteur principal de la criminalité organisée transfrontière est l'appât du gain, qui pousse les délinquants à commettre toujours plus d'infractions pour s'enrichir encore davantage* »[12].

La problématique de l'insertion de la criminalité organisée dans les circuits financiers, et l'utilisation de ceux-ci dans le cadre de ses activités criminelles, n'est pas nouvelle en soi. Les institutions européennes avaient déjà abordé cette problématique sous l'angle du blanchiment de l'argent sale. Conformément aux recommandations du GAFI (Groupe d'action financière)[13], deux directives anti-blanchiment avaient été adoptées, la première précitée, datant de juin 1991, et la seconde le 4 décembre 2001, visant compléter le droit existant[14]. Plus exactement, ce texte actualise la directive de 1991 en étendant la définition du blanchiment à des phénomènes criminels allant au-delà du seul trafic de drogues[15]. La première et la deuxième directives érigent en droit contraignant les prescriptions figurant jusqu'à présent dans les recommandations du GAFI. Il est vrai que l'impact de cette soft law sur le droit national est déjà notable[16]. Le droit européen prend en compte cette situation en venant, quant à lui, prolonger des mesures internationales mises en place. En particulier, le Conseil a adopté une décision destinée à améliorer la coopération entre les cellules de renseignement financier (CRF), à savoir les cellules chargées de recueillir les déclarations de soupçon de blanchiment[17]. Ces cellules, instituées conformément aux recommandations du GAFI, sont destinées à collecter et à analyser les informations, en premier lieu les déclarations de soupçon, et à échanger ces informations avec les CRF des autres États, qu'il s'agisse des États membres ou de pays tiers[18].

Parallèlement à cela, sur le plan pénal, le Conseil a adopté en 1998 une action commune destinée à renforcer les dispositions de la convention du Conseil de l'Europe sur la lutte anti-blanchiment du 8 novembre 1990, ainsi que le protocole de 2001 à la convention d'entraide judiciaire du 29 mai 2000, facilitant l'identification des titulaires de comptes et le suivi des mouvements de compte[19]. 2001 marque à ce sujet un tournant dans la LBC puisqu'à compter de cette date, il existe une nette convergence entre la lutte contre le blanchiment d'argent et le financement du terrorisme.

B. La LBC/FT : une convergence entre la lutte contre ces deux phénomènes

Il est possible de faire remonter la lutte contre le financement du terrorisme à l'échelle de l'Union à la fin des années 1990. Une recommandation a été adoptée à cet effet par le Conseil le 9 décembre 1999[20]. La lutte contre ce phénomène est toutefois devenue une composante « majeure »[21] de l'action de l'Union après les attaques de 2001.

La lutte contre le FT constitue une priorité politique. Elle occupe en effet une place centrale des stratégies de lutte contre le terrorisme[22]. Comme le résume

la Commission, « *la lutte contre le blanchiment de capitaux est depuis longtemps une priorité politique essentielle de l'Union européenne, qui découle de la nécessité de protéger le système financier et de soutenir les efforts de lutte contre la criminalité organisée. Suite aux événements tragiques du 11 septembre 2001 et au consensus international sur la nécessité de cibler le financement du terrorisme, l'importance de cette tâche est devenue encore plus notoire* »[23].

Il est question pour l'Union d'affaiblir les groupes terroristes à travers un contrôle des flux financiers[24]. Les moyens de financement du terrorisme ont évolué. Jadis appuyé par un État, celui-ci trouve ces moyens sur le marché en agissant comme une multinationale. Mobile, il puise, dans un monde globalisé, diverses sources de financement dans le marché[25]. Il existe en effet une grande mutabilité des méthodes de financement du terrorisme[26].

Le programme de La Haye a fait de la question de la lutte contre le financement du terrorisme une priorité politique de l'Union européenne[27]. Dans le sillage de ce programme, le Conseil a approuvé, le 2 décembre 2004, un plan d'action à l'heure où le terroriste constitue, pour l'Union, une préoccupation de premier plan au regard des attaques perpétrés à Madrid[28]. Ce texte reprend une partie des mesures suggérées par la Commission européenne dans sa communication du 20 octobre 2004[29]. Parmi celles prévues figurent l'échange et l'analyse des informations via le réseau CRF.NET qui, comme son nom l'indique, connecte les CRF entre elles, ainsi que le renforcement de l'investigation financière, par la création notamment, d'organismes nationaux capables de repérer et de geler les avoirs terroristes et criminels. D'autres mesures sont prévues, en particulier la traçabilité des fonds financiers. Bien les phénomènes soient différents[30], le système de contrôle des mouvements de capitaux mis en place dans le cadre de la lutte anti-blanchiment est vu par les institutions européennes comme étant pertinent dans la lutte contre financement du terrorisme, ce qui justifie l'extension de ce système à ce phénomène[31].

À l'instar du blanchiment, l'action de l'Union dans la lutte contre le FT menée à l'échelle de l'Union complète et renforce celle élaborée au niveau international. Les mesures que comporte ce plan d'action s'inscrivent en effet, elles-mêmes, dans le sillage de l'action entreprise par le Groupe d'action financière (GAFI), qui, avec les recommandations spéciales et les notes interprétatives qu'il a édictées[32], « *forme de diapason mondial et aiguillon intergouvernemental de la lutte contre le blanchiment d'argent et le financement du terrorisme* »[33].

La jonction entre la LBC/FT, réalisés au niveau international se retrouvent aussi à l'échelle de l'Union. Dans une communication du 29 mars 2004, la Commission associe clairement la criminalité organisée et le terrorisme. Elle écrit à ce propos qu'il « *convient d'établir un lien entre les mesures de lutte contre la criminalité organisée et le terrorisme. Le lien entre le terrorisme et d'autres formes de criminalité, en particulier la criminalité organisée n'apparaît pas toujours de manière évidente. Des liens entre ces deux phénomènes existent cependant : dans les méthodes, dans le financement, et parfois, entre les groupes eux-mêmes* ». Elle ajoute que « *dans leur recherche de financement, les organisations terroristes utilisent aussi fréquemment des méthodes similaires à celles utilisées par les organisations criminelles en se livrant à des activités telles que des extorsions de fonds, des enlèvements suivis de demandes de rançon ou encore des trafics et fraudes de toute nature. Tout comme les organisations criminelles, ils peuvent avoir recours à la corruption et utilisent le blanchiment* »[34]. Cette combinaison criminalité organisée/terrorisme se retrouve tout logiquement au sein de la troisième et la quatrième directives anti-blanchiment (les deux premières ne s'appliquant qu'au phénomène de blanchiment). La lutte contre ces phénomènes appréhendés de manière conjointe tend à reposer sur une approche commune, celle de la gestion (du risque et de la menace).

II. Une dynamique de gestion : l'approche par le risque et la menace

La troisième et la quatrième directives anti-blanchiment consacrent une approche fondée sur le risque (A). Il s'agit de le gérer, c'est-à-dire prévenir et atténuer ses conséquences néfastes sur le marché intérieur. Cette logique de gestion se retrouve en matière de sécurité intérieure, (B). Les stratégies de sécurité intérieure, qu'il s'agisse de 2010 ou de 2015, dont la finalité est de pouvoir gérer les menaces à laquelle l'Union et les États membres sont confrontés, constituent un document programatique au regard duquel est défini l'agenda institutionnel de la LBC/FT.

A. Une approche fondée sur la gestion du risque : les troisième et quatrième directives anti-blanchiment

La LBC est caractérisée par l'existence, au niveau de l'Union, d'un « régime complet et sophistiqué »[35] sur le plan juridique avec, au centre du dispositif, les différentes directives anti-blanchiment. Leur adoption successive reflète la volonté des institutions européennes de s'engager dans un processus de renforcement continuel marqué par l'extension, la modification et la consolidation de la législation européenne[36]. Sur base de ce plan ont été adoptés notamment la troisième directive anti-blanchiment en 2005[37]. Ce texte est adopté en parallèle à d'autres : le règlement relatif aux informations concernant l'émetteur de virements, le règlement destiné à instaurer un contrôle commun des mouvements d'argent liquide aux frontières extérieures de l'Union[38], et le code de conduite relatif au secteur non lucratif[39], l'objectif étant d'imposer la transparence des flux d'argent[40].

La troisième directive anti-blanchiment adapte la législation européenne aux prescriptions du GAFI, en l'occurrence ses quarante Recommandations révisées. La troisième directive met en oeuvre une approche moins légaliste et plus pragmatique, davantage fondée sur le risque[41]. Concrètement, les entités assujetties à l'obligation de déclaration doivent appliquer des mesures de vigilance renforcées en fonction du risque présenté. Les vérifications et contrôles supplémentaires de transactions financières destinées à prévenir et détecter les transactions suspectes sont donc graduées, selon le risque évalué.

Or, cette dimension du risque a été renforcée avec la quatrième directive. La Commission a publié le 11 avril 2012 un rapport énumérant les différentes questions soulevées par le réexamen de la troisième directive anti-blanchiment. D'une manière générale, le cadre existant semblait relativement bien fonctionner d'après elle[42]. Néanmoins, la troisième directive anti-blanchiment a dû faire l'objet d'une révision pour l'adapter aux recommandations approuvées en février 2012 par le GAFI. Dans le sillage de ce rapport, la Commission européenne a présenté au début de l'année 2013 une proposition de directive visant à modifier cette troisième directive anti-blanchiment[43], qui couvrait elle-même la plupart des quarante Recommandations et quelques-unes des neuf Recommandations spéciales du GAFI[44]. La proposition de quatrième directive, adoptée par le législateur en 2015[45], visait à améliorer la lutte anti-blanchiment, en intégrant notamment les dispositions de la décision du Conseil du 17 octobre 2000 concernant les modalités de coopération entre les cellules de renseignement financier. Il est possible de considérer qu'elle était destinée à dépasser certaines prescriptions du GAFI, « *marquant la volonté de l'Union de créer un arsenal réglementaire efficient et le plus pragmatique possible, face aux fléaux (conjugués ou non) du blanchiment et du financement du terrorisme* »[46]. La création de cet arsenal s'insère désormais, depuis le début des années 2010, dans l'optique de la mise en oeuvre de la stratégie européenne de sécurité intérieure.

B. Une approche fondée sur la gestion des menaces : la stratégie de sécurité intérieure

Comme l'indique la stratégie révisée de lutte contre le financement du terrorisme approuvée par le Conseil des 24 et 25 juillet 2008, les attentats du 11 septembre 2001 ont amené l'Union à réaliser des « efforts considérables »[47] en matière de lutte contre le financement du terrorisme. Depuis ces attentats, l'action de l'Union européenne a consisté, dans le prolongement des efforts menés

sur le plan international à empêcher la commission d'attentats en privant les terroristes de leurs moyens financiers[48]. La stratégie révisée de lutte contre le FT des 24 et 25 juillet 2008 indique qu'« *en empêchant les terroristes d'utiliser les moyens et ressources dont ils disposent pour mettre leurs projets à exécution, l'UE protège ses citoyens de la manière la plus efficace possible* »[49]. Cette volonté d'assurer une meilleure protection des citoyens se trouve au c oeur de la stratégie européenne de sécurité intérieure adoptée par le Conseil de l'UE les 25 et 26 février 2010 et approuvée par le Conseil européen les 25 et 26 mars 2010, qui déclare que *« la grande criminalité et la criminalité organisée prennent une importance croissante. Sous leurs différentes formes, elles ont tendance à apparaître partout où elles peuvent obtenir le plus gros bénéfice financier avec le minimum de risques, sans se préoccuper des frontières* »[50]. Une telle stratégie, qui couvre la période 2010-2015, est fondée sur cinq objectifs stratégiques, en particulier perturber les réseaux criminels internationaux et prévenir le terrorisme. C'est dans ce contexte qu'a été présentée en 2013 la proposition de quatrième directive anti-blanchiment précitée, celle-ci ayant été programmée dans le cadre de liste des mesures destinées à parvenir à une Europe plus sûre[51]. Dans sa deuxième évaluation de stratégie de sécurité intérieure, la Commission rappelle que le paquet législatif dans lequel s'insère la directive est destiné à traiter des nouveaux risques et menaces, notamment en promouvant la transparence des entités juridiques[52].

Dans le programme européen en matière de sécurité de 2015, la Commission confirme le fait que la LBC est placée sous l'égide de la gestion des menaces et des risques. D'abord, elle entend appliquer la méthodologie d'évaluation des risques telle que déployée en matière de gestion des catastrophes (qui constitue le cinquième objectif stratégique de la stratégie de sécurité intérieure) et de sûreté aérienne, à d'autres domaines couverts par la stratégie, en l'occurrence les infrastructures critiques, et surtout le blanchiment de capitaux et le financement du terrorisme. Par effet d'imbrication, la LBC/FT sont englobés dans une perspective globale de gestion des menaces prises en compte par la stratégie de sécurité intérieure au nom de risques systémiques en cascade. La stratégie de 2015-2020 consacre les options prises par la stratégie 2010, en identifiant parmi les types de risques menaçant la sécurité des citoyens européens, la grande criminalité organisée, et en faisant de la lutte contre ce phénomène une priorité. Dans ce document, approuvé par le Conseil le 16 juin 2015, les ministres du Conseil « Justice et affaires intérieures » soulignent qu'« il convient d'accorder une attention particulière à toute activité liée au blanchiment de capitaux et au réinvestissement des produits du crime, visant notamment à infiltrer l'économie légale ». Ils insistent à cet égard sur l'importance de la prévention et de l'anticipation, qu'il s'agisse des actes criminels et des attentats terroristes, et proconisent à cette fin une approche proactive et fondée sur le renseignement. Cette conception se trouve au coeur des conclusions approuvant le plan d'action de 2016, estimant que les cellules de renseignement financier pourraient passer d'un système de divulgation basé sur des suspicions à un système de divulgation davantage fondé sur le renseignement. Un tel plan d'action concourt à la dynamique d'intégration. Conjugué à d'autres, il concourt au renforcement continuel de la LBC/FT qui elle-même, contribue à l'édification d'une Europe de la sécurité.

III. Une dynamique d'intégration : le renforcement continuel de la LBC/FT

Approuvé quelques semaines après les attaques de Paris de novembre 2015, le plan d'action de février 2016 sur le financement du terrorisme fait écho au programme européen en matière de sécurité d'avril 2015 insistant sur la nécessité de prendre des mesures pour s'attaquer au FT de manière plus efficace et plus globale[54]. Les deux grands axes retenus sont d'une part, renforcer les mécanismes de surveillance des

mouvements financiers et d'autre part, réduire les sources utilisées par les organisations terroristes. Tant les conclusions du Conseil « Justice et affaires intérieures » du 20 novembre 2015, que celles du Conseil « Affaires économiques et financières» du 8 décembre 2015, et du Conseil européen du 18 décembre 2015, ont mis en évidence l'importance de renforcer l'action de l'Union dans ce domaine, en perfectionnant les dispositions figurant dans la quatrième directive (A), et en transférant des compétences des États membres vers l'UE (B).

A. Un renforcement du cadre juridique de l'UE dans le domaine du LBC/FT

Le plan d'action, approuvé par le Conseil le 12 février 2016[55], prévoit notamment la présentation d'une proposition de modification de la quatrième directive, ce qu'a fait la Commission le 5 juillet 2016[56]. Désireuse de colmater certaines brèches identifiées dans le plan d'action (par exemple le recours illicite à l'argent liquide, aux monnaies virtuelles ou aux cartes prépayées anonymes), ce texte en cours d'adoption par le législateur fait écho aux résolutions adoptées par le Conseil de sécurité des Nations Unies pour empêcher les groupes terroristes d'avoir accès aux institutions financières internationales.

Cette volonté de compléter et de renforcer la cadre juridique international relatif au FT se retrouve également dans une proposition de directive, évoquée en introduction, présentée le 21 décembre 2016 par la Commission visant à lutter contre le blanchiment de capitaux au moyen du droit pénal. Ce texte reprend les dispositions de la Convention de Varsovie relative à la LBC qui, elle-même va, sur certains aspects, au-delà des exigences exprimées dans les Recommandations révisées du GAFI. Une telle proposition est destinée à établir un socle de sanctions et d'infractions en modifiant certaines dispositions de la décision-cadre 2001/500/JAI[57]. Elle constitue, avec la cinquième directive anti-blanchiment en cours d'adoption, un nouvel élément de l'arsenal réglementaire de l'Union.

Cet arsenal se développe au fil du temps puisqu'outre les textes précédemment évoqués, ont été adoptés la nouvelle directive concernant le gel et la confiscation des produits du crime et le règlement sur les virements de fonds[58]. De surcroît, trois propositions législatives ont été présentées concomitamment par la Commission le 21 décembre 2016, pour renforcer le cadre juridique de l'UE dans le domaine LBC/FT : la proposition de directive précitée établissant un socle de sanctions et d'infractions, une proposition de règlement destinée à identifier les mouvements illicites d'argent liquide et une proposition de règlement concernant à la reconnaissance mutuelle des décisions de gel[59]. Viennent se surajouter à cet ensemble normatif une proposition présentée le 13 juillet 2017 visant à lutter contre le trafic de biens culturels exportés illicitement depuis un pays tiers, complétant une directive du 15 mars 2017 visant à mieux sanctionner les personnes qui apportent un soutien matériel au terrorisme[60].

B. Un transfert de compétence des États membres vers l'UE

Le mouvement d'intégration correspond également à un transfert progressif de compétences des États membres vers l'Union. Il existe à cet égard un dynamisme législatif continu, sous forme d'actes contraignants dont le nombre est toujours croissant (et au regard desquels la législation des États membres doit se conformer).

Or, un tel mouvement, stimulé par cette dynamique législative, ne devrait pas s'arrêter, puisqu'un rapport présenté le 26 juin 2017 par la Commission consacré à une évaluation supranationale des risques révèle que le marché intérieur européen reste vulnérable aux risques de financement du terrorisme et de blanchiment de l'argent du crime[61]. Dans ce texte, elle recense toute une série de produits ou services potentiellement vulnérables, et préconise à cette fin un ensemble mesures, par exemple une initiative permettant de renforcer la transparence des paiements en espèces. Les conclusions présentées d'ici juin 2019, sur le suivi des mesures

adoptées par les États membres, devraient à ce propos déboucher sur de nouvelles initiatives législatives destinées à renforcer toujours davantage cet arsenal de l'Union en matière LBC/FT.

Notes :

1 p.3 de la proposition de directive (COM(2016) 826).

2 Amicelle, A., « Gestion différentielle des illégalismes économiques et financiers », *Champ pénal*, vol. 10, 2013. URL : http://champpenal.revues.org/

3 Wesseling, M., *Evaluation of EU measures to combat terrorism financing*, Études du Parlement européen, DG des politiques internes, Département C, 2014, p. 14-15.

4 Sandholtz, W. Stone Sweet, A., « *Neofunctionalism and Supranational Governance* », in Menon, A. Jones, E., Weatherill, S. (dir.) *The Oxford Handbook of the European Union*, Oxford: Oxford University Press, 2012.

5 Haas, E. B., *The Uniting of Europe : Political, Social and Economic Forces 1950-1957*, Stanford (Ca.), Stanford University Press, 1958.

6 Broyer, P., « Le financement de l'hyperterrorisme », *in* François, L., Chaigneau, P., Chesney, M. (dir.), *Blanchiment et financement du terrorisme*, Paris, Ellipses, 2004, p. 42.

7 p. 3 de la communication du 20 novembre 2008 (COM(2008)766).

8 Manacorda, S., « La riposte pénale contre la criminalité organisée dans le droit de l'Union européenne », *in* Manacorda, S. (dir.), *L'infraction d'organisation criminelle en Europe*, Paris, Presses universitaires de France, coll. Presses universitaires de Poitiers, 2002, p. 248.

9 3e considérant de la directive 91/308/CEE (*J.O.U.E.* L 166 du 28.6.1991, p. 77).

10 Mani, M., *L'Union européenne dans la lutte contre le blanchiment d'argent. Entre intérêts nationaux et intérêts communautaires*, Paris, L'Harmattan, coll. Entreprises et management, 2003, p. 131.

11 Point 22 de la communication (COM(2005) 232).

12 Doc. du Conseil des 1er et 2 juin 2006, n° 9409/06 (Presse 144).

13 Jamin, V., « Le blanchiment et l'espace pénal européen », *in* Brayer, G. (dir.), *La lutte internationale contre le blanchiment et le financement du terrorisme ?* Paris, Société de législation comparée, 2007, p. 81.

14 Directive 2001/97/CE du 4 décembre 2001 (*J.O.U.E.* L 344 du 28.12.2001 p. 76).

15 Dehousse, F., Garcia Martinez, J., *La coopération policière et judiciaire pénale de l'Union européenne. Les lents progrès d'un projet européen*, Studia Diplomatica, vol. 55, n° 4, 2002, p. 45-46 ; Mani, M., *op. cit.*, p. 86 ; Hotte, D. G., Heem, V., *La lutte contre le blanchiment de capitaux*, Paris, LGDJ, coll. Systèmes – Fiscalité, 2004, p. 26.

16 Cassani, U., « Le puzzle des infractions préalables au blanchiment : hasard ou système ? », *in* Perrin, P. (dir.), *La lutte contre le blanchiment d'argent : pistes d'actions entre prévention et répression*, Paris, L'Harmattan, coll. Les Actes de l'ILCE, 2009, p. 20-21.

17 Décision du Conseil du 17 octobre 2000 (*J.O.U.E.* L 271 du 24.10.2000 p. 4).

18 Boyle, R., « Les mesures internationales de lutte contre le blanchiment de capitaux et le financement du terrorisme », *in* Brayer, G. (dir.), *op. cit.*, p. 41-42 ; Defferrard, F., « Les forces normative du Groupe d'Action Financière », *in* Collectif, *Questions de droit pénal européen et compare. Mélanges Fournier*, Nancy, Presses universitaires de Lorraine, 2013, p. 104-105.

19 Resp. action commune 98/699/JAI, du 3 décembre 1998 (*J.O.U.E.* L 333 du 9.12.1998 p. 1) ; convention européenne n° 141du 8 novembre 1990 ; protocole du 16 octobre 2001 (*J.O.U.E.* C 326 du 21.11.2001 p. 2).

20 Recommandation du 9 décembre 1999 (*J.O.U.E.* C 373 du 23 décembre 1999, p. 1).

21 Wesseling, M., *op. cit.*, p. 9.

22 Frantangelo, P., « L'Union européenne face à la lutte contre le financement du terrorisme », *Revue du droit de l'Union européenne*, n° 4, 2006, p. 840.

23 Point 5 de la communication du 16 avril 2004 (COM(2004)262).

24 Kornobis-Romanowska, D., « La lutte contre la corruption et le blanchiment de capitaux dans l'Union européenne », *in* Auvret-Finck, J. (dir.), *L'Union européenne et la lutte contre le terrorisme. État des lieux et perspectives*, Bruxelles, Larcier, 2010, p. 254.

25 Chesney, M., « Le terrorisme se privatise et défie l'Occident », *in* François, L., Chaigneau, P., Chesney, M. (dir.), *op. cit.*, p. 16-17.

26 Peyró Llopis, A., « Le rôle des organisations européennes dans la lutte contre le financement du terrorisme », *in* Sorel, J.-M. (dir.), *La lutte contre le financement du terrorisme : perspective transatlantique*, Paris, Pedone, Cahiers internationaux n° 21, CERDIN, 2009, p. 80.

27 Au 6e paragraphe du point 2.2 du programme de La Haye.

28 Doc. du Conseil du 14 décembre 2004 n° 16089/04.

29 Communication sur le FT (COM(2004)700).

30 Amicelle, A., « La lutte contre le financement du terrorisme », *in* Bigo, D., Bonelli, L., Deltombe, T. (dir.), *Au nom du 11 septembre… Les démocraties à l'épreuve du terrorisme*, Paris, La Découverte, coll. Cahiers libres, 2008, p. 135.

31 Roberge, I., « Le financement du terrorisme », *in* Kirschbaum, J.(dir.), *Terrorisme et sécurité internationale*, Bruxelles, Bruylant, coll. Études stratégiques internationales, 2004, p. 153 ; Spence, D., « International terrorism: The quest for a coherent EU response », *in* Spence, D. (dir.), *The European Union and terrorism*, Londres, John Harper Publishing, 2008, p. 24.

32 Sur ces recommandations et ces notes, voir Martin, J.-C., « Les institutions financières internationales et la lutte contre le financement du terrorisme », *in* Sorel, J.-M. (dir.), *op. cit.*, p. 65-68.

33 Dantinne, M., « Blanchiment de capitaux et crise économique et financière », *in* Blais, E., Perrin, B., *La lutte contre la criminalité économique : réponses interdisciplinaires à un défi global*, Paris/Genève, L'Harmattan/Schultess, 2010, p. 26.

34 p. 2 de la communication du 29 mars 2004 (COM(2004)221)).

35 Scherrer, A., Mégie, A., Mitsilegas, V., « La stratégie de l'Union européenne contre la criminalité organisée : entre lacunes et inquiétudes », *Cultures et Conflits*, n° 74, été 2009, p.96.

36 Beaussier, M., Quintard, H., *Blanchiment de capitaux et financement du terrorisme*, Paris, Revue Banque Édition, 2010, p. 23.

37 Directive 2005/60/CE du 26 octobre 2005 (*J.O.U.E.* L 309 du 25.11.2005 p. 15). Pour une présentation de la directive, voir Rietrae, J., « The 3rd EU anti-money laundering directive – main issues and intriguiguing details », *in* Brayer, G. (dir.), *op. cit.*, p. 97-129 ; Kornobis-Romanowska, D., *op. cit.*, p. 258-260 ; Bertoni, P., « La lutte contre le blanchiment de capitaux à des fins terroristes », *in* Saulnier-Cassia, E. (dir.), *La lutte contre le terrorisme dans le droit et la jurisprudence de l'Union européenne*, Paris, LDGJ, 2014, p. 1173-174.

38 Resp. règlement (CE) n° 1781/2006 du 15 novembre 2006 (*J.O.U.E.* L 345 du 8.12.2006, p. 1) ; règlement (CE) n° 1889/2005 du 26 octobre 2005 (*J.O.U.E.* L 309 du 25.11.2005 p. 9).

39 Doc. du Conseil du 2 décembre 2005 n° 14390/05 (presse 296).

40 Brayer, G., « Le défi de l'économie criminelle et du terrorisme », *in* Brayer, G. (dir.), *op. cit.*, p. 21.

41 Beaussier, M., Quintard, H., *op. cit.*, p. 25. Pour un approfondissement de la réflexion, voir Herlin-Karnell, E., « The EU's anti-money laundering agenda: Built on risk? », *in*, C., Konstadinides, T. (dir.), *Crime within the Area of freedom, security and justice*, Cambridge, Cambridge University Press, 2011, p. 89-92.

42 p. 20 du rapport de la Commission (COM (2012)168).

43 Proposition de directive du 5 février 2013 (COM(2013)45).

44 Pour une présentation de ces Recommandations : Boyle, R., *op. cit.*, p. 37-39.

45 Directive (UE) 2015/849 du 20 mai 2015 (*J.O.U.E.* L 141 du 5.6.2015, p. 73-117).

46 Dumoulin, L., « Lutte anti-blanchiment et lutte contre le terrorisme : de nouvelles propositions européennes », *RUEDELSJ*, 23 février 2014, URL : http://www.gdr-elsj.eu/

47 p. 1 du doc. du Conseil du 17 juillet 2008, n° 11778/1/08.

48 Brayer, G., « Le défi de l'économie criminelle et du terrorisme », *op. cit.*, p. 20-21 ; Gilmore, W. C., *L'argent sale. L'évolution des mesures internationales de lutte contre le blanchiment de capitaux et le financement du terrorisme*, Strasbourg, Éditions du Conseil de l'Europe, 2005, p. 130-140 ; Auvret-Finck, J., « Le cadre juridique de référence de la lutte contre le terrorisme », *in* Auvret-Finck, J. (dir.), *op. cit.*, p. 33 ; Le Floch, G., « La contribution des Nations Unies à la lutte contre la financement du terrorisme », *in* Sorel, J.-M. (dir.), *op. cit.*, p. 9. Sur cette question, voir Chappez, J. « La lutte internationale contre le blanchiment des capitaux d'origine illicite et le financement du terrorisme », *Annuaire français de droit international*, vol. 49, 2003. p. 542-562 ; Frantangelo, P., *op. cit.*, p. 815-840 ; Dantinne, M., Seron, V., « Financement du terrorisme », *Revue de droit pénal et de criminologie*, 2003, p. 840-874 ; Banifatemi, Y., « La lutte contre le financement du terrorisme international », *Annuaire français de droit international*, vol. 48, 2002, p. 103-128

49 p. 4 du doc. du Conseil du 17 juillet 2008, n° 11778/1/08.

50 p. 5 du doc. du Conseil de l'UE du 23 février 2010, n° 5842/2/10.

51 Voir à ce propos la p. 5 du rapport final de la Commission, du 20 juin 2014 (COM(2014) 365).

52 p. 10 de la communication du 28 avril 2015 (COM(2015) 185).

53 Doc. du doc. du Conseil du 10 juin 2015, n° 9798/15.

54 Communication du 2 février 2016 (COM (2016)50).

55 Doc. du Conseil du 12 février 2016, n° 6068/16.

56 Proposition de la Commission du 5 juillet 2016 (COM(2016)450).

57 Décision-cadre 2001/500/JAI du 26 juin 2001 (*J.O.U.E.* L 182 du 5.7.2001, p. 1).

58 Directive 2014/42/UE du 3 avril 2014 (*J.O.U.E.* L 127 du 29.4.2014, p. 39) ; règlement (UE) 2015/847 du 20 mai 2015 (*J.O.U.E.* L 141 du 5.6.2015, p. 1).

59 Resp. proposition de directive visant à harmoniser la définition des infractions et sanctions pénales (COM(2016)826) ; proposition de règlement présenté par la Commission visant à découvrir les mouvements illicites d'argent liquide (COM(2016)825) ; proposition de règlement présenté par la Commission relatif à la reconnaissance mutuelle des décisions de gel et de confiscation d'avoirs d'origine criminelle (COM(2016) 819).

60 Resp. proposition de règlement concernant l'importation de biens culturels (COM(2017)375 ; directive (UE) 2017/541 du 15 mars 2017 (*J.O.U.E.* L 88 du 31.3.2017, p. 6).

61 Rapport du 6 juin 2017(COM(2017)340).

OUVRAGES RÉCENTS

LE RENSEIGNEMENT

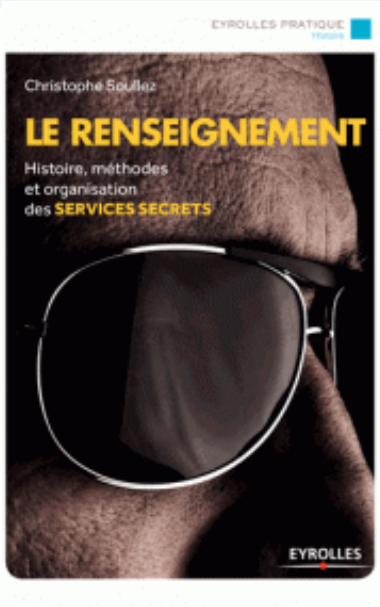
HISTOIRE, MÉTHODES ET ORGANISATION DES SERVICES SECRETS

AUTEUR : CHRISTOPHE SOULLEZ

EDITEUR : EYROLLES

Résumé

Le renseignement vise à recueillir, exploiter et diffuser des informations afin d'éclairer les choix stratégiques d'un pays et de ses dirigeants mais aussi de préserver ses capacités militaires et civiles et de prévenir les menaces. Il fait aujourd'hui l'objet de mises en cause de plus en plus fréquentes, en particulier dans le cadre de la lutte contre le terrorisme. Pour cerner une réalité obscure, mal connue et mal comprise, cet ouvrage conçu par un spécialiste présente l'histoire, les méthodes et les acteurs du renseignement, en France, des origines à nos jours.



© 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

LES OBJETS CONNECTÉS, OPPORTUNITÉS ET DÉFIS POUR LA SÉCURITÉ ET LE DROIT

MYRIAM QUÉMÉNER,

MAGISTRAT, DOCTEUR EN DROIT

ADEL JOMNI

ENSEIGNANT-CHERCHEUR À L'UNIVERSITÉ DE MONTPELLIER, EXPERT AUPRÈS DU CONSEIL DE L'EUROPE

Les objets connectés sont devenus omniprésents dans notre vie (une voiture, une montre, un compteur d'électricité, une serrure, un pacemaker, etc.). Ils occupent désormais une place centrale en tant qu'outils au service des utilisateurs, bouleversant ainsi le fonctionnement de nos sociétés.

Selon les chiffres de Gartner[1] 8,4 milliards d'objets connectés sont dénombrés aujourd'hui dans le monde soit une croissance de 31% par rapport à 2016. Toutes les études au sujet des objets connectés confirment que le nombre d'objets connectés progresse inexorablement. D'ici 2020, il devrait y en avoir environ 20 milliards[2].

Dans un contexte de digitalisation croissante, les entreprises investissent des milliards de dollars dans le développement de nouvelles applications et services associés aux objets connectés. Ces nouvelles applications orientées vers les utilisateurs représentent une énorme opportunité commerciale et un retour sur investissement significatif pour les entreprises. Le marché des objets et des services liés générera alors près de 2 000 milliards de dollars de chiffre d'affaires en 2017 et près de 3 000 milliards en 2020 selon Gartner.

Il n'existe pas de définition officielle des objets connectés. Un objet connecté correspond à tout dispositif physique doté d'une intelligence et d'une capacité de captation et de transfert de données sur un réseau sans la nécessité d'une intervention humaine. Il lui est attribué un identifiant unique.

Les objets connectés interagissent entre eux et/ou avec des individus via des réseaux de communication et sont capables de collecter des données relatives à leur état et à celui de leur environnement.

Pour échanger, les objets connectés exploitent plusieurs technologies de communication notamment le Wifi, 3G/4G/ Bluetooth, etc. Ces moyens classiques de connexion, déjà utilisés pour se connecter au réseau Internet ou pour échanger des fichiers entre appareils, ont fait leur preuve avec l'Internet et la téléphonie mobile. Ils sont aujourd'hui proches de la saturation en raison d'importantes sollicitations opérées par les smartphones et les tablettes. Il semble donc difficile de les surcharger avec les milliards de données échangées par les objets connectés. En outre, ils doivent intégrer les exigences des objets connectés comme la rapidité de transfert des données captées, la consommation réduite d'énergie, la distance à couvrir et la sécurité des échanges.

Ainsi, aux réseaux traditionnels sans fil (Bluetooth, Wifi) et réseaux cellulaires (3G, 4G et bientôt la 5G), de nouvelles techniques de communication dédiées aux objets connectées sont apparues. Il s'agit par exemple :

- des technologies NFC (Near Field Communication) : c'est un standard de communication radiofréquence sans contact à très courte distance (paiement sans contact, badges d'accès à des locaux, abonnements transports, ..etc),
- des protocoles de communication Zigbee et Z-Wave : ce sont des technologies de communication radio développées spécifiquement pour les applications de domotique (éclairage

connecté, volets roulants connectés, etc.). D'une portée moyenne de 10 à 30 mètres, ils utilisent une faible bande passante et ils sont peu consommateurs d'énergies,

– des protocoles Sigfox (même nom que l'entreprise qui le propose) et LoRa[3]. Ce sont des réseaux de communication radio sans fil qui reposent sur la technologie LPWAN (Low Power Wide Area) facilitant les communications longue portée (jusqu'à 50 km) à bas débits et à basse fréquence. Ces protocoles conviennent à des dispositifs à basse consommation, procurant ainsi une grande autonomie. Ils sont souvent utilisés pour des projets de villes intelligentes.

La diversité des technologies de radiocommunication employées avec les objets connectés est à l'image de la diversité des usages (domotique, téléphonie, e-santé, ..), du public visé (personnes, collectivités, industriels, ..) et de la réglementation (bandes de fréquences libres ou sous licence). Ainsi, de multiples protocoles de communication sans fil entre objets continuent, à être développés par les industriels et les fabricants d'objets connectés. Certains industriels ont privilégié l'installation de réseaux de communication propriétaires (ou privés). Le développement de ce type de réseau n'est rentable que s'il est déployé à grande échelle comme pour relier les compteurs d'eau, les compteurs électricité ou les capteurs des voitures appartenant à un constructeur d'automobiles.

Comme le montre le graphique[4] ci-contre, le choix de la technologie de communication entre les objets connectés se fera selon essentiellement trois critères : la portée, la consommation d'énergie (autonomie) et le débit.

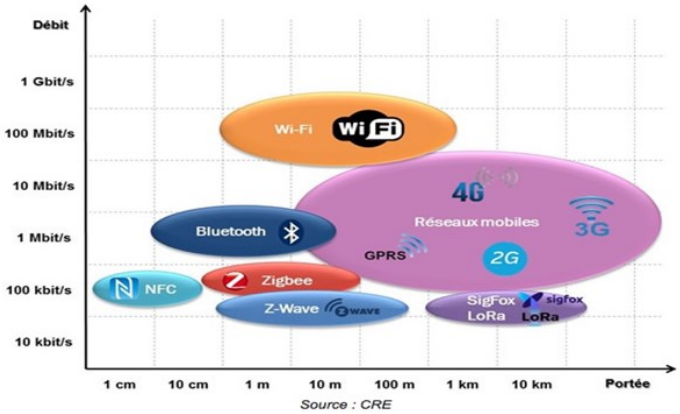
La croissance du marché et des services autour des objets connectés exigera certainement, à moyen terme, une obligation de standardisation à l'instar de ce qui s'est passé dans le monde de la vidéo, des périphériques réseaux ou de stockage. L'interopérabilité est la condition sine qua non pour le développement de l'industrie et des services autour des objets connectés. Le dernier rapport[5] (The Industrial Internet of Things : Connectivity Framework) publié par l'Industrial Internet Consortium constitue une avancée vers la recherche de passerelles standardisées entre les différentes normes proposées.

Par définition, l'Internet des objets (IoT) fait référence à une interconnexion des objets connectés avec le réseau Internet. L'IoT est issu de la convergence des technologies sans fil et d'Internet assurant ainsi l'extension d'Internet dans le domaine physique, grâce au déploiement généralisé des objets connectés. La mise en réseau des différents objets en utilisant la communication machine-à-machine (M2M[6], Machine-to-Machine) et leur connexion au réseau Internet constituent le coeur du concept IoT. Internet n'est plus seulement un réseau de réseaux d'ordinateurs. Il connecte, désormais, différents dispositifs capables d'envoyer et de recevoir des données sur l'état des appareils connectés au réseau. En connectant des objets à internet, l'IoT donne accès à un grand nombre de données et d'informations qui n'étaient pas disponibles auparavant.

L'IoT est considéré aujourd'hui comme l'évolution technologique la plus importante du XXIème siècle. Certains spécialistes[7] le considèrent comme la troisième révolution informatique et son ampleur dépassera celles des deux précédentes. D'autres estiment que l'extension des capacités des objets intelligents connectés et les données qu'ils génèrent conduisent à une nouvelle ère[8]. L'IoT pourrait peser plus de 10 % du PIB mondial en 2025.

I. Objets connectés : quelles opportunités ?

L'adoption de l'Internet des objets (IoT) s'accélère et touche de plus en plus de secteurs d'activité. Les concepts comme smarthome (maison intelligente), smart cities (ville connectée) et santé connectée se développent rapidement et ouvrent la voie à de nouvelles applications permettant d'améliorer et de faciliter la vie des êtres humains.



Source : CRE

Nous proposons ci-dessous trois exemples de secteurs qui bénéficient des opportunités offertes par les objets connectés.

A. Objets connectés et santé

Les objets connectés dans le domaine du bien être et de la santé ont récemment connu une progression spectaculaire. De simples gadgets comme les trackers, les wearables médicaux, les objets connectés se sont transformés progressivement en dispositifs permettant la prévention des maladies et une meilleure prise en charge des personnes souffrant de maladies chroniques.

Certains objets connectés « médicaux » sont d'ailleurs déjà disponibles sur prescription médicale comme le suivi des diabétiques (contrôle du taux de glycémie à partir d'un bracelet) et la surveillance de la tension artérielle. La caractéristique principale de ces objets est l'automesure. A partir de son smartphone, le patient s'appuie sur une application dédiée pour avoir des graphiques permettant de visualiser et d'interpréter en un coup d'oeil l'évolution de sa tension artérielle au fil du temps. Les données affichées peuvent être une source de motivation afin de poursuivre le traitement préconisé. Partagées avec le médecin, ces données contribuent à un meilleur diagnostic de la maladie, améliorent le suivi des patients et facilitent l'adaptation des traitements proposés.

Les dispositifs de détection de chute peuvent également jouer, dans certains cas, un rôle important dans la surveillance médicale continue des patients âgés. L'avantage principal de ces dispositifs est de réduire le temps pour la prise en charge d'un patient à la suite d'une chute ou d'une dégradation brutale de son état de santé. L'objet connecté de surveillance permet d'avertir plusieurs structures (hôpital, secours, famille, voisins, ..) susceptibles d'apporter un secours.

Ces objets connectés de santé sont également une mine d'or pour les chercheurs. En collectant les données issues des capteurs et en effectuant des agrégations et des analyses de ces grands volumes de données (technologies Big data), les scientifiques seront capables de mieux comprendre les facteurs aggravants une maladie ou facilitant son apparition (environnement, habitudes de vie, etc.).

Grâce au progrès de l'intelligence artificielle, les technologies d'analyse des données sont devenues un appui considérable pour les médecins. Le programme Watson d'IBM est capable d'analyser 20 millions de pages en quelques secondes. Il explore ainsi plusieurs corpus de publications scientifiques ou l'historique des rapports médicaux de patients.

Le programme Watson vise à aider les médecins à trouver le traitement le plus approprié pour soigner un cancer chez leurs patients. Chaque proposition de traitement s'accompagne d'un degré de pertinence, déterminé par Watson. Les médecins disposent d'un outil pour réaliser le diagnostic le plus précis possible, en un minimum de temps. C'est une forme d'expertise, une seconde opinion que les médecins peuvent utiliser en complément de leur savoir personnel[9].

Enfin, d'un point de vue politique et économique, le sujet des objets connectés de santé devrait faire l'objet d'une réelle analyse de la part des gouvernements afin d'étudier dans quelle mesure il contribue à améliorer la qualité des soins et le suivi post opératoire tout en réduisant la présence du patient à l'hôpital.

B. Objets connectés et transport

Les équipementiers, les constructeurs automobiles et les principaux acteurs de l'Internet se mobilisent pour la voiture connectée permettant, grâce à des applications, d'améliorer le confort et de faciliter la conduite (l'assistant de parking), le suivi de la consommation et de l'usure des pièces, le dépannage, la gestion du trafic et la simplification des déplacements.

Avec la connectivité des moyens de transport, l'autonomie du transport (sans chauffeur) et les services disruptifs autour des innovations apportées par les objets connectés comme le transport à la demande et le transport partagé, l'IoT donne la possibilité de réinventer la mobilité urbaine et périurbaine en changeant la physionomie des territoires avec un aménagement urbain intelligent. En facilitant la mobilité des usagers (réduction des temps d'attente, guidage optimisé en temps réel), il résultera nécessairement un effet positif sur l'environnement et une opportunité pour accélérer la transition énergétique.

Le transport des marchandises est également impacté par l'arrivée massive des objets connectés. L'usage des drones promet de révolutionner l'acheminement des colis et de résoudre les difficultés de l'acheminement dans des zones difficiles d'accès. Amazon et DHL ont commencé l'expérimentation de ce moyen de transport de marchandises. Néanmoins, l'utilisation de drones est aujourd'hui limitée par un cadre

réglementaire contraignant, notamment pour des usages dans une zone urbaine grand public.

Enfin, les objets connectés comme les drones peuvent offrir une opportunité intéressante dans le domaine de la maintenance des réseaux (physiques) de transport et la sécurisation des trajets. A titre d'exemple, la SNCF[10] a installé plusieurs drones pour améliorer l'inspection de 30 000 km de voies ferrées, la surveillance des ouvrages d'art et la prévention des actes de malveillance. Ces drones peuvent également identifier les besoins d'entretien et détecter les possibles vols de métaux ou les incidents techniques. Le survol par les drones permet, d'une part, d'éviter les interventions humaines coûteuses et chronophages qui auraient été nécessaires pour faire les mêmes observations et, d'autre part, d'avertir en temps réel, grâce à l'interconnexion de ces objets, des incidents survenus afin de s'adapter à la situation (réduction de la vitesse, arrêt d'urgence, etc).

Ces évolutions nécessitent des investissements dans des infrastructures couvertes par des réseaux de communication de bonne qualité autorisant un débit et une vitesse permettant l'échange, à distance, de grandes quantités de données entre les dispositifs numériques intelligents comme les objets connectés.

C. Les objets connectés : une opportunité pour l'investigation et les enquêtes criminelles

Les objets connectés présentent, également, de nombreuses opportunités pour les activités des forces de l'ordre, que ce soit pour la police judiciaire, la sécurité publique ou le renseignement. S'agissant de l'exploitation des objets connectés en matière de police judiciaire, on pense en premier lieu aux capteurs automatisés (cf. lecteurs automatisés de plaques d'immatriculation ou LAPI) ou aux dispositifs mis en oeuvre dans le cadre de techniques spéciales de surveillance (balises, dispositifs de sonorisation, drones, etc.).

On songe moins naturellement à l'exploitation des objets connectés utilisés par des victimes ou par des criminels et susceptibles à ce titre de contenir des informations utiles à la manifestation de la vérité dans le cadre d'enquêtes pénales. Ainsi, le Washington Post rapporte[11] que suite à un meurtre à Bentonville dans l'Arkansas, la justice a demandé à Amazon de livrer les enregistrements stockés sur leur serveur, car un objet connecté (un assistant virtuel « echo »), se trouvait sur les lieux du crime. Cette enceinte est dotée d'un micro qui détecte la voix et peut exécuter un ordre (« Alexa, appelle-moi un Uber! ») ou répondre à une question (« Alexa, quel temps fait-il ? »).

Dans le domaine de la sécurité intérieure, les drones occupent une place de plus en plus importante dans la stratégie opérationnelle. Un rapport d'inspection les considère comme un complément plutôt qu'une alternative à l'hélicoptère. Si leur emploi est soumis à de fortes restrictions de nuit, en zone urbaine, par temps venteux ou à proximité des aéroports, il n'en demeure pas moins que les progrès technologiques rendent leur utilisation très attractive notamment grâce à leurs qualités d'observation et leur discrétion.

Si la saisie et l'exploitation forensique[12] des ordinateurs, des supports informatiques associés (disques durs externes, clés USB) et des téléphones mobiles sont désormais quasi systématiques dans les services d'enquêtes, celles des objets connectés, pourtant potentiellement utiles et juridiquement possibles, demeurent pour l'heure marginales et exploratoires. Ces objets représentent, grâce à leurs contenus et leurs omniprésences dans tous les compartiments de notre environnement, de formidables outils pour les forces de sécurité tant sur le plan de la conduite « forensique » d'une enquête que d'un usage opérationnel pour le maintien de l'ordre ou le renseignement.

Les officiers de police judiciaire sont autorisés à avoir accès aux données informatiques contenues dans ces objets lors d'une perquisition (articles 56 et 57 du CPP), y compris en accédant, depuis le lieu de perquisition ou depuis leur bureau, à un « cloud » ou à des applications distantes utilisées depuis des systèmes informatiques saisis lors de la perquisition.

Certains objets sont d'ores et déjà utilisés au sein du ministère de l'Intérieur qui se positionne comme l'un des acteurs les plus innovants en matière de technologies numériques. D'autres sont testés à titre expérimental. Les opérations techniques liées à l'exploitation des objets connectés en matière pénale paraissent couvertes, à l'échelle nationale, par les diverses dispositions du Code de procédure pénale (CPP) relatives au recueil de la preuve numérique.

Il est désormais indispensable de former les primo-intervenants sur les scènes de crime, les enquêteurs menant des perquisitions et les magistrats sur les défis liés à l'Internet des objets.

II. Les objets connectés et les défis pour la sécurité et le droit

L'IoT présente des avantages indéniables pour les citoyens, les entreprises et les industries. Malheureusement, l'engouement de plus en plus important autour de ces objets et l'inondation du marché par des objets fabriqués, parfois contrefaits, sans le moindre respect des normes de sécurité et des règles minimales de protection de la vie privée, soulèvent plusieurs questions et représentent de nouveaux défis en termes de sécurité, de liberté individuelle et de droit.

A. Objets connectés et les défis de sécurité

La sécurité est le principal défi à relever par l'IoT. Ce sujet, déjà évoqué lors de la démocratisation des usages de l'Internet, prend plus d'ampleur avec les objets connectés étant donné qu'il s'agit souvent d'objets personnels.

i. La vulnérabilité : principal source d'insécurité des objets connectés

La forte concurrence qui caractérise aujourd'hui le marché des objets connectés en matière d'innovation, de facilité d'utilisation et de réduction des coûts, relègue au second plan la prise en compte de la sécurité. L'absence de sécurité dans le code associé aux applications embarquées par ces objets, le manque de chiffrement des identifiants et des données captées par les objets, l'utilisation de protocoles de communication non sécurisés, sont des exemples de vulnérabilités critiques qui caractérisent souvent les objets connectés.

- **Quelles conséquences ?**

Les objets connectés constituent à la fois des cibles et des vecteurs de cyber-risques. La vulnérabilité de ces objets constitue un eldorado pour les cybercriminels. Cette situation est très préoccupante pour les particuliers et pour les entreprises.

Concernant les particuliers, les vulnérabilités des objets connectés peuvent engendrer le vol des données personnelles, l'altération du fonctionnement de l'objet (voiture connectée, alarme, ..), le cambriolage des maisons (serrure connectée), l'atteinte à l'intégrité physique d'un patient (manipulation des objets de surveillance médicale ou d'administration de médicament). En effet, de nombreux cas de violation et de compromission de ces objets ont eu lieu ces dernières années, comme la prise de contrôle à distance d'une voiture connectée, la manipulation d'une alarme ou la surveillance à distance des personnes à l'intérieur de leur domicile. Dans le domaine de la santé, une étude[13] a montré qu'un stimulateur cardiaque peut enfermer plus de 8.000 vulnérabilités connues !

En ce qui concerne les entreprises, les dégâts liés à l'insécurité des objets connectés sont également très préjudiciables. La course à l'innovation et la commercialisation rapide de nouveaux objets laissent peu de temps pour les tests de vulnérabilités et les vérifications des programmes développés pour ces objets. Par conséquent, l'IoT élargit la surface pour des cyber-attaques devenues de plus en plus sophistiquées et lourdes de conséquences.

- **Une aubaine pour les attaques DDoS**

Les attaques de type DDoS (Distributed Denial of Service) consistent à submerger ou paralyser un système informatique afin de l'empêcher de recevoir de l'information et d'interagir avec un autre système. Ce sont des cyber-attaques qui ciblent la disponibilité des services (en ligne ou non) ou la paralysie d'une entreprise. Le mode opératoire repose sur l'exploitation des vulnérabilités des ordinateurs connectés à l'Internet afin de constituer une « armée » de machines (ordinateurs appelés zombies) capables de paralyser le système informatique d'une entreprise ou d'un État.

L'attaque dirigée contre le prestataire DNS Dyn, le 21 octobre 2016, a permis de constater l'ampleur des dégâts occasionnés par ce type de menaces. L'attaque contre Dyn a perturbé l'accès à Internet dans une grande partie des États Unis. Plusieurs sites web dont Amazon, Netflix, Twitter, Reddit, Imgur, Twitter, GitHub, Soundcloud, Spotify, PayPal ont été inaccessibles pendant plusieurs heures. Ces entreprises ont un prestataire commun, Dyn, qui assure des services de DNS[14]. L'hébergeur français OVH a été également victime de cette cyber-attaque.

La nouveauté constatée dans cette dernière cyber-attaque contre Dyn est la présence de plusieurs milliers d'objets connectés (caméras de surveillance essentiellement) dans le botnet[15] baptisé Mirai qui a orchestré cette cyber-attaque. Ce botnet composé de plusieurs centaines de milliers d'objets connectés a généré des charges allant de 623 Gbit/s[16] à 1,5 Tb/s.

La prolifération des objets connectés, souvent vulnérables, va renforcer les capacités de ces « armées » de dispositifs électroniques.

- **Vers la multiplication du Ransomware**

Le Ransomware (rançongiciels ou chantage) est une forme d'extorsion utilisée par des cybercriminels. Il s'agit de bloquer totalement ou

partiellement le système informatique d'une cible (chiffrement du contenu d'un disque par exemple). Une procédure est proposée à la victime (reposant sur le paiement d'une rançon) afin de remettre le système informatique dans son état initial.

Ce mode opératoire est facilité par la présence de milliards d'objets connectés dont la majeure partie ne dispose pas d'un protocole facilitant la mise à jour du code embarqué en cas de détection de vulnérabilité. Contrairement aux ordinateurs (tablettes, Smartphones), qui s'appuient sur des équipes d'ingénieurs assurant le suivi, le test et la distribution rapide de correctifs sur les bugs et les vulnérabilités constatées, rares sont les objets connectés (caméras, système d'éclairage, montres, ..) disposant de ce type de plateforme de suivi, de facilité de mise à jour et de réponse en cas de piratage.

Cette fragilité technique et organisationnelle des objets connectés sera de plus en plus exploitée par les cybercriminels pour bloquer ces objets ou voler les données captées par ces derniers. Le fabricant de téléviseurs LG a subi ce type d'attaque en décembre 2016. Certains propriétaires de cette marque de smart TV ont vu leur téléviseur bloqué avec une demande de rançon de 500 $. On s'achemine dangereusement vers une nouvelle variante des Ransomwares : le ransomware of things (RoT).

ii. Quelles solutions de sécurité pour les objets connectés ?

Malheureusement, selon le premier rapport[17] de la délégation ministérielle aux industries de sécurité et à la lutte contre les cyber menaces (DMISC), la sécurité des objets connectés ne constitue pas une préoccupation réelle des industriels et ce sont les utilisateurs qui risquent de payer ce manque de vigilance.

Parmi les solutions de sécurisation avancées, on peut citer l'action des plateformes de « bug bounty »[18] qui permet de contrôler avant commercialisation si les objets connectés contiennent des failles de sécurité. Le recours à ces plateformes largement développées aux États Unis par des grandes entreprises comme Microsoft pourraient l'être également en France et en Europe. Elles pourraient ainsi contribuer à sécuriser le marché des objets connectés à la condition d'être labellisées par l'ANSSI par exemple.

D'autres méthodes sont préconisées comme celles proposées par OWASP Internet of Things project[19] pour faciliter la prise en compte des problèmes de sécurité des objets connectés.

Il est également urgent de mettre en place un référentiel de sécurité auxquels pourront se conformer les industriels et les fabricants d'objets connectés afin d'instaurer la confiance. Cette confiance ne peut être obtenue que si les industriels et les fabricants d'objets connectés intègrent le concept de « security by design » (sécurité dès la conception) dans leur processus de développement. Ce concept impose la réflexion sur la sécurité dès la conception des produits. C'est une nouvelle culture à intégrer dans la formation des développeurs et dans les ateliers de conception des objets.

B. Objets connectés et le droit

i. Protection des données

Sur le plan juridique, la loi « informatique et libertés » du 6 janvier 1978 pose un cadre qui est toujours d'actualité en ce qui concerne la collecte et l'utilisation de données à caractère personnel. Cette protection offerte à chaque individu trouve toutefois sa limite dès que celui-ci a manifesté son consentement même implicitement (exemple : l'inscription aux réseaux sociaux comme Facebook, ...).

La question du consentement est un enjeu fort. Celle-ci va être amenée à évoluer prochainement dans le cadre du règlement européen RGPD qui vise à renforcer le consentement avec notamment la possibilité pour les utilisateurs finaux de le retirer à tout moment.

Le responsable du traitement devra néanmoins respecter de son côté les principes imposés par la loi (proportionnalité, pertinence, durée et finalité) ainsi que l'obligation de déclaration à la CNIL ou la demande d'autorisation pour les traitements les plus sensibles.

En outre, les opérateurs économiques vont se voir imposer, par le RGPD, une obligation de protéger la vie privée dès la conception (Privacy by Design). Il s'agit ainsi d'intégrer la protection des données dès la conception des systèmes et des programmes informatiques. Ce règlement implique également que les développeurs s'imposent de ne pas recueillir de données sans lien avec le service rendu.

Il s'avère donc nécessaire d'adapter la règlementation au moins au niveau européen, de sensibiliser les consommateurs aux usages et aux risques liés aux objets connectés, de renforcer les règles en matière de consentement des utilisateurs et de valoriser les bonnes pratiques des entreprises. Il faudrait également mener une réflexion sur la mise en place d'une notation « Empreinte numérique » (type

Fitch, S&P, ...) par la CNIL, permettant d'évaluer les objets connectés de manière équitable et transparente. Il est aussi important de renforcer les moyens des instances de contrôle (CNIL, ARCEP, ...).

ii. Responsabilité juridique des différents acteurs du traitement des données

Au-delà des données personnelles échangées via les objets connectés se pose la question de leur traitement via des mécanismes de plus en plus complexes, les algorithmes. Dans nos actes de consommation réalisés via Internet, qu'il s'agisse d'acheter des paires de chaussures ou de regarder un film en VOD depuis une « Smart TV » ou via une « Box Internet », dans les relations avec une banque en ligne, il y a une forte probabilité qu'un algorithme intervienne à un moment ou à un autre de l'opération. Cet « ensemble de règles opératoires dont l'application permet de résoudre un problème énoncé au moyen d'un nombre fini d'opérations[20] » est aujourd'hui devenu un incontournable de notre vie quotidienne.

Les techniques algorithmiques mises en oeuvre aujourd'hui par les grands opérateurs (GAFA[21]) de l'Internet démontrent des capacités insoupçonnées jusqu'alors : détection des cancers de la peau par exemple mais aussi des capacités de manipulation des utilisateurs à leur insu comme l'a démontré l'expérimentation de Facebook sur 700 000 utilisateurs en 2012. La confiance que l'utilisateur peut accorder aux algorithmes doit donc reposer sur la transparence de ceux-ci.

Sur le plan juridique, la question de la responsabilité se pose : les algorithmes dits « intelligents » sont souvent centralisés, le traitement ne se fait donc pas sur l'objet connecté directement mais sur un système central déporté, ce qui complexifie la problématique de la responsabilité légale si ce système n'est pas résidant en France, ni même dans l'UE.

Comme le souligne Alain Bensoussan, avocat spécialisé dans le droit des robots : « Qui est responsable de l'erreur inhumaine des « chatbots » (ces agents conversationnels capables de prendre des décisions, algorithme concentré d'intelligence artificielle) : le concepteur, l'utilisateur, le propriétaire ou le « chatbot » ? »

Dans le domaine du traitement des données personnelles, il apparaît donc nécessaire de fixer à priori les responsabilités juridiques des différents acteurs élaborant et mettant en oeuvre des algorithmes de type « intelligence artificielle », intégrés dans les objets connectés.

B. L'objet connecté, système de traitement automatisé de données (STAD)

Les objets connectés peuvent être considérés comme des systèmes de traitement automatisés de données dont les atteintes sont sanctionnées par la loi « Godfrain »[22].

Si les évolutions technologiques ont permis de démocratiser la possession d'objets connectés, elles ont aussi conduit à la commission de nouveaux types d'infractions. Il peut s'agir de piratages sanctionnés en tant qu'atteintes aux systèmes de traitement automatisé de données, en cas d'accès ou de maintien frauduleux.

L'article 323-2 du Code pénal réprime « le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données ». Cette disposition pourra s'appliquer dans le cadre d'insertion de virus, chevaux de Troie et autres bombes logiques au sein du système piloté par l'IoT. Ce texte permet aussi de sanctionner l'introduction sans titre ni autorisation dans un service quelconque du réseau pour perturber par exemple les dispositifs de sécurité ou fausser le fonctionnement du système.

Les cyber-attaques ciblant les objets connectés peuvent aussi être réprimés sur le fondement de l'article 323-3 du Code pénal qui sanctionne l'introduction frauduleuse de données dans un système de traitement automatisé, de l'extraction, de la détention, de la reproduction, de la transmission, de la suppression ou de la modification frauduleuse des données qu'il contient.

Il paraît évident que le cadre législatif actuel devrait progressivement s'adapter au déploiement massif des objets connectés dans notre société. L'individu « consommateur » a pour sa part besoin d'être tenu informé de façon transparente, pertinente et équitable de la transformation massive de biens de consommation qui deviennent de véritables « concierges numériques » connaissant de plus en plus d'informations sur chacun grâce aux données personnelles qui sont captées, traitées et échangées dans l'Internet des objets.

Notes :

1 Gartner, « Internet of Things. Endpoints and Associated Services, Worldwide », étude prévisionnelle de décembre 2015.

2 L'IDATE anticipe 80 milliards d'appareils connectés d'ici 2020, CISCO en envisage 50 milliards.

3 Proposé par Bouygues Telecom.

4 Source : CRE (Commission de régulation de l'énergie).

5 The Industrial Internet of Things : Connectivity Framework. https://www.iiconsortium.org/pdf/IIC_PUB_G5_V1.0_PB_20170228.pdf

6 Communication de machine à machine : permettre des communications entre objets ou dispositifs électroniques sans intervention humaine.

7 Michael E. Porter, Professor at Harvard Business School. Spécialiste de la concurrence et des stratégies de l'entreprise moderne.

8 Haas G., Crenn J.P., Quéméner M., L'internet des objets : la 3ème révolution informatique, Edition Kawa, 2017.

9 citation de Jérôme de Nomazy de l'équipe «Cognitive Solutions» d'IBM.

10 https://www.sncf-reseau.fr/fr/a-propos/notre-strategie/drones-et-entreprises

11 https://www.washingtonpost.com/news/the-switch/wp/2016/12/28/can-alexa-help-solve-a-murder-police-think-so-but-amazon-wont-give-up-her-data/?utm_term=.9ea29f421d66

12 La science forensique, ou la forensique, applique une démarche scientifique et des méthodes techniques dans l'étude des traces qui prennent leur origine dans une activité criminelle, ou litigieuse en matière civile, réglementaire ou administrative (in criminologie.com).

13 http://blog.whitescope.io/2017/05/understanding-pacemaker-systems.html

14 DNS (Domain Name Server) : système de noms de domaine ou système d'adressage de nom de domaine. Il assure la correspondance entre les noms de domaine (www.nomdedomaine.fr) et les adresses IP.

15 Botnet : réseaux d'ordinateurs (de bots ou zombies) jouant le rôle d'un relais pour des opérations de spamming, de phishing ou pour des attaques par Déni de service (ou DDos- Distributed Denial of Service). La constitution d'un Botnet est précédée par l'installation, sur les ordinateurs ou les objets connectés de plusieurs utilisateurs, d'un programme malveillant permettant la prise de contrôle à distance de ces dispositifs.

16 Source AKAMAI : https://www.akamai.com/fr/fr/multimedia/documents/state-of-the-internet/akamai-mirai-botnet-threat-advisory.pdf

17 http://www.interieur.gouv.fr/content/download/101311/797853/file/Etat-de-la-menace-Janvier-2017.pdf

18 Un bug bounty est un programme proposé par de nombreux sites web et développeurs de logiciel qui permet à des personnes de recevoir reconnaissance et compensation après avoir rapporté des bugs, surtout ceux concernant des failles et des vulnérabilités.

19 https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

20 Définition du Larousse : http://www.larousse.fr/dictionnaires/francais/algorithme/2238

21 Google, Amazon, Facebook, Apple.

22 https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000875419

OUVRAGES RÉCENTS

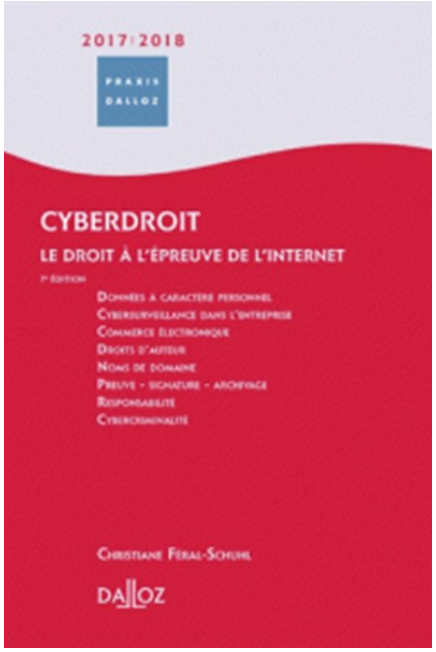
CYBERDROIT - LE DROIT À L'ÉPREUVE DE L'INTERNET

AUTEUR : CHRISTIANE FÉRAL-SCHUHL

EDITEUR : DALLOZ

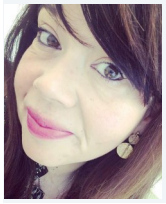
Résumé

Les hautes juridictions françaises et européennes continuent à construire la jurisprudence en droit des technologies de l'information et de la communication. Dans l'ensemble des disciplines juridiques des solutions adaptées sont recherchées aux questions posées. Comment la collecte et le transfert de données à caractère personnel peuvent-ils être au service de chacun sans porter atteinte aux libertés individuelles ?Sur la cybersurveillance, où placer la frontière entre pouvoir de contrôle de l'employeur, devoir de loyauté de l'employé et protection de ses libertés fondamentales ?
Comment encourager le commerce en ligne tout en protégeant le cyberconsommateur ? Le dispositif protecteur à l'égard des cybercommerçants a été renforcé, particulièrement des opérateurs de communications électroniques.



Sur la protection du droit d'auteur, le dispositif a évolué. Le système de nommage en se précise. Comment accorder le régime de responsabilité des acteurs de l'internet avec les nouveaux métiers du web ? La jurisprudence n'en finit pas d'osciller entre le régime de responsabilité éditoriale et celui de la responsabilité de l'hébergeur. Contre l'inflation des actes de cybercriminalité, de nouvelles mesures nationales, européennes et internationales ont modernisé les méthodes d'investigation des autorités d'enquête et renforcent la coopération entre autorités judiciaires, particulièrement pour la protection des mineurs.

LA LOI N° 2017-1510 DU 30 OCTOBRE 2017 RENFORÇANT LA SÉCURITÉ INTÉRIEURE ET LA LUTTE CONTRE LE TERRORISME EST-ELLE CONFORME À LA CONSTITUTION ?



DOROTHÉE GOETZ

DOCTEURE EN DROIT ET EN SCIENCE CRIMINELLE, ASSISTANTE SPÉCIALISÉE AU PARQUET DU TRIBUNAL DE GRANDE INSTANCE DE STRASBOURG

Depuis le 14 novembre 2015, six lois sont venues proroger l'état d'urgence. La dernière en date, la loi du 11 juillet 2017, a prorogé cet état d'exception jusqu'au 1er novembre 2017. Ces prorogations successives étaient justifiées par la persistance du péril imminent résultant d'une atteinte grave à l'ordre public. Or, l'état d'urgence est un régime par essence temporaire et limité dans le temps qui ne peut être activé que dans des circonstances exceptionnelles. C'est ainsi qu'inévitablement, les prorogations successives de cette législation d'exception associées au caractère devenu durable de la menace terroriste ont rendu nécessaire de doter l'État d'instruments nouveaux et permanents de prévention et de lutte contre le terrorisme. Toutefois, ce besoin n'est pas nouveau. En effet, depuis 2012, six lois - dont la récente loi du 3 juin 2016 - ont déjà eu pour objectif de prévenir, d'identifier et de réprimer la menace terroriste[1].Dans cette perspective, le 22 juin 2017 le Conseil des ministres a entériné deux textes au destin lié : le projet de loi relatif à l'état d'urgence et le projet de loi renforçant la sécurité intérieure et la lutte contre le terrorisme. Alors que le projet de loi relatif à l'état d'urgence a prorogé pour la sixième et dernière fois l'état d'urgence jusqu'au 1er novembre 2017, le projet de loi renforçant la sécurité intérieure et la lutte contre le terrorisme avait pour but de prendre le relai pour pouvoir s'appliquer dès la fin de l'état d'urgence. Ce texte vise en effet à doter l'État « de nouveaux moyens juridiques de droit commun permettant de mieux prévenir la menace terroriste hors période d'état d'urgence ». Après réunion d'une commission mixte paritaire, la loi est entrée en vigueur le 1er novembre 2017.

Le texte comprend 21 articles répartis en 4 chapitres. Le chapitre Ier, intitulé « dispositions renforçant la prévention d'actes de terrorisme », insère dans le droit commun de nouveaux outils présentés comme adaptés et nécessaires à la lutte antiterroriste contemporaine. Le chapitre II est consacré aux techniques de renseignement. Le chapitre III s'intéresse aux contrôles dans les zones frontalières. Enfin, le chapitre IV est relatif aux dispositions relatives aux Outre -mer.

On remarquera que l'article 5 impose aux autorités administratives d'informer « sans délai » le Parlement de la mise en oeuvre des mesures issues de l'état d'urgence[2] et assigne à celles-ci un terme fixé au 31 décembre 2020. L'article 6 définit, pour sa part, les conditions dans lesquelles les structures de lutte contre la radicalisation pourront bénéficier de subventions publiques, tandis que l'article 8 renforce la protection des repentis et de leur famille. L'article 11 permet la réalisation d'enquêtes administratives dans le cas où le comportement d'un agent exerçant dans les domaines de la sécurité ou de la défense et titulaire d'une autorisation, d'un agrément ou d'une habilitation fait naître des doutes sur la compatibilité de

son évolution avec les missions qui lui sont confiées[3]. L'article 16 ajoute à la liste des documents transmis à la délégation parlementaire au renseignement ceux qui concernent la surveillance des communications hertziennes. Enfin, l'article 17 étend l'application de l'article L. 851-3 du Code de sécurité intérieure (CSI) jusqu'en 2020, l'expérimentation des algorithmes de détection de la menace terroriste ayant pris du retard.

La lecture de ce nouveau texte de loi pose inévitablement la question de savoir comment le législateur a t-il procédé pour mettre un terme à l'état d'urgence ? Nous démontrerons que cette sortie de l'état d'urgence s'est en réalité opérée via une normalisation de cette législation d'exception (I), ce qui nous amènera à évoquer l'hypothèse d'une inconstitutionnalité de ce nouveau texte (II).

I. La normalisation de l'état d'urgence

Dans un contexte où la menace terroriste est toujours présente, sortir de l'état d'urgence ne peut pas signifier abandonner totalement les mesures issues de l'état d'urgence. La difficulté est donc bien réelle pour le législateur qui doit réussir à sortir de l'état d'urgence tout en adaptant certaines mesures propres à ce cadre aux exigences du droit commun.

Cela explique que les mesures implantées dans la légalité ordinaire mais empruntées à la légalité d'exception sont introduites, dans la loi, par la formule « aux seules fins de prévenir la commission d'actes de terrorisme ». L'article 3 dispose en effet que « *aux seules fins de prévenir la commission d'actes de terrorisme, toute personne à l'égard de laquelle il existe des raisons sérieuses de penser que son comportement constitue une menace d'une particulière gravité pour la sécurité et l'ordre publics et qui soit entre en relation de manière habituelle avec des personnes ou des organisations incitant, facilitant ou participant à des actes de terrorisme, soit soutient, diffuse, lorsque cette diffusion s'accompagne d'une manifestation d'adhésion à l'idéologie exprimée, ou adhère à des thèses incitant à la commission d'actes de terrorisme ou faisant l'apologie de tels actes peut se voir prescrire par le ministre de l'Intérieur les obligations prévues au présent chapitre* ». L'article 2 énonce que « *aux seules fins de prévenir la commission d'actes de terrorisme, le représentant de l'État dans le département ou, à Paris, le préfet de police peut prononcer la fermeture des lieux de culte dans lesquels les propos qui sont tenus, les idées ou théories qui sont diffusées ou les activités qui se déroulent provoquent à la violence, à la haine ou à la discrimination, provoquent à la commission d'actes de terrorisme ou font l'apologie de tels actes* ». Dans cette même veine, l'article 4 précise que « *sur saisine motivée du représentant de l'État dans le département ou, à Paris, du préfet de police, le juge des libertés et de la détention du tribunal de grande instance de Paris peut, par une ordonnance écrite et motivée et après avis du procureur de la République de Paris, autoriser la visite d'un lieu ainsi que la saisie des documents, objets ou données qui s'y trouvent, aux seules fins de prévenir la commission d'actes de terrorisme et lorsqu'il existe des raisons sérieuses de penser qu'un lieu est fréquenté par une personne dont le comportement constitue une menace d'une particulière gravité pour la sécurité et l'ordre publics et qui soit entre en relation de manière habituelle avec des personnes ou des organisations incitant, facilitant ou participant à des actes de terrorisme, soit soutient, diffuse, lorsque cette diffusion s'accompagne d'une manifestation d'adhésion à l'idéologie exprimée, ou adhère à des thèses incitant à la commission d'actes de terrorisme ou faisant l'apologie de tels actes* ». En outre, la transposition de ces mesures dans la légalité ordinaire s'accompagne de conditions nouvelles, inconnues de l'état d'urgence.

Enfin, le législateur a choisi de normaliser l'état d'urgence en adoucissant les termes employés. Ainsi, les zones de sécurité ou de protection deviennent des « périmètres de protection », les assignations à résidence des « mesures individuelles de contrôle administratif et de surveillance » et les perquisitions administratives se transforment en « visites ».

Ce courant de normalisation est particulièrement perceptible au travers de l'étude de quatre mesures prévues par la loi nouvelle, à savoir la création des périmètres de protection (A), la fermeture des lieux de culte (B), les mesures individuelles de surveillance (C) et les visites et saisies (D).

A. La création de périmètres de protection

L'article 1 de la loi instaure des

périmètres de protection en prévoyant qu'« *afin d'assurer la sécurité d'un lieu ou d'un évènement soumis à un risque d'actes de terrorisme à raison de sa nature ou de l'ampleur de sa fréquentation, le représentant de l'État dans le département ou, à Paris, le préfet de police peut instituer par arrêté motivé un périmètre de protection au sein duquel l'accès et la circulation des personnes sont réglementés* ». Cette nouvelle disposition vise à assurer la sécurité d'événements ou de lieux particulièrement exposés à un risque d'attentats, tel des manifestations culturelles ou sportives. En pareille circonstance, le texte permet au préfet d'autoriser des inspections visuelles des bagages et des palpations de sécurité y compris par des agents de sécurité privés, sous contrôle des policiers et gendarmes. Ceux-ci pourront également visiter les véhicules avec le consentement du conducteur sans que ces mesures soient soumises à une réquisition judiciaire. Si la personne refuse de se soumettre à ces mesures pour accéder ou circuler à l'intérieur du périmètre de sécurité, l'accès lui sera interdit et elle devra, le cas échéant, être reconduite d'office à l'extérieur du périmètre. Contrairement à ce qui est prévu par la législation d'exception, la loi ordinaire n'octroie pas au préfet le pouvoir de décider de pratiquer des contrôles d'identité. Ceux-ci continueront donc de relever du pouvoir judiciaire.

B. La fermeture des lieux de culte

L'article 2 de la loi permet au préfet, pour prévenir la commission d'actes de terrorisme, de prononcer la fermeture des lieux de culte, « *dans lesquels les propos qui sont tenus, les idées ou théories qui sont diffusées ou les activités qui se déroulent, provoquent à la commission d'actes de terrorisme en France ou à l'étranger, incitent à la violence, ou font l'apologie de tels actes* ». Cette nouvelle disposition est importante puisqu'auparavant, hors état d'urgence, le pouvoir de fermeture d'un lieu de culte relevait du maire et ce n'était qu'en cas d'état d'urgence que ce pouvoir appartenait au préfet. Le texte encadre doublement l'exercice de ce pouvoir par l'instauration d'une procédure contradictoire préalable et par un délai d'exécution qui ne peut être inférieur à quarante-huit heures. L'intérêt de ce délai est de permettre l'introduction d'un recours en référé devant le juge administratif qui aura un effet automatiquement suspensif. Alors que le Conseil d'État recommandait de limiter la période de fermeture à une durée de quatre mois, la nouvelle loi prévoit que celle-ci peut atteindre une durée maximale de six mois.

C. Les mesures individuelles de surveillance

L'article 3 crée les articles L. 228-1 à L. 228-7 dans le CSI, qui autorisent le ministre de l'Intérieur à soumettre, par une décision écrite et motivée, toute personne à l'encontre de laquelle existent « *des raisons sérieuses de penser que son comportement constitue une menace d'une particulière gravité pour la sécurité et l'ordre publics et qui soit entre en relation de manière habituelle avec des personnes ou des organisations incitant, facilitant ou participant à des actes de terrorisme, soit soutient, diffuse, lorsque cette diffusion s'accompagne d'une manifestation d'adhésion à l'idéologie exprimée, ou adhère à des thèses incitant à la commission d'actes de terrorisme ou faisant l'apologie de tels actes* », à des « *mesures individuelles de contrôle administratif et de surveillance* ». Ces mesures individuelles de surveillance, qui succèdent, du point de vue terminologique, aux assignations à résidence, sont mises en oeuvre par le ministre de l'Intérieur, après en avoir informé le procureur de la République de Paris. Dans son avis du 15 juin 2017, le Conseil d'État préconisait de limiter toutes ces mesures individuelles de surveillance à une durée maximale de six mois[4]. Or la loi permet que certaines des obligations prévues dans le cadre de cette surveillance soient renouvelées tous les trois mois sur la base d'éléments nouveaux ou complémentaires. Si une information du procureur de la République est bien prévue par la loi pour la définition des périmètres de sécurité, cette information a pour but exclusif d'éviter que l'initiative préfectorale ou ministérielle n'obère d'éventuelles investigations en cours. En effet, le magistrat du parquet n'a aucun pouvoir de mettre fin à la mesure[5].

D. Les visites et saisies

L'article 4 autorise les visites et saisies dans les lieux fréquentés par des individus répondant

aux mêmes critères que ceux exigés pour la mise en oeuvre des mesures de surveillance individuelle. Laissées à l'initiative du préfet, ces visites et saisies doivent avoir été autorisées par l'autorité judiciaire, après information du procureur de la République de Paris. En ce sens, le texte prévoit que « *la visite et les saisies sont autorisées par une ordonnance motivée du juge des libertés et de la détention près le tribunal de grande instance de Paris qui est communiquée au procureur de la République de Paris* ». L'ordonnance d'autorisation du juge des libertés et de la détention (JLD) peut être contestée devant la cour d'appel de Paris et, le cas échéant, devant la Cour de cassation. La visite doit avoir lieu entre 6 h et 21 h (sauf décision contraire du JLD). L'occupant ou son représentant, auquel l'ordonnance est notifiée, doit être présent et assisté d'un conseil s'il le souhaite. Cette visite s'effectue sous l'autorité et le contrôle du juge qui l'a autorisée, celui-ci pouvant se rendre sur place et/ou délivrer commission rogatoire à un juge local[6].

Malgré le changement de sémantique, le terme « visite » succédant à celui de « perquisition administrative » et en dépit de l'introduction du juge judiciaire dans la chaîne administrative, il faut souligner l'absence de références précises du texte à une infraction pénale ce qui, nécessairement, fait planer sur le texte l'ombre de la justice prédictive tant décriée par le Conseil constitutionnel et la Commission nationale consultative des droits de l'homme (CNCDH). De telles visites sont en effet possibles lorsque la personne présente une « menace d'une particulière gravité pour la sécurité et l'ordre publics » et qu'elle est en relation avec des personnes liées au terrorisme ou adhère à des thèses terroristes. En outre, à défaut de précisions, dans quelles conditions et avec quels moyens le JLD, maillon de la chaîne pénale, pourra t-il contrôler la chaîne administrative ? À défaut de précisions dans le texte, la réponse à cette question semble aujourd'hui difficile à formuler. Il faut en effet avouer que le contrôle d'une mesure administrative par un juge judiciaire relève d'une contorsion peu naturelle de l'ordre juridique et, dans un contexte de pénurie des magistrats, peut laisser penser que cette entrée du JLD dans la chaîne administrative s'inscrit dans une conception restrictive du contrôle.

Pour toutes ces raisons, il se dégage de cette loi une certaine ambivalence entre, d'un côté, des signes allant dans le sens d'une sortie maîtrisée de l'état d'urgence et, de l'autre, des indices qui témoignent d'une volonté de transposition de l'état d'urgence dans la légalité ordinaire. Ce faisant, se pose la question de la constitutionnalité de ce nouveau dispositif.

II. Réflexions sur la constitutionnalité de la loi nouvelle

Dès lors que des lois au caractère opportuniste survivent aux circonstances qui les ont fait naître, « les crises laissent derrière elles, comme une marée d'épais sédiments de pollution juridique »[7]. Cette affirmation est particulièrement vraie au sujet de la législation anti terroriste[8], qui, depuis 1986, a connu de nombreuses lois qui ont abondé le Code pénal, le Code de procédure pénale et le Code de la sécurité intérieure[9]. En 1991, dans son rapport intitulé « de la sécurité juridique» le Conseil d'État dénonçait déjà cet activisme pénal en le qualifiant de « marée normative », de « logorrhée législative et réglementaire »[10]. Julie Alix remarque même qu'« on n'ose plus dire législateur, tant sa part contributive est faible lorsque les lois sont votées en urgence, et surtout lorsqu'elles concernent des sujets aussi fédérateurs dans la classe politique que la lutte contre le terrorisme »[11].

Ces précisions sont sans nul doute une des raisons pour lesquelles la législation antiterroriste récente a été émaillée de plusieurs déclarations d'inconstitutionnalité (A). L'étude de ces récentes inconstitutionnalités conforte l'existence de doutes quant à la constitutionnalité de certaines dispositions contenues dans la loi du 30 octobre 2017 (B).

A. Les récentes inconstitutionnalités de la législation antiterroriste

Le but de cette contribution n'est pas de retracer l'intégralité des déclarations d'inconstitutionnalité ayant affecté la législation antiterroriste. C'est pourquoi, seront uniquement évoquées deux inconstitutionnalités récentes.

Premièrement, dans un numéro précédent de cette revue, nous avions déjà fait part de nos

doutes au sujet de la constitutionnalité de certaines dispositions de la loi du 21 juillet 2016 prorogeant l'application de la loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence[12]. Ce point de vue était partagé puisque le 16 septembre 2016, le Conseil d'État avait saisi le Conseil constitutionnel d'une question prioritaire de constitutionnalité (QPC) au sujet de la conformité aux droits et libertés que la Constitution garantit des troisième à dixième alinéas du paragraphe I de l'article 11 de la loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence, dans sa rédaction issue de la loi n° 2016-987 du 21 juillet 2016[13]. Le 2 décembre 2016, le Conseil constitutionnel a répondu à cette QPC qui était a minima pour deux raisons l'une des plus attendues de la fin d'année 2016. Primo, la dite QPC est venue enrichir la jurisprudence récente du Conseil constitutionnel sur l'état d'urgence[14]. Secundo, en étant à nouveau sollicité sur les saisies de données ou de matériels informatiques lors de perquisitions administratives dans le cadre de l'état d'urgence, le Conseil constitutionnel s'est prononcé, pour la seconde fois en quelques mois, sur la conformité à la Constitution de cette procédure. En effet, dans sa décision n° 2016-536 QPC du 19 février 2016, le Conseil constitutionnel avait déclarée contraire à la Constitution la saisie, par copie, de données informatiques lors d'une telle perquisition[15]. La raison de la contrariété à la Constitution était l'absence d'intervention d'un juge, condition d'autant plus essentielle que les éléments susceptibles d'être copiés pouvaient être sans lien avec la personne qui constituait la menace. Le défi de la loi du 21 juillet 2016, en faisant renaître de ses cendres la procédure de saisie des données informatiques au cours d'une perquisition administrative, était donc de s'entourer des garanties nécessaires pour échapper à une nouvelle censure. Pour éviter l'inconstitutionnalité, la loi n° 2016-987 du 21 juillet 2016 avait créé un système d'autorisation a posteriori délivrée par le juge administratif des référés saisi à l'initiative du préfet signataire de l'ordre de perquisition. En outre le texte permettait, en plus de la saisie et de l'exploitation de données informatiques, la saisie de supports matériels pouvant contenir de telles données[16]. Le challenge que s'est fixé le législateur n'a toutefois pas été complètement relevé puisque le Conseil constitutionnel, dans sa décision du 2 décembre 2016, a déclaré à nouveau partiellement inconstitutionnelle cette procédure[17]. Les Sages ont effet considéré qu'en étant muet sur le devenir des données copiées qui caractérisent une menace et qui ont fait l'objet d'une autorisation d'exploitation par le juge sans conduire à la constatation d'une infraction, le législateur n'a pas prévu de garanties légales propres à assurer une conciliation équilibrée entre le droit au respect de la vie privée et la sauvegarde de l'ordre public.

Deuxièmement, de multiples enseignements peuvent être retirés de l'inconstitutionnalité du délit de consultation habituelle de sites terroristes dans sa rédaction issue de la loi du 3 juin 2016. En effet, en légiférant « tous azimuts »[18], le législateur a confirmé, dans la loi du 3 juin 2016, sa volonté d'ériger la législation antiterroriste en un outil d'anticipation. Née au lendemain des attentats commis à Paris en 1995, cette mutation législative « de la réaction vers la prévention » se traduit, depuis plusieurs années, par une répression croissante des actes de soutien au terrorisme. Le but est d'ériger la législation pénale en un outil d'anticipation permettant d'aboutir à une répression antérieure à la perpétration d'une action terroriste[19]. Le délit de consultation habituelle de sites terroristes, inséré par la loi n° 2016-731 du 3 juin 2016 à l'article 421-2-5-1 du Code pénal, en était l'archétype. En effet, la particularité de cette infraction terroriste était qu'elle se fondait sur un élément matériel qui n'était pas susceptible en lui-même de porter atteinte à la sécurité, à la dignité ou à la vie des personnes. Aussi, le texte permettait-il une répression très anticipée du processus de radicalisation. En effet, en agissant en amont, le but était de prévenir la commission d'actes de terrorisme en réprimant un comportement susceptible d'entraîner une radicalisation et, éventuellement ensuite, un passage à l'acte terroriste. Fruit d'une histoire démarrée en 2012 dans le projet de loi renforçant la prévention et la répression du terrorisme, ce délit controversé s'inspirait de celui de consultation habituelle de sites internet pédopornographiques prévu par le cinquième alinéa de l'article 227-23 du Code pénal[20]. Symbole d'une législation d'anticipation du terrorisme, ce texte n'était pas sans susciter des réserves par

rapport au respect des droits fondamentaux. Ce qui devait arriver arriva le 7 septembre 2016 lorsque le Conseil constitutionnel fut saisi par la Cour de cassation d'une question prioritaire de constitutionnalité relative à la conformité aux droits et libertés que la Constitution garantit de l'article 421-2-5-2 du Code pénal. Les nombreux griefs d'inconstitutionnalité développés par le requérant attestent de la richesse des questions soulevées par cette incrimination. Il était en effet soutenu qu'elle méconnaissait la liberté de communication, le principe de légalité des délits et des peines, celui d'accessibilité et d'intelligibilité de la loi, le principe d'égalité, le principe de proportionnalité et enfin le principe de la présomption d'innocence. Dans sa décision n° 2016-611 rendue le 10 février 2017, le Conseil constitutionnel a appliqué le principe de l'économie des moyens et a statué uniquement sur le grief tiré de l'atteinte à la liberté de communication. Ce seul grief lui a suffi pour sanctionner cette logique législative d'anticipation du prix le plus fort : celui d'une non-conformité totale et à effet immédiat.

Pour y parvenir, le Conseil constitutionnel a démontré méthodiquement l'absence de nécessité et de proportionnalité de l'atteinte portée à la liberté de communication. Les Sages ont constaté que les magistrats et les services de police disposaient déjà d'outils, parmi lesquels figurent l'association de malfaiteurs en vue de la commission d'actes de terrorisme et l'entreprise individuelle de terrorisme, pour condamner les personnes se livrant à de telles consultations et pour prévenir des passages à l'acte terroriste. Le Conseil relève en ce sens que « la législation comprend un ensemble d'infractions pénales autres que celle prévue par l'article 421-2-5- 2 du Code pénal et de dispositions procédurales pénales spécifiques ayant pour objet de prévenir la commission d'actes de terrorisme ». Du point de vue procédural, le Conseil a précisé que « les magistrats et enquêteurs disposent de pouvoirs étendus pour procéder à des mesures d'interception de correspondances émises par voie de communication électronique, de recueil des données techniques de connexion, de sonorisation, de fixation d'images et de captation de données informatiques ». Ils ont ajouté qu'en plus de ces outils pénaux, le législateur a « également conféré à l'autorité administrative de nombreux pouvoirs afin de prévenir la commission d'actes de terrorisme ». En conséquence, le Conseil constitutionnel a estimé qu'« au regard de l'exigence de nécessité de l'atteinte portée à la liberté de communication, les autorités administrative et judiciaire disposent, indépendamment de l'article contesté, de nombreuses prérogatives, non seulement pour contrôler les services de communication au public en ligne provoquant au terrorisme ou en faisant l'apologie et réprimer leurs auteurs, mais aussi pour surveiller une personne consultant ces services et pour l'interpeller et la sanctionner lorsque cette consultation s'accompagne d'un comportement révélant une intention terroriste, avant même que ce projet soit entré dans sa phase d'exécution ».

Ensuite, sur la gravité de l'atteinte portée à la liberté de communication, le Conseil constitutionnel a souligné que « les dispositions contestées n'imposent pas que l'auteur de la consultation habituelle des services de communication au public en ligne concernés ait la volonté de commettre des actes terroristes ni même la preuve que cette consultation s'accompagne d'une manifestation de l'adhésion à l'idéologie exprimée sur ces services. Ces dispositions réprimment donc d'une peine de deux ans d'emprisonnement le simple fait de consulter à plusieurs reprises un service de communication au public en ligne, quelle que soit l'intention de l'auteur de la consultation, dès lors que cette consultation ne résulte pas de l'exercice normal d'une profession ayant pour objet d'informer le public, qu'elle n'intervient pas dans le cadre de recherches scientifiques ou qu'elle n'est pas réalisée afin de servir de preuve en justice ». Ce faisant, il est fait grief au législateur d'avoir péché par excès de prévention et d'intrusion en s'attaquant à la liberté de pensée de l'internaute en dehors de tout expression publique ou acte matériel dangereux[21].

Ces récentes déclarations d'inconstitutionnalité expliquent que dans le cadre d'une étude consacrée à la loi du 30 octobre 2017, il n'est pas possible de faire l'économie de la question de la constitutionnalité de ce texte. Or, les enseignements issus des inconstitutionnalités passées font naître certains doutes sur la constitutionnalité de la loi nouvelle.

B. Réflexions sur la constitutionnalité de la loi nouvelle

Les principales interrogations sur la constitutionnalité du nouveau texte proviennent du fait que plusieurs mesures prévues par la loi du 30 octobre 2017 semblent en réalité s'apparenter à des doublons de mesures de police administrative ou de police judiciaire déjà existantes[22], étant rappelé que ce grief était précisément au c oeur des deux déclarations d'inconstitutionnalités évoquées supra.

Tel semble être le cas des périmètres de protection. Il convient en effet de relever que des mesures similaires peuvent déjà être ordonnées dans les lieux où se déroule une manifestation sportive[23] ou autour de certains lieux « d'importance vitale »[24]. En outre, les agents de police municipale peuvent déjà procéder à des palpations de sécurité et à la fouille des bagages pour sécuriser une manifestation sportive, récréative ou culturelle[25]. Parallèlement, le Code de procédure pénale permet également au procureur de la République d'autoriser la police judiciaire à procéder à la fouille des véhicules et à celle des bagages qu'ils contiennent « aux fins de recherche et de poursuite des [...] actes de terrorisme » ou « pour prévenir une atteinte grave à la sécurité des personnes et des biens[26]».

Des interrogations similaires peuvent se poser au sujet de la fermeture des lieux de culte. Le Conseil d'État a en effet rappelé dans son avis du 15 juin 2017 qu'une décision similaire pouvait déjà être prise « par les autorités compétentes au titre de leur pouvoir de police administrative générale ».

À cela s'ajoute que les mesures individuelles de contrôle et de surveillance entretiennent des similitudes troublantes avec les mesures pouvant déjà être ordonnées par le juge judiciaire, en cas d'ouverture d'une instruction pour association de malfaiteurs terroristes, apologie du terrorisme ou provocation au terrorisme, dans le cadre d'un contrôle du même nom[27]ou d'une assignation à résidence sous surveillance électronique[28].

Enfin, le même constat peut être dressé au sujet des visites et saisies, dont le Code de procédure pénale permet la réalisation à tout moment en matière de criminalité organisée, dans le cadre de l'enquête comme de l'instruction[29].

Compte tenu des enseignements issus des précédentes déclarations d'inconstitutionnalité, il nous semble que le seul fait que les nouveaux textes prévoient, pour certaines de ces mesures, que leur intensité et leur durée doivent être proportionnées aux circonstances ne saurait suffire à préjuger de leur constitutionnalité. Au jour de l'écriture de cet article, ni le Conseil d'État ni le Conseil constitutionnel n'ont encore eu l'occasion de se prononcer sur la constitutionnalité des dispositions contenues dans cette nouvelle loi antiterroriste. Un peu de patience car cela ne saurait tarder...

En effet, le tribunal administratif de Versailles a transmis au Conseil d'État le 22 novembre 2017 une question prioritaire de constitutionnalité sur l'article L. 227-1 du Code de la sécurité intérieure, relatif à la fermeture des lieux de culte (TA Versailles, 22 novembre 2017, n° 1708063). Surtout, le 1er décembre 2017, le Conseil d'État a transmis au Conseil constitutionnel question prioritaire de constitutionnalité relative aux mesures individuelles de contrôle, qui ont remplacé les assignations à résidence en vigueur sous l'état d'urgence.

Notes :

1 Dossier Le volet « procédure pénale » de la loi du 3 juin 2016, AJ pénal 2016. 457 ; Dalloz actualité, 14 juin 2016, obs. S. Fucini ; O. Cahn, Réflexions désabusées sur le chapitre I du titre I de la loi n° 2016-731 du 3 juin 2016, AJ pénal 2016. 408.

2 article L. 22-10-1 du Code de la sécurité intérieure.

3 article L. 114-1 modifié du Code de la sécurité intérieure.

4 CE 15 juin 2017, n° 393348.

5 O. Cahn et J. Leblois-Happe, Loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme : perseverare diabolicum, AJ pénal 2017.468.

6 article L. 229-1 et L. 229-2 du Code de la sécurité intérieure.

7 G. Braibant, « L'État face aux crises », Pouvoirs 1979, p. 8.

8 Y. Mayaud, La politique d'incrimination du terrorisme à la lumière de la législation récente, AJ Pénal 2013.442.

9 M. Léna, 1986-2016 : trente ans de lois antiterroristes, AJ Pénal 2016.105 ; C. Lazerges, De la fonction déclarative de la loi pénale, RSC 2004.194 ; H. Rouidi, La loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme : quelles

évolutions ? AJ Pénal 2014.555.

10 CE, « De la sécurité juridique », rapport public annuel, La Documentation française, 1991.

11 J. Alix, Réprimer la participation au terrorisme, RSC 2014.849.

12 D. Goetz, Libre propos sur la loi n° 2016-987 du 21 juillet 2016 prorogeant l'application de la loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence et portant mesures de renforcement de la lutte antiterroriste, Grasco, n° 17, novembre 2016, p. 31-40.

13 CE 16 sept. 2016, n° 402941, AJDA 2016. 1718.

14 Cons. const. 23 sept. 2016, n° 2016-567/568 QPC, AJDA 2016. 1776 ; D. 2016. 1864 ; Constitutions 2016. 540, chron. ; L. Dutheillet de Lamothe et G. Odinet, L'urgence dans tous ses états, AJDA 2016. 247.

15 Cons. const. 19 févr. 2016, n° 2016-535 QPC, AJDA 2016. 340 ; D. 2016. 429, et les obs. ; AJCT 2016. 202, étude J.-C. Jobart ; Constitutions 2016. 100, chron. L. Domingo ; ibid. 191, Décision ; Dalloz actualité, 22 juill. 2016, obs. M.-C de Montecler ; Dalloz actualité, 26 juill. 2016, obs. D. Goetz

16 S. Sontag Koenig, Les perquisitions 2.0 : quand l'informatique se saisit de l'immatériel, AJ Pénal 2016. 238).

17 Cons. Const. 2 décembre 2016, n° 2016-600 QPC, dalloz actualité, 8 décembre 2016, obs. D. Goetz.

18 CNCDH, Avis sur le projet de loi renforçant la lutte contre le crime organisé, le terrorisme et leur financement et améliorant l'efficacité et les garanties de la procédure pénale, ass. plén., 17 mars 2016, p. 2.

19 J. Alix, Réprimer la participation au terrorisme, RSC 2014. 849.

20 Projet de loi renforçant la prévention et la répression du terrorisme, Étude d'impact, p. 19 ; Rapport d'activité du Conseil d'État 2013, Doc. fr., p. 202-203).

21 Cons. Cons. 10 février 2017, n° 2016-611 QPC, dalloz actualité 14 février 2017, obs. D. Goetz.

22 O. Cahn et J. Leblois-Happe, Loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme : perseverare diabolicum, AJ pénal 2017.468.

23 article L. 332-16-2 du Code du sport.

24 article L. 1332-2-1 du Code de la défense.

25 article L. 511-1 du Code de la sécurité intérieure.

26 articles 78-2-2 et 78-2-4 du Code de procédure pénale.

27 article 138, 1°, 2°, 3°, 4°, 5°, 9° du Code de procédure pénale.

28 article 142-5 s du Code de procédure pénale.

29 articles 706-89 à 706-91 du Code de procédure pénale.

OUVRAGES RÉCENTS

THÉORIE DES HYBRIDES
TERRORISME ET CRIME ORGANISÉ

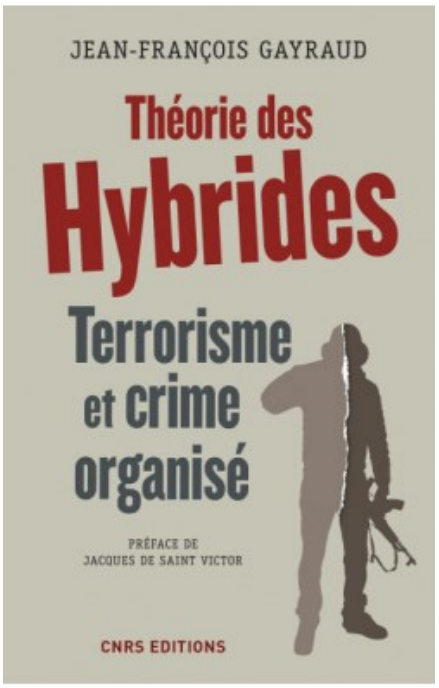
AUTEUR : JEAN-FRANÇOIS GAYRAUD

EDITEUR : CNRS ÉDITIONS

Résumé

Dans le monde post-Guerre froide, l'hybridation est devenue la règle et non plus l'exception, générant des entités inclassables : guérillas marxistes vivant du trafic de cocaïne ; gangsters salafisés ; sectes religieuses vouées au terrorisme ; financiers à la fois spéculateurs et criminels ; paramilitaires mutant en cartels de la drogue... Tous les entrepreneurs du crime tendent aujourd'hui à changer d'ampleur et de forme.

L'ère de l'hybridation a commencé... Et le terrorisme trouve ainsi des nouvelles sources de financement. Des corps hétérogènes et inconciliables font désormais symbiose. Hier, acteurs « politiques » (terrorisme, guérillas, milices, mouvements de libération) et criminels de « droit commun » (bandes, gangs, cartels, mafias) vivaient séparés dans les espaces et selon les logiques de la Guerre froide : ils fusionnent aujourd'hui sur la même scène violente et prédatrice.



Jean-François Gayraud livre une analyse lucide et sans concession de ces hybrides qui bousculent toutes les certitudes héritées du XXe siècle.

« La figure du "prédateur" mondialisé appelle la figure nouvelle du petit criminel global qui se présente souvent sous l'aspect plus "noble" du terroriste. Cet "hybride" prend de multiples aspects que Jean-François Gayraud décline dans une casuistique savoureuse. »

L'OBTENTION DE LA « PREUVE ÉLECTRONIQUE » AUX ÉTATS-UNIS : UN POSSIBLE RÊVE ?

MARIE-LAURENCE NAVARRI

MAGISTRAT DE LIAISON AUX ÉTATS-UNIS

À l'heure où la Cour Suprême vient de se saisir de l'Affaire dite « Microsoft »[1], à l'heure où toutes les instances internationales et régionales, des Nations Unies à l'Union européenne et au Conseil de l'Europe, conduisent d'importants travaux sur l'obtention de la fameuse preuve électronique, il paraît nécessaire de réfléchir à l'accès à ces données sous l'angle des besoins de l'enquête pénale française.

La donnée électronique est-elle une donnée à part dans l'enquête pénale ? Quelle est-elle ? Où se trouve-t-elle ? À qui appartient- t-elle ? À quoi sert-elle ? Quelle légitimité pour y avoir accès et l'utiliser ?

Sans prétendre à l'exhaustivité dans un débat qui fait rage de part et d'autre de l'Atlantique, cet article a pour objet d'apporter l'éclairage du magistrat de liaison français aux États-Unis dont le rôle, à mi-chemin entre les deux pays, est d'acheminer, préparer et tenter de faire aboutir les demandes quotidiennes des enquêteurs français auprès de Google, Facebook, Microsoft et autres « GAFA ».

Le chemin est ardu, semé d'embûches et force est de constater que malgré un travail assez colossal côté français comme côté américain d'ailleurs (ce que ne savent pas forcément les magistrats ou enquêteurs français prompts à penser que les autorités américaines n'ont cure de leurs demandes), force est de constater que les résultats sont maigres voire indigents.

Faut-il alors imaginer un autre cadre législatif ? National ? Européen ? Américain ? International ?

Examinons d'abord les tenants du problème avant d'examiner d'éventuelles pistes de réflexion pour un avenir plus ou moins proche.

I. De quelles données électroniques s'agit-il ?

L'on distingue, communément, trois types de données « électroniques » et le présent exposé se limitera à ces trois seulement dans un souci de clarté et de bonne compréhension de l'objet « preuve électronique » qui peut recouvrir des réalités plus larges (copie de serveur, infiltration en ligne, perquisition à distance, etc.).

- La donnée dite « de base ». Il s'agit, en réalité, de plusieurs données à caractère personnel, fournies de leur plein gré par les utilisateurs, à un fournisseur afin de souscrire un contrat d'abonnement, de créer un profil d'utilisateur ou d'ouvrir un compte. C'est en général et selon les opérateurs, le nom et prénom, l'adresse, le numéro de téléphone, l'adresse physique et l'adresse mail d'un individu, la data de naissance, voire une autre adresse email et le numéro de carte bleue.

Ce sont aussi les dates, heures et adresses IP pour chaque connexion (à ceci près que certains fournisseurs considèrent l'adresse IP comme une donnée de transaction nécessitant une décision de justice).

- La donnée de « transaction » afin d'obtenir non plus seulement les données d'une personne mais celles liées à son entourage ou aux personnes

avec qui il est en contact puisque cette donnée est l'entête d'un message électronique par exemple « message envoyé à telle date par untel à X ». Elles comprennent donc l'adresse mail de l'expéditeur et du destinataire y compris leurs adresses IP, les dates et heures des correspondances et la durée ou « taille » de celles-ci, c'est-à-dire tout sauf l'objet et le contenu.

- La donnée de contenu, comme son nom l'indique est la reproduction de la teneur des échanges entre les individus, sur Internet, la publication de contenus sur des sites, les pièces jointes etc.

A. Quelle utilité/utilisation des données électroniques ?

Nul n'est besoin de gloser pour dire que la donnée électronique est indispensable à la quasi-totalité des enquêtes pénales qu'il s'agisse d'homicides, disparitions, attaques terroristes ou escroqueries.

À l'heure où nous tous communiquons avec le reste du monde y compris nos voisins essentiellement par Internet, l'accès à ces échanges est nécessaire, parfois indispensable à l'avancée des procédures et à l'apport d'une réponse judiciaire à des victimes, en chair et en os, qui ne comprennent pas grand-chose aux débats qui ont lieu dans la Sillicon Valley.

Ainsi, et pour ne prendre que quelques exemples, savoir si la jeune femme qui a tenté, il y a quelques mois de faire sauter la cathédrale Notre-Dame de Paris, a agi seule ou comme membre d'une cellule, implique d'avoir accès à la liste de ses amis sur Facebook et au contenu de ses « posts ».

De même, la seule manière de savoir ce qui est arrivé aux deux jeunes aventuriers de 22 et 25 ans partis dans un lointain pays étudier les tortues de mer et assassinés un mois après, est d'avoir accès au contenu de leurs conversations sur leur smartphone et ordinateur portable, seuls équipements qu'ils avaient emportés.

La disparition d'un jeune homme de seize ans, il y a plus de deux ans, reste, à ce jour, pour les enquêteurs, un mystère, faute d'avoir obtenu de réponse (même négative) de l'opérateur Snapchat qu'utilisait la victime.

Ainsi, et sans lister jusqu'à l'épuisement la liste des demandes transmises aux États-Unis, l'obtention d'un nom, d'une date, d'une liste de contacts, de messages postés est quotidiennement nécessaire aux enquêtes que ce soit pour identifier une piste d'enquête, un auteur, un complice, un suspect, déterminer un mode opératoire.

C'est pourquoi les enquêteurs français, policiers, juges d'instruction ou procureurs de la République multiplient les demandes d'entraide aux États-Unis, représentant ainsi la plus grosse part de la coopération pénale entre les deux pays.

B. Comment obtient-on (en théorie) les données électroniques ?

Il y a deux cas, l'un qui concerne une toute petite minorité de situations exceptionnelles et l'autre, l'immense majorité des demandes

Cet article ne s'attardera pas sur le premier qui est la possibilité, en cas d'extrême urgence, d'obtenir tout type de donnée de fournisseur d'accès Internet, sur la base de leur libre coopération, y compris des données de contenu.

Ainsi, Microsoft et ses représentants débutent, systématiquement, leur discours dans les conférences et apparitions publiques sur la preuve électronique par l'expression de leur « bonne volonté » et « souci de coopérer » manifestés, selon eux, suite aux attentats contre l'hebdomadaire Charlie Hebdo où et alors que certains des membres de la cellule terroriste courraient encore dans la nature, les données de leurs comptes avaient été transmises aux enquêteurs français dans les 45 minutes de la demande.

Cette coopération, exceptionnelle tant sur la forme (extrême rapidité) que sur le fond (transmission de données de contenu) est réservée aux cas d'urgence absolue caractérisée par un danger imminent pour la vie humaine.

Pour ces dossiers et pour ceux-là seulement, il est possible de faire une requête aux fournisseurs de service Internet qui, sur la base du volontariat, peuvent transmettre aux enquêteurs des données de leurs utilisateurs y compris des contenus et ce avec des délais très rapides d'exécution.

Dans la pratique, cela représente un très, voir extrêmement faible nombre de cas qui, s'ils sont emblématiques, ne peuvent servir d'exemple tant ils correspondent à des situations particulières et heureusement plutôt rares.

Dès lors cette coopération « exemplaire » est l'arbre qui ne cache hélas pas la forêt. En effet, cette transmission de données qu'aucun texte national ou international, il est vrai, n'encadre est déterminée, au cas par cas, pour une poignée de demandes. Si c'est un outil dont il ne faut pas

se priver et qui mérite d'être connu des enquêteurs, il ne peut être utile et utilisé que très rarement et n'aide guère à résoudre la question de l'accès à la preuve électronique dans l'immense majorité des cas.

En effet, pour tout le reste, lorsque ce critère d'urgence ou de danger imminent dont les fournisseurs ont seuls, in fine, l'appréciation n'est pas ou pas suffisamment établi, il faut passer par le système non dérogatoire décrit ci-dessous, instauré, depuis 1986 par la loi américaine ECPA (Electronic Communications Privacy Act).

Le congrès américain a, à l'époque, imaginé une construction à étages en fonction de l'intrusion plus ou moins grande dans la vie privée des usagers d'Internet avec, comme complexité accrue, des règles légèrement différentes selon que le demandeur à la donnée est un enquêteur américain ou étranger.

i. L'accès aux données « de base »

Contrairement aux enquêteurs américains qui doivent obtenir un mandat judiciaire, les enquêteurs français peuvent, sur simple réquisition, directement adressée aux États-Unis, aux fournisseurs d'accès Internet (FAI), obtenir la transmission de ces données. La demande se fait au moyen de formulaires dédiés avec un rapide exposé des faits.

Cette facilité, qui est bien la seule dans cette complexe et frustrante matière, doit être soulignée et si l'on ose l'écrire, préservée tant elle permet à ceux qui poursuivent les criminels d'avoir là, déjà, un début de preuve ou la confirmation d'une piste d'enquête dans des temps adaptés.

ii. L'accés aux données de « transaction »

À la différence du nom, prénom adresse et autres données fournies volontairement par l'utilisateur au fournisseur, il s'agit de données plus « privées » en ce sens qu'elles ont trait aux relations d'un particulier. Il faut donc, pour les obtenir, et ce, que le demandeur soit un enquêteur américain ou français, une décision de justice. Celle-ci ne peut être rendue que par un juge américain pour les données stockées par des fournisseurs américains.

La loi prévoit un critère ou standard de preuve à atteindre sans lequel le juge refusera la demande : il faut ainsi démontrer au juge que l'on dispose de solides arguments pour établir que la donnée demandée est non seulement étroitement liée au crime qui fait l'objet de l'enquête mais est essentielle à sa résolution[2].

Pour les enquêteurs français, cela signifie qu'il faut passer par une demande d'entraide pénale internationale.

iii. L'accès aux données de contenu

À ingérence suprême dans la vie privée, garanties les plus élevées : il faut, comme pour les données de « transaction » aller devant le juge américain mais non plus pour obtenir un ordre de transmission mais un véritable mandat de perquisition. En effet, le compte mail ou la page Facebook est considérée comme une maison, un box ou toute propriété fermée et cadenassée, sanctuaire de la vie privée.

Ce mandat de perquisition, contrairement au droit français où le Code pénal octroie de grands pouvoirs à l'officier de police judiciaire et au procureur de la République est, sans contestation, l'acte d'enquête le plus encadré en procédure pénale américaine. Le quatrième amendement de la constitution fédérale protège « le droit des citoyens d'être garantis dans leurs personne, domicile, papiers et effets, contre les perquisitions et saisies non motivées » et précise qu' « aucun mandat ne sera délivré, si ce n'est sur présomption sérieuse, corroborée par serment ou affirmation. »

Le juge doit décrire précisément le lieu à fouiller et les personnes ou les choses à saisir et ce, compte par compte, pour chaque fournisseur et établir, à chaque fois, le lien quasi certain entre le contenu éventuel et le crime ou son auteur.

Et, c'est là que la difficulté commence pour le magistrat français qui doit « plancher » sur sa demande d'entraide pour établir cette fameuse « présomption sérieuse » ou « probable cause » en anglais. Ce concept, totalement étranger à notre droit, est une réalité incontournable du droit américain. Si l'on veut une donnée qui se trouve sur leur territoire ou en possession d'un fournisseur basé aux États-Unis, alors il faut se plier à l'exercice.

Ce qui est sûr c'est que cet exercice n'est jamais aisé et, malgré toutes les formations et explications dûment fournies, ainsi que les modèles du FBI que l'on peut recopier à l'infini, il nécessite un travail fastidieux et parfois impossible. (Comment, en effet, en début d'enquête, alors que celle-ci n'a pas démarré ou n'est en rien étoffée, construire un argumentaire à même de satisfaire les fourches caudines américaines ? Comment savoir, demandent sans cesse les magistrats français, que le mail dont le contenu est demandé apportera la fameuse preuve

d'une implication, de la cause d'une disparition, d'un lien peut être essentiel entre un auteur et un complice puisque précisément « ce » mail, on ne l'a pas !

Il existe des astuces ou des mécanismes : par exemple, tenter dans un premier temps d'obtenir, par une première demande, une donnée de transaction qui pourra indiquer que puisque le mail a été envoyé ou reçu quelques heures avant l'infraction, il y a sans doute un lien avec celle-ci qui pourrait convaincre le juge et lui faire délivrer ce fameux mandat.

Hélas, la tentation du découragement est grande et de nombreux magistrats français, procureurs de la République et juges d'instruction confondus, préfèrent ne même plus demander des données pourtant absolument indispensables.

En effet, la procédure est longue, au minimum une dizaine de mois et sans aucune garantie de succès Les dossiers où des conversations, des contenus de page Facebook et autres ont été transmis se comptent sur le doigt d'une seule main.

Le plus souvent, après un an, au bas mot, d'échanges transatlantiques et de commissions rogatoires internationales affinées, peaufinées, précisées, l'enquêteur français, reçoit, un CD-Rom lui annonçant que sa demande a été exécutée mais en réalité, il n'y a pas ou quasiment pas de données de contenu. Ainsi, par exemple, dans un dossier pourtant signalé comme archi sensible pour infraction terroriste, un an après la rédaction et transmission de sa demande, le juge d'instruction a reçu les données d'un compte Facebook présentant moins de contenu que ce qu'avaient pu lire les enquêteurs sur la partie publique du même compte un an auparavant. Dans le dossier des deux jeunes humanitaires ci-dessus mentionné et malgré un argumentaire très étayé, les éléments de réponse reçus ne correspondent absolument pas à la longue et très détaillée liste de données demandées.

Ainsi, peut-on affirmer, sans se tromper, que si le système de l'entraide a le mérite d'exister, c'est en matière d'obtention de la preuve électronique, son seul mérite !

Pour reprendre les propos du sénateur Sheldon Whitehouse lors de l'audition, par le Comité judiciaire du Sénat américain, relative à la proposition de loi du ministère de la justice, en juillet 2017, la commission rogatoire internationale est « un système qui marchait au temps de la plume »[3].

La frustration est d'autant plus grande du côté français que les enquêtes pour lesquelles ces données sont demandées ne concernent, en rien, les États-Unis : dans la quasi-totalité des procédures, la donnée ne concerne ni un citoyen américain ni même une infraction commise dans ce pays. Quelle est donc la légitimité de la loi américaine pour en contrôler l'accès ? Pourquoi les enquêteurs français doivent-ils se plier aux exigences d'un système totalement étranger au leur ? Au seul motif de la détention de la preuve numérique par un opérateur basé aux États-Unis ?

Avant de réfléchir à la nécessaire invention d'un nouveau cadre légal, encore faut-il analyser les défaillances du système actuel.

C. Pourquoi est-ce si difficile d'obtenir des données électroniques ?

La réponse n'est pas simple, ou plutôt elle est multiple.

En premier lieu, elle tient, à l'évidence, à la nature de la demande qui crée un conflit certain entre, d'une part, la légitime attente de l'usager vis-à-vis de l'intimité de ses communications et de sa vie privée et le besoin, dans une société démocratique, de limiter ce droit pour les besoins de la sécurité et de la répression des crimes.

Pour citer Rob Wainwright, directeur d'Europol, lors d'un symposium sur la cybersécurité, organisée par le procureur de Manhattan en novembre 2016[4], depuis les théories du contrat social développées par Hobbes et Rousseau, les citoyens admettent que le droit à la vie privée n'est pas absolu et peut être limité par les forces de l'ordre pour assurer leur sécurité à condition de garde-fous et de contrôle judiciaires.

Deuxièmement et sans vouloir polémiquer sur tel ou tel fournisseur d'accès, la différence d'approches et de réponses aux sollicitations des enquêteurs n'est un mystère pour personne et certains font de l'obstruction ou en tout cas, refusent de coopérer au nom notamment de la vie privée de leurs clients.

Enfin, au niveau procédural, l'inefficacité du système de l'entraide tient à son assez incroyable lourdeur. En effet, la commission rogatoire internationale après avoir été rédigée par le juge d'instruction ou le procureur de la République français, passe dans plus d'une dizaine de mains différentes. Une fois rédigée par le procureur ou juge d'instruction français, elle est envoyée au magistrat de liaison

à Washington pour des échanges franco-français afin de présenter, dès le départ, la meilleure demande possible. Dès que validée, elle doit être traduite avant d'être transmise à l'autorité centrale française (bureau de l'entraide pénale du ministère de la justice) qui la transmet officiellement.

Côté américain, les choses se compliquent encore davantage. Elle est d'abord envoyée au magistrat de liaison américain à Paris, point d'entrée officiel de toutes les demandes judicaires françaises qui l'attribue, ensuite, à un procureur américain du bureau de l'entraide internationale, section cyber du ministère de la Justice. La demande fait alors l'objet d'une véritable analyse qui prend parfois plusieurs semaines au cours desquelles de très nombreux échanges franco-américains ont lieu pour étoffer, expliquer la demande afin de l'« américaniser », c'est-à-dire de la présenter selon les règles américaines, et ce, pour un dossier qui n'a, rappelons-le, strictement rien à voir avec les États-Unis.

Ainsi, une enquête française pour un meurtre commis en France par un français devra suivre ce chemin américain, tracé par le parlement de ce pays selon un système totalement étranger au nôtre pour la seule raison que la donnée est détenue par un tiers, en l'espèce un fournisseur implanté aux États-Unis.

Une fois le procureur américain satisfait qu'il dispose du meilleur dossier possible, il opère un choix sans consulter plus avant le demandeur français.

Ainsi, alors que l'enquêteur français a demandé des données de contenu, il se peut, et c'est le cas dans la plupart des dossiers, que le ministère de la Justice estime que le critère de « cause probable » n'est, in fine, pas suffisamment rempli et dès ce stade, la porte se referme puisqu'il est alors impossible d'obtenir la donnée de contenu sans que l'enquêteur français n'en soit même informé puisque le retour d'exécution n'intervient que bien plus tard.

Dès lors, dès ce moment, la demande française n'est plus celle d'origine mais une version américaine dont on ne sait si elle correspond ou si elle a été censurée.

Dans ce deuxième cas, la section cyber va alors demander au juge les données de « transaction ». Le juge va ou non délivrer un ordre d'obtention de ces données qui sera alors envoyé au fournisseur.

Deuxième difficulté : il n'y a pas de délai de réponse prescrit par la loi ; l'ordre du juge américain peut fixer un délai mais son absence d'exécution du fournisseur dans le délai imparti n'est jamais sanctionnée.

Troisième obstacle et non des moindres : dans le meilleur des cas, assez rare, si le procureur américain estime que la demande française satisfait au sacro-saint principe de « cause probable » et que le dossier présente suffisamment d'éléments pour demander à un juge un mandat de perquisition, là aussi, la suite, pour l'enquêteur français reste totalement mystérieuse et incontrôlable. Quelle est la décision du juge ? Que demande-t-il au fournisseur et dans quel délai ?

Il faut savoir que lorsqu'un contenu est transmis par un fournisseur, il n'est pas transmis directement à l'enquêteur français ni même à l'autorité centrale mais passe d'abord par une opération appelée « filtre », de la seule compétence du FBI.

Cette ultime étape est légale et même obligatoire puisque tout mandat de perquisition d'un juge doit être exécuté conformément aux dispositions de la loi américaine dont le FBI est le gardien. Il doit donc veiller à ce que les données transmises par le fournisseur n'excèdent pas ce qui a été autorisé par le juge et ce qui correspond à l'enquête. En effet, toutes les conversations pour lesquelles la « cause probable », c'est-à-dire le lien avec le crime ou l'enquête, ne serait pas démontrée doivent être expurgées des pièces d'exécution. De plus, le FBI opère aussi un contrôle de proportionnalité ou de nécessité en retirant les contenus qu'il considère ne pas être nécessaires à l'enquête et ce, avec une connaissance extrêmement limitée du dossier ne reposant que sur la commission rogatoire de départ et de la langue de ces conversations qui peut être du français familier voir de l'argot.

Ainsi, les données transmises sont passées au « peigne fin » par des agents qui ne connaissent pas le dossier et qui, de surcroît, à la date d'aujourd'hui, ne sont que six pour traiter les demandes du monde entier.

Ce « filtre » doit s'opérer contenu par contenu et ce pour des demandes parfois de mails sur plusieurs années.

Il n'est pas rare d'obtenir ainsi des données qui, trop expurgées, ne contiennent hélas plus guère de valeur ajoutée pour l'enquête.

Ainsi, il apparaît qu'obtenir des données de contenu et ce alors même que la France fait partie des pays les mieux placés pour

avoir, avec les États-Unis, une longue relation d'entraide judiciaire en matière pénale, l'obtention de la preuve électronique, celle qui sert aux enquêtes est un rêve quasi impossible.

II. Des solutions pour améliorer l'obtention de la preuve électronique aux États-Unis

Afin de ne pas finir ces propos sur un constat sans appel, il importe de réfléchir aux éventuelles solutions qui se dessinent de ce côté-ci de l'Atlantique, sans développer quant aux travaux de l'Union européenne ou du Conseil de l'Europe (Comité de suivi de la convention de Budapest).

A. L'obtention de données électroniques stockées à l'étranger

En premier lieu, la Cour Suprême a, au mois d'octobre cette année, accepté le pourvoi en cassation du ministère de la Justice américain contre la décision Microsoft vs US (829 F.3d 197) rendue, le 14 juillet 2016 par la cour d'appel du second circuit (région de Washington DC).

Pour mémoire, cette juridiction avait rendu une décision très attendue et très controversée affirmant l'incapacité pour les autorités de poursuite américaines d'obtenir des données électroniques stockées à l'étranger.

En l'espèce, dans cette affaire, Microsoft Corporation v. USA, débutée en 2013 dans une procédure d'infraction à la législation sur les stupéfiants, un juge de l'État de New york (juge fédéral du Southern District) avait émis un mandat de perquisition ordonnant à Microsoft la production de données de contenu d'un compte hotmail.

Microsoft avait fourni les données stockées aux États-Unis mais refusé de transmettre celles détenues sur le sol irlandais arguant de l'incompétence d'un juge américain pour exiger la production de données détenues hors du territoire américain et avait, par conséquent, subi une procédure de « civil contempt » pour n'avoir pas respecté le mandat du juge.

La compagnie avait fait appel et la cour lui a donné raison.

En droit, si le critère de la juridiction compétente est celui de la localisation physique de la donnée, l'arrêt de la cour semble imparable. En effet, la Electronic Communications Privacy Act de 1986 n'a aucun caractère extraterritorial.

L'arrêt Morrison Vs National Australian Bank, rendu par la Cour Suprême des États-Unis, en 2010, affirme une présomption d'extraterritorialité des lois américaines.

Ainsi, sauf intention explicite du Congrès traduite dans la loi, une loi américaine ne s'applique que sur le territoire des États-Unis et c'est le cas de la loi ECPA. Donc le mandat du juge américain n'a pas de force en Irlande.

Mais la cour suprême, et c'est là la lueur d'espoir tant attendue, peut également décider qu'à l'heure du cloud et à l'heure où les données sont stockées par ceux qui les détiennent où bon leur semble pour des raisons qui ne regardent qu'eux, le critère de localisation physique de la donnée est absurde.

D'ailleurs, en termes de protection des citoyens et de leur possible accès à une autorité de protection des données, dire que la juridiction compétente est celle de la localisation physique de la donnée sur un serveur revient à les priver de tout recours effectif.

Dans l'exemple Microsoft, la donnée stockée en Irlande concernait un citoyen américain. Si la loi américaine ne s'applique pas en raison du stockage physique de sa donnée à l'étranger, celui-ci devrait, par conséquent, pour exercer un éventuel droit d'accès, s'adresser à l'Irlande qui ne sait même pas que la donnée est sur son territoire.

Ainsi, deux conséquences particulièrement néfastes sont immédiatement prévisibles en cas de confirmation par la Cour Suprême de la jurisprudence Microsoft.

D'une part, l'enquêteur français se verra privé de la possibilité, certes imparfaite, d'obtenir la donnée électronique, en la demandant aux autorités américaines.

C'est déjà en partie le cas puisque depuis l'affaire Microsoft, certains GAFA répondent aux demandes d'entraide par une lettre type ainsi rédigée « le mandat que nous avons reçu vise l'obtention d'informations stockées hors du territoire des États-Unis. Les mandats pris en application de la loi ECPA ne peuvent obliger à produire des données stockées hors des États-Unis » avec, à l'appui, citation de l'arrêt Microsoft.

Dans ces cas qui ne manqueront pas de devenir légion en cas de décision favorable à Microsoft, l'enquêteur qui voudra accéder à la preuve électronique devra, au préalable, savoir où elle se trouve, ce qui relève d'une mission quasi impossible. Par exemple, certains fournisseurs, à l'instar de Google stocke les composantes d'un même mail dans des juridictions différentes.

La localisation de la donnée est une réalité évolutive, qui échappe à tout contrôle.

En second lieu, le propriétaire légitime de la donnée, c'est-à-dire l'usager du compte n'a aucun moyen de savoir où se trouve l'information le concernant. Il sait, cependant, qu'il a ouvert un compte auprès de tel fournisseur et c'est auprès de ce dernier qu'il doit pouvoir se tourner.

Il faut donc espérer que la Cour, dont la décision sera rendue, au plus tard, en juin prochain, reconnaisse les difficultés ci-dessus décrites pour dire que le lieu d'accès de la donnée doit être celui où elle est contrôlée, détenue, et accessible c'est-à-dire entre les mains du fournisseur de service Internet et non là où elle est stockée.

B. Projets de modification de la loi ECPA de 1986

Autre lueur d'espoir, des travaux législatifs d'envergure sont entamés devant les comités judiciaires du Congrès américain afin de mettre la loi ECPA à la page et de l'adapter à des réalités technologiques totalement inexistantes et imprévisibles en 1986.

Deux propositions de loi poursuivent ainsi une existence parallèle.

La première, proposée par le ministère de la justice, le « Microsoft Fix », vise à revenir à la situation antérieure à l'arrêt de la cour du second circuit : le mandat du juge américain est contraignant pour les compagnies de l'Internet quel que soit le lieu de stockage de la donnée demandée.

La seconde, directement inspirée si ce n'est rédigée par les compagnies, limite encore davantage les possibilités d'accès aux données de part et d'autre des frontières en prévoyant un système de notification entre pays : en cas de demande d'accès, par exemple, par le gouvernement américain, à une donnée auprès d'un fournisseur américain mais concernant un français, l'autorité américaine se verrait dans l'obligation de notifier sa demande d'utilisation à la France qui aurait un droit de veto, les conflits étant réglés...devant le juge américain.

C. Projet d'accord bilatéral entre les États-Unis et le Royaume-Uni

Enfin, troisième vecteur et non des moindres, existe un projet d'accord bilatéral entre les États-Unis et le Royaume-Uni qui pourrait permettre de sortir de l'écueil de la loi américaine puisqu'il permettrait au pays signataire un accès direct au fournisseur américain y compris pour les données de contenu, non plus sur la base de la loi américaine mais en vertu de la loi de ce pays.

L'accès à la preuve électronique ? Un rêve peut-être à portée de main.

Note :

1 Microsoft vs US, 14/07/2016, arrêt de la cour d'appel du Second Circuit des États-Unis qui a validé le refus de cette compagnie de transmettre aux autorités américaines le contenu d'un email stocké sur un serveur irlandais au motif qu'il était hors de portée du juge américain.

2 18 U.S Code § 2703 - - Required disclosure of customer communications or record (d): "A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation".

3 Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights - Subcommittee on Crime and Terrorism-Judiciary Committee Senate. July 2017

4 DANY financial Crime and Cybersecurity Symposium November 2016 Manhattan

© 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

Inscription à la revue du GRASCO

Par mail : abonnement@larevuedugrasco.eu

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

Par mail : information@grasco.eu

1 après validation de la rédaction