LA REVUE DU
GRASCO

www.grasco.eu
www.larevuedugrasco.eu

N°20— Octobre 2017

Parution trimestrielle
Gratuite
ISSN 2272-981X

EDITORIAL

CHANTAL CUTAJAR

DIRECTRICE DU GRASCO

Le Parquet européen, enfin !

Les 19 et 20 octobre 2000, l'Université de Strasbourg avait, sur mon initiative, organisé un colloque sur le thème : « Le parquet européen, peut-on encore attendre ? » dans l'espoir d'influer sur les négociations du Traité de Nice (http://www.syndicat-magistrature.org/Le-parquet-europeen-peut-on-encore.html#nb1). Nous avions, avec le syndicat de la magistrature et des signataires de l'appel de Genève, proposé à la signature de la société civile le « Manifeste de Strasbourg », pour une libre circulation de la Justice et du droit en Europe et l'adoption d'un parquet européen, dont l'idée était apparue au sein du groupe de travail de juristes réunis autour du professeur Mireille Delmas-Marty pour assurer la protection des intérêts financiers des Communautés européennes.

Le Traité de Nice fût, de ce point de vue, un échec. La Conférence intergouvernementale n'a pas ajouté au traité, comme l'avait pourtant proposé la Commission, une disposition qui aurait permis de créer un Procureur européen pour la protection des intérêts financiers de la Communauté. Il aura fallu attendre le 12 octobre 2017 pour que, dans le cadre d'une coopération renforcée à laquelle participent 20 Etats membres, les ministres de la justice de l'UE approuvent enfin la création d'un parquet européen dont la mission est circonscrite aux infractions pénales portant atteinte aux intérêts financiers de l'UE prévues par la directive (UE) 2017/1371 du Parlement européen et du Conseil du 5 juillet 2017 relative à la lutte contre la fraude portant atteinte aux intérêts financiers de l'Union au moyen du droit pénal et de toute autre infraction « inextricablement liée » aux comportements visés et aux infractions relatives à la participation à une organisation criminelle telles qu'elles sont définies dans la décision-cadre 2008/841/JAI relative à la lutte contre la criminalité organisée, si les activités criminelles d'une telle organisation consistent essentiellement à commettre une infraction contre les intérêts financiers de l'UE.

Le parquet européen n'est pas encore né, que des voix s'élèvent pour étendre sa compétence à la criminalité organisée et au terrorisme. On ne peut que soutenir une telle initiative, accueillie favorablement par Vera Jourova, Commissaire européen à la Justice, aux Consommateurs et à l'égalité des genres qui vient d'annoncer la publication prochaine d'une Communication de la Commission sur l'extension des compétences du parquet européen à la lutte contre le terrorisme.

Pour lutter contre des cas complexes de fraudes de grande ampleur qui affectent les fonds structurels de l'UE et la perception de la TVA, le Parquet européen devra mettre en œuvre des investigations financières et développer l'analyse financière criminelle. Le Collège européen des investigations financières a, au sein de l'Université de Strasbourg acquis un savoir faire unique en matière de formation des autorités de poursuite et de justice. Depuis sa création, 33 procureurs, 96 policiers, 25 gendarmes et 53 douaniers issus de tous les Etats membres ainsi que d'Etats associés ou candidats à l'adhésion

SOMMAIRE

ont participé et enrichi les programmes de formation de leurs expériences. Il ne fait guère de doute que l'efficacité du parquet européen sera tributaire de la capacité des procureurs européens délégués, dans chaque Etat membre à s'ouvrir aux pratiques de leurs homologues étrangers pour une coopération policière et judiciaires plus efficiente.

Le colloque qui se tiendra le 27 octobre à l'Université de Strasbourg à l'initiative du CEIFAC autour des auditeurs de la session d'octobre 2017, sera l'occasion d'échanger à propos de ce nouvel acteur judiciaire européen en présence notamment d'Eliane Houlette, Procureur national financier français, Michel Claize, Juge d'instruction belge, spécialiste de la criminalité financière, Chris Perryman, chef de projet, point de contact EUROPOL pour les fraudes TVA intracommunautaire et Nathalie Griesbeck, députée européenne.

Notes :

1. **Les premiers signataires étaient Bernard Bertossa, procureur général de Genève, Vittorio Borraccetti, procureur adjoint au parquet national antimafia italien, Miguel Carmona, président de la Cour d'appel de Séville, Antonio Cluny, procureur adjoint de la Cour des comptes portugaise, Gherardo Colombo, substitut à Milan, Anne Crenier, ancienne présidente du Syndicat de la magistrature (France), Benoît Dejemeppe, procureur du roi à Bruxelles, Carlos Jimenez Villarejo, chef du parquet anti-corruption de Madrid, Paul Perraudin, juge d'instruction à Genève, Teresa Romer, magistrate à la Cour suprême de Varsovie, Valéry Turcey, ancien secrétaire général de l'Union syndicale des magistrats (France)**

CEIFAC Collège Européen des Investigations Financières et Analyse financière Criminelle

FSI Fonds Sécurité Intérieure Union européenne — l'Europe se mobilise

GRASCO Groupe de Recherches Actions Sur la Criminalité Organisée

LA CRÉATION DU PARQUET EUROPÉEN

TABLE RONDE OUVERTE AU PUBLIC

27 OCTOBRE 2017, 08H00 – 12H00

AMPHITHÉÂTRE N°3
INSTITUT LE BEL, 4 RUE BLAISE PASCAL
67000 STRASBOURG

Eliane HOULETTE
Procureur national financier
FRANCE

Michel CLAISE
juge d'instruction à BRUXELLES,
BELGIQUE

Chantal CUTAJAR
Directrice générale du CEIFAC
FRANCE

Inscription sur contact@ceifac.eu

Retransmission en direct sur http://www.canalc2.tv

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Grand Est
ALSACE CHAMPAGNE-ARDENNE LORRAINE

Strasbourg.eu
eurométropole

Université de Strasbourg

dres
Droit, religion, entreprise et société

Conception CEIFAC

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

VĚRA JOUROVÁ, COMMISSAIRE EUROPÉEN À LA JUSTICE, AUX CONSOMMATEURS ET À L'ÉGALITE DES GENRES

PROPOS RECUEILLIS PAR JOCELYNE KAN
TRADUITS DE L'ANGLAIS PAR ÉLÉNA PELLISER

L.R.D.G. : Pouvez-vous nous parler de vos différentes missions à la Commission européenne ?

Mon travail en tant que Commissaire à la Justice, aux Consommateurs et à l'Égalite des genres repose sur les valeurs européennes inscrites dans les Traités et la Charte des droits fondamentaux.

Je travaille à protéger nos valeurs fondamentales, tout particulièrement l'État de droit, dans l'Europe et au-delà. Je suis également chargée de faire en sorte que la discrimination soit combattue et que l'égalité entre les genres soit promue. En tant que membre de l'équipe sur le marché unique numérique, je contribue à développer un marché unique numérique connecté reposant sur des règles claires en matière de protection des données où les règles relatives à la protection des consommateurs sont protégées aussi en ligne. Dans ce domaine, j'ai également instauré un cadre, le Bouclier UE -États-Unis pour la protection de la vie privée, qui garantit que les données personnelles transférées aux États-Unis sont dûment protégées par des normes élevées de protection des données. Enfin, mon équipe et moi luttons

contre les phénomènes criminels et le terrorisme en renforçant la coopération judiciaire en Europe, notamment par l'établissement du Parquet européen qui traitera l'évasion fiscale et la fraude transfrontalières, des infractions représentant des milliards d'euros chaque année. Nous avons également proposé de nouvelles règles pour prévenir le blanchiment d'argent et le financement du terrorisme.

L.R.D.G. : La Charte des droits fondamentaux, mise en place par les États membres de l'Union européenne en 1989, est actuellement confrontée à plusieurs difficultés telles que les vagues de réfugiés, le déséquilibre économique et les attentats terroristes. Comment ce texte a-t-il été appliqué ?

En temps de crise, les gens remettent en question la capacité des institutions et systèmes à faire ce qu'on attend d'eux et à protéger les populations de ces difficultés.

Nous ne devons jamais perdre de vue nos valeurs dans les efforts que nous déployons pour tenter de résoudre ces difficultés.

Aujourd'hui, nous avons une Agence de l'UE pour les droits fondamentaux, qui travaille étroitement avec d'autres Agences de l'UE afin de mieux protéger les droits fondamentaux de chacun.

Nous intégrons la Charte des

droits fondamentaux, qui est juridiquement contraignante, dans toutes les propositions législatives et politiques de la Commission.

Cela signifie que les propositions de la Commission ne sont pas seulement systématiquement évaluées sous l'angle de leurs effets économiques et sociaux, mais aussi qu'elles font l'objet d'une évaluation détaillées sous l'angle des droits de l'homme.

Cette nouvelle culture des droits fondamentaux doit toutefois pénétrer davantage au sein du processus législatif de l'UE et « percoler » jusqu'à son niveau de mise en oeuvre, sur le terrain. L'un des sujets de frustration des citoyens à l'égard de la Charte tient à la portée limitée de son application dans les États membres, puisque ceux-ci ne sont tenus de la respecter que lorsqu'ils appliquent le droit de l'UE.

Notre Portail e-justice présente une explication claire sur la portée d'application de la Charte et, depuis octobre dernier, il met également à disposition une fonctionnalité « wizard des droits fondamentaux » qui aide les internautes à voir à qui s'adresser lorsque leurs droits fondamentaux sont violés.

Parallèlement à la Charte, nous disposons aussi d'un solide corpus de textes législatifs de l'UE qui sont en conformité avec les droits fondamentaux et renforcent la protection des droits les plus fondamentaux, par exemple les nouvelles règles de l'UE sur les droits des victimes ou la protection des données.

Malheureusement, nous sommes confrontés à une augmentation des crimes de haine et du discours de haine dans toute l'Europe. Les journalistes aussi sont visés. Ils finissent par s'autocensurer après avoir été menacés parce que la manière dont ils avaient rapporté des faits et des évènements n'a pas plu à quelqu'un.

Nous avons besoin d'une presse de qualité, d'une presse forte, pour donner les faits et faire échec aux fausses nouvelles, aux « fake news ».

Les médias sociaux se sont emparés de l'espace public. Internet n'est pas une zone où tout est permis, en particulier l'incitation publique à la violence et à la haine contre des minorités. Je suis heureuse de voir que les sociétés du Net qui ont signé le Code de conduite se sont engagées positivement.

Dans ce Code, Facebook, Twitter, YouTube et Microsoft se sont engagés à examiner en moins de 24 heures les notifications valides reçues de la part de citoyens ou de la société civile en vue du retrait de discours de haine illégaux. Ces acteurs du Net les évalueront également à la lumière des dispositions pénales nationales transposant les dispositions du droit communautaire.

Et nous devons absolument poursuivre nos efforts, par le biais du droit, par le biais du dialogue et, comme dans tous ces types de questions, par le biais de l'éducation.

Nous devrons également concentrer davantage nos travaux sur la littératie médiatique, la pensée critique et la promotion de narrations positives au niveau du terrain. Pour cela, nous comptons sur l'aide de l'Agence des droits fondamentaux.

Dans la défense des droits fondamentaux, de la démocratie et de l'État de droit, que les menaces viennent de l'intérieur ou de l'extérieur, il est impossible et hors de question de céder du terrain, nous sommes déterminés.

L.R.D.G. : Comment la protection des données à caractère personnel peut-elle contribuer à la lutte contre le terrorisme, le crime organisé et la cybercriminalité en Europe ?

La Commission européenne travaille de concert avec les pays de l'UE pour garantir la sécurité des citoyens de l'UE dans toute l'UE.

Les cyber-attaques et attentats terroristes qui se sont produits récemment ont mis en lumière la nécessité d'améliorer la coopération pour lutter contre le terrorisme, la criminalité organisée et la cybercriminalité en Europe.

Nous prenons actuellement plusieurs mesures pour répondre aux cyber-menaces et garantir la sécurité de l'Europe, par exemple, nous nous assurons que nos bases de données de l'UE sur la sécurité puissent mieux travailler ensemble et nous améliorons notre réponse aux cyber-attaques.

Dans cette bataille, l'élément clé est l'interopérabilité des systèmes d'information.

L'Europe doit relever ses défis en termes de sécurité en restant unie.

Des règles communes sur la protection des données permettront aux services répressifs et aux autorités judiciaires de coopérer plus efficacement, en même temps qu'elles

instaureront la confiance et garantiront la certitude juridique.

En avril 2016, nous avons adopté la Directive Protection des données pour les services de police et les autorités de justice pénale. De plus, l'Union européenne a négocié avec les États-Unis un accord-cadre international, l'Accord dit "Data Protection Umbrella Agreement", pour garantir un niveau élevé de protection des données personnelles transférées entre l'UE et les États-Unis pour la prévention, la détection, l'enquête et la poursuite de délits pénaux, y compris le terrorisme.

Il y a cependant encore moyen de faire mieux.

La cyber-résilience et la cybersécurité doivent être encore renforcées et nous travaillons à combler les failles du cadre actuel de cyber-sécurité. La Commission vient de présenter un règlement sur la cyber-sécurité qui prévoit notamment un fonds d'urgence dans ce domaine, lequel permettra d'aider les pays confrontés à des cyberattaques graves, mais également le renforcement de l'ENISA, l'agence cyber de l'UE, qui recevra 12 millions € supplémentaires chaque année et verra ses équipes étoffées de 41 personnes de plus.

Dans le domaine de la justice pénale, la Commission explore toutes les actions législatives possibles pour améliorer l'accès transfrontière à **la preuve électronique.** La Commission examine aussi actuellement les défis que pose l'utilisation d'outils de **cryptage** par les criminels et rendra compte de ses conclusions d'ici octobre 2017.

L.R.D.G. : Quelles ont été les mesures prises par la Commission européenne pour lutter contre la radicalisation dans le domaine de la justice pénale ?

En octobre 2015, j'ai organisé une conférence à haut niveau sur les moyens de lutter contre la radicalisation dans le système de justice pénale, afin de faire une synthèse de l'expérience des différents pays. Nous allons organiser un évènement similaire au printemps 2018.

La Commission travaille depuis 2015 avec des sociétés clés du net, notamment par le biais du Forum Internet de l'UE, en vue de détecter et de supprimer les contenus terroristes en ligne. Pour compléter les travaux du Service d'Europol chargé de demander le retrait de contenus (l'Internet Referral Unit - IRU), la Commission a invité tous les États membres à établir des IRU au niveau national.

La Commission va très rapidement établir un Groupe d'experts de haut niveau sur la radicalisation pour faciliter la poursuite de l'élaboration des politiques de l'UE dans ce domaine et en renforcer l'impact. Le Réseau RAN (Radicalisation Awareness Network) réalisera aussi une série d'ateliers destinés aux autorités nationales sur les combattants terroristes de retour.

De plus, dans le cadre de mesures à long terme contre la radicalisation, la Commission continuera de soutenir l'inclusion et l'intégration sociales par le biais d'initiatives telles qu'Erasmus +, le Pilier européen des droits sociaux ainsi que de travailler avec des pays partenaires par le biais de formations ciblées et d'un soutien financier.

L.R.D.G. : À l'occasion du Conseil Justice et Affaires intérieures, le 8 juin 2017 à Luxembourg, vingt États européens ont ratifié une proposition de règlement établissant la création du Parquet européen. Le Parlement européen doit maintenant donner son accord. Quelles sont les raisons qui ont présidé à la création de ce Parquet ?

La criminalité ne s'arrête pas aux frontière d'un pays, que ce soit dans l'UE ou ailleurs. Les pertes infligées au budget de l'Union – en définitive, l'argent des contribuables – sont significatives et représentent des milliards d'euros. Nos économies en pâtissent et les contribuables perdent confiance dans les institutions nationales autant qu'européennes. Il est de notre devoir de lutter contre cette criminalité, ce qui ne peut se faire qu'en conjuguant nos forces.

Actuellement, les autorités nationales sont responsables du suivi des affaires de fraude dans l'UE, mais leur compétence s'arrête aux frontières de leur pays. Nous ne pouvons ignorer la réalité d'aujourd'hui : en Europe, les personnes, y compris quand il s'agit de criminels, circulent librement. Les mesures de coopération entre les États membres sont encore très longues et complexes, et le niveau d'efficacité et de dissuasion reste encore insatisfaisant. Nous sommes confrontés à un problème européen, c'est pourquoi nous avons besoin d'une solution européenne.

Nous avons besoin d'une approche cohérente pour lutter contre les crimes à l'encontre

du budget de l'UE afin de garantir que la justice s'applique partout, ce qui est aussi une condition sine qua non pour l'égalité d'accès aux fonds communautaires et une concurrence loyale.

Les organes de l'Union existants, tels que l'OLAF, Eurojust et Europol, ne disposent pas des compétences nécessaires pour mener des enquêtes et poursuites pénales dans les États membres.

Avec l'EPPO (European Public Prosecutor's Office), il s'agit d'établir un organe de poursuite très spécialisé, entièrement dédié à la lutte contre la criminalité visant les intérêts financiers de l'UE dans toute l'UE. Cela aboutira à augmenter le nombre de poursuites, de condamnations et à récupérer davantage de fonds de l'Union perdus frauduleusement.

L.R.D.G. : Quels sont les différents points d'achoppement auxquels certains pays, tels que les Pays-Bas, la Suède et la Hongrie en particulier, ont été confrontés et qui nous empêchent d'avancer sur un projet prévu par tous les traités depuis 2009, et qui nous obligent à en passer par une coopération renforcée ?

Le droit pénal est indubitablement un domaine sensible et le Parquet européen est sans nul doute un énorme pas en avant sur la voie de l'établissement d'un véritable espace européen de justice pénale. Tous les États membres ne souhaitent pas s'associer au Parquet européen et je respecte pleinement leur décision.

Néanmoins, la protection du budget de l'Union contre les crimes est une obligation à la fois pour l'UE et pour tous les États membres. Riche de 20 États membres qui se sont associés à cette instauration, le Parquet européen apportera davantage de justice et des avantages accrus par rapport à la situation qui est la nôtre aujourd'hui, outre qu'il créera de la confiance et que les autres États membres pourront toujours le rejoindre ultérieurement.

L.R.D.G. : L'article 86 du Traité sur le fonctionnement de l'Union européenne (TFUE) prévoit qu'un Parquet européen peut être établi à partir d'Eurojust. Quels seront à la fois son statut juridique et ses missions ?

Le mandat du Parquet européen et celui d'Eurojust sont différents. Le Parquet européen diligentera en toute indépendance des enquêtes et des poursuites dans des affaires de fraude aux intérêts financiers de l'UE ; Eurojust, quant à lui, continuera de faciliter la coopération entre autorités nationales. Les deux instances joueront un rôle important dans leurs domaines respectifs, le Parquet se concentrant sur les crimes financiers à l'encontre du budget de l'UE et Eurojust sur d'autres formes de crimes graves tels que le terrorisme et la cybercriminalité. Les deux instances maintiendront une étroite relation qui peut dégager des synergies significatives dont l'une comme l'autre tireront avantage – et l'ensemble de l'UE surtout.

L.R.D.G. : Comment sera organisé le Parquet européen ?

Le Parquet européen sera un organe de poursuite indépendant et décentralisé, placé sous la direction d'un procureur principal européen et fonctionnant comme un Parquet unique dans tous les États membres participants. Du fait de sa structure décentralisée, des procureurs européens délégués, situés dans les États membres, diligenteront les enquêtes et poursuivront les crimes contre le budget de l'UE. Les procureurs européens délégués, étant aussi procureurs nationaux, n'auront aucune difficulté avec le système juridique et la langue de leur État membre de rattachement et pourront donc diriger les services de poursuite nationaux et saisir les tribunaux nationaux. Au niveau central, il y aura un procureur européen pour chaque État membre participant ; organisés en Chambres permanentes, ils suivront et superviseront les enquêtes et poursuites diligentées par les Procureurs européens délégués.

Cette structure permet un sain équilibre entre le niveau décisionnel européen et national ; elle est le meilleur garant que le Parquet européen sera véritablement efficace et accepté au niveau des États membres.

L.R.D.G. : Quelle forme prendront les relations entre le Parquet européen et Europol ?

Le Parquet européen maintiendra aussi une relation étroite avec Europol, ce qui veut dire qu'il pourra demander des informations et un soutien analytique à Europol aux fins des enquêtes et poursuites dans des affaires de fraude aux intérêts de l'UE.

L.R.D.G. : Quelles seront les ressources humaines et matérielles dont sera doté le Parquet européen ?

Le Parquet européen étant l'acteur clé dans la lutte contre les crimes visant le budget de l'Union, tout

sera fait pour qu'il soit doté de ressources nécessaires à sa mission. Du fait de sa structure décentralisée et intégrée, et puisque le Parquet européen réduira dans une large mesure la charge de travail d'autres organes tel que l'OLAF et Eurojust qui assurent actuellement le suivi d'affaires de fraude contre les intérêts de l'UE, le Parquet européen sera très rentable sur le plan budgétaire. Du point de vue des ressources humaines, j'estime que le Parquet au niveau central fonctionnera avec quelque 110 personnes, dont une grande partie émanant des organes que j'ai mentionnés, avec un nombre limité de procureurs européens délégués dans les États membres. Nous sommes actuellement en train de finaliser les états financiers (« Legislative Financial Statement »), autrement dit le budget pour le Parquet européen, mais voilà comment je vois le fonctionnement du Parquet européen à l'avenir.

L.R.D.G. : Quel sera le processus de sélection du procureur principal qui dirigera le Parquet financier européen ?

Le procureur européen principal sera nommé par le Parlement européen et le Conseil pour un mandat non renouvelable de sept ans. Les procureurs européens seront nommés par le Conseil pour un mandat non renouvelable de six ans, et les procureurs européens délégués seront nommés par le Collège des Procureurs européens pour un mandat renouvelable de cinq ans. Je voudrais souligner une fois encore que tous les procureurs travaillant avec le Parquet européen seront indépendants.

L.R.D.G. : Quel est le calendrier des opérations jusqu'au démarrage du Parquet européen ?

Le Conseil est parvenu à un accord politique sur le Règlement du Parquet européen le 8 juin 2017 et a transmis ce texte législatif au Parlement européen pour que celui-ci donne son consentement. Une fois ce consentement donné, le Règlement sur le Parquet européen pourra être adopté par le Conseil, ce qui pourrait intervenir en octobre de cette année.

Le Règlement prévoit que le Parquet européen prendra ses fonctions au plus tôt trois ans après l'entrée en vigueur du Règlement. Durant ces trois années, le Parquet européen sera progressivement mis en place, le personnel recruté et les procureurs nommés. N'oublions pas que les États membres doivent aussi transposer la Directive sur la lutte contre la fraude et la protection des intérêts financiers de l'Union européenne par le droit pénal, dite Directive PIF. Cette Directive, adoptée le 5 juillet 2017, est essentielle pour le Parquet européen puisqu'elle donne les définitions des infractions pénales relevant de la compétence de ce dernier. Les États membres ont deux ans pour transposer la Directive.

L.R.D.G. : Le Parquet européen aura à traiter d'enquêtes complexes concernant des fraudes aux Fonds structurels et à la TVA transfrontière, pour lesquelles il faudra peut-être dispenser une formation spécifique aux procureurs de chaque État membre de l'UE. Un volet de formation spécifique aux investigations financières est-il prévu ?

Une formation complète non seulement pour le personnel du Parquet européen mais aussi pour les autorités nationales compétentes qui travailleront avec celui-ci, par exemple la police, les douanes et les services fiscaux, est envisagée et sera dispensée durant la phase préparatoire de trois ans avant l'entrée en fonction du Parquet européen et ultérieurement à cette entrée en fonction.

L.R.D.G. : Quelle forme prendront les relations avec les États membres de l'UE qui ne sont pas liés par la coopération renforcée ?

Je voudrais rappeler que tous les États membres, et pas uniquement ceux qui participent au Parquet européen, ont l'obligation de lutter contre les infractions portant atteinte au budget de l'Union. C'est pour cette raison que nous avons besoin d'une coopération étroite et efficace entre les États membres qui ne participent pas au Parquet européen. Pour cela, il est envisagé de conclure des arrangements de travail, qui porteront sur des problématiques telles que l'échange d'information, la désignation de points de contact pour faciliter la coopération. Le Parquet européen pourrait aussi utiliser les instruments juridiques en vigueur à disposition au niveau de l'Union pour coopérer avec des États membres qui ne participent pas au Parquet européen. Mon objectif, toutefois, demeure qu'à un certain moment, et le plus tôt sera le mieux, tous les États membres participent au Parquet européen.

VĚRA JOUROVÁ, EUROPEAN COMMISSIONER FOR JUSTICE, CONSUMERS AND GENDER EQUALITY

INTERVIEW BY JOCELYNE KAN

L.R.D.G. : Can you describe your different missions at the European Commission ?

As Commissioner for Justice, Consumers and Gender Equality, my work is is based on the European values spelt out in the Treaties and in the Charter of Fundamental Rights.

I work to protect our core values, especially the Rule of Law, inside and outside of Europe. I am also in charge of ensuring that discrimination is fought against and gender equality is promoted. As part of the Digital Single Market team, I contribute to developing a connected digital single market base on clear data protection rules and where consumer rules are protected online as well. In this area, I've also set up a framework, the EU-U.S. Privacy Shield, to guarantee that personal data transferred to the U.S. are duly protected by high data protection standards. Finally my team and I fight against criminal matters and terrorism by reinforcing judicial cooperation in. This includes the setting up of the European Public Prosecutor's Office to tackle cross border tax evasion and fraud worth billions of euros every year. We also proposed new rules to prevent money laundering and terrorist financing.

L.R.D.G. : The Charter of Fundamental Rights, implemented by the European Union (EU) state members in 1989, is currently facing several difficulties such as the waves of refugees, the economic imbalance and terrorist attacks. How has it been enforced ?

In times of crisis, people question the ability of institutions and systems to deliver and protect them from such challenges.

We must never lose sight of our values in our efforts to deal with such challenges.

Today, we have an EU Agency for fundamental Rights that works closely with other EU Agencies for a better protection of people's fundamental rights.

We mainstream the legally binding Charter of fundamental rights in all Commission legislative proposals and policies. This means that the Commission's proposals are not only systematically vetted for their economic and social effects. They undergo a detailed fundamental rights assessment.

This new fundamental rights culture must however spread further into the EU's legislative process and all the way to implementation on the ground. One of the frustrations of citizens when it comes to the Charter is its

limited scope of application in the Member States, as they are only under the obligation to respect it when implementing EU law.

Our e-justice Portal contains a clear explanation on the scope of application of the Charter and since last October it also includes a "fundamental rights wizard" which helps people to identify where to turn to when their fundamental rights are being violated.

Next to the Charter, we now also have a sound body of EU laws that are fundamental rights compliant and strengthen the protection of people's most fundamental rights – for example - the new EU rules on victims' rights or Data protection. These have a direct effect on people's lives.

Unfortunately, we observe an increase in hate crimes and hate speech throughout Europe. This also targets journalists who end up self-censoring because they get threats when they write about facts and events that are not to the liking of some.

We need a strong quality press to give the facts and defeat fake news.

Social media have occupied the public space. Internet is not a free haven for public incitement to violence and hatred against minorities. I am happy to see a positive engagement by the internet companies who signed up to the Code of conduct.

In this Code, Facebook, Twitter, YouTube and Microsoft have committed to review in less than 24 hours valid notifications received from citizens and civil society for removal of illegal hate speech. They will also assess them in the light of national criminal laws transposing EU law.

And we must continue our efforts, through the law, through dialogue and, as in all such matters, through education.

We will also need to further concentrate our work on media literacy, critical thinking and promoting positive narratives at grassroots level. For this, we count on the Fundamental Rights Agency to help.

We cannot and will not yield when it comes to upholding fundamental rights, democracy and the rule of law, whether threats come from the inside or outside.

L.R.D.G. : How can the protection of private data contribute to the combat against terrorism, organized crime and cybercrime in Europe ?

The European Commission is working together with EU countries to ensure the security of EU citizens across the EU.

The recent cyberattacks and the terror attacks have highlighted the need to improve cooperation to fight terrorism, organized crime and cybercrime in Europe.

We are taking several measures to tackle the cyber threats and to keep Europe safe, like making sure our EU security databases can work better together and improving our response to cyberattacks.

Interoperability of information systems is key in this battle.

Europe must face its security challenges together.

Common rules on data protection will enable law enforcement and judicial authorities to cooperate more effectively with each other, as well as building confidence and ensuring legal certainty.

In April 2016, we adopted the Data Protection Directive for police and criminal justice authorities.

In addition, the European Union has negotiated with the United States an international framework agreement, the "Data Protection Umbrella Agreement", in order to ensure a high level protection of personal data transferred between the EU and the US for the prevention, detection, investigation and prosecution of criminal offences, including terrorism.

Nonetheless, there is still room for improvement.

Cyber resilience and cybersecurity need to be strengthened even further and we are working to close the gaps in the current cybersecurity framework. The Commission just presented a cybersecurity regulation, which includes a cybersecurity emergency fund to help countries facing serious cyberattacks and the reinforcement of ENISA, the EU's cyber agency with an additional €12 million yearly, and 41 more staff.

In the field of criminal justice the Commission is looking into possible legislative action to improve cross border access to electronic evidence. The Commission is

also examining the challenges posed by the use of encryption by criminals and will report on its findings by October 2017.

L.R.D.G. : What measures have been taken by the European Commission for combating radicalisation in the field of criminal justice ?

I've organised a high level conference on tackling radicalisation in the criminal justice system in October 2015 to bring together the experience of the different countries. We'll follow up with a similar event in spring 2018.

The Commission has been working with key internet companies since 2015 including through the EU Internet Forum to detect and remove online terrorist content. To complement the work of Europol's Internet Referral Unit, the Commission has called on all Member States to establish national Internet Referral Units.

The Commission will swiftly establish a High-Level Expert Group on Radicalisation to facilitate the further development and enhance the impact of EU policies in this area. The Radicalisation Awareness Network (RAN) will also carry out a series of workshops on returning terrorist fighters for national authorities.

In addition, as part of long-term measures against radicalisation, the Commission will continue to support social inclusion and integration through initiatives such as Erasmus +, the European Pillar of Social Rights as well as work with partner countries through targeted training and financial support.

L.R.D.G. : At the Justice and Home Affairs Council on 8th of June 2017 in Luxemburg, twenty European states ratified a regulation proposal establishing the creation of the European Public Prosecutor's Office. The European Parliament must now give its agreement. What are the reasons that lead to the creation of such an office ?

Crime does not stop at national borders, neither in the EU, nor elsewhere. The damage caused to the Union budget – being ultimately taxpayers' money – is significant and amounts to billions of Euros. This is harming our economies and decreasing trust of tax payers in the national as well as the European institutions. It is our duty to fight against this crime which can be done only by joining forces.

Currently, national authorities are responsible for the follow-up of EU fraud cases but their powers end at national borders. We cannot ignore today's reality in Europe, where people, including criminals, circulate freely. Cooperation procedures amongst Member States are still lengthy and complex and the level of effectiveness and deterrence is still unsatisfying. We are facing a European problem and this is why we need a European solution.

We need a coherent and consistent approach to fight crimes against the EU budget in order to ensure that justice is served everywhere. This is also a prerequisite for an equal access to EU funds and fair competition.

The existing Union bodies, such as OLAF, Eurojust and Europol do not have the necessary powers to conduct criminal investigation and prosecutions in the Member States.

The idea of the EPPO is to establish a highly specialised prosecution body, fully dedicated to the fight against crimes against the EU budget across the EU.

This will lead to a greater number of prosecutions, convictions and a higher level of recovery of fraudulently lost Union funds.

L.R.D.G. : What are the different issues some countries have been facing, such as Netherland, Sweden and Hungary in particular, that prevent us from going forward into the project planned by all treaties since 2009, and that are requiring to get through an enhanced cooperation ?

Criminal law is without doubt a sensitive area and the EPPO is certainly a leap forward in the development of a truly European area of criminal justice. Not all Member States wish to join the EPPO and I fully respect their decision.

Protecting the Union budget against crimes is however a duty for the EU and all Member States. With 20 Member States on board, the EPPO will bring more justice and greater benefits compared to today's situation. This is conducive to creating trust and will also allow the other Member States to join in at a later stage.

L.R.D.G. : The article 86 of the Treaty on the Functioning of

the European Union (TFUE) provides that it may be established a European Public Prosecutor's Office from Eurojust. What will be both its legal status and its missions ?

The mandates of EPPO and Eurojust differ. While EPPO will independently carry out investigations and prosecutions into EU fraud, Eurojust will continue to facilitate cooperation between national authorities. Both will play an important role in their respective areas, with the EPPO focusing on financial crime against the EU budget and Eurojust on other forms of serious crime, such as terrorism and cybercrime. They will maintain a close relationship, which may lead to significant synergies to the benefit of both institutions - and more specifically to the benefit of the whole EU.

L.R.D.G. : How will the European Public Prosecutor's Office be organized ?

The EPPO will be an independent and decentralised prosecutorial body headed by a European Chief Prosecutor and operating as a single office across all participating Member States. The decentralised structure means that European Delegated Prosecutors will be located in the Member States and investigate and prosecute crimes against the EU budget. Being also national Public Prosecutors, the European Delegated Prosecutors will be familiar with the legal system and the language of the Member State where they are located. In this way they will be able to direct the national law enforcement authorities and bring cases before national courts for decision. At the central level there will be one European Prosecutor from each participating Member State, who – organised in so called Permanent Chambers – will monitor and supervise the investigations and prosecutions carried out by the European Delegated Prosecutors.

This structure offers a sound balance between European and national decision making, as well as the best chance that the EPPO will truly be effective and accepted at Member State level.

L.R.D.G. : What will the relationships between the European Public Prosecutor's Office and Europol be like ?

The EPPO will also maintain a close relationship with Europol. This means that EPPO will be able to request information and analytical support from Europol for the purpose of investigations and prosecutions of EU fraud cases.

L.R.D.G. : With what human and material resources the European Public Prosecutor's Office will be able to work ?

As the key actor to fight crimes against the EU budget, it will be ensured that the EPPO will be equipped with the necessary resources. Because of its decentralised and integrated structure and the fact that the EPPO to a large extent will decrease the workload of other bodies which are currently involved in following up on cases of EU fraud, such as OLAF and Eurojust , the EPPO budget will be very cost efficient. From a human resources point of view, I estimate that the central EPPO will operate with around 110 staff, a great part of which will come from the bodies I have mentioned, as well as a limited number of European Delegated Prosecutors in Member States. We are currently in the process of finalising the so called "Legislative Financial Statement", i.e. the budget for the EPPO but this is the way I see the EPPO operating in the future.

L.R.D.G. : By what process the head of the European Public Prosecutor's Office will be chosen ?

The European Chief Prosecutor will be appointed by the European Parliament and the Council for a non-renewable term of seven years. The European Prosecutors will be appointed by the Council for a non-renewable term of six years, while the European Delegated Prosecutors will be appointed by the College of European Prosecutors for a renewable term of five years. Let me underline again that all Prosecutors working with the EPPO will be independent.

L.R.D.G. : What will the timetable be until the start of the European Public Prosecutor's Office ?

The Council found a political agreement on the EPPO Regulation on 8 June 2017 and transmitted this legislative act to the European Parliament in order to obtain its consent. After the Parliament gave its consent, the EPPO Regulation can be adopted by the Council, which could ten-

tatively happen in October this year.

The Regulation foresees that the EPPO will assume its tasks not earlier than three years after the entry into force of the Regulation. During this time period the EPPO will be gradually built-up, staff recruited and the Prosecutors appointed. We must also not forget that the Member States need to transpose the Directive on the fight against fraud to the EU's financial interests by means of criminal law, the so called PIF Directive. This Directive, which was adopted on 5 July 2017, is essential for the EPPO as it provides the definitions of criminal offences falling within the EPPO's competence. Member States have two years to transpose the Directive.

L.R.D.G. : The European Public Prosecutor's Office will have to deal with complex investigations regarding frauds of both Structural Funds and the cross-border VAT, which, may require a particular training for the prosecutors of each EU member state. Is that a specific financial investigations training component planned ?

A comprehensive training not only of EPPO staff but also competent national authorities who will work with the EPPO, such as police, customs and tax authorities, is envisaged and will be conducted during the three year build-up phase of the EPPO and thereafter.

L.R.D.G. : What will the relationships with the EU member states that are not bound by the enhanced cooperation be like ?

Let me stress that all Member States are obliged to fight crimes affecting the Union budget, not only those participating in the EPPO. This is why we need a close and effective cooperation between those Member States which do not participate in the EPPO. For that purpose it is envisaged to conclude working arrangements, which contain issues such as exchange of information, designation of contact points to facilitate cooperation. The EPPO might also use the current legal instruments available at Union level to cooperate with Member States who do not participate in the EPPO. My goal remains, however, that at one point in time, hopefully sooner than later, all Member States will participate in the EPPO.

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

« QUELLES STRATÉGIES POUR LUTTER CONTRE LA PROSTITUTION ET LA TRAITE DES ÊTRES HUMAINS À DES FINS SEXUELLES ? L'EXEMPLE DE L'EUROPE »

CATHERINE GOLDMANN

CHARGÉE DE COMMUNICATION ET DE DOCUMENTATION À LA FONDATION SCELLES (WWW.FONDATIONSCELLES.ORG/)

L'exploitation sexuelle, sous ses diverses formes de prostitution, traite des êtres humains, tourisme sexuel, pornographie..., est aujourd'hui un phénomène qui dépasse les frontières. Dans ce vaste marché mondialisé, les exploiteurs, de plus en plus innovants, ne reculent devant rien, les techniques d'exploitation, enrichies par le développement des nouvelles technologies, ne cessent de se perfectionner et les victimes sont toujours plus nombreuses et plus jeunes.

Plus de 20 millions de personnes sont victimes de traite des êtres humains dans le monde. 22% d'entre elles (soit environ 4.5 millions) le sont à des fins d'exploitation sexuelle. Il s'agit, à plus de 95%, de femmes et d'enfants[1]. En France, on compte approximativement 37 000 personnes prostituées, dont 85% de femmes[2]. Selon les estimations, 93% de ces personnes sont de nationalité étrangère, la plupart venant des pays d'Europe de l'Est (Roumanie et Bulgarie), d'Afrique de l'Ouest (Nigéria) et de Chine[3].

Face à ces chiffres, le nombre des poursuites et des condamnations paraît dérisoire : 4 079 personnes poursuivies pour traite des êtres humains en Europe (en 2013-2014), 3 129 personnes condamnées (pour la même période), environ 600 condamnations pour proxénétisme en France[4].

Les États prennent progressivement conscience de la gravité et de l'ampleur des phénomènes d'exploitation sexuelle : des commissions discutent, des lois sont adoptées, des coopérations judiciaires ou policières se construisent.... Mais le processus est lent et il y a urgence. Quels sont les enjeux ?

La défense des populations vulnérables. Ce sont les plus fragiles, ceux et celles que nos sociétés devraient protéger en priorité, qui sont exploités : femmes, enfants, personnes migrantes et/ou issues des minorités, victimes de conflits armés, victimes de catastrophes naturelles, personnes en précarité, victimes de discrimination ethnique ou de genre, victimes de violences et traumatismes.... Cet état de vulnérabilité caractérise l'exploitation de la prostitution.

La protection des mineurs. Face aux dangers d'exploitation sexuelle, les mineurs, qu'ils soient à Bangkok, Paris, Montréal ou Delhi, sont les plus exposés. Enfants vendus par leur famille pour leur donner quelque espoir d'avenir ou assurer la survie des siens, enfants des rues, jeunes en fugue et en rupture familiale, adolescents abusés sur les réseaux sociaux, jeunes dans une « débrouille » aux relents de prostitution.... Sur l'ensemble des victimes de traite des êtres humains, 48% sont âgés de moins de 18 ans. En France, le nombre des victimes mineures demeure limité : la Brigade de protection des mineurs traite entre 20 et 60 cas

d'exploitation sexuelle de mineurs par an à Paris. Mais, si l'on en croit les associations, la réalité serait bien supérieure : de l'ordre de 6 000 à 10 000 mineurs prostitués en France[5].

La lutte contre la criminalité organisée. En même temps que le phénomène se mondialisait, le crime organisé transnational en a pris le contrôle. En effet, l'exploitation sexuelle assure une rentabilité maximale pour un investissement minimal et une prise de risque limitée. C'est aujourd'hui la 3e source de profits criminels, après le trafic des armes et des stupéfiants. Ses profits sont considérables. Selon des estimations, le chiffre d'affaires de l'industrie du sexe s'élèverait à plus de 1,5 milliard d'euros en Grèce (soit environ 0,70% du PIB du pays), plus de 2 milliards d'euros en Fédération de Russie, jusqu'à 18 milliards d'euros en Espagne[6]... En France, une étude du Centre des Hautes Etudes du Ministère de l'Intérieur (2014) estime les profits générés par la prostitution en France à 1,15 milliard d'euros[7].

La défense de l'économie légale. Loin d'appartenir à une économie parallèle, les profits tirés de l'exploitation sexuelle sont réinjectés dans l'économie légale, sous forme de corruption, blanchiments, investissements... Des milieux très divers sont concernés : agences de voyage, bars, hôtels, taxis, mais aussi patrons de presse, publicitaires, producteurs de sites internet, médias divers... Ainsi, l'exploitation sexuelle sous toutes ses formes s'immisce progressivement dans nos sociétés au risque de devenir un marché économique comme un autre contribuant à la croissance des États, au point que l'institut de statistiques de l'Union européenne, Eurostat, a proposé en 2014 aux pays membres d'accroître leur richesse nationale en incluant le chiffre d'affaires de cette économie souterraine (prostitution et stupéfiants) dans le calcul de leur PIB. Si la France a refusé, la Belgique, l'Espagne, le Royaume-Uni... se sont pliés à cette demande et ont ainsi relevé leur PIB d'environ 10 milliards d'euros[8].

I. Les politiques publiques face au système prostitutionnel : La guerre des modèles

Le 2 décembre 1949, l'Assemblée des Nations Unies adoptait la Convention pour la répression de la traite des êtres humains et de l'exploitation de la prostitution d'autrui. Dès le préambule, ce texte proclame, pour la première fois, que *« la prostitution et le mal qui l'accompagne, à savoir la traite des êtres humains, en vue de la prostitution, sont incompatibles avec la dignité et la valeur de la personne humaine et mettent en danger le bien-être de l'individu, de la famille et de la communauté ».*

Trente ans plus tard, en 1979, la Convention des Nations Unies pour l'élimination de toutes les formes de discrimination à l'égard des femmes (CEDAW) réaffirmait cet engagement abolitionniste et appelait les États parties à prendre *« toutes les mesures appropriées, y compris des dispositions législatives, pour supprimer sous toutes leurs formes, le trafic des femmes et l'exploitation de la prostitution des femmes »* (article 6).

Dans ce cadre, les États signataires, bien qu'enjoints à lutter contre les différentes formes d'exploitation sexuelle, ont toute latitude pour développer des politiques nationales en accord ou non avec les prescriptions internationales.

En Europe, au-delà des notions juridiques de prohibitionnisme, abolitionnisme et réglementarisme, deux approches, voire deux philosophies, s'affrontent : le modèle réglementariste, porté par les Pays-Bas et l'Allemagne, et le modèle néo-abolitionniste dit nordique, issu de la loi adoptée par la Suède en 1999. Les divergences entre ces deux modèles tournent autour de quelques points :

- La définition de la prostitution : une violence qui fait obstacle à l'égalité hommes/femmes ou un travail librement choisi, à distinguer d'une prostitution « forcée » englobant la traite criminelle ;

- Le statut des personnes prostituées : victimes à protéger ou travailleuses du sexe ;

- Le rôle joué par le client : responsable d'un système d'exploitation et de violences ou simple consommateur.

Il s'agit là d'un débat éminemment politique et controversé dans lequel il est difficile d'avoir un regard neutre. La France, dans ce débat, a fait son choix en 2016, en se ralliant au

modèle nordique. Quelles analyses ont conduit les parlementaires à faire ce choix ? Quel est le sens de ralliement ? Pour répondre à ces questions, il convient d'abord de revenir sur les contenus de ces deux politiques.

A. La vision de la Suède

Le 1er janvier 1999, la Suède, au nom de la défense des droits des femmes, devient le premier pays à incriminer l'achat d'actes sexuels, tout en exemptant les personnes prostituées de toute poursuite pénale. L'objectif du gouvernement est de mettre un coup d'arrêt au phénomène prostitutionnel, considéré comme un obstacle à l'égalité entre les femmes et les hommes et comme un véritable fléau pour la société toute entière.

Simon Haggström, chef de la brigade antiprostitution de Stockholm, explique plus précisément le sens de ce choix politique: *« En Suède, nous avons choisi de ne pas pénaliser le « vendeur » de services sexuels, parce que nous l'avons regardé comme une victime dans la plupart des cas et que le pénaliser, cela reviendrait à fragiliser encore plus une personne qui est déjà en difficulté. En pénalisant le client, le législateur, la société dans son ensemble, envoient un message plus positif aux individus qui se prostituent, en leur proposant de l'aide plutôt que de les sanctionner. La vente de services sexuels n'est pas punie, ni encouragée, le message c'est que la prostitution endommage l'individu et la société tout entière, c'est que la solution n'est pas de criminaliser, de punir les personnes prostituées, mais de les aider à s'en sortir. »*[9].

La loi sanctionne donc le fait d'obtenir (ou de tenter d'obtenir) une « relation sexuelle en contrepartie d'un paiement ». S'entend par « relations sexuelles » les rapports sexuels stricto sensu mais aussi tout autre acte de nature sexuelle. De même la notion de paiement renvoie à une rémunération en numéraire mais aussi à toute forme de rétribution en nature. Les peines encourues vont de l'amende, modulable en fonction des revenus, à un an d'emprisonnement. Un accompagnement thérapeutique est également proposé aux clients pour éviter tout risque de récidive.

La loi prévoit donc la protection et l'aide à la réinsertion de la personne prostituée et sanctionne l'achat et/ou la tentative d'achat d'un acte sexuel par une amende, une peine d'emprisonnement, un accompagnement thérapeutique.

Par ailleurs, la vision suédoise part du postulat que la prostitution n'est jamais libre et choisie. Elle trouve au contraire son origine dans un parcours de violence, de précarité et d'addiction. Dès lors, pénaliser les personnes qui se livrent à la prostitution viendrait donc encore amoindrir leurs possibilités de sortie de ce milieu et de réinsertion. Plutôt que de pénaliser les personnes prostituées, la loi prévoit la mise en place de programmes d'accompagnement pour permettre leur sortie de la prostitution.

B. Le pragmatisme des Pays-Bas et de l'Allemagne

En 2000, les Pays-Bas puis l'Allemagne (en 2002) optaient pour une politique radicalement opposée. La prostitution est considérée comme un fait social, détaché de tout débat éthique, qu'il faut encadrer et réguler. Seules la traite des êtres humains à des fins sexuelles et la prostitution des mineurs sont pénalisées.

Selon la chercheuse néerlandaise Karin Werkman, *« cette loi (des Pays-Bas) est l'expression d'une approche pragmatique de la prostitution. Elle se fonde sur l'idée que la prostitution est inévitable, qu'elle a toujours existé et qu'elle existera toujours. Dans cette optique, le mieux est de la rendre aussi sure et paisible que possible, en accordant un statut d'emploi et des conditions de travail aux femmes, en les « autonomisant » dans la prostitution (...). En outre, la loi repose sur l'idée qu'il existerait une prostitution « forcée », par définition la traite des êtres humains, et une prostitution « volontaire », considérée comme un choix et une profession : le « travail du sexe »... »*[10].

Dans ces pays, l'objectif est à la fois le contrôle par l'État en séparant la prostitution et ses « effets collatéraux » criminels et l'amélioration des conditions d'exercice pour les femmes. Le système juridique autorise donc et organise le système prostitutionnel : les maisons closes sont légalisées ; les personnes prostituées peuvent bénéficier d'une couverture sociale, signent des contrats de travail, sont enregistrées et contrôlées ; le proxénète est considéré comme un

chef d'entreprise, il ne peut pas tomber sous le coup de la loi, sauf si la personne, dont il tire un bénéfice, est mineure ou en situation illégale ; le client est un consommateur ordinaire qu'il faut attirer et satisfaire. La prostitution devient ainsi un métier comme un autre.

II. Allemagne, Pays-Bas : une prostitution difficilement contrôlée

Plus de dix ans après leur entrée en vigueur, les deux modèles affichent des résultats contrastés. En Allemagne ou aux Pays-Bas, qui ont fait le choix de dépénaliser le proxénétisme, la législation réglementariste et, du même coup, ses principes sous-jacents, n'ont pas atteint les objectifs fixés.

A. Le marché de la prostitution

La déréglementation a entraîné une explosion de la prostitution et du tourisme sexuel. Les Pays-Bas comptaient 2 500 personnes prostituées en 1981, entre 20 et 30 000 aujourd'hui, pour un chiffre d'affaires d'environ un milliard d'euros ; l'Allemagne comptait entre 3 000 et 3 500 établissements de prostitution en 2013, qui auraient généré 5,475 milliards d'euros de chiffre d'affaires, entre 100 000 et 200 000 personnes prostituées, 1,5 million d'hommes rencontreraient chaque jour des personnes prostituées[11]...

Un marché clandestin de la prostitution, en dehors de tout contrôle officiel, s'est développé dans des salons de massage, des appartements... Une large partie de ce marché est encore entre les mains du crime organisé. Malgré la loi, malgré une politique développée de lutte contre la traite des êtres humains (en particulier aux Pays-Bas[12]), les réseaux et les mafias ont en effet pris une place croissante dans « l'industrie du sexe », y compris dans les établissements légaux. Le nombre de victimes identifiées augmente chaque année dans ces pays. Et si l'on en croit les observateurs *« Nous ne voyons que la partie visible de l'iceberg »*[13].

B. La situation des personnes prostituées

Contrairement à ce qui avait été imaginé, l'image sociale de la prostitution n'a pas véritablement évolué dans ces pays et la stigmatisation reste forte, au point que la grande majorité des personnes prostituées ont préféré rester dans l'anonymat et ne sont pas entrées dans le système de protection sociale. En Allemagne, seul 1% des personnes prostituées (soit 44 femmes) bénéficie d'une protection sociale ; aux Pays-Bas, 5% des personnes prostituées sont enregistrées[14].

D'autre part, la réglementation ne protège pas les femmes de la violence. Dès 2004, une enquête du ministère allemand des Affaires sociales soulignait l'omniprésence de la violence dans les milieux de prostitution : 87% des femmes prostituées interrogées avaient subi des violences physiques, 82% des violences psychologiques, 59% des violences sexuelles[15]. D'autres rapports de police indiquent qu'au moins 50% des personnes prostituées ont été au moins une fois victimes de violences de la part des clients ou des proxénètes[16]. Les conditions d'exercice qu'on leur impose sont souvent inhumaines, et contraires à la dignité de la personne : refus de soins médicaux, des formes de prostitution d'abattage...

C. La perception de la prostitution

Au-delà des données chiffrées, la loi, en normalisant l'achat d'actes sexuels a provoqué une véritable industrialisation du commerce du sexe. Le proxénète, en Allemagne en particulier, est devenu un modèle entrepreneurial, qui crée des méga-bordels, sorte de supermarchés du sexe et du bien-être masculin, pouvant accueillir jusqu'à 1000 clients par jour. Poussant la logique libérale jusqu'au bout, les méga-bordels se multiplient, toujours plus grands, toujours plus rutilants ; ils proposent des forfaits discount attrayants, étalent leur publicité sur les murs des villes, sont les vedettes de programmes de télévision ....[17].

Bordell Deutschland - Wie der Staat Frauenhandel und Prostitution fördert, titrait l'hebdomadaire allemand *Der Spiegel* en mai 2013[18]. Et, depuis 2007, la ville d'Amsterdam, généralement considérée comme un des premiers centres européens de tourisme sexuel, s'efforce de réduire le nombre des vitrines de prostitution pour lutter contre la criminalité croissante. Aux Pays-Bas comme en Allemagne, les profonds dysfonctionnements des lois réglementaristes sont aujourd'hui reconnus et un nombre

croissant d'élus n'hésitent pas à dénoncer des formes d'exploitation, de violence et de criminalité.

Depuis plusieurs années, ces deux pays sont à la recherche d'une évolution législative. Cette réflexion les a d'ailleurs menés à étudier le modèle nordique et à envisager l'éventualité de pénaliser le client. Pour autant, l'importance des profits enregistrés bloque ou ralentit le processus législatif et les avancées possibles. Les Pays-Bas continuent à renvoyer d'une Assemblée parlementaire à l'autre un projet de loi en débat depuis 2009, et l'Allemagne, après plusieurs mois de débats, vient d'adopter une loi contestée de tous bords[19], les uns parce qu'elle met des obstacles au développement de l'industrie du sexe, les autres parce qu'elle est insuffisante pour modifier la situation en profondeur.

III. Suède : la prostitution n'est plus acceptée, ni acceptable

En 2010, soit dix ans après l'entrée en vigueur de la loi sur la prostitution, une commission gouvernementale présidée par la Chancelière Anna Skarhed, évaluait ses effets et saluait son plein succès[20].

A. Le marché de la prostitution

La prostitution de rue a diminué de moitié. *« On estime que la Suède comptait 3 000 personnes prostituées dans les années 1970, 2 500 en 1995 et un millier aujourd'hui »,* explique Simon Haggström, chef de la brigade antiprostitution de Stockholm. Stockholm, pour 2 millions d'habitants, comptait en moyenne 80 personnes prostituées en activité simultanée avant la loi. Il y en aurait une quinzaine aujourd'hui[21].

La loi a eu un effet dissuasif sur les clients potentiels qui hésitent désormais à acheter une prestation sexuelle : en 1996, 13,6 % des hommes déclaraient avoir acheté des services sexuels ; dans une enquête récente, leur proportion est de 7,9 %[22].

Cette évolution n'a pas été accompagnée de l'émergence de nouveaux lieux de prostitution ou d'une augmentation du phénomène ailleurs. Aux détracteurs qui affirment que la prostitution s'est reportée sur internet, le gouvernement suédois répond que la prostitution a effectivement augmenté sur internet, mais dans des proportions bien moindres que dans les pays voisins.

La traite des êtres humains n'a pas connu les mêmes développements que dans les pays voisins *:« La Suède passe désormais pour un « mauvais marché » auprès des proxénètes, explique Simon Haggström. Nous le savons à travers des enregistrements téléphoniques qui montrent clairement la difficulté de s'implanter et la préférence des proxénètes pour d'autres pays signe que la loi a contrecarré la criminalité organisée et détourné les réseaux internationaux vers des pays plus « accueillants »*[23].

B. La situation des personnes prostituées

Avec une diminution des violences et une multiplication des mesures sociales en leur faveur, la situation des personnes prostituées se serait améliorée. La Suède serait même un des pays d'Europe où le taux de violences sur les personnes prostituées est le plus faible. Les mesures en faveur des victimes ont été renforcées par plusieurs textes entrés en vigueur depuis la promulgation de la loi : mise en oeuvre de programmes de sortie de la prostitution, intégration dans le régime social... De manière plus générale, l'évolution de l'image de la prostitution a libéré la parole des personnes prostituées, désormais plus confiantes dans l'aide apportée par les services de police et plus disposées à coopérer dans les cas de traite des êtres humains.

C. La perception de la prostitution

Les mentalités ont évolué. Une des ambitions de la loi suédoise était en effet de sensibiliser l'ensemble de la population aux questions relatives à la prostitution afin que ce phénomène ne soit plus banalisé. Campagnes d'information nationale, éducation dans les écoles, formations auprès des acteurs concernés.... En 10 ans, le nombre de personnes favorables à la pénalisation des clients est passé d'environ 30% à plus de 70% de la population totale (en 2014). L'achat d'un acte sexuel n'est plus un acte normalisé et accepté.

Bien que ces conclusions aient été corroborées par d'autres évaluations (en particulier en 2015), la loi est l'objet, aujourd'hui encore, d'une critique assez vive[24] : ses principes sont

régulièrement remis en cause, les méthodes d'évaluation et leurs résultats sont contestés... Pour autant, la loi suédoise est devenue un modèle, le modèle nordique, reconnu par les autorités nationales mais aussi par les instances internationales. En mai 2014, dans son Rapport final sur la législation suédoise, le Groupe d'experts sur la lutte contre la traite des êtres humains (GRETA) se félicitait *« des mesures adoptées par les autorités suédoises pour lutter contre la traite des êtres humains et soutenir les victimes...* ». De même, le Parlement européen, dans sa résolution du 26 février 2014, voit lui-même dans l'approche légale du phénomène prostitutionnel prônée par la Suède un moyen de « *lutter contre la traite des femmes et des filles à des fins d'exploitation sexuelle et d'améliorer l'égalité entre les hommes et les femmes* »[25]. Et plusieurs pays se sont inspirés de ce modèle pour faire évoluer leur législation dans le même sens : pénalisation des clients et des proxénètes, protection des personnes prostituées, programmes de sensibilisation, de prévention et de réinsertion des victimes. Ainsi la Norvège en 2008, l'Islande en 2009, l'Irlande du Nord en 2015, la France en 2016 et l'Irlande en 2017, sans oublier le Canada en 2014 et, bientôt, Israël, ont aujourd'hui adopté le modèle nordique.

IV. Le choix de la France : la loi du 13 avril 2016

Le chemin avant d'arriver à l'adoption de la loi « *visant à renforcer la lutte contre le système prostitutionnel et à accompagner les personnes prostituées* » a réclamé près de six années de débat, d'analyses et de controverses avant d'en arriver là. Depuis 2010, la France est mobilisée pour prévenir et combattre la traite des êtres humains et la prostitution. Cette mobilisation a connu plusieurs étapes :

- La lutte contre les violences faites aux femmes est Grande cause nationale en 2010. À la demande des associations, « la prostitution et la traite qui en découle » sont inscrites dans la liste des violences à combattre.

- Le plan interministériel de lutte contre les violences faites aux femmes 2011-2013 prend en compte la prostitution : l'achat d'un acte sexuel est dénoncé comme une violence.

- Une mission parlementaire sur la prostitution, présidée par Danielle Bousquet, est constituée. Elle rend ses conclusions en avril 2011 : « *Prostitution, l'exigence de responsabilité : en finir avec le mythe du plus vieux métier du monde* ». Elle dresse un état des lieux de la prostitution en France ; elle propose une trentaine de recommandations qui constituent les premiers éléments de la loi actuelle.

- La Mission interministérielle pour la protection des femmes contre les violences et la lutte contre la traite des êtres humains, la MIPROF, est créée en 2013.

- Le premier plan d'action national contre la traite des êtres humains (2014-2016), axé sur la protection des victimes et la poursuite des auteurs, est mis en oeuvre.

- La loi du 13 avril 2016 « visant à renforcer la lutte contre le système prostitutionnel et accompagner les personnes prostituées » est adoptée, après plus de deux ans de débats parlementaires.

En 2011, l'Assemblée nationale adoptait à l'unanimité une résolution réaffirmant les principes abolitionnistes de la France. Ce positionnement, dont l'ambition est à terme « une société sans prostitution », s'appuie sur les grands principes de la République française : la non patrimonialité du corps humain, le respect de son intégrité, l'égalité entre les sexes.

C'est une des ambitions de la loi de 2016 sur la prostitution que de répondre à ces différents objectifs. Quels sont les principaux axes de la loi du 13 avril 2016 ?

A. Protéger les victimes

Conformément au modèle nordique, la loi reconnaît les personnes prostituées comme des victimes à protéger. Le délit de racolage (actif et passif), en vigueur, sous différentes formes, depuis 1939, est abrogé, mettant ainsi fin aux poursuites pénales à l'encontre des victimes de la prostitution.

Par ailleurs, la loi développe une politique sociale globale à même de proposer un parcours de sortie de la prostitution aux victimes. Des commissions départementales, qui rassemblent les préfets, des représentants

de l'État, des représentants des collectivités territoriales, des magistrats, des professionnels de la santé, de représentants d'associations agréées, sont constituées pour mettre en place et coordonner l'action de protection et de prise en charge en faveur des victimes.

Le parcours de sortie prévoit : aide à l'insertion sociale et professionnelle, accès à un hébergement adapté, remise (totale ou partielle) des dettes fiscales, accès à une autorisation provisoire de séjour pour les victimes étrangères engagées dans un parcours de sortie, actions d'insertion sociale pour favoriser la socialisation et l'autonomie des victimes dans leur vie quotidienne et développer un projet d'insertion professionnelle, accompagnement vers les soins pour une prise en charge globale.

Un fonds spécial est constitué pour les actions mises en oeuvre dans le cadre du parcours de sortie et d'insertion. Il est alimenté par le budget de l'État et par les confiscations des biens et produits du proxénétisme et de la traite des êtres humains[26].

B. Poursuivre et sanctionner les auteurs de cette violence

« *Seuls les responsables – réseaux, proxénètes, clients – sont désormais condamnables* ». Le recours à la prostitution d'autrui est désormais interdit. Le client de la prostitution est passible d'une contravention de 1 500€, assortie de la participation à un stage de sensibilisation à la lutte contre l'achat d'actes sexuels, ou d'une peine d'emprisonnement en cas de recours à la prostitution d'une personne mineure ou vulnérable.

La lutte contre le proxénétisme est renforcée. La loi prévoit en particulier de s'attaquer au proxénétisme sur internet : « *Elle responsabilise les fournisseurs d'accès et les hébergeurs de site en créant l'obligation de participer à la lutte contre la diffusion de contenus proposant des offres de services sexuels tarifés et d'informer les autorités publiques en cas de contenus illégaux* ».

C. Prévenir et sensibiliser les citoyens

« *Aucune politique de lutte contre la traite des êtres humains et l'exploitation sexuelle, dans tous ses aspects, ne pourra être développée si elle ne s'appuie pas sur un consensus social, qui peine à être obtenu en l'état, faute d'information* » déclarait Laurence Rossignol en mars 2017. « *Il faut développer et transmettre notre connaissance des réalités de la prostitution dans des campagnes de sensibilisation. Il est essentiel de faire connaître au grand public les enjeux que représentent la prostitution et l'exploitation sexuelle pour nos sociétés*[27]».

La loi prévoit une éducation à l'égalité et à la sexualité, avec en particulier une information sur les réalités de la prostitution et les dangers de la marchandisation des corps dans les établissements de l'enseignement secondaire. Dans la foulée de l'entrée en vigueur de la loi, plusieurs campagnes à destination du grand public ont été lancées : « *Le prix d'une passe n'est pas celui que tu crois* » (campagne de la Mairie de Paris), « *Les hommes disent non à la prostitution* » (diffusé sur des affiches, des flyers, un clip vidéo pendant l'Euro 2016), « *Acheter un acte sexuel est désormais interdit* » (à l'occasion de la Journée européenne de lutte contre la traite des êtres humains du 18 octobre 2016).

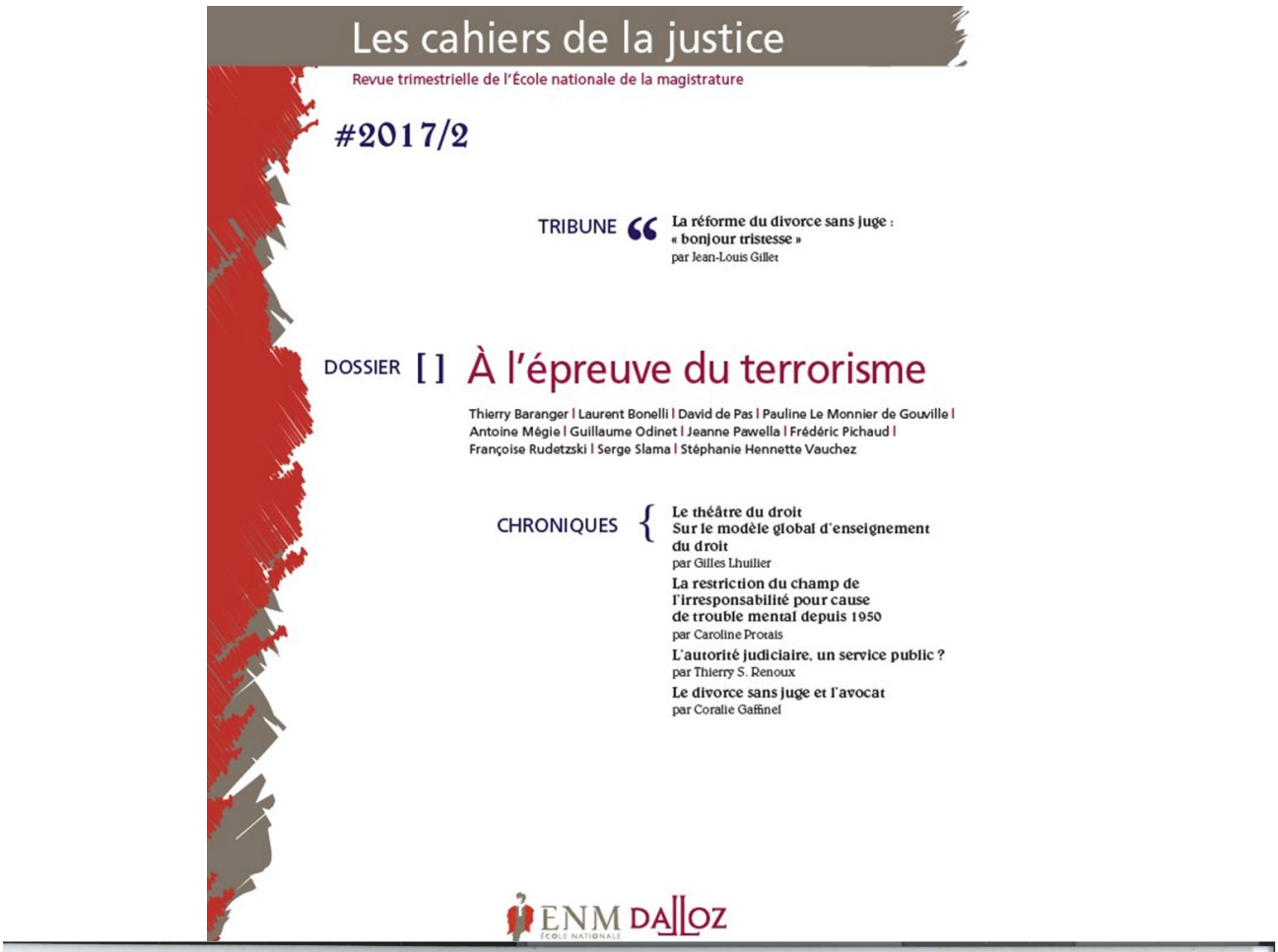
Le premier bilan de la loi d'avril 2016, après une année d'application, est encore limité, la promulgation des décrets d'application ayant réclamé plusieurs mois. Au 1er juin 2017, 1164 clients avaient été verbalisés[28]. Les premiers stages de responsabilisation à leur intention ont débuté pendant l'été 2017. Les commissions départementales en charge de la coordination des actions de protection et d'assistance du parcours de sortie sont en train de se constituer. De leur côté, les médias ont largement relayé les plaintes de quelques personnes prostituées, dénonçant une précarisation et une insécurité croissantes, appelant à l'abrogation de la loi[29]. L'évaluation globale de la loi, prévue en avril 2018, dira ce qu'il en est.

Il faut aussi prendre la mesure du changement profond en train de s'opérer. « *L'adoption de cette loi abolitionniste constitue une étape historique,* » déclarait Laurence Rossignol, alors ministre des Familles, de l'Enfance et des Droits des femmes, en mars 2016. « *Elle impulse au*

sein de notre société, un véritable changement de regard sur la prostitution»[30] ». La société toute entière doit maintenant apprendre à prendre en compte les réalités de l'exploitation sexuelle et à s'impliquer dans ce combat.

Notes :

1. International Labour Office (ILO), *Profits and Poverty: The Economics of Forced Labour,* 2014, p.7.2
2. 85% de femmes / 10% hommes / 5% personnes transgenres – 30% prostitution de rue / 62% prostitution sur internet / 8% prostitution indoor (bars à hôtesses, salons de massages... Cf. Mouvement du Nid, Psytel, ProstCost. *Estimation du coût économique et social de la prostitution en France*, 2015.
3. « Prostitution en France : ampleur du phénomène et impact sur les personnes prostituées », *La Lettre de l'Observatoire national des violences faites aux femmes*, n°7, octobre 2015.
4. Pour 15 846 victimes enregistrées (67% d'entre elles l'étaient à des fins d'exploitation sexuelle). *Rapport de la Commission au Parlement européen et au Conseil, Rapport sur les progrès réalisés dans la lutte contre la traite des êtres humains (2016) SWD(2016) 159 final*, p.4-5. *La Criminalité en France. Rapport annuel 2016 de l'ONDRP, novembre 2016*, p.12
5. F. Hénault, M. Ngalikpima, F. Reviglio, Violence et exploitation sexuelles des mineurs. Un état des lieux en France, Agir Contre la Prostitution des Enfants (ACPE), 2016, p. 82-83.
6. Fondation Scelles, *Exploitation sexuelle. Prostitution et crime organisé*, Paris, 2012, p. 2.
7. L'étude *ProstCost* (Mouvement du Nid – Psytel) avance l'estimation d'un chiffre d'affaires annuel d'environ 3,2 milliards d'euros en France. Pour comparaison, le budget annuel de l'ensemble des forces de police concourant annuellement au démantèlement des réseaux et à la condamnation des proxénètes est de l'ordre de 12 millions d'euros.
8. Cette économie souterraine représentait 11 milliards d'euros en 2013 pour le Royaume-Uni (soit 0,5% du PIB national), 9,2 milliards d'euros en 2010 pour l'Espagne (soit 0,85% du PIB national).Cf. « Au Royaume-Uni, la drogue et la prostitution ont contribué au PIB pour 11 milliards d'euros », *Le Monde*, 30 septembre 2014.
9. Audition de Simon Haggström, chef de la brigade antiprostitution de Stockholm, par la Commission spéciale sur la lutte contre le système prostitutionnel du Sénat, 20 mai 2014, http://www.senat.fr/compte-rendu-commissions/20140519/cs_prostitution.html
10. « Pays-Bas – Voyage au coeur du réglementarisme », Entretien avec Karin Werkman, *Fondation Scelles Infos*, n°24, avril 2013.
11. J. Eigendorf, L.M. Nagel, M. Neller, « Drei Dinge, die Deutschlands Prostituierten helfen können », *Die Welt*, 4 novembre 2013. « Allemagne » et « Pays-Bas » dans Fondation Scelles, *Prostitutions. Exploitations, Persécutions, Répressions – 4e rapport mondial*, Paris, 2016.
12. Les Pays-Bas étaient en 2004 le premier pays à mettre en place un Rapporteur national sur la traite des êtres humains. Le rapport des experts du GRETA saluent d'ailleurs cette action : « *Les autorités néerlandaises ont notamment adopté une législation anti-traite et des plans d'action nationaux complets, et créé une task force chargée de coordonner les actions contre la traite menées par les pouvoirs publics* ». (Rapport GRETA 2014 (10), p.7).
13. Propos du porte-parole de CoMensha, organe de coordination de la lutte contre la traite des êtres humains aux Pays-Bas. Cf. Fondation Scelles, *Exploitation sexuelle. Une menace qui s'étend – 3e rapport mondial*, Paris, 2014, p. 450.
14. 14 J. Bindel, « Why even Amsterdam doesn't want legal brothels », *The Spectator*, 2 février 2013.
15. U. Müller, M. Schröttle, *Lebenssituation, Sicherheit und Gesundheit von Frauen in Deutschland*, 2004, p. 25.
16. Chiffres extraits des rapports de la *Bundeskriminalamt* Fondation Scelles, *Rapport mondial sur l'exploitation sexuelle. La prostitution au coeur du crime organisé*, Paris, 2012, p. 29.
17. Les établissements proposent des forfait « all inklusiv », comprenant boisons, repas, préservatifs, et « du sexe avec toutes les femmes aussi longtemps que tu veux, aussi souvent que tu veux et comme tu veux » (Fondation Scelles, *Exploitation sexuelle. Prostitution et crime organisé... op. cit.*, p. 35). Exemple de programme télévisé : « Pimp my Puff » (Soutenez mon bordel) de RTL2 (Fondation Scelles, *Prostitutions. Exploitations, Persécutions, Répressions... op. cit.*, p. 196).
18. L'Allemagne est un bordel – Comment l'Etat favorise le trafic de femmes et la prostitution – *Der Spiegel*, n°22, 27 mai 2013.
19. Cette loi « *sur la protection des personnes prostituées* » (Prostituiertenschutzgesetz (ProstSchG), entrée en vigueur en juillet 2017, prévoit entre autres mesures l'obligation de déclaration de leur activité et de contrôle sanitaire pour les personnes prostituées, renforce les autorisations administratives pour l'exploitation d'un établissement de prostitution, établit l'obligation du port du préservatif pour les clients
20. *Evaluation of the ban on purchase of sexual services*, juillet 2010, http://www.government.se/articles/2011/03/evaluation-of-the-prohibition-of-the-purchase-of-sexual-services/.
21. Audition S. Haggström, , op. cit.
22. K. Claude, *S'attaquer au client de services sexuels*, Institut suédois, 2011
23. Audition de S. Haggström, op. cit.
24. Fondation Scelles, *Prostitutions. Exploitations, Persécutions, Répressions... op. cit,*, p.501-502.
25. Résolution du 26/02/2014 sur l'exploitation sexuelle et la prostitution et leurs conséquences sur l'égalité entre les hommes et les femmes (2013/2103(INI) §29
26. Sur la loi du 13 avril 2016 : *Loi française du 13 avril 2016 visant à renforcer la lutte contre le système prostitutionnel et à accompagner les personnes prostituées. Principes, objectifs, mesures et processus d'adoption d'une loi historique*, CAP International, 2017. Fondation Scelles, *Combattre le système prostitutionnel. Que dit la loi ?* Infographie explicative de la loi du 13 avril 2016, https://www.fondationscelles.org/fr/la-prostitution/la-loi-francaise
27. Intervention de Laurence Rossignol, Ministre des Familles, de l'Enfance et des Droits des Femmes, *Strategies to Adress Prostitution & Sex Trafficking,* conférence organisée par la Fondation Scelles, Consulat général de France à New York, mars 2017, http://www.fondationscelles.org/pdf/NY2017/SPEECH_Rossignol.pdf
28. Données au 1er juin 2017
29. A Lille par exemple. Cf P. Neves, « Loi prostitution, un an après : à Lille, « ça rend fou tout le monde », *Marianne*, 10 juillet 2017.
30. Intervention de Laurence Rossignol, Ministre des Familles, de l'Enfance et des Droits des Femmes, *Strategies to Adress Prostitution & Sex Trafficking, op. cit.*



SOMMAIRE

Cahiers de la justice #2017/2

« CODE PÉNAL ET LUTTE CONTRE LA CYBERCRIMINALITÉ : PROPOSITIONS POUR UNE EFFICACITÉ JURIDIQUE RENFORCÉE »

CORINNE THIÉRACHE

AVOCAT AU BARREAU DE PARIS,
ASSOCIÉ DE ALERION SOCIÉTÉ D'AVOCATS,
RESPONSABLE DU DÉPARTEMENT TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION (INNOVATION)

ÉRIC FREYSSINET

COLONEL, CHEF DE LA MISSION NUMÉRIQUE DE LA GENDARMERIE NATIONALE

Cet article présente et met en perspective le rapport du 25 janvier 2017« Code pénal et lutte contre la cybercriminalité : propositions pour une efficacité juridique renforcée », fait de la réflexion collective de membres de l'association Cyberlex[1], Association du droit des nouvelles technologies, et du CECyF[2],(Centre Expert contre la Cybercriminalité Français, lancée à l'initiative d'Éric FREYSSINET et de Corinne THIÉRACHE afin de concrétiser le partenariat avec la complémentarité des compétences de ces deux organisations, inauguré en juin 2014.

Le Code pénal a subi depuis son origine en 1810 de nombreuses modifications au coup par coup. Celles-ci se sont récemment accélérées, avec plus ou moins de pertinence, souvent dans l'urgence, au fil des lois comportant des dispositions pénales ayant trait aux technologies de l'information et de la communication et en particulier à la suite des attentats terroristes et de l'émergence de nouveaux comportements facilités par le numérique.

L'inflation des textes concernant la cybercriminalité, leur complexité, accompagnée de leur superposition ou juxtaposition voire contradiction ainsi que la multiplication des autorités peuvent avoir pour conséquence de rendre délicate l'appréhension juridique des situations rencontrées dans le monde du numérique.

Pourtant, les acteurs économiques avec l'assistance de leurs conseils (juristes internes, avocats) doivent traduire en droit les faits auxquels ils sont confrontés pour déterminer la réglementation applicable et s'y conformer. Les services d'enquête élaborent des procédures en proposant des qualifications, puis les magistrats ont pour missions de caractériser ou non des infractions et de retenir la qualification adaptée. Souvent ces infractions sont complexes en raison des aspects techniques de leurs modes opératoires, et une politique efficace de lutte contre la cybercriminalité passe par l'application effective des textes légaux.

Cette situation est accentuée par l'évolution constante des technologies qui, en quelques années, a profondément transformé les habitudes et les usages des internautes et ouvert une multitude de possibilités de développements. Cette même situation offre aussi un nouveau terrain de jeux particulièrement attractif pour les cybercriminels qui exploitent toutes failles ou faiblesses, à la fois techniques ou juridiques, animés par un sentiment réel d'impunité face à des infractions aux effets les plus souvent dématérialisés. Il existe ainsi un écart important entre la simplicité de la commission des infractions et la gravité de leurs effets et des préjudices qu'elles causent.

La cybercriminalité n'est donc pas une criminalité comme les autres,

elle est protéiforme, à l'image des cyber-délinquants dont les profils sont diversifiés et complexes.

Les décisions de justice rendues dans le domaine de la cybercriminalité illustrent les difficultés rencontrées pour qualifier la nature des faits, rattacher leur auteur à des catégories préexistantes, et ainsi déterminer l'infraction applicable, selon les principes d'interprétation stricte et de non rétroactivité de la loi pénale. Or, il s'agit d'un point majeur. Des qualifications retenues des faits découle, en effet, l'infraction pénale qui leur sera applicable. Il apparaît alors souvent salutaire de se reposer sur des concepts juridiques classiques qui animent le droit positif français depuis des décennies, avant même l'apparition de l'économie numérique, pour raisonner et tenter de qualifier les faits de façon pertinente.

Toutefois, le recours à des infractions classiques peut apparaître par trop artificiel voire inadapté dans certaines situations offertes par les technologies du numérique. Face à la croissance des cyberattaques et aux menaces que constituent notamment le terrorisme et la criminalité organisée, le législateur est ainsi récemment intervenu à plusieurs reprises pour compléter l'arsenal juridique en matière pénale pour mieux appréhender et punir des actes liés à la cybercriminalité.

Cette méthode d'adaptation réalisée de façon ponctuelle du droit aux faits n'est pas sans inconvénient, créant ainsi un éparpillement dans différents Codes (notamment Code pénal, Code des postes et des communications électroniques, Code de la sécurité intérieure, Code de la défense…), une superposition de textes (« effet mille-feuilles »), et enfin un risque d'obsolescence des dispositions pénales par ailleurs parfois sous utilisées par les praticiens du droit.

Il était donc important d'apporter un nouvel éclairage et de formuler des propositions d'aménagement du Code pénal en vue d'une meilleure lisibilité du texte légal, notamment en harmonisant les termes après identification des problèmes de définition et de redondances, condition essentielle pour mieux appréhender la lutte contre la cybercriminalité alors qu'il est particulièrement difficile de corriger la lettre du Code pénal.

C'est le propos du rapport rendu public le 25 janvier 2017 dans le cadre du Forum international sur la cybersécurité (FIC) qui rassemble le résultat des travaux et des réflexions d'un Groupe de travail composé de membres des deux associations Cyberlex et CECyF.

Ainsi, ce rapport propose de contribuer à rendre plus lisible la loi tant pour les praticiens que pour les justiciables. Dans cette perspective, il s'est attaché modestement à relever les éventuelles scories, les redondances des textes et faire le cas échéant des propositions pertinentes afin d'aider le législateur à y voir plus clair et participer ainsi à une meilleure cohérence des textes dans le cadre d'une réforme plus globale de la politique pénale, et ainsi participer à une meilleure sécurité juridique dans l'application des textes.

Loin des modifications massives des dispositions du Code pénal, il s'agit plutôt d'une relecture permettant de relever des lacunes ou des incohérences. Le but est de proposer des pistes de réflexion au législateur pour des évolutions futures y compris ouvrant si nécessaire sur une approche plus globale du droit pénal appréhendé par d'autres Codes que le Code pénal. L'essentiel, pour une lutte efficace contre la cybercriminalité, se situe en réalité dans les règles de procédure pénale et dans les ressources qui y sont affectées.

I. Les multiples débats autour des infractions d'atteinte aux systèmes de traitement automatisé de données (STAD)

A. Le « vol de données »

Peut-on voler une donnée ? Telle est la question à laquelle la loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme voulait répondre en modifiant l'article 323-3 du Code pénal[3]. La réponse est-elle satisfaisante ou faut-il préciser davantage le texte qui en résulte ?

i. Peut-on voler une donnée ?

C'est une question tout à fait légitime eu égard au sens courant donné au terme « vol » qui est défini dans le Petit Robert comme *« le fait de s'emparer du bien d'autrui par la force ou à son insu »* et *« l'action qui consiste à soustraire frauduleusement le bien d'autrui ».*

En l'espèce, ne sera pas ici évoqué le vol d'un support (clé USB, disque dur, etc.) qui répond à la qualification classique du vol comme étant *« la soustraction frauduleuse de la chose d'autrui »*. Seul est envisagé le « vol » de données, le support n'étant pas l'objet de l'action du prédateur. Dans cette hypothèse, on confond souvent la soustraction de la donnée qui échappe ainsi à la *« volonté du maître du système »* et la copie de données, malgré la *« volonté du maître du système »*.

C'est bien la copie qu'évoquait M. Sébastien Pietrasanta, rapporteur de la loi précitée du 13 novembre 2014, en affirmant, lors des débats, que : *« L'article 331-1 du Code pénal définissant le vol comme la soustraction frauduleuse de la chose d'autrui pose deux conditions qui s'avèrent inadaptées au vol de données : d'une part, une donnée n'est pas une chose, mais un élément immatériel distinct de tout support de stockage ; d'autre part, une donnée extraite d'un STAD à la suite d'un accès ou d'un maintien frauduleux n'est pas nécessairement soustraite de celui-ci mais seulement extraite par sa reproduction sur un autre support »*.

Pour le vol d'énergie, bien immatériel, le législateur a dû recourir à une incrimination spécifique (article 311-2 du Code pénal[4]).

La copie de données n'est pas, en effet, une soustraction, puisque le légitime propriétaire les conserve et n'en est à aucun moment dépossédé. En ce qui concerne les données à caractère personnel, les constituants de la propriété (usus-abusus-fructus) sont aussi inadaptés : peut-on parler de propriété sur ces données, puisque, tout en étant éventuellement exploitées commercialement, elles ne peuvent faire l'objet d'un abandon de la part de leur détenteur ? Pour éviter cet écueil, plusieurs voies éta l'affaire « Bluetouff », ient possibles avant la loi : accès ou maintien frauduleux à un STAD, poursuites pour atteintes aux droits du producteur de bases de données, pour abus de confiance, pour collecte déloyale ou frauduleuse de données personnelles etc. Mais elles ne couvraient pas toutes les hypothèses.

La jurisprudence a tenté de remédier à cette difficulté en reconnaissant le vol de données.

Dans un arrêt non publié du 4 mars 2008 (n° pourvoi : 07-84002) opposant X/ Société Graphibus, la chambre criminelle de la Cour de cassation avait déjà qualifié de vol une copie de données, mais cette décision s'écartait du principe selon lequel la loi pénale est d'interprétation stricte.

Plus récemment, par un arrêt du 20 mai 2015 (n° pourvoi : 14-81336 ; affaire dite « Bluetouff »), postérieur à la loi du 13 novembre 2014 mais pour des faits qui lui sont antérieurs, la chambre criminelle de la Cour de cassation a confirmé l'arrêt du 5 février 2014 de la Cour d'appel de Paris en considérant que le vol était bien constitué. En l'espèce, la Cour d'appel avait condamné pour vol de données (7,7 giga-octets) un blogueur qui s'était introduit dans le site extranet de l'ANSES. Dans ses conclusions, l'avocat général Frédéric Desportes s'est ainsi exprimé : *« Tout en respectant le principe d'interprétation stricte de la loi pénale, vous avez toujours su adapter les incriminations aux évolutions technologiques, veillant à ce que soient atteints les objectifs du législateur et donc à ce que la loi soit appliquée conformément à la fois à sa lettre et à son esprit. Cela est particulièrement vrai s'agissant du vol dont la définition a révélé une certaine plasticité. [...] Il serait paradoxal que la soustraction frauduleuse d'un document papier sans intérêt soit passible de trois ans d'emprisonnement mais non celle de milliers de fichiers stratégiques alors même que ces fichiers ne sont jamais que des documents numériques ou numérisés pouvant être imprimés et donc matérialisés. »*

ii. L'extraction (avec et sans copie des données) sanctionnée

Pour éviter les difficultés liées à la définition même du vol, le Parlement a décidé, à l'occasion de l'examen de la loi du 13 novembre 2014, de modifier l'article 323-3 du Code pénal. Celui-ci, sans jamais évoquer le « vol » (ni le recel), réprime désormais l'extraction, la détention, la reproduction, la transmission frauduleuses de données contenues dans le système.

La notion d'« extraction » de données apparaît dans l'article 2 de la loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés qui qualifie de traitement de données à caractère personnel comme étant : *« toute*

opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment [...] l'extraction, [...]. »

Il est possible de s'interroger sur le fait de savoir si le terme « extraction » permet de sanctionner la copie de données qui demeurent à la disposition du « maître du système ». Les définitions ou les usages du mot « extraction » impliquent généralement en effet un transfert, un changement de lieu (extraction d'un détenu, d'une dent, d'un minerai, extrait d'un texte ou d'un reportage etc.).

Le transfert est ainsi bien défini juridiquement par l'article L.342-1 du Code de la propriété intellectuelle qui dispose que le producteur d'une base de données a le droit d'interdire : « 1° L'extraction, par transfert permanent ou temporaire de la totalité ou d'une partie qualitativement ou quantitativement substantielle du contenu d'une base de données sur un autre support, par tout moyen et sous toute forme que ce soit ; 2° La réutilisation, par la mise à disposition du public de la totalité ou d'une partie qualitativement ou quantitativement substantielle du contenu de la base, quelle qu'en soit la forme. »

Toutefois, cette première interprétation est contredite par la pratique. En effet, certes, la copie de ces données est hors du contrôle du « maître du système », mais les données sources, quant à elles, demeurent au sein dudit système. Par ailleurs, le terme « reproduire » tel que visé dorénavant à l'article 323-3 du Code pénal permet à notre sens de couvrir les actes de copie. C'est d'ailleurs bien ce même terme qui est utilisé par le législateur pour adapter certaines dispositions au numérique. Tel est le cas par exemple de l'apologie publique des actes de terrorisme ou leur provocation telles que réprimées par l'article 421-2-5-1 du Code pénal[5].

B. Les actions bienveillantes associées aux infractions d'atteintes aux systèmes de traitement automatisé de données (STAD)

Aux côtés de l'offre régalienne proposée par les institutions et de la stratégie de cybersécurité menée par des acteurs privés de la sécurité des systèmes d'information se sont glissés les « hackers éthiques », ou « éthico -hackers » et « hackers blancs », internautes agissant généralement seuls. Contribuant de manière collaborative et originale à la sécurité des systèmes en détectant les failles, la question de leur statut au regard de la loi pénale se pose. Il convient donc de s'interroger sur le fait de savoir si la réponse récente du législateur pour encadrer l'action d'une certaine catégorie de hackers est satisfaisante.

i. Les hackers contractuels

On peut d'ores et déjà écarter le cas des hackers agissant dans le cadre d'un contrat de « bug bounty[6]». En effet, ils sont sollicités par des entreprises pour détecter des failles dans la sécurisation de leurs systèmes ou de leurs produits. Ils sont recrutés (inside) ou agissent par contrat (outside) pour effectuer des tests d'intrusion, « entraîner » le personnel des SOC (Security Operation Center), effectuer des audits de sites, de produits. Dès lors que le contrat délimite clairement dans le temps et dans l'espace le périmètre des investigations permises sur l'infrastructure, les sites ou les logiciels tout en excluant toute altération du système et toute destruction de données, le cocontractant agit dans les limites autorisées par l'entreprise pour découvrir ses propres failles et formuler des recommandations.

Ainsi, si le contrat de « bug bounty » offre un cadre juridique clair, il n'en est pas de même du lanceur d'alerte.

ii. Les lanceurs d'alerte

D'après le Conseil d'État, les lanceurs d'alerte seraient des personnes qui *« signalent, de bonne foi, librement et dans l'intérêt général, de l'intérieur d'une organisation ou de l'extérieur, des manquements graves à la loi ou des risques graves menaçant des intérêts publics ou privés, dont ils ne sont pas l'auteur »*. Ainsi, selon cette définition, le lanceur d'alerte au regard du Code pénal n'est pas l'auteur des faits qu'il dénonce ou signale. Il leur est extérieur. Le lanceur d'alerte ne participe pas à un ou plusieurs actes matériels de l'infraction, sinon il serait auteur, coauteur ou complice. Sont donc clairement exclus les chasseurs de prime.

Le lanceur d'alerte peut également saisir l'opinion publique quand il a échoué en tant que déontologue de l'entreprise ou de l'administration, voire de son supérieur hiérarchique, et que les autorités régaliennes ne prennent pas sérieusement en considération les

manquements dénoncés.

Pour les agents publics qui se retrouveraient dans cette situation, l'article 40 du Code de procédure pénale les oblige à porter à la connaissance du procureur de la République les faits susceptibles de constituer un crime ou un délit.

Outre les hackers contractuels et lanceurs d'alerte, existent les « hackers autonomes » qui occupent une toute autre place au regard du Code pénal.

iii. Les hackers autonomes

Ces hackers sont autonomes dans la mesure où ils agissent sans concertation avec le « maître du système ». Ils testent les systèmes et, pour ce faire, y pénètrent ou s'y maintiennent le plus souvent sans droit ni titre. Ils commettent donc des actes matériels qui entrent dans la définition des infractions à la loi no 88-19 du 5 janvier 1988 relative à la fraude informatique (loi Godfrain).

Après avoir envisagé, dans le cadre des différents débats parlementaires autour de l'adoption de la loi « Sapin II[7] » et la loi pour une République numérique[8], une exemption de peine en cas d'avertissement immédiat par le hacker autonome mais de bonne foi, de l'autorité administrative, judiciaire ou du responsable de traitement automatisé de données en cause d'un risque d'atteinte aux données ou au fonctionnement du système en évitant ainsi toute atteinte ultérieure aux données, le législateur a préféré se diriger vers une autre solution.

iv. Protection des « hackers éthiques »

Désormais, après adoption de la loi Sapin II, la définition donnée à l'article 6 du lanceur d'alerte est la suivante : *« Un lanceur d'alerte est une personne physique qui révèle ou signale, de manière désintéressée et de bonne foi, un crime ou un délit, une violation grave et manifeste d'un engagement international régulièrement ratifié ou approuvé par la France, d'un acte unilatéral d'une organisation internationale pris sur le fondement d'un tel engagement, de la loi ou du règlement, ou une menace ou un préjudice graves pour l'intérêt général, dont elle a eu personnellement connaissance.*

Les faits, informations ou documents, quel que soit leur forme ou leur support, couverts par le secret de la défense nationale, le secret médical ou le secret des relations entre un avocat et son client sont exclus du régime de l'alerte défini par le présent chapitre. »

Dans un but de protection du lanceur d'alerte, il ne fallait pas provoquer un risque de confusion avec le « statut » de repenti dans le « monde réel » (cf. la loi n° 2004-204 « Perben II » du 9 mars 2004 qui avait pour objectif d'empêcher la concrétisation d'une menace imminente et non un risque potentiel, ou de limiter les effets d'une infraction consommée). Or, une faille dans un logiciel est un risque et non une menace, tant qu'une personne mal intentionnée ne l'a pas exploitée. L'amendement aurait remis en cause l'équilibre de l'article 323-1 du Code pénal[9] et l'aurait même fortement affaibli.

La solution récemment retenue peut donc paraître d'un prime abord raisonnable et plus sage, car sans risque de déstabiliser les principes fondamentaux des règles pénales et d'entraîner des confusions ou des mélanges de genre. Mais il apparaît qu'elle ne résout pas complètement le problème.

Est désormais instaurée, à la suite de l'adoption de l'article 47 de la loi pour une République numérique une dispense des obligations prévues par l'article 40 du Code de procédure pénale au profit de l'ANSSI (Autorité nationale en matière de sécurité et de défense des systèmes d'information), dès lors que celle-ci est saisie par un hacker ayant agi de bonne foi, sans avoir donné une publicité à sa découverte : *« Pour les besoins de la sécurité des systèmes d'information, l'obligation prévue à l'article 40 du Code de procédure pénale n'est pas applicable à l'égard d'une personne de bonne foi qui transmet à la seule autorité nationale de sécurité des systèmes d'information une information sur l'existence d'une vulnérabilité concernant la sécurité d'un système de traitement automatisé de données ».*

L'ANSSI préserve la confidentialité de l'identité de la personne à l'origine de la transmission ainsi que des conditions dans lesquelles celle-ci a été effectuée. Elle peut procéder aux opérations techniques strictement nécessaires à la caractérisation du risque ou de la menace qui lui est présenté pour avertir l'hébergeur, l'opérateur ou le responsable du système d'information.

On notera toutefois que l'expression *« de bonne foi »* est restée dans le texte, alors qu'il eût été préférable de mentionner l'absence de volonté de nuire.

Pour autant, la dispense ainsi reconnue ne fait pas obstacle à l'exercice de l'action publique qui demeure une prérogative du parquet. Libre à lui de poursuivre s'il estime que l'infraction est constituée et, en particulier, en cas de plainte de la victime. On peut éventuellement espérer qu'un « blanc-seing » de l'ANSSI entraîne, pour des motifs d'opportunité, un classement sans suite par le Parquet.

Mais il convient de noter les réserves exprimées sur la solution finalement adoptée par les professionnels et « hackers blancs » eux-mêmes, qui s'interrogent à bon droit sur la réelle marge de manoeuvre dont disposera l'ANSSI pour juger de la bonne foi et préserver la confidentialité. Ils ont parfaitement compris que la nouvelle loi n'offrait *in fine* aucune garantie absolue à celui qui trouve et signale une faille. Quid également du délai dans lequel les failles seront effectivement traitées si l'objectif poursuivi est bien celui de contribuer à la détection puis résolution des failles ?

Reste également ouverte la question des personnes qui ne sont pas des hackers et qui découvrent une faille par un pur hasard. Fort est à parier qu'elles n'auront jamais l'idée de contacter l'ANSSI. Plutôt que l'affaire « Bluetouff » précitée, qui avait concentré et égaré les débats, il faudrait se référer à l'affaire « Tati contre Kitetoa[10] », dans laquelle un internaute, qui avait découvert par hasard une faille de sécurité dans un site web et l'avait signalée au propriétaire du site, avait été attaqué en justice par ce dernier pour accès frauduleux au système. L'internaute avait été condamné en première instance avant d'être relaxé en appel. Un tel précédent n'incite pas l'internaute moyen à signaler les failles qu'il peut découvrir par hasard.

Enfin, il est à nouveau regrettable que cette disposition soit intégrée dans le Code de la défense (art. L. 2321-4)[11], ce qui affaiblit une fois de plus l'unité de la loi « Godfrain » dont les dispositions (notamment article 323-1) sont insérées dans le Code pénal.

Compte tenu de la solution actuellement adoptée, ne convient-il pas de travailler sur des règles d'éthique à mettre en place par les professionnels et les « hackers blancs, » et de chercher une solution simple pour le cas (pas si hypothétique) de l'internaute moyen qui découvre une faille par hasard, et qui n'a connaissance, ni du Code de la défense, ni même de l'existence de l'ANSSI ?

C. La bande organisée

Il convient également de s'interroger sur le fait de savoir si les règles applicables en matière de criminalité organisée sont pertinentes dans le cadre d'une lutte efficace contre la cybercriminalité.

Le Code pénal prévoit deux cas relevant de la criminalité organisée s'appliquant aux infractions d'atteinte aux systèmes de traitement automatisé de données : l'association de malfaiteurs (article 323-4 du Code pénal), permettant de poursuivre des personnes s'entendant pour commettre ensemble une atteinte à un STAD ; la commission d'une atteinte à un système de traitement automatisé de données à caractère personnel mis en oeuvre par l'État, en bande organisée (article 323-4-1du Code pénal).

Or seul ce dernier cas permet d'appliquer les dispositions procédurales spécifiques résultant de l'application combinée des articles 706-72 et 706-73-1 du Code de procédure pénale. Ainsi, la diffusion en bande organisée de logiciels malveillants (virus informatiques) ne peut faire l'objet d'une enquête sous pseudonyme, alors même qu'une telle infraction est souvent facilitée par des échanges électroniques sur des plates-formes réservées à ces criminels. Cette technique pourrait faciliter l'identification des auteurs de ces infractions, en particulier au moment des premières étapes de leur commission.

Il est en conséquence dommage qu'une des dispositions les plus emblématiques introduites pour lutter contre certaines formes de cybercriminalité ne puisse s'appliquer aux infractions qui sont au coeur de cette cybercriminalité.

Il est donc proposé la définition d'une infraction d'atteintes aux systèmes de traitement automatisé de données en bande organisée en étendant les dispositions de la bande organisée aux infractions de cybercriminalité

dont le mode opératoire et la complexité le justifient selon les options suivantes :

- Option 1 : Pour tous les types de systèmes de traitement automatisé de données, avec une peine maximum de 7 ans (contre 10 ans en ce qui concerne les systèmes de l'État traitant des données à caractère personnel) ;

- Option 2 : Pour les systèmes de traitement automatisés de données de l'État, des collectivités locales, de leurs établissements publics et des personnes privées exerçant une mission de service public ;

- Option 3 : Pour les atteintes aux systèmes de traitement automatisé de données permettant de faciliter la commission des infractions visées aux articles 706-73 et 706-73-1 du Code de procédure pénale.

II. Références aux communications électroniques

A. Références simples aux technologies numériques

Certaines références simples viennent uniquement rappeler que des responsabilités spécifiques peuvent résulter des dispositions particulières aux communications électroniques, ou que certains outils numériques peuvent être utilisés. Il convient d'harmoniser ces différentes dispositions entre elles.

Dans un certain nombre de cas, il est proposé d'ajouter une mention explicite aux formes numériques de réalisation des infractions pour souligner l'importance de leur répression et permettre le cas échéant leur comptabilité disjointe dans les systèmes de statistiques judiciaires (classification NATINF pour Nature de l'Infraction).

Ainsi il est proposé :

- d'harmoniser toutes les références aux technologies numériques, pour faciliter leur compréhension et leur mise en oeuvre (cf. articles 226-8, 313-1, 411-3, 411-9, 413-13, 432-9, 434-4, 434-23, 441-1, 444-3 du Code pénal concernant les infractions de diffusion de montages photographiques, l'escroquerie et diverses infractions d'atteinte à la nation) ;

- d'étendre de façon explicite les infractions qui peuvent s'appliquer dans un contexte numérique pour améliorer leur répression et leur comptabilité.

B. Les circonstances aggravantes liées à l'utilisation d'Internet

L'utilisation d'Internet ne saurait en tant que telle constituer une circonstance aggravante. En effet, il s'agit d'une modalité particulière de commission de l'infraction, mais ne porte pas en soi une dimension aggravante ou péjorative comme le sont l'usage d'une arme pour accompagner des menaces ou la commission d'une infraction à l'encontre d'une personne vulnérable.

En revanche, certaines techniques disponibles sur Internet permettent effectivement de renforcer, dans des proportions non négligeables, la portée de la publication d'un message ou d'une information. La portée d'une publication sur un site Web est potentiellement plus importante qu'un simple échange entre plusieurs personnes, même prononcé en public.

Ainsi, l'article 227-23 du Code pénal relatif aux incriminations ciblant la pédopornographie prévoit que : *« Les peines sont portées à sept ans d'emprisonnement et à 100 000 euros d'amende lorsqu'il a été utilisé, pour la diffusion de l'image ou de la représentation du mineur à destination d'un public non déterminé, un réseau de communications électroniques. »*

On y précise donc l'action concernée, le média utilisé (un réseau de communications électroniques) et la façon de l'utiliser (à destination d'un public non déterminé). Était alors visée par exemple la diffusion sur un site Web librement accessible ou sur un réseau pair à pair où les informations sont partagées avec toute personne s'y connectant.

Il nous apparaît dès lors opportun que les dispositions prévoyant des circonstances aggravantes liées à Internet soient harmonisées en reprenant chaque fois qu'elle est appropriée la terminologie utilisée par l'article 227-23 du Code pénal (cf. articles 225-12-2 et 421-2-5 du Code Pénal concernant les infractions de recours à la prostitution de mineurs et de provocation à des actes de terrorisme et apologie de ces actes). Par ailleurs, dans quelques cas nouveaux, ces

circonstances aggravantes pourraient être introduites (cf. articles 226-4-1, 226-8, 226-13, 227-24-1, 312-2 6°, 313-2, 322-12, 322-13, 322-14, 433-3 et 433-5 du Code Pénal concernant les infractions d'usurpation d'identité, de diffusion des montages photographiques, de diffusion de secrets, de recours à la mutilation sexuelle, d'extorsion, l'escroquerie, différentes infractions de menace de destruction, de détérioration ou dégradation , menaces de délit ou crime contre des personnes ou des biens, outrage à une personne chargée d'une missions de service public).

Une série de critères simples pourrait être prise en compte dans l'application de cette circonstance aggravante, qui cible la notion de public non déterminé (c'est-à-dire non déterminé au moment de la publication du message ou de l'information) :

- Le média électronique utilisé est ouvert à tous les publics ;

- ou visible par un public dont le nombre est nettement supérieur à l'entourage immédiat de la victime (famille proche, collègues de travail, amis) ;

- ou le protocole utilisé est destiné à la diffusion à un large public (site Web librement accessible, protocole de communication pair à pair).

En outre, lors de l'évaluation du quantum de peine réclamé, l'utilisation de techniques de camouflage ou d'anonymisation des actions et des transactions pourrait être retenue.

C. Infractions de consultation habituelle de contenus prohibés

Deux infractions du Code pénal prévoient à ce jour la notion de *« consultation habituelle »* de contenus prohibés.

L'article 227-23 du Code pénal qui traite de pédopornographie a été modifié à la suite d'un amendement de la Commission des affaires culturelles de l'Assemblée nationale qui reprenait les motifs suivants : « Il est proposé de compléter le Code pénal avec deux nouvelles dispositions : Aujourd'hui, seul le fait de détenir sur un disque dur d'ordinateur ou tout autre support une image à caractère pornographique est puni par la loi de deux ans d'emprisonnement et de 30 000 euros d'amende. Il est proposé d'élargir cette incrimination non plus seulement à la détention mais également à la consultation de telles images qui est aujourd'hui pratiquée par les pédophiles via internet. »

En effet, l'évolution des technologies et en particulier la possibilité d'être connecté en permanence à Internet (câble, puis ADSL et les smartphones) a amené de nombreux adeptes de tels contenus à ne plus les télécharger et les stocker (par exemple pour ne pas être découverts par leurs proches), mais à les consulter au moment qui leur convenait. Les données illégales étaient alors éventuellement stockées (parfois en grandes quantités) dans le cache du navigateur, mais ne constituaient pas forcément le délit de détention d'images pédopornographiques. Il s'est donc ici agi de réprimer une action qui porte autant atteinte aux mineurs qui en sont indirectement victimes que la simple détention (par la démarche de recherche de nouveauté). L'aspect commercial fut d'ailleurs rajouté ultérieurement à ce même alinéa : *« article 227-23 alinéa 4 du Code pénal : Le fait de consulter habituellement ou en contrepartie d'un paiement un service de communication au public en ligne mettant à disposition une telle image ou représentation, d'acquérir ou de détenir une telle image ou représentation par quelque moyen que ce soit est puni de deux ans d'emprisonnement et 30 000 euros d'amende. »*

C'est cette même notion de « consultation habituelle » de contenus prohibés, et selon une même démarche, qui a conduit le législateur à créer une disposition similaire en matière d'accès à des contenus relatifs à l'apologie du terrorisme, dans l'article 421-2-5-2 du Code pénal (dans sa rédaction annulée par le Conseil constitutionnel le 10 février 2017 cf. infra) : *« Le fait de consulter habituellement un service de communication au public en ligne mettant à disposition des messages, images ou représentations soit provoquant directement à la commission d'actes de terrorisme, soit faisant l'apologie de ces actes lorsque, à cette fin, ce service comporte des images ou représentations montrant la commission de tels actes consistant en des atteintes volontaires à la vie est puni de deux ans d'emprisonnement et de 30 000 € d'amende.*

Le présent article n'est pas applicable lorsque la consultation est

effectuée de bonne foi, résulte de l'exercice normal d'une profession ayant pour objet d'informer le public, intervient dans le cadre de recherches scientifiques ou est réalisée afin de servir de preuve en justice. »

L'infraction est ici limitée aux services comportant des images montrant la commission d'actes d'atteintes volontaires à la vie.

Il apparaît dès lors pertinent de ne recourir à d'autres cas d'infractions de consultation habituelle que pour les contenus les plus graves et s'il est démontré que cette nouvelle infraction pourra apporter une véritable contribution à la lutte contre l'infraction principale et à sa prévention.

Sur ce point, le délit de consultation habituelle de sites terroristes a été finalement annulé à la suite d'une Question Prioritaire de Constitutionnalité (QPC) par le conseil constitutionnel le 10 février 2017 et pour finalement être réintroduit avec une nouvelle rédaction prenant en compte la notion d'absence de « motif légitime », par la loi sur la sécurité intérieure du 28 février 2017 publiée le 1er mars 2017 au JO comme suit : *« Le fait de consulter habituellement et sans motif légitime un service de communication au public en ligne mettant à disposition des messages, images ou représentations soit provoquant directement à la commission d'actes de terrorisme, soit faisant l'apologie de ces actes lorsque, à cette fin, ce service comporte des images ou représentations montrant la commission de tels actes consistant en des atteintes volontaires à la vie est puni de deux ans d'emprisonnement et de 30 000 € d'amende lorsque cette consultation s'accompagne d'une manifestation de l'adhésion à l'idéologie exprimée sur ce service.*

Constitue notamment un motif légitime tel que défini au premier alinéa la consultation résultant de l'exercice normal d'une profession ayant pour objet d'informer le public, intervenant dans le cadre de recherches scientifiques ou réalisée afin de servir de preuve en justice ou le fait que cette consultation s'accompagne d'un signalement des contenus de ce service aux autorités publiques compétentes. »

III. Les peines complémentaires

Le droit pénal comporte un certain nombre de mesures relatives au prononcé de la peine et à son application.

A. La confiscation de ressources immatérielles

Dans certains cas, les ressources immatérielles utilisées pour faciliter la commission d'une infraction constituent non seulement un outil indispensable à sa réalisation (et donc ne doit pas retomber entre les mains de délinquants), mais aussi un moyen de communication qui peut être utilisé pour sensibiliser le public (les utilisateurs d'un service cybercriminel, ceux qui cherchent à s'informer à son sujet ou ceux qui pourraient en être victimes). Enfin, dans certains cas, ces ressources pourraient faciliter la collecte de preuves numériques. Ainsi, un nom de domaine (et le site Web associé) ou un compte de réseau social pourraient-ils être utilement placés sous-main de justice au moment de l'enquête judiciaire et au-delà ?

C'est par exemple ce que réalisent régulièrement les autorités américaines lors d'opérations relatives à la lutte contre la contrefaçon ou à des escroqueries.

Il est intéressant de noter que des biens immatériels ont déjà fait l'objet de confiscation et, en particulier, les crypto-monnaies lors d'une affaire judiciaire traitée par la gendarmerie et jugée par le tribunal correctionnel de Foix en juillet 2014.

Ainsi il pourrait être créé une peine complémentaire de confiscation de ressources immatérielles (noms de domaines, comptes de réseaux sociaux ou de courrier électronique, etc). Cette peine complémentaire pourrait aussi trouver à s'appliquer comme peine de substitution à l'emprisonnement (art. 131-6). Cette disposition trouvera écho dans l'application des dispositions correspondantes du Code de procédure pénale en matière de saisie conservatoire et s'agissant du rôle de l'Agence de gestion et de recouvrement des avoirs saisis et confisqués (AGRASC).

Comme peine complémentaire ou comme mesure d'application des peines, plusieurs dispositions du Code pénal apportent des contraintes supplémentaires à la personne condamnée pour éviter la réitération de l'infraction.

B. L'interdiction d'entrer en contact via Internet

Certaines trouvent à s'appliquer plus particulièrement en matière de cybercriminalité telle l'interdiction d'entrer en contact avec certaines catégories de personnes (visée au 13° de l'article 132-45). Toutes ces mesures peuvent trouver une application numérique et il pourrait être explicitement prévu qu'elles soient applicables y compris par un procédé de communication électronique.

L'interdiction d'accéder à Internet de façon générale a été explicitement écartée par le Conseil constitutionnel dans sa décision 2009-580 DC du 10 juin 2009 (loi favorisant la diffusion et la protection de la création sur internet) : *« La libre communication des pensées et des opinions est un des droits les plus précieux de l'homme [...] : en l'état actuel des moyens de communication et eu égard au développement généralisé des services de communication au public en ligne ainsi qu'à l'importance prise par ces services pour la participation à la vie démocratique et l'expression des idées et des opinions, ce droit implique la liberté d'accéder à ces services ».*

Au vu de ce qui précède, il n'est pas proposé d'explorer à nouveau la question de l'interdiction de l'accès à Internet, mais il est en revanche recommandé la pleine application des mesures existantes, en exploitant systématiquement leur effectivité dans le cyberespace.

Toutefois, dans tous les cas où un juge d'application des peines souhaiterait s'assurer de l'interdiction qui est faite à une personne condamnée d'entrer en contact via Internet avec certaines catégories de personnes, il faudrait qu'il puisse s'en assurer à l'aide de mesures d'enquête appropriées (ex : investigations numériques) pour vérifier le respect des mesures prononcées.

CONCLUSION

L'étude effectuée pendant plusieurs mois par les membres du Groupe de travail Cyberlex – CECyF aboutit à une première conclusion somme toute assez rassurante : l'arsenal pénal de lutte contre la cybercriminalité existe d'ores et déjà et ne demande plus qu'à être appliqué dans les faits. Alors pourquoi ce sentiment d'inefficacité, voire de frustration, ressenti par les acteurs de la lutte contre la cybercriminalité ? Répondre à cette interrogation nous conduit à développer des réflexions complémentaires en guise de seconde conclusion pour aboutir à d'autres pistes de réflexions.

À l'issue de nos réflexions, il apparaît que les modifications qui sont proposées dans la présente contribution, allant de la simple coquille à rectifier jusqu'à quelques changements plus substantiels, ne changeront pas en réalité de manière profonde l'efficacité de la lutte contre la cybercriminalité. En effet, le droit rien que le droit, en particulier dans un domaine à haute implication technique et à l'évolution constante, peut rapidement montrer ses limites. Au-delà de la règle de droit applicable et de son efficacité, la question de l'efficience des disposions légales doit être au centre de tout dispositif mis en place.

L'urgence est réelle de mettre la question de la lutte contre la cybercriminalité au coeur des débats politiques et de la volonté de l'ensemble des acteurs impliqués qui doivent être rassemblés autour d'un objectif commun. Cela signifie une prise de conscience de chacun face à la montée croissante des cyberattaques. Cela concerne les enquêteurs, les magistrats du parquet et du siège, les pouvoirs publics, gendarmerie nationale et police judiciaire, les partenaires publics et privés, les auxiliaires de Justice (dont les avocats) et ce jusqu'au plus haut sommet de l'État en passant par les ministères de l'Intérieur, de la Justice, de la Défense nationale, de l'Économie.

Des dispositions du Code pénal peuvent avoir un effet totalement neutre sur le terrain de la lutte contre la cybercriminalité si les personnes en charge de cette mission ne sont pas formées, et convaincues de la nécessité de fournir les efforts nécessaires pour assurer l'efficience de l'ensemble de cet arsenal pénal et protéger les citoyens. La question de la mise à disposition des moyens nécessaires (humains, financiers et techniques) et de leur pérennité doit être posée avec l'inscription de la lutte contre la cybercriminalité comme une priorité nationale.

Par nature transverse et protéiforme, la lutte contre la cybercriminalité ne peut enfin se

concevoir que de manière globale et ne saurait se contenter que d'une vision nationale. La recherche d'une coopération toujours plus étroite entre États, certes dans un domaine par nature régalien (et l'on connaît les difficultés d'application de la Convention de Budapest sur la cybercriminalité signée le 23 novembre 2001), est le moyen pour permettre une meilleure collecte de preuves et éloigner de plus en plus l'impunité derrière laquelle se retranchent trop souvent à raison les cyberdélinquants.

Cette réflexion ne sera pleinement aboutie que par l'élaboration de recommandations en matière de procédure pénale (la captation de données, l'interception, la géolocalisation, chiffrement et accès de la preuve) et pour l'ensemble des textes de loi et règlements qui concourent à la lutte contre la cybercriminalité.

À cet effet, il convient de signaler :

- Au niveau européen : les conclusions du 9ème rapport de la Commission européenne sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective du 26 juillet 2017 ; Les travaux de la Commission européenne sur l'amélioration de l'accès à la preuve numérique pour laquelle elle vient de lancer un questionnaire à la société civile « afin de recueillir les avis des parties intéressées (États membres, institutions et agences européennes, représentants du secteur privé, associations, ...) sur ces travaux. Les questions posées visent à recueillir des informations sur les pratiques actuelles en matière d'obtention de preuves électroniques transfrontalières dans les États membres ainsi que sur les problèmes pratiques et juridiques rencontrés. »

- Au niveau international (Convention de Budapest sur la cybercriminalité) : des travaux sont en cours pour élaborer un protocole additionnel à Budapest et améliorer également l'accès à la preuve numérique (notamment entre Europe et USA) ; la publication cet été de la version en langue arabe de la Convention de Budapest.

C'est la raison pour laquelle rendez-vous est pris au FIC de janvier 2018 pour rendre publiques les recommandations du Groupe Cyberlex-CECyF dans le domaine de la procédure pénale pour une efficacité juridique renforcée de la lutte contre la cybercriminalité.

Notes :

1. Cyberlex www.cyberlex.org réunit, depuis 1996, des juristes d'entreprise, des avocats, des professeurs de droit, des magistrats ainsi que des professionnels du marché d'Internet et des technologies numériques.

Cyberlex ne représente pas une opinion mais des opinions, à l'image de la diversité de ses membres, excluant tout lobbying. L'ambition de Cyberlex est de contribuer à mieux comprendre le monde des nouvelles technologies et l'évolution des usages, appréhender les différents aspects du droit et ainsi participer à sa meilleure lisibilité.

Membres du Groupe de travail : Carole BUI, Avocat, Matthieu CAMUS, Expert sécurité des données et vie privée, Fabrice MATTATIA, Ingénieur et docteur en droit, Myriam QUEMENER, Magistrat, docteur en droit, Corinne THIÉRACHE, Avocat associé.

2. Le CECyF www.cecyf.fr est une association créée en 2014 regroupant des services de l'Etat chargés de la lutte contre la cybercriminalité, des établissements d'enseignement et de recherche ainsi que des entreprises de toutes tailles.

Ils ont réuni leurs forces pour mener des actions de prévention, de formation et de recherche et développement contre la cybercriminalité.

Membres du Groupe de travail : Philippe BAUDOIN, Officier de gendarmerie, Éric FREYSSINET, Officier de gendarmerie (également membre de Cyberlex), Catherine HORNAIN, Inspectrice de la concurrence, de la consommation et de la répression des fraudes, Alexandre HUGLA, Juriste, Marc WATIN-AUGOUARD, Général d'armée de gendarmerie (2S).

3. Article 323-3 CP : *« Le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 150 000 € d'amende.*

Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en oeuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 300 000 € d'amende. »

4. Article 311-2 CP : *« La soustraction frauduleuse d'énergie au préjudice d'autrui est assimilée au vol. »*

5. Article 421-2-5-1 : *« Le fait d'extraire, de reproduire et de transmettre intentionnellement des données faisant l'apologie publique d'actes de terrorisme ou provoquant directement à ces actes afin d'entraver, en connaissance de cause, l'efficacité des procédures prévues à l'article 6-1 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique ou à l'article 706-23 du Code de procédure pénale est puni de cinq ans d'emprisonnement et de 75 000 € d'amende. »*

6. 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 reporté des bugs, surtout ceux concernant des exploits et des vulnérabilités.

7. 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.

8. Loi n° 2016-1321 du 7 octobre 2016.

9. Article 323-1 CP : *« Le fait d'accéder ou*

de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende.

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 € d'amende.

Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en oeuvre par l'État, la peine est portée à cinq ans d'emprisonnement et à 150 000 € d'amende. »

10. Arrêt du 30 octobre 2002 de la 12ème chambre, section A des appels correctionnels de la cour d'appel de Paris.

11. Article L2321-4 du Code de la défense : *« Pour les besoins de la sécurité des systèmes d'information, l'obligation prévue à l'article 40 du code de procédure pénale n'est pas applicable à l'égard d'une personne de bonne foi qui transmet à la seule autorité nationale de sécurité des systèmes d'information une information sur l'existence d'une vulnérabilité concernant la sécurité d'un système de traitement automatisé de données.*

L'autorité préserve la confidentialité de l'identité de la personne à l'origine de la transmission ainsi que des conditions dans lesquelles celle-ci a été effectuée.

L'autorité peut procéder aux opérations techniques strictement nécessaires à la caractérisation du risque ou de la menace mentionnés au premier alinéa du présent article aux fins d'avertir l'hébergeur, l'opérateur ou le responsable du système d'information. »

OUVRAGES RÉCENTS

ATLAS DU TERRORISME ISLAMISTE : D'AL-QUAIA À DAECH

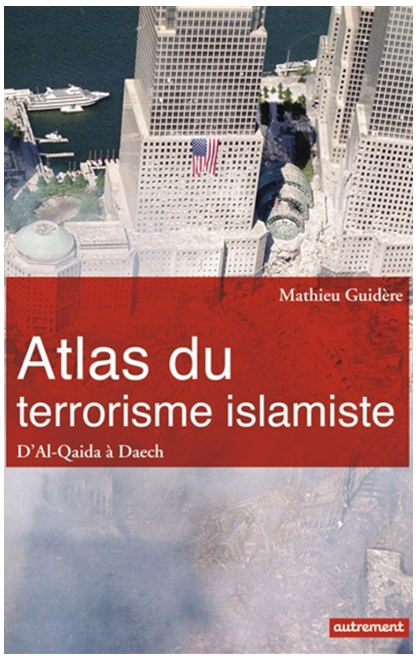
AUTEUR : MATHIEU GUIDÈRE

EDITEUR : AUTREMENT

Présentation de l'éditeur

« Le terrorisme islamiste apparaît plus que jamais au coeur des enjeux mondiaux. » Près de 70 cartes et infographies pour mieux connaître le terrorisme islamiste et comprendre ses racines, sa logique et son mode opératoire.

Pourquoi et depuis quand les groupes terroristes actuels se réclament-ils de l'islam ? Quels sont leurs modes d'action et d'organisation et comment se financent-ils ? Outre Al-Qaida, l'État islamique, les talibans et Boko Haram, plusieurs autres organisations islamistes mènent des actions terroristes en Afrique, en Asie, au Moyen-Orient... Les attaques subies par les pays occidentaux et leurs méthodes de lutte contre la radicalisation.



Pour la première fois, un atlas propose une analyse claire et distanciée du terrorisme islamiste à l'échelle mondiale. L'auteur associe connaissance pointue du sujet et souci de clarification.

DOCTRINE JURIDIQUE :

« RÉFLEXIONS SUR LE LANCEUR D'ALERTE EN DROIT FRANÇAIS »

MARIE-CHRISTINE SORDINO

PROFESSEUR À L'UNIVERSITÉ DE MONTPELLIER, DIRECTRICE DE L'ÉQUIPE DE DROIT PÉNAL (EDPM-UMR 5815)

L'alerte n'est pas un phénomène entièrement nouveau, puisque différentes périodes de l'histoire ont connu des mécanismes voisins, désignés de manière plurielle. Cependant, au sein d'une démocratie ouverte sur l'information, sa prise en considération pose un questionnement renouvelé. Ainsi, il est difficile de s'accorder sur une définition unique, car les situations visées sont multiples. Pourtant, des propositions de définitions ont été formulées.

Pour Transparency International France, qui a publié en 2009 *le Guide des principes directeurs pour une législation de l'alerte,* puis a rédigé un rapport intitulé *Whistleblowing in Europe,* au cours de l'année 2013, le lanceur d'alerte est *« tout employé qui signale un fait illégal, illicite ou dangereux pour autrui, touchant à l'intérêt général, aux instances ou aux personnes ayant le pouvoir d'y mettre fin ».*

Ces travaux successifs ont contribué à éclairer les réflexions du Conseil de l'Europe, pour l'élaboration de la *« Recommandation du Comité des Ministres aux États membres »* le 30 avril 2014, qui constitue l'ébauche d'un statut européen du lanceur d'alerte et d'une Convention cadre entre les États.

Le Conseil de L'Europe définit le lanceur d'alerte comme *« toute personne qui fait des signalements ou révèle des informations concernant des menaces ou un préjudice pour l'intérêt général dans le contexte de sa relation de travail, qu'elle soit dans le secteur public ou dans le secteur privé ».*

En droit interne, une étude, réalisée par le Conseil d'État, à la demande du Premier Ministre et a été rendue publique le mercredi 13 avril 2016, propose que le lanceur d'alerte soit *« un acteur civique qui signale, de bonne foi, librement et dans l'intérêt général, des manquements graves à la loi ou des risques graves menaçant des intérêts publics ou privés, dont il n'est pas l'auteur ».*

Après d'importantes discussions parlementaires, ont été promulguées le 9 décembre 2016, d'une part, la loi n° 2016-1691 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique et, d'autre part, la loi organique n° 2016-1690 relative à la compétence du Défenseur des droits pour l'orientation et la protection des lanceurs d'alerte. La promulgation des deux textes constitue un pas en avant certain en direction de la reconnaissance et de la protection du lanceur d'alerte. Cependant, toutes les incertitudes ne sont pas levées. Quels sont, d'une part, le domaine de l'alerte (I) et, d'autre part, la procédure d'alerte (II), désormais consacrés par le droit français ?

I. Le domaine de l'alerte

Il est intéressant de s'attacher,

d'abord, au sujet de l'alerte (A), puis à son objet (B).

A. Le sujet de l'alerte

La loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique pose une définition du lanceur d'alerte, dans son article 6, aux termes duquel *« un lanceur d'alerte est une personne physique qui révèle ou signale, de manière désintéressée et de bonne foi, un crime ou un délit, une violation grave et manifeste d'un engagement international régulièrement ratifié ou approuvé par la France, d'un acte unilatéral d'une organisation internationale pris sur le fondement d'un tel engagement, de la loi ou du règlement, ou une menace ou un préjudice graves pour l'intérêt général, dont elle a eu personnellement connaissance ».*

Cette disposition a été déclarée conforme à la Constitution par la décision du Conseil constitutionnel n° 2016-741 DC du 8 décembre 2016.

Alors que le projet de loi visait *« toute personne »,* le texte ne retient que la seule personne physique. Est, dès lors, écarté l'argument consistant à s'interroger afin de réserver la qualité (et, donc la protection qui lui est attachée) de lanceur d'alerte à une personne initiée ou ayant une qualité, comme cela est le cas pour le commissaire aux comptes. La CNIL avait, en effet, mis en garde contre la « délation organisée ».

Le nouveau texte réserve le statut de lanceur d'alerte à la personne physique, ce qui exclut le cas de la personne morale, notamment l'association, qui sert souvent de relai à la défense de certaines causes. Au sein d'une association, le lanceur de l'alerte sera, très certainement, le représentant légal de celle-ci.

Le déclenchement de l'alerte suppose un lanceur d'alerte agissant de bonne foi et de manière désintéressée. Ceci est très important, car l'alerte rendant son auteur pénalement irresponsable ne peut reposer sur une personne poursuivant un but intéressé. Pourtant, de manière contradictoire, l'administration fiscale peut désormais indemniser des lanceurs d'alerte qui ont signalé certaines formes de fraudes fiscales (article 109 de la loi de finances n°2016-1917 du 29 décembre 2016). Ainsi, «*à titre expérimental et pour une durée de deux ans, le Gouvernement peut autoriser l'administration fiscale à indemniser toute personne étrangère aux administrations publiques, dès lors qu'elle lui a fourni des renseignements ayant amené à la découverte d'un manquement aux règles fixées à l'article 4 B, au 2 bis de l'article 39 ou aux articles 57, 123 bis, 155 A, 209, 209 B ou 238 A du code général des impôts ou d'un manquement aux obligations déclaratives prévues au deuxième alinéa de l'article 1649 A ou aux articles 1649 AA ou 1649 AB du même code ».*

L'exigence de bonne foi du lanceur d'alerte est absolument indispensable, afin que le mécanisme de l'alerte ne constitue pas un prétexte pour régler des conflits préexistants entre plusieurs personnes.

Il est, en revanche, regrettable, à notre sens, que la loi assimile, au sein de la même définition, des situations très différentes, correspondant, d'une part, à l'alerte professionnelle interne à l'entreprise et, d'autre part, aux lanceurs d'alerte avertissant de menaces à l'intérêt général, par exemple, comme cela est le cas de scientifiques ou chercheurs. L'enjeu est d'autant plus fort que la procédure créée par l'article 8 de la loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique leur est commune, alors que les deux formes d'alerte procèdent d'une philosophie différente, même si le coeur du mécanisme, à savoir la révélation, est identique.

B. L'objet de l'alerte

Le texte vise le fait de révéler ou de signaler l'existence, soit d'abord, d'un crime et d'un délit, soit ensuite d'une violation grave et manifeste d'un engagement international régulièrement ratifié ou approuvé par la France, d'un acte unilatéral d'une organisation internationale pris sur le fondement d'un tel engagement, de la loi ou du règlement, soit enfin d'une menace ou un préjudice graves pour l'intérêt général.

Apparaissent plusieurs types de comportements pouvant engendrer l'alerte. Certains d'entre eux suscitent des interrogations et ne sont pas exempts d'ambiguïtés.

Peut être signalée, ainsi, l'existence d'un crime ou d'un délit,

donc d'une infraction pénale. La contravention est exclue de ce champ d'application. Celui qui entend effectuer le signalement dans ce cadre, devrait donc porter une appréciation pénale sur les faits, antérieurement à la mise en oeuvre de sa démarche et, donc, cette étape est insérée au sein de celle-ci. Cela ajoute une difficulté et pourrait être de nature à freiner une volonté de lancer une alerte dans certaines situations.

Le lanceur d'alerte peut également signaler une menace ou un préjudice graves pour « l'intérêt général ». Ceci vise, notamment, une personne ayant eu accès à une information qui a des répercussions importantes, comme cela a pu être le cas face à la révélation publique de certains scandales sanitaires. Cette situation peut être très différente de la première, la qualification pénale de crime ou de délit n'étant pas démontrée car le lanceur d'alerte peut ici agir en prévention de l'imminence d'une catastrophe de santé publique. La référence à l'intérêt général place quasiment le lanceur d'alerte à côté du procureur de la République, dans sa mission de défense de l'intérêt de la société.

Est-ce une manière de montrer que les pouvoirs publics se reconnaissent impuissants à dénoncer et réprimer tous les comportements illégaux ou porteurs de risques graves et appellent la société civile, la partie citoyenne, à l'aider à prendre part à la politique nationale ?

Le lanceur d'alerte peut aussi signaler *« une violation grave et manifeste d'un engagement international régulièrement ratifié ou approuvé par la France, d'un acte unilatéral d'une organisation internationale pris sur le fondement d'un tel engagement ».* Il est intéressant de remarquer le fait que le législateur n'a pas entendu cantonner la procédure d'alerte uniquement aux Conventions de lutte contre la corruption, mais l'ouvrir à toutes les conventions internationales, à partir du moment où elles ont été régulièrement ratifiées. Cependant, cette volonté d'ouverture est contrebalancée par l'exigence de signalement d'une violation grave et manifeste de cet engagement international, les deux conditions de gravité et de démonstration du caractère manifeste de la violation n'étant pas aisées à caractériser.

Quant à la violation grave et manifeste de la loi ou du règlement, nous retrouvons les deux mêmes exigences quant aux caractères de la violation. La référence à la violation d'un texte législatif n'est pas surprenante, dans la mesure où la loi peut faire l'objet d'une violation sans constituer pour autant, au regard de la qualification pénale, un crime ou un délit. Il est, en revanche contradictoire d'avoir prévu la violation grave et manifeste d'un règlement, car si, justement, une telle violation est démontrée, elle constituera à n'en pas douter une contravention, contravention exclue du domaine de l'alerte, puisque le législateur n'a prévu que le signalement d'un crime ou d'un délit.

Comme cela avait été envisagé depuis le début des débats, les faits, informations ou documents, quel que soit leur forme ou leur support, couverts par le secret de la défense nationale, le secret médical ou le secret des relations entre un avocat et son client sont exclus du régime de l'alerte.

Les conditions relatives à la gravité et au caractère manifeste de la violation sont intéressantes, car tout ne peut ni ne doit être révélé. Le législateur a, d'ailleurs, choisi le terme de « signalement », plutôt que celui de « dénonciation », lorsqu'il érige une définition du lanceur d'alerte et construit son régime de protection. Il est en effet souhaitable d'opérer une distinction entre le signalement et la dénonciation, voire la délation. Les deux consistent à lever le secret sur des informations, mais la dénonciation renvoie à une connotation péjorative, pouvant engendrer une défiance de la société française, en raison des événements tragiques qui ont ponctué l'histoire de France.

II. La procédure d'alerte

Le nouveau texte décrit le canal de l'alerte, à savoir, le signalement (A), ce qui soulève des questions relatives aux droits des personnes concernées par l'alerte (B).

A. Le canal de l'alerte : le signalement

Le signalement d'une alerte est porté à la connaissance du supérieur hiérarchique, direct ou indirect, de l'employeur ou d'un référent désigné par celui-ci.

En l'absence de diligences de la

personne destinataire de l'alerte, dans un délai raisonnable, relatives à la recevabilité du signalement, celui-ci est adressé à l'autorité judiciaire, à l'autorité administrative ou aux ordres professionnels.

En dernier ressort, à défaut de traitement dans un délai de trois mois, le signalement peut être rendu public.

En cas de danger grave et imminent ou en présence d'un risque de dommages irréversibles, le signalement peut être porté directement à la connaissance des organismes et il peut être rendu public. Le lanceur d'alerte peut également adresser son signalement au Défenseur des droits, afin d'être orienté vers l'organisme approprié de recueil de l'alerte. Le législateur a créé, pour toute personne, un délit d'obstacle à la transmission d'un signalement dans les conditions de l'article 8 de la loi, qui expose son auteur à 1 an d'emprisonnement et 15 000 € d'amende (article 13 de la loi). En pratique, comment ne pas penser, en effet, aux intermédiaires concernés par la procédure d'alerte, tentés de ne pas transmettre les informations et bloquant les canaux de signalement...

Si les conditions posées par le texte sont respectées, une cause d'irresponsabilité pénale est créée à l'article 122-9 du Code pénal, afin de protéger le lanceur d'alerte, car, en pratique, les juges du fond ne sont pas toujours sensibles à une défense pénale axée sur l'existence d'un statut potentiel de lanceur d'alerte. Ainsi, n'est pas pénalement responsable la personne qui porte atteinte à un secret protégé par la loi, dès lors que cette divulgation est nécessaire et proportionnée à la sauvegarde des intérêts en cause, qu'elle intervient dans le respect des procédures de signalement définies par la loi et que la personne répond aux critères de définition du lanceur d'alerte prévus à l'article 6 de la loi n° 2016-1691 du 9 décembre 2016. Dès lors, le texte reprend les conditions de nécessité et proportionnalité à la sauvegarde des intérêts en cause attachées à la divulgation du secret protégé par la loi, comme cela est le cas pour les autres causes d'irresponsabilité pénale prévues dans le Code pénal, mais il ajoute que l'irresponsabilité pénale dépend également du respect, à la fois, de la nouvelle définition du lanceur d'alerte et du déroulement des procédures de signalement, tous deux prévus par la loi du 9 décembre 2016.

Cette nouvelle cause d'irresponsabilité pénale constitue un cas de dérogation autorisée à la protection du secret, l'irresponsabilité étant la conséquence d'une atteinte portée à une justice matérielle qui justifie la révélation, l'intérêt en cause pouvant être l'intérêt général.

La loi crée l'obligation de mettre en place un dispositif de prévention de la corruption pour les grandes entreprises. Ainsi, « *les présidents, les directeurs généraux et les gérants d'une société employant au moins cinq cents salariés, ou appartenant à un groupe de sociétés dont la société mère a son siège social en France et dont l'effectif comprend au moins cinq cents salariés, et dont le chiffre d'affaires ou le chiffre d'affaires consolidé est supérieur à 100 millions d'euros sont tenus de prendre les mesures destinées à prévenir et à détecter la commission, en France ou à l'étranger, de faits de corruption ou de trafic d'influence* ». Ces mesures consistent, notamment, en l'adoption d'un code de conduite, la mise en place d'un dispositif d'alerte interne ou d'une cartographie des risques. Ceci prend place dans le cadre d'une volonté de mise en place de dispositifs de conformité pour les entreprises de grande taille.

Dans le sens de l'amélioration des canaux de signalement, les autorités de marché doivent désormais se doter de dispositifs qui permettent de recueillir des signalements.

La loi renforce son ambition de lutte contre la corruption en créant l'Agence française anticorruption qui est destinée à remplacer le service central de prévention de la corruption. Il s'agit d'un service à compétence nationale, placé auprès du ministre de la Justice et du Ministre chargé du Budget, ayant pour mission d'aider les autorités compétentes et les personnes qui y sont confrontées à prévenir et à détecter les faits de corruption, de trafic d'influence, de concussion, de prise illégale d'intérêt, de détournement de fonds publics et de favoritisme. L'Agence est dotée d'une commission des sanctions chargée de prononcer des sanctions, par décision motivée, et peut enjoindre à la société et

à ses représentants d'adapter les procédures de conformité internes à la société destinées à la prévention et à la détection des faits de corruption ou de trafic d'influence, selon les recommandations qu'elle leur adresse à cette fin, dans un délai qu'elle fixe et qui ne peut excéder trois ans ou prononcer une sanction pécuniaire dont le montant ne peut excéder 200 000 € pour les personnes physiques et un million d'euros pour les personnes morales.

B. Les droits des personnes concernées par l'alerte

Mieux encadrer la procédure de l'alerte suppose de protéger, avant tout, le lanceur d'alerte. Ainsi, est-il constant de s'interroger sur le caractère anonyme ou confidentiel de la procédure. L'anonymat ne paraît pas réaliste dans le cadre de l'alerte professionnelle en entreprise.

En revanche, assurer la confidentialité de l'identité du lanceur d'alerte est une nécessité. C'est la raison pour laquelle la loi du 9 décembre 2016 dispose que les procédures mises en oeuvre pour recueillir les signalements, garantissent une stricte confidentialité de l'identité des auteurs du signalement, des personnes visées par celui-ci et des informations recueillies par l'ensemble des destinataires du signalement. Les éléments de nature à identifier le lanceur d'alerte ne peuvent être divulgués, sauf à l'autorité judiciaire, qu'avec le consentement de celui-ci.

Doit être assurée l'absence de discrimination pour celui qui signale. La loi n° 2016-483 du 20 avril 2016 relative à la déontologie et aux droits et obligations des fonctionnaires modifie l'article 6 ter A de la loi n° 83 -634 du 13 juillet 1983, afin de protéger contre toute sanction le fonctionnaire qui révèle une situation de conflit d'intérêts et la loi n°2016-1691 du 9 décembre 2016 inclut dans la protection le fonctionnaire qui effectue un signalement constitutif d'une alerte au sens de son article 6.

Aucune mesure ne pourra venir freiner sa carrière. En revanche, l'agent qui aura relaté ou témoigné de faits relatifs à une situation de conflit d'intérêts de mauvaise foi ou de tout autre fait susceptible d'entraîner des sanctions disciplinaires, avec l'intention de nuire ou avec la connaissance au moins partielle de l'inexactitude des faits rendus publics ou diffusés sera puni des peines prévues à l'article 226-10 alinéa 1 du Code pénal (5ans d'emprisonnement et 45 000 € d'amende).

Certains textes de droit interne avaient déjà abordé les garanties applicables au lanceur d'alerte. Il en est ainsi de la loi n° 2013-1117 du 6 décembre 2013 relative à la lutte contre la fraude fiscale et la grande délinquance économique et financière et de l'article L1132-3-3 du Code du travail, ledit article ayant été adapté par la loi n° 2016-1691 du 9 décembre 2016 afin de renvoyer aux nouvelles dispositions.

L'objectif est de garantir au salarié lanceur d'alerte une protection légale contre d'éventuelles « mesures de rétorsion » susceptibles d'avoir un impact sur sa carrière professionnelle dans l'entreprise. Le texte vise expressément le cas de la personne qui relate ou témoigne de bonne foi de faits constitutifs d'un crime ou d'un délit, à l'exception des contraventions ou, désormais, qui signale une alerte dans le respect des articles 6 à 8 la loi n°2016-1691 du 9 décembre 2016. La démarche semble toutefois réservée à des cas où l'infraction paraît démontrée.

En effet, la loi vise l'existence de faits *« constitutifs »* (et non « susceptibles de constituer ») d'un crime ou délit. Le fait d'exiger que la personne ait eu *« connaissance »* des faits paraît l'exclure du bénéfice de la protection, dans le cas où il aurait participé ou tenté de participer à l'infraction en qualité d'auteur, de coauteur ou de complice, ce qui conduit à s'interroger sur la place d'un éventuel repentir. Dès lors que la personne présente des éléments de fait qui permettent de présumer qu'elle a relaté ou témoigné de bonne foi de faits constitutifs d'un délit ou d'un crime, ou qu'elle a signalé une alerte dans le respect des articles 6 à 8 de la loi n° 2016-1691 du 9 décembre 2016 précitée, il incombe à la partie défenderesse, au vu des éléments, de prouver que sa décision est justifiée par des éléments objectifs étrangers à la déclaration ou au témoignage de l'intéressé.

La Chambre sociale de la Cour de cassation a franchi une étape importante dans la protection du lanceur d'alerte, le 30 juin 2016 (n°15-10.557), en affirmant pour la première fois qu' *« en raison de*

l'atteinte qu'il porte à la liberté d'expression, en particulier au droit pour les salariés de signaler les conduites ou actes illicites constatés par eux sur leur lieu de travail, le licenciement d'un salarié prononcé pour avoir relaté ou témoigné, de bonne foi, de faits dont il a eu connaissance dans l'exercice de ses fonctions et qui, s'ils étaient établis, seraient de nature à caractériser des infractions pénales, est atteint de nullité ». Cette décision s'inscrit dans un courant jurisprudentiel qu'elle a développé et qui admet la nullité du licenciement ou de toute mesure de rétorsion portant atteinte à une liberté fondamentale du salarié.

Cette prise de position, favorable au lanceur d'alerte, se situe dans le prolongement des décisions de la Cour européenne des droits de l'homme qui considèrent que les sanctions prises à l'encontre de salariés ayant critiqué le fonctionnement d'un service ou divulgué des conduites ou des actes illicites constatés sur leur lieu de travail constituent une violation à leur droit d'expression au sens de l'article 10-1 de la CESDH (CEDH, 18 octobre 2011, Sosinowska n°10247/09 ; CEDH 12 février 2008 Guja c/Moldavie n°14277/04).

Dans le prolongement de ces réflexions, la loi n°2016-1691 du 9 décembre 2016 prévoit, dans son article 11 qui crée un nouvel article L.911-1-1 du Code de justice administrative, que lorsqu'il est fait application de l'article L. 911-1 du Code de justice administrative, la juridiction peut prescrire de réintégrer toute personne ayant fait l'objet d'un licenciement, d'un non-renouvellement de son contrat ou d'une révocation en méconnaissance du deuxième alinéa de l'article L. 4122-4 du Code de la défense, du deuxième alinéa de l'article L. 1132-3-3 du Code du travail ou du deuxième alinéa de l'article 6 ter A de la loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires, y compris lorsque cette personne était liée par une relation à durée déterminée avec la personne morale de droit public ou l'organisme de droit privé chargé de la gestion d'un service public.

Et la loi poursuit, d'abord, en déclinant une disposition spécifique aux militaires afin de protéger celui qui signale une alerte dans les conditions légales (article L.4122-4 alinéa 2 du Code de la défense) et, ensuite, en abrogeant les textes spéciaux relatifs aux lanceurs d'alerte présents dans le Code de la santé publique (articles L.1351-1 et L.5312-4-2), dans le Code du travail (articles L.1161-1 et L.4133-5), dans la loi n° 2013-316 du 16 avril 2013 relative à l'indépendance de l'expertise en matière de santé et d'environnement et à la protection des lanceurs d'alerte (articles 1, 2.3° et 4° et 12) et dans la loi n° 2013-907 du 11 octobre 2013 relative à la transparence de la vie publique (article 25).

L'article 13.II de la loi augmente, en parallèle, à 30 000 € le montant de l'amende civile encourue dans le cas d'une plainte pour diffamation contre un lanceur d'alerte qui s'avèrerait abusive ou dilatoire, dans les conditions posées par les articles 177-2 et 212-2 du Code de procédure pénale.

La loi organique n° 2016-1690 du 9 décembre 2016 relative à la compétence du Défenseur des droits pour l'orientation et la protection des lanceurs d'alerte attribue en effet compétence au Défenseur des droits pour orienter les lanceurs d'alerte vers les autorités appropriées et pour veiller à leurs droits et libertés.

Le Conseil constitutionnel a déclaré contraire à la Constitution la phrase *« et, en tant que de besoin, de lui assurer une aide financière ou un secours financier »*, dans sa décision n° 2016-741 DC du 8 décembre 2016. Selon le Conseil, les dispositions de l'article 71-1 de la Constitution permettent au Défenseur des droits d'aider toute personne s'estimant victime d'une discrimination à identifier les procédures adaptées à son cas. En revanche, la mission confiée au Défenseur des droits de veiller au respect des droits et libertés ne comporte pas celle d'apporter directement une aide financière. Dès lors, le Conseil constitutionnel considère que le Défenseur des droits n'a pas pour attribution *« d'apporter lui-même une aide financière, qui pourrait s'avérer nécessaire, aux personnes qui peuvent le saisir »*. Par voie de conséquence, le Conseil constitutionnel a déclaré contraire à la Constitution l'article 14 de la loi qui déterminait les conditions et les modalités de versement de l'aide financière prévue par la loi organique.

Pour la personne qui fait l'objet du signalement, la présomption d'innocence et les droits fondamentaux doivent, également, faire l'objet de protection, car elle peut se trouver victime d'une dénonciation obéissant à d'autres motifs qu'un motif louable. C'est le cas, par exemple, lorsque ce signalement prend place au coeur d'un conflit préexistant, officiel ou officieux, avec d'autres personnes.

Il conviendra, également, d'articuler le bon déroulement de la procédure d'alerte avec les dispositions relatives au secret professionnel et les délits de diffamation et de dénonciation calomnieuse. La prudence est d'autant plus de mise que la dénonciation, effectuée par tout moyen et dirigée contre une personne déterminée, d'un fait qui est de nature à entraîner des sanctions judiciaires, administratives ou disciplinaires et que l'on sait totalement ou partiellement inexact, lorsqu'elle est adressée soit à un officier de justice ou de police administrative ou judiciaire, soit à une autorité ayant le pouvoir d'y donner suite ou de saisir l'autorité compétente, soit aux supérieurs hiérarchiques ou à l'employeur de la personne dénoncée, constitue une dénonciation calomnieuse passible de 5 ans d'emprisonnement et de 45 000 € d'amende, aux termes de l'article 226-10 du Code pénal.

La loi du 9 décembre 2016 poursuit en ce sens et dispose, d'une part, que les procédures mises en oeuvre pour recueillir les signalements garantissent une stricte confidentialité de l'identité des personnes visées par celui-ci et, d'autre part, que les éléments de nature à identifier la personne mise en cause par un signalement ne peuvent être divulgués, sauf à l'autorité judiciaire, qu'une fois établi le caractère fondé de l'alerte.

Afin de renforcer ces garanties, l'article 9.II de la loi n°2016-1691 du 9 décembre 2016 crée un délit spécifique, puni de deux ans d'emprisonnement et de 30 000 € d'amende, en cas de divulgation des éléments confidentiels relatifs à l'identité des lanceurs de l'alerte, des personnes visées et des informations contenues dans l'alerte.

En conclusion, la situation du lanceur d'alerte en droit français a fait l'objet d'une forte évolution depuis deux ans. Cependant, les nouveaux textes ne tranchent pas totalement tous les questionnements juridiques, voire philosophiques et politiques relatifs au mécanisme de l'alerte. Ces enjeux aux ramifications plurielles sont complexes, car le mécanisme de l'alerte constitue, selon nous, le corollaire du système démocratique, questionnant, au-delà de la règle précise qui est violée ou de la menace qui est signalée, le cadre normatif et sociétal dans son entier.

Bibliographie

- Lanceurs d'alerte : innovation juridique ou symptôme social ?, sous la direction de MC. Sordino, Presses de la Faculté de droit et science politique de l'Université de Montpellier, coll. Actes de colloque, décembre 2016.
- P. Abadie, Le salarié lanceur d'alerte en France et aux États-Unis : pour une articulation harmonieuse entre dissidence et loyauté, Les lanceurs d'alerte et les droits de l'homme, Universités de La Sorbonne et de Paris-Ouest-Nanterre-La Défense, 9 avril et 10 avril 2015.
- E. Daoud et E. Bailly, La Cour de Cassation recadre le périmètre de l'alerte des systèmes d'alerte professionnelle, Sécurité et stratégie 1/2010 (3), p.75 à 82.
- D. Lochak, La dénonciation, stade suprême ou perversion de la démocratie, in l'Etat de droit, Mélanges en l'honneur de G. Braibant, Dalloz, 1996, p.451 et s.
- D. Lochak, L'alerte éthique, entre dénonciation et désobéissance, AJDA, 2014, p. 2236 ; C.Vigouroux, Déontologie des fonctions publiques, Dalloz, 2e éd., 2012, p. 485 et s.
- C.Noiville et M.-A. Hermitte, Quelques pistes pour un statut juridique du chercheur lanceur d'alerte, EDP Sciences | Natures Sciences Sociétés, 2006/3.
- L. Ragimbeau, La liberté d'expression des agents publics : l'exemple du lanceur d'alerte, RFDA, 2015, p.975 et s.
- Chartes d'éthique, alerte professionnelle et droit du travail français : état des lieux et perspectives, Rapport rédigé par Messieurs PH. Antonmattéi et Ph. Vivien, La Documentation française, coll. des Rapports officiels, 2007.
- Délibération n° 2014-042 du 30 janvier 2014 modifiant l'autorisation unique n° 2005-305 du 8 décembre 2005 n°AU-004 relative aux traitements automatisés de données à caractère personnel mis en oeuvre dans le cadre de dispositifs d'alerte professionnelle.
- Recommandation CM/Rec(2014)7, Protection des lanceurs d'alerte, Comité des ministres du Conseil de l'Europe, 30 avril 2014.
- Conseil d'Etat, Le droit d'alerte : signaler, traiter, protéger, Les études du Conseil d'État, Étude adoptée le 25 février 2016 par l'assemblée générale plénière du Conseil d'État, La documentation française, 2016.

LA RESTITUTION DES PRODUITS DE LA CORRUPTION, PRINCIPE FONDAMENTAL DE LA CONVENTION DES NATIONS UNIES CONTRE LA CORRUPTION

JEAN-PIERRE BRUN

MAGISTRAT, SPÉCIALISTE FINANCIER SENIOR À LA BANQUE MONDIALE, PROFESSEUR ASSOCIÉ DE DROIT À L'UNIVERSITÉ CASE WESTERN RESERVE (CLEVELAND, USA)

L'article 1(b) de la Convention des Nations Unies contre la corruption (CNUCC) stipule que l'objectif du traité est de promouvoir, faciliter et soutenir la coopération internationale et l'assistance technique dans la lutte contre la corruption, y compris le recouvrement des produits d'infractions commises dans un pays signataire (notamment la corruption active et passive, le détournement ou le vol de biens publics, le recel, le blanchiment...) et « blanchis » ou investis dans un autre pays signataire.

Le recouvrement des « biens mal acquis » issus de la corruption fait aussi l'objet d'un chapitre spécifique, le chapitre V de la Convention, qui établit un cadre juridique cohérent et contraignant en vue de la détection et de la récupération des flux financiers issus de la corruption. Les voies de droit et les procédures permettant aux parties à la convention de poursuivre le recouvrement des avoirs que le chapitre V vise à faciliter peuvent peut-être brièvement résumées comme suit[1] :

- Poursuites pénales et confiscation, suivies de demandes d'entraide judiciaire pour obtenir à l'étranger la reconnaissance et l'exécution des jugements de confiscation domestiques[2] ;

- Confiscation « civile » ou « sans condamnation », suivie de demandes d'entraide en vue de faire reconnaître et exécuter le jugement a l'étranger ;

- Recouvrement direct obtenu des juridictions étrangères dans le cadre d'actions civiles en revendication ou en dommages et intérêt[3];

- Demande de restitution ou de dommages et intérêt formulée par la partie signataire lésée dans le cadre de poursuites pénales ou civiles menées par une juridiction étrangère[4].

Ces procédures sont mises en oeuvre dans le cadre des lois et règlements applicables dans les États Parties, ainsi que des conventions internationales ou bilatérales pertinentes. Dans certains cas, la convention oblige les parties signataires à établir et à mettre en oeuvre un régime juridique conforme aux stipulations de la Convention. Par exemple, la coopération internationale en vue de la confiscation des produits de la corruption, ou leur recouvrement direct dans le cadre d'actions civiles jugées par les juridictions du pays territorialement compétent font l'objet de stipulations qui s'imposent aux parties signataires. L'article 53 de la Convention oblige ainsi les pays signataires à établir et à mettre en oeuvre un cadre juridique permettant à une partie lésée de revendiquer des actifs détournés ou de demander la réparation des dommages causés par les actes de corruption. Dans d'autres cas, les États parties ont simplement l'obligation d'examiner l'opportunité de prendre certaines mesures, par exemple pour permettre la « confiscation sans condamnation pénale » du produit du crime.

Le chapitre V de la Convention s'ouvre par l'article 51, qui stipule que « la restitution des avoirs ... est un principe fondamental de la présente Convention, et les États Parties s'accordent mutuellement la coopération et l'assistance la plus étendue à cet égard ». Il est

utile de s'interroger sur la portée pratique de cette formulation, qui est si générale qu'elle semblerait ouvrir la porte a des obligations inconditionnées, notamment en matière d'entraide judiciaire.

De fait, plusieurs pays comme la Tunisie, l'Égypte, le Nigeria ou l'Ukraine ont justifié des demandes d'entraide judiciaire tendant à l'identification, la saisie, la confiscation ou le retour des profits de la corruption, en invoquant l'article 51. Ces requêtes ont parfois abouti à des décisions positives des autorités requises fondées sur des dispositions législatives ou des stipulations spécifiques de la convention ou d'autres traités multilatéraux ou bilatéraux. En l'absence de conventions ou de dispositions spécifiques, le résultat de ces demandes d'entraide fondées sur le seul article 51 s'est avéré beaucoup plus contrasté. En d'autres termes, de nombreuses requêtes ainsi formulées ont été purement et simplement ignorées ou rejetées.

Dans ces conditions, à quoi sert l'article 51 et quelle est la portée juridique du « principe fondamental » qu'il établit dans le cadre de la mise en oeuvre des procédures de recouvrement des avoirs volés ?

Dans une première approche, une note interprétative de la Convention[5] indique que l'expression « principe fondamental » n'a « aucune conséquence juridique pour les autres dispositions du chapitre V de la Convention ». L'article 51 ne serait ainsi qu'une « déclaration d'intention ». Cela signifie-t-il qu'il est juridiquement inopérant ? Nous ne le pensons pas, pour au moins trois raisons.

En premier lieu, il convient de rappeler que les « principes », même non écrits, qu'ils soient appelés « généraux » ou « fondamentaux », sont depuis longtemps une source de droit et constituent des règles juridiques sanctionnées par les tribunaux internes ou les cours de justice internationales. En droit interne français, le Conseil d'État, pour refuser de donner effet à des actes administratifs ou les annuler[6], la Cour de cassation, pour appliquer des règles de droit non expressément prévues par les textes[7], et le Conseil constitutionnel, pour dégager des normes générales à valeur constitutionnelle opposables au législateur, ont ainsi largement « reconnu », voire créé, et en tout cas, mis en oeuvre des principes non écrits souvent formulés de façon très lapidaire. Le droit international, pour sa part, a été largement fondé sur des principes généraux dégagés par la jurisprudence ou reconnus par les traités[8]. Il existe donc des principes normatifs, que les juges appliquent, y compris « contra legem[9] ». Dans le cas de l'article 51, le principe de recouvrement des biens mal acquis et de la coopération internationale est mentionné, en toute lettre, dans un article négocié et signé par 182 États Parties[10]. Même s'il est exprimé de façon très générale, peut-on l'évacuer d'un trait de plume et le considérer comme une simple déclaration philosophique, un moyen rhétorique « de ne rien exprimer »[11] ?

En second lieu, la note interprétative de la Convention qui dénie toute conséquence juridique au principe de l'article 51, finit par en reconnaître au moins une : en cas de doute concernant l'interprétation des dispositions du chapitre V sur le recouvrement d'actifs, la question, dit-elle, devrait être résolue en adoptant la solution favorable à l'objectif central de récupération des avoirs[12]. L'article 51 serait donc un outil d'interprétation des autres dispositions de la Convention. Il permettrait de renforcer les dispositions du chapitre V lorsqu'un doute sur la portée des obligations qu'il comporte conduit les parties à envisager plusieurs interprétations plus ou moins favorables à l'objectif final de recouvrement. Encore faudrait-il établir dans quel cas les parties sont en présence d'un véritable « doute » juridique, et non d'une simple divergence d'opinions. Mais, quoi qu'il en soit, le rôle de « renfort » est loin d'être négligeable : après tout, c'est bien l'arrivée de Blücher à Waterloo qui a décidé de l'issue d'une bataille incertaine, et réglé le destin d'un empire...

Enfin, sur le plan technique et pratique, de nombreux pays admettent qu'à défaut d'obligation juridique contenue dans une loi ou un traité, la fourniture de l'entraide judiciaire demandée par les autorités d'un pays étranger peut être acceptée sous simple condition de réciprocité. Dans cet esprit, l'article 51 peut être un encouragement, dans certains cas une obligation, à fournir l'entraide sollicitée par la partie lésée mais non prévue par un texte ou un instrument international. Il faut supposer que cette fourniture ne viole aucun principe fondamental ou aucune disposition législative substantielle s'imposant aux autorités de la partie requise.

Le principe fondamental de l'article 51 ne peut donc pas rester lettre morte. Il constitue au minimum un outil juridique d'interprétation de la Convention. Il peut sous certaines conditions suppléer à certaines carences des

droits internes et du droit international, voire permettre aux parties de passer outre à certains obstacles juridiques ou politiques. Finalement, il donne un fondement aux évaluations, faites dans le cadre du traité, de la conformité des États Parties à leurs engagements en matière de recouvrement des biens mal acquis. Mais comme pour tous les principes, il convient de déterminer la portée juridique et pratique qu'on peut accorder à une formulation aussi abstraite et générale, voire absolue.

Précisément, l'article 51 peut s'avérer pertinent lors des différentes étapes du processus de recouvrement des biens mal acquis : au stade de la prévention et de la détection des actifs blanchis, à celui de la recherche et de la collecte des preuves, à celui des mesures conservatoires de gel ou de saisie, et enfin lors de la mise en oeuvre de l'entraide judiciaire. En outre, l'article 51 peut représenter un argument juridique majeur pour justifier la restitution, au profit d'un État lésé, de biens confisqués ou confiscables dans le cadre d'une procédure ouverte pour blanchiment (ou recel) par un autre État Partie.

I. La prévention et la détection de la corruption et du blanchiment

La Convention est fondée sur une approche globale et « proactive » de la lutte contre la corruption. Celle-ci est vue comme un phénomène qu'il faut traiter de façon holistique y compris celui de la prévention et de la détection du transfert des produits du crime dans les États signataires. De ce fait, les politiques anti-corruption vont clairement au-delà de la fourniture de l'entraide judiciaire lors des investigations internationales.

En particulier, la collecte d'informations sur les transactions suspectes commises dans un pays signataire et leur transmission aux pays dans lesquels les actes de corruption sont commis est un élément majeur. C'est ainsi que l'article 52 de la convention oblige chaque État Partie à s'assurer que ses institutions financières vérifient l'identité de leurs clients, prennent des mesures raisonnables pour déterminer l'identité des bénéficiaires de comptes bancaires et mettent en oeuvre une vigilance renforcée en ce qui concerne les comptes ou les transactions des « personnes politiquement exposées » qui sont, ou ont été chargées d'éminentes fonctions publiques (ministres, chefs d'État, hauts fonctionnaires...).

Les États Parties doivent prendre des « mesures en vue de s'assurer que des sommes d'argent provenant d'affaires de corruption étrangères ne sont pas clandestinement déposées dans les banques ou institutions financières », et fournir aux États concernés les renseignements sur des fonds susceptibles de provenir de la commission d'infractions pénales ou fiscales.

En somme, pour être en conformité avec le principe de l'article 51 et, plus généralement, le chapitre V de la Convention, il est nécessaire d'établir, et de mettre en oeuvre efficacement, un cadre juridique permettant l'identification des transactions en lien avec la corruption d'agents publics étrangers et la transmission spontanée de cette information aux États Parties[13].

II. La recherche initiale d'informations en matière de corruption et de détournements d'actifs

Pour recouvrer les profits de la corruption, il faut conduire des investigations. Les éléments d'information nécessaires et les preuves sont recherchés et recueillis par diverses autorités d'enquête (policières, douanières, fiscales...), les cellules de renseignement financiers, les procureurs ou les juges d'instruction. Ces autorités d'enquête peuvent utiliser des informations publiquement disponibles ou des techniques spéciales d'enquête.

Certaines de ces techniques nécessitent l'autorisation d'un procureur ou d'un juge (surveillance électronique, de perquisition et de saisie, divulgation, production de documents bancaires...). D'autres mesures, non coercitives, relèvent de la seule compétence des administrations ou des enquêteurs (surveillance physique, recherches d'informations provenant de sources publiques, entretiens ou interrogatoires de témoins...). Les informations ainsi obtenues peuvent souvent être partagées avec des autorités étrangères en application de la législation, de traités internationaux ou de mémorandums ad hoc.

Cette entraide administrative évite la longueur des procédures d'entraide judiciaire dans la recherche des informations sur la localisation ou la propriété d'actifs à recouvrer. Elle permet de dessiner ce que les enquêteurs appellent « l'environnement du dossier », d'orienter les recherches à partir d'indices initiaux, et de déterminer une stratégie d'enquête. Les premiers éléments réunis sont par ailleurs très utiles pour rédiger des demandes d'entraide justifiant

l'utilisation de techniques plus coercitives lorsqu'il s'agit, cette fois, de réunir des preuves.

Le principe posé par l'article 51, qui incite les États à s'accorder l'entraide la plus étendue, peut être entendu comme s'appliquant non seulement à l'entraide judiciaire, mais à ces formes plus administratives d'échange de renseignements. Il en résulte trois conséquences importantes.

Tout d'abord, la conclusion d'accords internationaux et le renforcement de la coopération en matière d'échange de renseignements administratif sont donc essentiels pour respecter la lettre et l'esprit de l'article 51.

Par ailleurs, lorsqu'il s'agit de mesures non coercitives, les autorités administratives pourraient, même en l'absence de loi ou de traité applicable, considérer l'article 51 comme le fondement juridique de la transmission de renseignements à leurs homologues d'un autre État Partie. Tel pourrait notamment être le cas dans des pays qui, comme la France, considèrent que les conventions internationales régulièrement ratifiées et publiées s'intègrent immédiatement dans la hiérarchie des normes et ont un effet direct en droit interne[14].

Enfin, notamment dans ces pays, l'article 51 peut aussi être envisagé comme permettant de passer outre à certaines conditions formelles de l'octroi de l'entraide judiciaire. Dans certaines procédures relatives à l'un des pays dits du « printemps arabe », la France a par exemple accepté, au vu de l'article 51 de la Convention, des demandes d'entraide qui n'étaient pas rédigées en français, alors qu'en droit commun les requêtes doivent être dument traduites par les autorités étrangères.

III. Les mesures conservatoires de saisie ou de gel des produits de la corruption

Les biens mal acquis situés dans un pays signataire doivent être confisqués ou recouvrés sur demande du pays victime. Cela suppose toutefois qu'ils ne puissent être soustraits à l'action des autorités judiciaires. Ils doivent donc être « sécurisés » rapidement après détection pour éviter leur dissipation ou leur disparition. Le pouvoir d'ordonner la saisie ou le gel des actifs est accordé, selon le pays aux enquêteurs, aux procureurs, aux juges d'instructions, aux tribunaux.... Les autorités de l'État requérant ces mesures conservatoires peuvent invoquer l'article 51 pour justifier leurs requêtes ou accélérer la mise en oeuvre des décisions sollicitées. Cela peut s'avérer particulièrement utile en l'absence de convention bilatérale d'entraide judiciaire couvrant ces mesures. Dans le même esprit, l'article 51 doit aussi inciter un État partie à agir de façon proactive pour identifier, saisir ou geler des avoirs détenus par des agents publics étrangers s'il y a lieu de soupçonner qu'ils sont le produit d'infractions de corruption.

IV. La coopération et l'entraide internationales dans la conduite des investigations

Essentielle pour rassembler les preuves de la commission d'infractions et de l'origine illicite d'actifs blanchis ou recelés, la coopération internationale prend la forme soit d'une simple entraide administrative, soit de procédures plus formelles d'entraide judiciaire et d'extradition. Alors que l'entraide administrative est souvent utilisée pour échanger des informations et des renseignements en début d'enquête, l'entraide judiciaire est utilisée pour recueillir des éléments de preuve (y compris en utilisant des techniques coercitives), demander la mise en oeuvre de mesures conservatoires, et obtenir la reconnaissance ou l'exécution des décisions nationales sur le territoire d'un autre État Partie. C'est ainsi par exemple que la Tunisie a obtenu des juridictions libanaises le retour d'environ 29 millions de dollars déposés sur un compte à Beyrouth par l'épouse de l'ex-président tunisien. La Tunisie a pour cela demandé aux autorités libanaises l'exequatur d'une décision de confiscation prise par le tribunal de Tunis, qui a été accordée en application d'une convention d'entraide bilatérale entre les deux pays.

Dans ce contexte, l'article 51 a une portée juridique importante dans trois domaines principaux. Tout d'abord, pour se conformer à la convention et au principe du recouvrement des avoirs, chaque État signataire doit s'efforcer de négocier, de ratifier et de mettre en oeuvre des conventions d'entraide couvrant le recouvrement des produits de la corruption. Un État qui n'aurait signé qu'un nombre insuffisant de conventions multilatérales ou bilatérales, ou qui, les ayant signées, ne les met pas en oeuvre de façon appropriée, pourrait se trouver en situation de non-conformité avec ses engagements.

En second lieu, rappelons que l'entraide judiciaire est généralement fournie en application d'accords multilatéraux ou bilatéraux ou au simple titre de la réciprocité. Certains États Parties ont ainsi considéré que l'article 51

était un fondement juridique de la coopération administrative voire judiciaire lorsque aucun autre traité multilatéral ou bilatéral n'était applicable.

Enfin, une coopération internationale n'est possible qui si les autorités centrales jouent leur rôle de point d'entrée, communiquent les demandes d'entraide judiciaire aux autorités compétentes et s'assurent qu'elles sont exécutées dans des délais raisonnables. Pour se conformer à l'article 51, les pays signataires doivent donc désigner les autorités qui seront chargées de jouer ce rôle de coordination, d'accepter les demandes d'entraide, d'apprécier si ces demandes sont raisonnablement étayées, et de les transmettre aux parquets ou aux juges compétents. En d'autres termes, le désordre institutionnel et l'insuffisance d'organisation ne devraient pas être des excuses valables en cas de retard ou d'absence d'exécution de demandes d'entraide....

V. La confiscation et le rapatriement des actifs en vertu de l'article 57 de la CNUCC

En vertu de l'article 57 de la Convention, les produit de détournements de biens publics ou d'infractions de corruption doivent être restitués à un État Partie requérant si certaines conditions sont remplies. Pour les infractions de détournement de fonds, le retour est obligatoire en vertu de la Convention si les biens ont été confisqués en application d'un jugement définitif de confiscation pris par une juridiction de la partie requérante.

Pour les infractions autres que le détournement de fonds ou biens publics, le rapatriement est obligatoire si une condition supplémentaire est remplie : l'État requérant doit établir, au-delà d'un jugement définitif, un titre de propriété sur les biens ou l'existence d'un préjudice réparable par des dommages-intérêts.

Dans les deux cas, la condition liée à l'existence d'un jugement définitif pris par les tribunaux de l'État requérant peut-être levée par la partie requise. Or, la note d'interprétation officielle de la Convention stipule que l'État Partie requis doit au moins « envisager » de renoncer à cette exigence lorsque l'auteur des faits ne peut être poursuivi en raison du décès, de l'absence, ou de la fuite de la personne mise en cause, ou « dans d'autres cas appropriés[15] ». Ainsi, l'article 51 peut être utile, soit comme fondement juridique d'une renonciation à l'application de la condition[16], soit comme un encouragement à considérer la levée de cette exigence comme l'option à privilégier.

VI. L'échange d'informations sur les procédures pénales ou civiles engagées devant les juridictions d'un État Partie

Deux ou plusieurs États Parties peuvent avoir compétence pour poursuivre et juger la même affaire de corruption. Par exemple, les actes constituant l'élément matériel de l'infraction peuvent être commis dans différents pays. De même, une infraction de corruption peut être commise dans un pays tandis que l'un des accusés (souvent le corrupteur) réside ou est domicilié dans une autre juridiction. Enfin, le blanchiment d'argent peut être organisée dans un pays diffèrent de celui dans lequel les actes de corruption ont été commis.

Les autorités d'un État Partie souhaitant recouvrer des avoirs volés, puis détenus dans un pays étranger, peuvent ainsi apprendre que des poursuites pénales ou civiles, ou des procédures de confiscation ou de « plaider-coupable » sont en cours dans ce pays étranger. Dans cette situation, l'article 56 de la Convention dispose que, sans préjudice de son droit interne et de ses propres enquêtes, un État Partie devrait « prendre des mesures » afin de permettre à ses autorités de transmettre spontanément à l'État lésé des informations sur ces actifs.

À l'issue de la procédure, le pays lésé par les activités de corruption peut obtenir la restitution des biens situés dans le pays du blanchiment soit en compensation des dommages causés par la corruption, soit en prouvant qu'il est leur propriétaire légitime.

Dans ce contexte, l'article 51 est particulièrement utile pour, d'une part, encourager les États Parties à partager l'information en temps utile avec les pays lésés et, d'autre part, permettre à ceux-ci de faire valoir leurs droits avant confiscation. Il devrait ainsi les conduire à autoriser ou à rendre obligatoire l'information spontanée de l'État étranger victime en temps utile pour que celui puisse faire examiner ses demandes de restitution.

En conclusion, l'article 51 ne peut certes pas ouvrir un droit absolu à la saisie, à la confiscation ou au retour des biens mal acquis dans les Etats victimes de corruption ou de détournement. Il ne permet pas de passer outre à toutes les exigences du droit interne ou du droit international qui conditionnent la fourniture de l'entraide judiciaire. Il ne

pourra donc pas obliger des États Partie à exécuter des demandes d'entraide judiciaire insuffisamment explicitées en fait, non justifiées en droit, ou tout simplement impossibles à mettre en oeuvre compte tenu de contraintes pratiques.

En revanche, l'action d'un principe général posé par une Convention des Nations Unies qui a été signée par 182 États Parties ne peut pas être tenue pour négligeable. Dans un cadre normatif international lacunaire mais en plein développement, elle peut inciter et parfois obliger les États Parties à agir de bonne foi pour respecter leurs engagements, leur donner un contenu concret, et finalement renforcer l'efficacité des efforts de la communauté internationale.

Notes

1 Voir Jean-Pierre Brun, Clive Scott, Kevin M. Stephenson Larissa Gray: Manuel de Recouvrement des Biens Mal Acquis: Un Guide pour les Praticiens (Washington DC: World Bank 2011), page 7-18.

2 Voir CNUCC, article 54(1)(a).

3 Voir CNUCC article 53.

4 Voir CNUCC article 54(1)(b) et (c).

5 UNODC Technical Guide, https://www.unodc.org/documents/treaties/UNCAC/Publications/TechnicalGuide/09-84395_Ebook.pdf, page 229, A/58/422/Add.1, para. 48.

6 Depuis notamment les arrêts « Aramu » en 1945, et Syndicat General des Ingénieurs Conseil en 1959

7 Que l'on songe à la responsabilité des « choses que l'on a sous sa garde » qui a bouleversé le droit de la responsabilité.

8 Voir l'article 38, § 1du Statut de la Cour permanente de justice internationale faisant référence aux « principes généraux de droit reconnus par les nations civilisées ».

9 Voir sur ces points l'article de M. Patrick Morvan, « Le Principe en Droit, le principe de Droit « http://patrickmorvan.over-blog.com/article-6469413.html

10 https://www.unodc.org/unodc/en/corruption/uncac.html

11 http://patrickmorvan.over-blog.com/article-6469413.html

12 UNODC Technical Guide, https://www.unodc.org/documents/treaties/UNCAC/Publications/TechnicalGuide/09-84395_Ebook.pdf, page 191.

13 Consulter sur ce point: UNCAC Guidance note "Guidance to filling in the revised draft self-assessment checklist on the implementation of chapters II (Preventive measures) and V (Asset recovery) of the United Nations Convention against Corruption", CAC/COSP/IRG/2016/CRP.1, pages 81 et 82.

14 Article 55 de la constitution, qui, de surcroît, accorde aux traités régulièrement ratifiés et publiés une autorité supérieure aux lois.

15 En visant "d'autres cas appropriés", le texte oblige les Etats parties à se demander si les circonstances spécifiques du dossier (au-delà de la mort, de l'absence, ou de la fuite de l'accusé, pourraient justifier la renonciation à la condition.

16 Ce fondement juridique est très important pour justifier que des valeurs patrimoniales soient reversées à un État étranger et non simplement versées au Trésor de l'Etat sont situées et confisquées.

OUVRAGES RÉCENTS

ONU : LA GRANDE IMPOSTURE

AUTEUR : PAULINE LIÉTAR

EDITEUR : ALBIN MICHEL

Présentation de l'éditeur

Pour la première fois, une enquête inédite brise l'omerta qui règne au coeur d'une organisation moins vertueuse qu'elle le proclame : l'ONU. Au terme d'un long travail d'investigation, la journaliste Pauline Liétar en dévoile les pratiques hallucinantes... et courantes : les soutiens politiques s'achètent, les gaspillages sont légion.

Des diplomates et des fonctionnaires ont d'ailleurs été poursuivis pour trafic d'influence et corruption. L'argent des contribuables est dilapidé : près d'un demi-milliard d'euros dans un intranet défectueux, des emplois quasi fictifs dans certains départements et missions.

En dépit des beaux discours, même des ennemis de l'ONU, comme des trafiquants d'armes et des groupes terroristes, ont profité de l'argent de l'organisation. Notamment via d'obscures ONG locales. Après le scandale Pétrole contre nourriture, les choses devaient pourtant changer...

L'impunité règne aux Nations unies. Ce document accablant le prouve.

« FOCUS SUR LA COMPÉTENCE DU SERVICE NATIONAL DE LA DOUANE JUDICIAIRE »

DOROTHÉE GOETZ

DOCTEURE EN DROIT PÉNAL ET SCIENCES CRIMINELLES, ASSISTANTE SPÉCIALISÉE AU PARQUET DU TRIBUNAL DE GRANDE INSTANCE DE STRASBOURG

Dans son arrêt de principe du 28 juin 2017 (n° de pourvoi : 16-83372), la chambre criminelle de la Cour de cassation rappelle avec fermeté que *« les agents des douanes habilités ne peuvent effectuer des enquêtes judiciaires que sur réquisition du procureur de la République ou sur commission rogatoire du juge d'instruction visant les infractions mentionnées par l'article 28-1, I du Code de procédure pénale »*.

Fruit d'une interprétation stricte du texte, ce principe ne saurait, sur le fond, être contesté. Toutefois, pour saisir toute la portée de cette solution, il importe de rappeler qu'en l'espèce, une note d'information de la cellule Tracfin signalait plusieurs anomalies dans le fonctionnement des comptes bancaires d'une personne seule et âgée. Il était relevé que l'individu qui disposait d'une procuration sur les comptes de cette personne réalisait concomitamment des investissements immobiliers et souscrivait à des contrats d'assurance-vie. En outre, ses comptes bancaires ainsi que ceux de sa famille présentaient des soldes positifs élevés. Le procureur de la République confiait une enquête préliminaire au service national de la douane judiciaire. L'individu qui disposait de la procuration était poursuivi des chefs d'abus de confiance, faux et usage. Le tribunal correctionnel l'a déclaré coupable du seul chef d'abus de confiance, choix qui a ensuite été confirmé en appel.

Dans son pourvoi en cassation, l'intéressé reprochait à la cour d'appel d'avoir rejeté son moyen de nullité de l'enquête diligentée et des actes de procédure subséquents. Il estimait en effet que le service national de douane judiciaire auquel l'enquête avait été confiée n'avait pas compétence pour enquêter sur les faits signalés par Tracfin. La base juridique de son raisonnement reposait sur l'article 28-1 du Code de procédure pénale. Selon cet article, le procureur de la République peut habiliter des agents des douanes à effectuer des enquêtes portant sur une liste limitative d'infractions, dont le blanchiment, et sur toute infraction qui lui serait connexe., Il considérait ainsi que le procureur de la République avait requis les agents des douanes pour enquêter sur des faits constitutifs d'abus de faiblesse, infraction qui ne figure pas parmi celles visées par l'article 28-1 du Code de procédure pénale.

Pour rejeter la demande en nullité, la cour d'appel avançait un raisonnement pragmatique et audacieux. Tout en reconnaissant que ni le signalement Tracfin ni le soit-transmis ne visaient expressément le blanchiment ou une infraction énumérée à l'article 28-1 du Code de procédure pénale, les seconds juges considéraient que le signalement Tracfin ne se limitait pas à décrire des faits susceptibles de caractériser un abus de faiblesse. En ce sens, ils soulignaient que le signalement mettait en lumière une situation financière suspecte. Dès lors, la cour d'appel en déduisait que

les fonds litigieux pouvaient provenir d'un abus de faiblesse connexe à un blanchiment. En conséquence, les juges du fond estimaient que, sans être explicitement nommé, le blanchiment était en réalité compris dans le signalement Tracfin. Ils en déduisaient donc logiquement que le service national de la douane judiciaire était compétent pour enquêter.

Séduisante, cette thèse n'a pas convaincu la Cour de cassation qui souligne que « ni les réquisitions du procureur de la République saisissant la douane judiciaire ni la note de Tracfin à laquelle ces réquisitions renvoyaient ne visaient l'une des infractions mentionnées par l'article 28-1, I, 1° à 7° du Code de procédure pénale ». Les hauts magistrats en concluent que la cour d'appel a méconnu l'article 28-1 du Code de procédure pénale. Signe de son refus d'adhérer à la logique pourtant audacieuse des juges du fond, la chambre criminelle rappelle fermement le principe suivant : « les agents des douanes habilités ne peuvent effectuer des enquêtes judiciaires que sur réquisition du procureur de la République ou sur commission rogatoire du juge d'instruction visant les infractions mentionnées par l'article 28-1, I, 1° à 7° du Code de procédure pénale ».

Ce faisant, dans une lecture rigoureuse – voire rigoriste – de l'article 28-1 du Code de procédure pénale, la Cour de cassation rejette l'analyse de la cour d'appel qui n'était pourtant pas dénuée de toute logique juridique. En effet, l'objet de ce signalement Tracfin était précisément de mettre en lumière une situation financière suspecte. Si Tracfin concluait sa note d'information en indiquant que les éléments relatés prêtaient « à de fortes suspicions d'abus de faiblesse » il était également précisé que « les ponctions opérées sur les comptes [...] pourraient avoir permis [au prévenu] de dégager les revenus nécessaires à la construction de son patrimoine ».

Cette phrase est importante. C'est précisément elle qui permettait à la cour d'appel de considérer que, sans le nommer, Tracfin faisait référence à un blanchiment, c'est-à-dire à une opération consistant à masquer l'origine frauduleuse des sommes d'argent litigieuses. En outre, cette vision était confirmée par le rapport de synthèse du service de la douane judiciaire qui concluait à la caractérisation de l'infraction de blanchiment.

Pourtant, la solution défendue par les juges du fond présentait, selon nous, au moins deux avantages. Premièrement, cette position hardie tirait opportunément, en matière de blanchiment, toutes les conséquences du « jeu de construction » intellectuel qu'est la qualification pénale (I)[1]. Deuxièmement, outre la logique juridique sur laquelle elle nous paraît reposer, cette position avait l'avantage de mettre à profit ce précieux outil qu'est la douane judiciaire. Il s'agit en effet d'une force de police judiciaire, une « police thématique », qui permet aux magistrats de confier, dans certaines matières économiques et financières, des enquêtes à des officiers de douane judiciaire spécialisés[2] (II).

I. Précisions sur la qualification de blanchiment

La particularité des faits de blanchiment est de toujours devoir se situer dans le sillage de la commission d'une infraction préalable. Le blanchiment - également dénommé blanchissage en droit suisse ou blanchissement en droit canadien[3] - compte parmi les quelques rares métaphores employées par le droit pénal. Cela explique qu'en l'espèce, la situation financière suspecte dégagée par le service de la douane judiciaire et sur laquelle insistent les juges du fond est mise en lien avec une infraction préalable, à savoir un abus de faiblesse.

Il faut reconnaître que ce critère de la suspicion d'origine frauduleuse des fonds est indéniablement au coeur de l'infraction de blanchiment. C'est d'ailleurs en ce sens que s'engage depuis de nombreuses années le législateur lorsqu'il précise le champ d'application des déclarations de soupçons de blanchiment. Ainsi, le décret n° 2009-874 du 16 juillet 2009 est venu préciser à quelles conditions peut intervenir une déclaration de soupçon de blanchiment en matière de fraude fiscale. Le texte précise que la déclaration prévue à l'article L. 561-15-II du Code monétaire et financier doit être effectuée par les personnes mentionnées à l'article L. 561-2 du même code « en fonction de la spécificité de leur profession, conformément aux obligations de vigilance exercées sur leur clientèle et au regard des pièces et documents qu'elles réunissent à cet effet ». L'intérêt de cette disposition est de poser seize critères destinés à guider

les professionnels dans la détection du blanchiment de fraude fiscale.

Ces critères sont les suivants :

1° L'utilisation de sociétés écran, dont l'activité n'est pas cohérente avec l'objet social ou ayant leur siège social dans un État ou un territoire qui n'a pas conclu avec la France une convention fiscale permettant l'accès aux informations bancaires, identifié à partir d'une liste publiée par l'administration fiscale, ou à l'adresse privée d'un des bénéficiaires de l'opération suspecte ou chez un domiciliataire au sens de l'article L. 123-11 du Code de commerce ;

2° La réalisation d'opérations financières par des sociétés dans lesquelles sont intervenus des changements statutaires fréquents non justifiés par la situation économique de l'entreprise ;

3° Le recours à l'interposition de personnes physiques n'intervenant qu'en apparence pour le compte de sociétés ou de particuliers impliqués dans des opérations financières ;

4° La réalisation d'opérations financières incohérentes au regard des activités habituelles de l'entreprise ou d'opérations suspectes dans des secteurs sensibles aux fraudes à la TVA de type carrousel, tels que les secteurs de l'informatique, de la téléphonie, du matériel électronique, du matériel électroménager, de la hi-fi et de la vidéo ;

5° La progression forte et inexpliquée, sur une courte période, des sommes créditées sur les comptes nouvellement ouverts ou jusque-là peu actifs ou inactifs, liée le cas échéant à une augmentation importante du nombre et du volume des opérations ou au recours à des sociétés en sommeil ou peu actives dans lesquelles ont pu intervenir des changements statutaires récents ;

6° La constatation d'anomalies dans les factures ou les bons de commande lorsqu'ils sont présentés comme justification des opérations financières, telles que l'absence du numéro d'immatriculation au registre du commerce et des sociétés, du numéro SIREN, du numéro de TVA, de numéro de facture, d'adresse ou de dates ;

7° Le recours inexpliqué à des comptes utilisés comme des comptes de passage ou par lesquels transitent de multiples opérations tant au débit qu'au crédit, alors que les soldes des comptes sont souvent proches de zéro ;

8° Le retrait fréquent d'espèces d'un compte professionnel ou leur dépôt sur un tel compte non justifié par le niveau ou la nature de l'activité économique ;

9° La difficulté d'identifier les bénéficiaires effectifs et les liens entre l'origine et la destination des fonds en raison de l'utilisation de comptes intermédiaires ou de comptes de professionnels non financiers comme comptes de passage, ou du recours à des structures sociétaires complexes et à des montages juridiques et financiers rendant peu transparents les mécanismes de gestion et d'administration ;

10° Les opérations financières internationales sans cause juridique ou économique apparente se limitant le plus souvent à de simples transits de fonds en provenance ou à destination de l'étranger notamment lorsqu'elles sont réalisées avec des États ou des territoires visés au 1° ;

11° Le refus du client de produire des pièces justificatives quant à la provenance des fonds reçus ou quant aux motifs avancés des paiements, ou l'impossibilité de produire ces pièces ;

12° Le transfert de fonds vers un pays étranger suivi de leur rapatriement sous la forme de prêts ;

13° L'organisation de l'insolvabilité par la vente rapide d'actifs à des personnes physiques ou morales liées ou à des conditions qui traduisent un déséquilibre manifeste et injustifié des termes de la vente ;

14° L'utilisation régulière par des personnes physiques domiciliées et ayant une activité en France de comptes détenus par des sociétés étrangères ;

15° Le dépôt par un particulier de fonds sans rapport avec son activité ou sa situation patrimoniale connues ;

16° La réalisation d'une transaction immobilière à un prix manifestement sous-évalué.

Cette énumération est intéressante car elle montre que tous ces critères ont un point commun : ils reposent tous sur une suspicion qui porte sur la situation financière de l'intéressé. Dans l'arrêt rapporté, cette suspicion ressortait du rapport de synthèse du service de la douane judiciaire. Aussi, les juges du fond pensaient-ils pouvoir s'appuyer sur ce climat de suspicion pour justifier la compétence du service de la douane judiciaire. En effet, selon leur analyse, ce service enquêtait, sans jamais le nommer, sur un abus de faiblesse connexe à un blanchiment.

II. le service de la douane judiciaire : un outil précieux

Le texte au coeur de cet arrêt est l'article 28-1 du Code de procédure pénale. Insérée dans le code par la loi du 23 juin 1999 renforçant l'efficacité de la procédure pénale, cette disposition autorise certains agents des douanes spécialement habilités à cet effet par l'autorité judiciaire à effectuer, sur réquisitions expresses du parquet ou sur commission rogatoire du juge d'instruction, des enquêtes judiciaires dans certains domaines limitativement énumérés et pour l'essentiel relatifs à la matière économique et financière. L'intérêt pratique du service de la douane judiciaire est évident : il s'agit de permettre aux magistrats du parquet et aux juges d'instruction de bénéficier du concours de véritables enquêteurs judiciaires spécialisés. L'expérience technique des agents composant la douane judiciaire constitue en effet une véritable plus-value utile à la justice pénale. La douane judiciaire ne doit donc pas être perçue comme une concurrente des autres services de police judiciaire mais comme un utile complément.

La spécificité du service national de la douane judiciaire est d'être dirigé par un magistrat de l'ordre judiciaire détaché auprès du ministère de l'Économie, des Finances et de l'Industrie et exerçant ses fonctions auprès du directeur général des douanes et droits indirects (articles. 28-1, II, R. 15-33-10 du Code de procédure pénale), ce qui constitue une garantie pour la sécurité juridique des investigations. Ce magistrat reçoit les commissions rogatoires des juges d'instruction et les « soit-transmis pour enquête » adressés par le parquet (article R. 15-33-12 du Code de procédure pénale). En outre, il peut faire des propositions aux autorités judiciaires sur les missions susceptibles d'être confiées au service national de la douane judiciaire (article R. 15-33-11).

Dès lors, pourquoi la Cour de cassation s'est-elle si fermement opposée à cette lecture pragmatique de l'article 28-1 du Code de procédure pénale proposée par les juges du fond ?

Il nous semble que la rédaction de cet article explique ce choix. Le texte est en effet rédigé exclusivement sur un mode négatif. Ainsi, au paragraphe 1, alinéa 3, il est précisé que : « ils n'ont pas compétence... », et au paragraphe 3, alinéa 1, le législateur indique que « les agents...ne sont pas compétents », dans le même esprit, au paragraphe 8, il souligne que « les agents ne peuvent... ». Il découle de ce choix rédactionnel que c'est en réalité avec prudence que le législateur a accueilli ces nouveaux enquêteurs. Cela s'explique par le souhait d'éviter tout conflit de compétence avec les services des ministres de l'Intérieur et de la Défense en ne créant pas une troisième force de police judiciaire. Dans le même esprit, le législateur a sans doute souhaité, par crainte d'une éventuelle inconstitutionnalité, éviter un cumul des pouvoirs entre le Code des douanes et le Code de procédure pénale. Sans doute pour ces deux raisons – et malgré tout l'attrait de la position des juges du fond-, la chambre criminelle a donc préféré opter pour une lecture stricte de l'article 28-1.

Notes :

1. J. Larguier, « Théorie des ensembles et qualification pénale », in Mélanges Chavanne, Litec, 1990, p. 99

2. M. Dobkine, La douane judiciaire, premier bilan d'une police thématique, D. 2002. 3284 ; La création d'une nouvelle force de police judiciaire : la douane judiciaire, D. 2001. 1475 ; P. Carli, Service national de douane judiciaire : officier de police judiciaire douanière ? officier de douane judiciaire ?, D. 2003. 2701

3. THONY, Les politiques législatives de lutte contre le blanchiment en Europe, RPDP 1997. 307

« LA CYBERCRIMINALITÉ ET L'ENTREPRISE : LE RÔLE DE L'AVOCAT »

CHRISTIANE FÉRAL-SCHUHL

AVOCAT ASSOCIÉ, ANCIEN BÂTONNIER DE PARIS

La cybercriminalité s'impose de plus en plus comme l'un des risques majeurs dans l'environnement numérique de l'entreprise, avec une progression exponentielle. Pas une semaine ne s'écoule sans qu'un grand groupe ne soit victime d'une faille majeure. Les agressions sont de plus en plus insidieuses car elles s'accompagnent de signaux faibles et laissent peu de traces, à l'exemple des menaces de type APT *(« advanced permanent threat »)* qui ciblent une entreprise en particulier, ou encore les attaquent pour cartographier puis pénétrer ses réseaux dans le but de dérober des données ou des informations. Les vols de mots de passe se chiffrent en centaines de millions.

S'il ne faut pas négliger la menace extérieure à l'entreprise d'autant que l'hébergement des données s'effectue de plus en plus à l'extérieur via le *cloud*, il ne faut pas sous-estimer la menace interne. En effet, dans 80 % des cas, ce sont toujours des employés ou d'ex-salariés qui, pour des raisons diverses surtout par négligence portent atteinte aux systèmes d'information de leurs employeurs ou ex-employeurs.

Face à ces menaces, l'avocat a un rôle central pour conseiller et accompagner le chef d'entreprise dans l'identification des zones de risques et des mesures préventives à déployer (I). Par ailleurs, en présence d'un acte de « cyber-malveillance », il est l'interlocuteur privilégié pour guider le chef d'entreprise dans les mesures à prendre et pour défendre ses intérêts (II).

I. Des actions pour prévenir les risques liés à la cybercriminalité

Afin de prévenir les risques liés à la cybercriminalité, l'avocat doit rappeler à son client les obligations de sécurité du chef d'entreprise (A) et l'orienter dans la mise en place de bonnes pratiques (B).

A. Une obligation de sécurité renforcée à la charge du chef d'entreprise

L'avocat doit s'assurer que son client a bien pris connaissance des obligations lui incombant au titre de la sécurité de ses systèmes d'information, tout particulièrement lorsqu'il s'agit de traitements de données à caractère personnel.

En effet, on rappellera que traditionnellement, la responsabilité du chef d'entreprise peut être engagée par les victimes, d'une part, sur le plan civil pour obtenir réparation du préjudice qu'elles ont subi suite à une faute ou une négligence (C. civ., art. 1240 ; anc. C. civ., art. 1383), lorsque la divulgation est volontaire (C. civ. art. 1241 ; ancien C. civ., art. 1383) ou résulte soit d'une négligence, soit d'une imprudence. D'autre part, sur le plan pénal, s'agissant de données à caractère personnel, l'article 34 de la loi Informatique et Libertés impose au responsable du traitement des données *« de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès »*. Tout manquement

à cette obligation expose le chef d'entreprise à des sanctions pénales lourdes à savoir cinq ans d'emprisonnement et 300 000 euros d'amende (C. pén., art. 226-17[1]).

Ce dispositif a été considérablement renforcé pour mettre à la charge du chef d'entreprise, non plus une obligation de moyens, mais des obligations de sécurité réglementaires, notamment avec le Règlement général pour la protection des données en date du 27 avril 2016 (RGPD) et la Directive network and information security du 6 juillet 2016 (NSI). Ces textes européens entreront en vigueur fin mai 2018. Par ailleurs, les États membres ont été fermement appelés *« à prévoir, dans le cadre de leur droit national, des mesures pertinentes permettant d'engager la responsabilité des personnes morales, lorsque celles-ci n'ont de toute évidence pas assuré un niveau de protection suffisant contre les cyberattaques »* (Dir. 2013/40/UE, 12 août 2013, Cons. 26). Cette directive, dont l'objectif affiché est de *« rapprocher le droit pénal des États membres dans le domaine des attaques contre les systèmes d'information »*, a été transposée en droit français par la loi n° 2015-993 du 17 août 2015[2] portant adaptation de la procédure pénale au droit de l'Union européenne.

Dans l'intervalle, la jurisprudence n'hésite pas à sanctionner les actes de négligence du chef d'entreprise. Ainsi, la Cour d'appel de Paris, dans un arrêt du 5 février 2014[3], constatant qu'un accès frauduleux avait été rendu possible par une défaillance technique, a refusé de caractériser la fraude. Même si les juges d'appel ont admis que l'internaute s'était maintenu frauduleusement dans le système[4], ils ont manifestement voulu sanctionner la négligence du maître du système qui n'avait pas suffisamment sécurisé l'accès. La même juridiction avait précédemment suivi un raisonnement similaire dans une affaire opposant une société dont le système d'information avait été infesté par un virus à son fournisseur de détecteur de virus : les juges ont considéré qu'elle ne pouvait invoquer la défaillance de la protection antivirus comme juste motif de la résiliation dès lors qu'elle avait laissé son personnel se connecter sur des « sites informatiques étrangers à son activité, voire illégaux tels que les sites qui permettent de télécharger gratuitement des programmes habituellement payants », et qu'elle avait donc « rendu, par sa faute, inefficace la protection que [l'autre société] s'était engagée à lui fournir »[5]. Précédemment, la Cour de cassation avait confirmé la condamnation des responsables d'un organisme au regard de l'insuffisance de formation du personnel, considérant que cela avait favorisé l'accès par des tiers non autorisés à des données nominatives (Cass. crim., 30 octobre 2001, n°99-82.136).

B. Les bonnes pratiques à mettre en oeuvre

L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) propose une méthodologie[6] sur divers thèmes, sous différentes formes (guides, recommandations, articles). Elle a notamment publié deux fiches de « bonnes pratiques »[7] et d'information à destination des administrateurs de sites, afin de rappeler des règles permettant de se prémunir contre les cyberattaques. Elle a également publié un Guide[8] d'hygiène informatique destiné aux entreprises, contenant quarante-deux règles simples à appliquer concernant la sécurité des messageries, du poste de travail, des imprimantes, etc. Ainsi, elle recommande d'utiliser des mots de passe complexes pour l'accès aux interfaces d'administration et d'appliquer les correctifs de sécurité. Sur ce point, la CNIL propose également quelques conseils pour la gestion des mots de passe[9]. Par ailleurs, le Guide[10] Afnor a publié en décembre 2014 sur la prévention et la gestion des fuites d'informations (BP Z 90-001).

En marge de ces préconisations, l'avocat peut anticiper, en concertation avec la direction juridique, la direction informatique et les services de sécurité des systèmes d'information, l'analyse des zones de risques au sein de l'entreprise. Pour l'essentiel, on retrouve les mêmes préoccupations telles que la continuité des services de l'entreprise, la conservation du patrimoine informationnel, la préservation du patrimoine incorporel ou encore la gestion sécurisée des objets connectés et BYOD (Bring Your Own Device) des employés. Pour chacune de ces thématiques, et d'autres encore à identifier en fonction de l'activité propre de l'entreprise, l'avocat peut accompagner ses interlocuteurs dans la vérification et/ou la mise en place de mesures spécifiques telles que les clauses organisant les délais d'intervention et de remise en ordre de marche opérationnelle en cas de rupture dans la continuité du service, ou encore définir la politique d'archivage permettant de garantir le conservation et la restitution des données avec toutes les garanties

d'intégrité, voire encore la mise en place d'une charte définissant notamment les conditions d'utilisation des objets connectés à distance par les salariés....

II. Des actions en présence d'un acte de malveillance

La réactivité et la maîtrise du dispositif à mettre en oeuvre sont déterminantes.

L'entreprise victime de cybercriminalité doit réagir immédiatement, en mode de gestion de crise lorsqu'il faut éradiquer le risque, qu'il s'agisse d'un virus à même de contaminer tous les serveurs ou encore du pillage du patrimoine informationnel. L'avocat a toute sa place dans le dispositif car il doit, cumulativement, accompagner son client dans le respect des formalités déclaratives obligatoires auprès des autorités compétentes en présence de failles de sécurité (A), diriger la collecte des éléments de preuve pertinents en vue d'une éventuelle action judiciaire, avec l'aide des équipes informatiques internes mais aussi d'experts et d'huissiers (B), déclencher les procédures adéquates en s'adressant aux interlocuteurs spécialisés (C).

A. La notification des failles de sécurité

L'obligation de notification des failles de sécurité exige une bonne maîtrise et connaissance des textes applicables, lesquels prennent en compte la nature des données concernées et/ou l'activité de l'entreprise.

La notification des failles de sécurité doit se faire auprès de la CNIL en présence de traitements de données à caractère personnel et auprès de l'ANSSI pour certains secteurs d'activités spécifiques.

Cette obligation de notification a d'abord visé les opérateurs télécoms et les fournisseurs d'accès à internet (FAI). Elle a vocation à se généraliser comme l'illustre le RGPD (art. 33 et 34) qui prévoit que le responsable de traitement est tenu de notifier les failles de sécurité à la CNIL dans les meilleurs délais (72h après en avoir pris connaissance). À défaut de pouvoir respecter ce délai, la notification doit être accompagnée des motifs du retard. En présence d'un sous-traitant, on rappellera que ce dernier est également tenu à de notifier la faille.

Cependant, cette notification n'est pas requise lorsque la violation n'est pas de nature à engendrer des risques pour les droits et les libertés des personnes physiques. Tel serait le cas d'une violation portant sur un fichier crypté ou anonymisé. D'où l'importance des mesures préventives évoquées précédemment.

Lorsque la notification s'avère indispensable, elle doit inclure des informations techniques telles que la description de la nature de la violation des données (catégories de données, nombre de personnes concernées), le nom du Délégué à la protection des données (DPO ou tout autre point de contact auprès duquel des informations peuvent être obtenues), la description des conséquences probables de la violation et des mesures que le responsable de traitement a prises ou se propose de prendre pour remédier à la violation ou pour en atténuer les conséquences négatives. S'il n'est pas possible de fournir toutes ces informations en même temps, celles-ci peuvent être communiquées de manière échelonnée sans autre retard indu.

Par ailleurs, le chef d'entreprise, en sa qualité de responsable du traitement des données personnelles, doit informer dans les meilleurs délais la personne concernée de la violation de ses données ; si la communication individuelle exige des efforts disproportionnés, la communication pourra se faire par voie de presse.

Enfin, lorsque l'activité de l'entreprise porte sur un des secteurs spécifiques tels qu'ils sont décrits dans les décrets d'application[11] de la loi de programmation militaire n°2013-1168 du 18 décembre 2013[12], il s'agit d'un organisme d'importance vitale (OIV)[13]. En France, les OIV sont au nombre environ de 250. Ils désignent des opérateurs publics ou privés exploitant des établissements ou utilisant des installations et ouvrages, dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation. Ces établissements, installations ou ouvrages sont désignés par l'autorité administrative (C. défense, art. L. 1332-1). Les trois premiers arrêtés relatifs à la sécurité des OIV publiés le 23 juin 2016[14], visent les secteurs de l'eau, la santé et l'alimentation. Il y a eu par la suite quatre nouveaux arrêtés publiés le 28 novembre 2016[15], concernant les secteurs de l'industrie, les finances, l'audiovisuel et de l'information, les communications électroniques et Internet. D'autres encore devraient suivre, dans les domaines de l'énergie, les transports, les activités civiles, militaires et judiciaires de l'État. Les OIV sont

tenus de notifier sans délai à l'ANSSI des incidents affectant le fonctionnement ou la sécurité de ses systèmes d'information (C. défense, art. L.332-6-2).

Cette obligation de notification des failles de sécurité va encore s'étendre avec l'entrée en vigueur, le 9 mai 2018, de la directive n°2016/1148 « Sécurité des réseaux et de l'information (SRI)[16]» du 6 juillet 2016[17]. En effet, elle prévoit que *« les opérateurs de services essentiels[18] et les fournisseurs de service numérique [soient] soumis à des exigences en matière de sécurité et de notification, afin de promouvoir une culture de gestion des risques et de faire en sorte que les incidents les plus graves soient signalés »* (considérant 4).

Dans tous les cas, l'entreprise ne pourra plus passer sous silence les cyberattaques dont elle est victime, l'objectif étant désormais de partager l'information le plus largement possible pour permettre aux victimes par ricochet de prendre des mesures préventives et d'éviter les effets induits.

B. Des éléments de preuve non contestables

Bien que la preuve soit libre en matière pénale, son appréciation par le juge reste souvent liée au respect de certaines exigences qui relèvent de la matière civile. Il est donc prudent de procéder rapidement, une fois l'acte malveillant identifié, à la collecte et à la conservation des éléments de preuve par un moyen fiable.

L'un des moyens de constituer une preuve numérique irrévocable consiste à passer par les services d'un expert dans le cadre de l'inforensique[19]. Ce concept consiste en l'application de processus et techniques d'investigation permettant de collecter et d'analyser des éléments ayant valeur de preuves en vue d'une procédure judiciaire. La technique d'investigation numérique la plus courante est celle de la copie-image, consistant en la représentation « bit à bit » intégrale de l'information numérique présente sur un support d'information, espaces non utilisés et non alloués inclus. Réalisée dans le cadre d'une investigation numérique légale, une copie-image doit être pure et parfaite ; dans le cas contraire, le rapport d'investigation doit expliquer les raisons de l'impureté ou de l'imperfection. À l'issue de ses investigations, l'expert consigne ses travaux dans un rapport d'investigation *(« chain of evidence »* en anglais) qui retrace l'ensemble des étapes permettant de garantir qu'une preuve numérique est issue de manière irrévocable d'une information numérique.

Le moyen le plus courant consiste à faire établir un constat d'huissier, parfois en présence d'experts agréés ou encore de prestataires tiers certifiés tels que l'Agence pour la Protection des Programmes (APP). Cette démarche exige une grande vigilance, les constats d'huissier ayant donné lieu à une jurisprudence fluctuante précisant progressivement les contraintes spécifiques qui s'attachent à l'établissement de preuves sur l'Internet, ajoutant aux conditions usuelles (mentions obligatoires, double original, *etc.*). Ainsi peut être citée l'ordonnance rendue par le juge des référés du tribunal de grande instance de Paris, écartant un constat d'huissier produit au motif que celui-ci ne faisait mention d'aucune des précautions préalables qu'il appartient à un huissier de prendre (indication du navigateur utilisé, horodatage de l'ordinateur conforme à celui du constat, « caches » vidés des cookies, fichiers temporaires et de l'historique des pages visitées, *etc.*). Dans cette affaire, le juge reprochait également à l'huissier de ne pas avoir procédé lui-même aux *« constatations qu'il est chargé de relever personnellement et sous sa responsabilité »*[20].

Le respect de la norme Afnor NFZ67-147 concernant « le mode opératoire de procès-verbal de constat sur Internet effectué par huissier de justice », publiée le 1er septembre 2010[21] constitue également un référentiel pertinent. Cette norme a fait émerger de nouveaux pré-requis techniques, ouvrant la voie à de nouvelles contestations sur la validité des constats lorsque ceux-ci, produits à titre de preuve, ne respectaient pas strictement les exigences énoncées par la norme, ceci alors même qu'ils étaient conformes aux exigences issues de la jurisprudence antérieure à 2010. Cependant, il convient de signaler cet arrêt de la cour d'appel de Paris du 27 février 2013[22] qui a retenu que la norme Afnor NFZ67-147 ne constituait qu'un recueil de recommandations de bonnes pratiques et, à ce titre, n'avait pas de caractère obligatoire. Les juges ont donc écarté les griefs qui étaient fondés exclusivement sur le non-respect de la norme pour s'attacher à l'examen des diligences préalables au constat : la description du matériel ayant servi aux constatations, indiquer l'adresse IP de l'ordinateur ayant servi aux opérations de constat, vider les caches de l'ordinateur préalablement à l'ensemble des constatations, désactiver la connexion

par proxy, supprimer l'ensemble des fichiers temporaires stockés sur l'ordinateur, supprimer les *cookies* ainsi que l'historique de navigation.

Ces éléments de preuve sont souvent au coeur des débats judiciaires qui vont suivre. D'où l'importance d'encadrer précisément la manière dont ils sont collectés et conservés.

C. Coopérer avec les autorités chargées d'enquête

La spécialisation des autorités chargées d'enquête participe de l'efficacité des procédures judiciaires, que ce soit à l'échelle nationale ou européenne.

La Brigade d'enquêtes sur les fraudes aux technologies de l'information (BEFTI) est l'un des acteurs les plus connus. Sa mission, limitée à Paris et aux trois départements constituant la petite couronne, consiste à lutter contre les atteintes aux systèmes de traitement automatisé de données, ainsi qu'aux infractions liées à la loi Informatique et Libertés, ou encore aux infractions plus classiques (escroquerie, abus de confiance, atteintes aux personnes et à la représentation de la personne, ou encore infractions à la loi du 29 juillet 1881 sur la liberté de la presse). Cette brigade peut être saisie directement par l'avocat, sur plainte de l'entreprise directement[23], sur transmission du dossier par le parquet dans l'hypothèse où la victime écrit directement au procureur de la République, ou encore sur délégation d'un juge d'instruction dans le cadre d'une commission rogatoire.

Par ailleurs, la sous-direction de lutte contre la cybercriminalité[24] créée au sein de la Direction centrale de la police judiciaire est en charge du pilotage et de la coordination de la lutte contre la cybercriminalité au plan national. Elle intègre l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC[25]) qui doit *« procéder, à la demande de l'autorité judiciaire, à tous actes d'enquête et de travaux techniques d'investigations en assistance aux services chargés d'enquêtes de police judiciaire sur les infractions dont la commission est facilitée par ou liée à l'utilisation des technologies de l'information et de la communication »*[26]. Il constitue également le point de contact en France pour la coopération policière internationale avec Europol, Interpol et le G8.

En effet, l'office européen de police EUROPOL est un organe de coordination des policiers européens, avec pour objectif le traitement des renseignements relatifs aux activités criminelles. En 2002[27], une décision-cadre de la Commission de Bruxelles *« prône la coopération en matière pénale contre la cybercriminalité, sur le territoire des quinze pays membres de l'Union, avec la possibilité d'avoir des commissions rogatoires directement par Europol, sans passer par des autorités diplomatiques ou judiciaires habituelles »*[28]. Dès lors, l'avocat peut également être sollicité à l'échelle européenne afin de coopérer avec cet office, dans le cadre d'une commission rogatoire. De même, il est important de rappeler qu'en 2013 a été créé le Centre européen de lutte contre la cybercriminalité (EC3) qui a pour mission la coordination européenne de la lutte contre la cybercriminalité incluant notamment les cyberattaques à l'encontre des Organismes d'Importance Vitale (OIV) des États membres.

Ces différents organismes, comme beaucoup d'autres, tel que le Centre de lutte contre les criminalités numérique (C3N), permettent d'enclencher des investigations permettant d'identifier l'auteur de l'infraction. Cet exercice s'avère souvent très délicat à raison du caractère transfrontière de la cybercriminalité.

On rappellera que si les textes sont indispensables pour appréhender l'infraction, la difficulté réside pour l'essentiel dans l'identification de l'auteur de cette infraction. En effet, en présence de réseaux cryptés, de localisation d'hébergeurs à l'étranger, de la généralisation des pseudos, de la profondeur du *darkweb*... l'investigation requiert désormais une coopération forte avec les autorités chargées d'enquête.

L'avocat est toujours le mieux placé pour accompagner, orienter, aider et défendre son client.

Néanmoins, une réalité s'impose : le préjudice est difficilement réparable sur internet.

Comme toujours, il vaut mieux prévenir que guérir....

Notes :

1. Code pénal, art. 226-17.
2. L. n° 2015-993, 17 août 2015 portant adaptation de la procédure pénale au droit de l'Union européenne, JO 18 août, p. 14331.
3. CA Paris, 5 février 2014, n°13/04833
4. Ces infractions d'accès et de maintien frauduleux dans un STAD sont prévues

et réprimées par l'article 323-1 du Code pénal.

5. CA Paris, 4 mai 2007, n°05/23284

6. https://www.ssi.gouv.fr/entreprise/bonnes-pratiques/methodologie/

7. http://www.ssi.gouv.fr/IMG/pdf/Fiche_des_bonnes_pratiques_en_cybersecurite.pdf et http://www.ssi.gouv.fr/IMG/pdf Fiche_d_information_Administrateurs.pdf

8. Agence nationale de la sécurité des systèmes d'information (ANSSI), Guide de l'hygiène informatique, version 1.0 - Janvier 2013, www.ssi.gouv.fr et www.securite-informatique.gouv.fr

9. https://www.cnil.fr/fr/les-conseils-de-la-cnil-pour-un-bon-mot-de-passe

10. Pour plus d'informations : http://www.afnor.org/liste-des-actualites/actualites/2015/janvier-2015/fuites-d-informations-un-guide-afnor-pour-les-prevenir-et-s-en-proteger

11. Conseil d'État, 10ème / 9ème SSR, 30 décembre 2015, 385019 , v. https://www.legifrance.gouv.fr/affichJuriAdmin.do?oldAction=rechJuriAdmin&idTexte=CETATEXT000031861287&fastReqId=1510033390&fastPos=1

12. Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale, JORF n° 0294 du 19 décembre 2013, p. 20.570

13. Les Organismes d'importance vitale (OIV) – environ 250 opérateurs en France – désignent les opérateurs publics ou privés exploitant des établissements ou utilisant des installations et ouvrages, dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation. Ces établissements, installations ou ouvrages sont désignés par l'autorité administrative (C. défense, art. L. 1332-1).

14. Arrêté du 10 juin 2016 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au sous-secteur d'activités d'importance vitale « Produits de santé » et pris en application des articles R. 1332-41-1, R. 1332-41-2 et R. 1332-41-10 du code de la défense v. https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=5BC87A29CCFFD11180B006E71ECE2A34.tpdila07v_2?cidTexte=JORFTEXT000032749532&dateTexte=&oldAction=rechJO&categorieLien=id&idJO=JORFCONT000032749513 Arrêté du 17 juin 2016 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au secteur d'activités d'importance vitale « Gestion de l'eau » et pris en application des articles R. 1332-41-1, R. 1332-41-2 et R. 1332-41-10 du code de la défense, v. https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=5BC87A29CCFF D11180B006E71ECE2A34.tpdila07v_2?cidTexte=JORFTEXT000032749580&dateTexte=&oldAction=rechJO&categorieLien=id&idJO=JORFCONT000032749513 Arrêté du 17 juin 2016 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au secteur d'activités d'importance vitale « Alimentation » et pris en application des articles R. 1332-41-1, R. 1332-41-2 et R. 1332-41-10 du code de la défense, v. https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=5BC87A29CCFFD11180B006E71ECE2A34.tpdila07v_2?cidTexte=JORFTEXT000032749626&dateTexte=&oldAction=rechJO&categorieLien=id&idJO=JORFCONT000032749513

15. Arrêté du 28 novembre 2016 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au sous-secteur d'activités d'importance vitale « Audiovisuel et information » et pris en application des articles R. 1332-41-1, R. 1332-41-2 et R. 1332-41-10 du code de la défense https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=FC57FC0C4DE1618501D5213E0F9044A1.tpdila07v_1?cidTexte=JORFTEXT000033521374&dateTexte=&oldAction=rechJO&categorieLien=id&idJO=JORFCONT000033521322 Arrêté du 28 novembre 2016 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au sous-secteur d'activités d'importance vitale « Communications électroniques et Internet » et pris en application des articles R. 1332-41-1, R. 1332-41-2 et R. 1332-41-10 du code de la défense https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=E6CA21E5E2FF056CCDE294E9F30F64C1.tpdila12v_3?cidTexte=JORFTEXT000033521327&dateTexte=&oldAction=rechJO&categorieLien=id&idJO=JORFCONT000033521322%20. Arrêté du 28 novembre 2016 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au secteur d'activités d'importance vitale « Industrie » et pris en application des articles R. 1332-41-1, R. 1332-41-2 et R. 1332-41-10 du code de la défense https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=A590DC7FE86CF4C8E1964312C24F08C0.tpdila07v_1?cidTexte=JORFTEXT000033518974&dateTexte=&oldAction=rechJO&categorieLien=id&idJO=JORFCONT000033518910 Arrêté du 28 novembre 2016 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au secteur d'activités d'importance vitale « Finances » et pris en application des articles R. 1332-41-1, R. 1332-41-2 et R. 1332-41-10 du code de la défense https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=A590DC7FE86CF4C8E1964312C24F08C0.tpdila07v_1?cidTexte=JORFTEXT000033518925&dateTexte=&oldAction=rechJO&categorieLien=id&idJO=JORFCONT000033518910

16. Directive « Network Security and information » (NIS)

17. Dir. 2016/1148, 6 juillet 2016, concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016L1148&from=FR

18. Les secteurs concernés sont ceux de l'énergie (électricité, pétrole et gaz), les transports (aérien, ferroviaire, par voie d'eau et routier), les services bancaires (établissements de crédit), les infrastructures de marchés financiers (plateformes de négociation, contreparties centrales), la santé (prestataires de soins de santé), l'eau (fourniture et distribution d'eau potable), l'infrastructure numérique (points d'échange internet qui permettent l'interconnexion entre les différents réseaux internet), prestataires de services relatifs au système des noms de domaine, registres de noms de domaine de premier niveau).

19. Formulation en français du concept d'investigation numérique légale, appelé aussi computer forensics dans le monde anglophone.

20. TGI Paris, ord. réf., 2 juill. 2007, Udaf de l'Ardèche a. c/Linden Research a., Gaz. Pal. 18 oct. 2007, p.37, note Jahan; https://www.legalis.net/jurisprudences/tribunal-de-grande-instance-de-paris-ordonnance-de-refere-02-juillet-2007-2/

21. Afnor NFZ67-147, « mode opératoire de procès-verbal de constat sur Internet effectué par huissier de justice », 1 sept. 2010, http://norminfo.afnor.org/structure/commid=73666

22. CA Paris, Pôle 5, ch. 1, 27 février 2013, David D c/ Thomas M et Pascal F, http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=3641

23. C'est l'un des rares services de la police judiciaire à prendre directement la plainte dans son domaine propre.

24. Arr. min., 29 avr. 2014, NOR : IOCC0916981A, modifiant l'arrêté du 5 août 2009 relatif aux missions et à l'organisation de la Direction centrale de la police judiciaire

25. Sur l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication, http://www.internet-mineurs.gouv.fr/

26. Décr. no 2000-405, 15 mai 2000, JO 16 mai, p. 7338.

27. Conseil de l'Europe, no 2002/630/JAI, 22 juill. 2002, établissant un programme-cadre concernant la coopération policière et judiciaire en matière pénale (AGIS), http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=URISERV:l33177&from=FR

28. Briat, « La cybercriminalité », LPA 6 févr. 2004, no 27, p. 25.

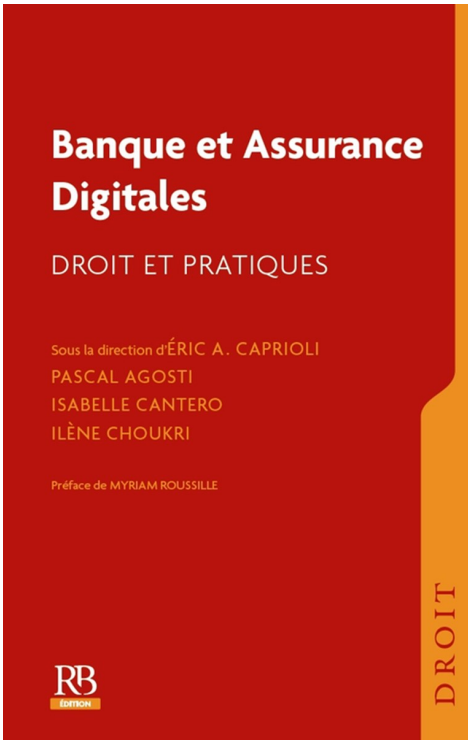
BANQUE ET ASSURANCE DIGITALES : DROITS ET PRATIQUES

AUTEURS : SOUS LA DIRECTION D'ÉRIC A. CAPRIOLI

PASCAL AGOSTI, ISABELLE CANTERO, ILÈNE CHOUKRI, PRÉFACE DE MYRIAM ROUSSILLE

EDITEUR : RB ÉDITION

Présentation de l'éditeur



Le secteur bancaire et assurantiel est au coeur de la révolution digitale qui innerve l'ensemble de la société. Précurseurs, les établissements bancaires et les entreprises d'assurance ont dû modifier en profondeur leurs pratiques et procédures pour satisfaire une clientèle toujours plus exigeante en termes de réactivité et de sécurité. La digitalisation de la banque et de l'assurance est la technique qui permet le passage de l'information analogique au numérique, au moyen des technologies de l'information, en vue de traitements et d'échanges entre systèmes d'information via les réseaux numériques, mais aussi avec les équipements personnels des clients. Les réglementations applicables sont de plus en plus complexes. Avec la digitalisation, le secteur bancaire et assurantiel doit non seulement prendre en compte les règles de droit commun, mais aussi les règles plus spécifiques qui encadrent les échanges digitaux/numériques : quelles sont les exigences de sécurité des systèmes d'information qu'il convient de mettre en oeuvre ? Quelles obligations juridiques pèsent sur l'entreprise de banque ou d'assurance en termes de conformité légale ou de protection des données à caractère personnel ? Selon quelles règles juridiques s'opèrent les relations digitalisées avec les clients ? Comment assurer le passage de la banque et de l'assurance traditionnelles au digital ? Quels sont les nouveaux services à valeur ajoutée et leurs cadres juridiques dont les banques et les assurances doivent se doter pour rester compétitives ? Cet ouvrage pratique et pragmatique a pour objectif de poser les fondements juridiques de la banque et l'assurance digitales. Les auteurs proposent une analyse approfondie, illustrée de références jurisprudentielles pour identifier les obligations et responsabilités des banques et des assurances, dans une optique de compliance réglementaire et de compétitivité.

« Aborder dans un seul et même ouvrage la banque et l'assurance digitales est à la fois un choix judicieux et audacieux. Le rapprochement des activités, l'émergence de règles transversales et la supervision commune des secteurs – peut-être bientôt étendue au niveau européen – donne tout son sens à cette démarche. Dégager les questions juridiques, esquisser les réponses opérationnelles à y apporter – dans un contexte réglementaire en mouvement incessant – constituait un beau challenge. Éric Caprioli et ses associés l'ont relevé ». Myriam Roussille (Extrait de la préface)

RAPPORT :

« 2016, UNE ANNÉE HISTORIQUE POUR TRACFIN »

BRUNO DALLES

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

Le service « Traitement du renseignement et action contre les circuits financiers clandestins » (Tracfin) participe à la protection de l'économie nationale et à la lutte contre les circuits financiers clandestins, le blanchiment de capitaux et le financement du terrorisme depuis sa création en 1990[1].

Devenu service à compétence nationale en 2006 et placé sous l'autorité du ministre chargé de l'Action et des Comptes publics, Tracfin répond à la dénomination de cellule de renseignement financier nationale au sens du groupe d'action financière (GAFI) et de l'Union européenne à savoir une « cellule nationale centrale chargée de recevoir et, dans la mesure de ses pouvoirs, de demander, d'analyser et de communiquer aux autorités compétentes les informations divulguées concernant un éventuel blanchiment de capitaux, un éventuel financement du terrorisme ou toute information requise par les dispositions législatives ou réglementaires nationales ». Tracfin a pour mission de recueillir, analyser, enrichir et exploiter tout renseignement propre à établir l'origine ou la destination délictueuse d'une opération financière.

Aux fins d'évaluation du dispositif, Tracfin publie chaque année un rapport d'activité donnant un état des lieux de la participation des professionnels assujettis au dispositif LCB/FT, de l'activité institutionnelle du Service et présentant des typologies de fraudes à l'usage des professionnels déclarants. Le rapport d'activité 2016 a été publié en juillet dernier, cet article en retrace les faits marquants.

I. 2016, une année d'activité historique pour Tracfin

L'année 2016 a constitué une année d'activité historique pour Tracfin en raison de l'explosion du nombre d'informations reçues et analysées par le Service (+ 43 %) et notamment par la réception massive de déclarations de soupçon (+ 44 %). Il s'agit de la plus forte hausse constatée depuis la création du Service, le flux d'informations reçues a augmenté de 69 % en 2 ans et de 169 % en 5 ans.

A. Les sources d'information de Tracfin

Tracfin est, en effet, le destinataire exclusif des déclarations de soupçon adressées par les professionnels assujettis qui ont identifié des sommes dont ils savent, soupçonnent ou ont de bonnes raisons de soupçonner qu'elles proviennent d'une infraction passible d'une peine privative de liberté supérieure à un an ou qu'elles sont liées au financement du terrorisme[2]. À ce titre, le professionnel doit être en mesure de justifier, avec les éléments d'information en sa possession, qu'il a procédé aux diligences nécessaires selon une approche par les risques qui le conduit à ajuster sa vigilance (allégée, normale ou renforcée) en fonction de la nature et du niveau du risque (client, produit ou opération) auquel il est confronté. En cas de manquement à son obligation de vigilance et de déclaration, sa responsabilité peut être mise en cause.

Le Service reçoit par ailleurs des

informations, en lien direct avec ses missions, de ses homologues étrangers, d'autres administrations de l'État et personnes chargées d'une mission de service public ou encore des autorités de contrôle des professionnels assujettis.

Cette activité exceptionnelle s'explique notamment par la forte implication des professions assujetties à la lutte contre le blanchiment et le financement du terrorisme. En effet, en 2016, près de 96 % des informations reçues par le Service émanent des professionnels déclarants, soit 62 259 déclarations de soupçon (+44 % par rapport à 2015). Plus précisément, sur la quarantaine de professions assujetties au dispositif, les déclarations reçues des professions financières représentent 94 % des signalements soit 58 517 déclarations de soupçon (+ 45 % par rapport à 2015).

Parmi les professions financières, les banques et établissements de crédit demeurent les premiers contributeurs avec 46 901 signalements en 2016 (80 % des déclarations de soupçon du secteur financier, soit 50 % d'augmentation par rapport à 2015).

B. Un secteur financier mobilisé mais une qualité inégale d'information

Si les chiffres d'activité enregistrés en 2016 démontrent une prise de conscience des professions assujetties au dispositif LCB/FT, il revient cependant à chacun de poursuivre la lutte contre le blanchiment et le financement du terrorisme en gardant à l'esprit que l'efficacité des dispositifs d'analyse de risque doit se coordonner avec une amélioration de la qualité des déclarations dans lesquelles le soupçon n'est parfois pas suffisamment caractérisé ni étayé. En effet, aux fins d'améliorer la connaissance qualitative du flux entrant, Tracfin a mis en place, au printemps 2016, un système d'identification de la principale infraction pénale/typologie soupçonnée par le déclarant, avant même que le signalement ne fasse l'objet d'investigations complémentaires par le Service. Ce système révèle une concentration des déclarations sur des typologies peu élaborées (et à faible, voire très faible enjeu financier) telles l'activité non déclarée, la donation non déclarée, les opérations de retrait d'espèces, au détriment de typologies à haute valeur ajoutée (complexité, enjeux financiers significatifs, etc.) concernant des réseaux d'escroqueries, la criminalité organisée (stupéfiants, trafic d'êtres humains, proxénétisme, trafic d'armes, etc.) ou la corruption, qui restent peu détectées, faute d'un réel travail d'analyse de la part des déclarants. Ainsi, la forte poussée du nombre de déclarations de soupçon émanant des banques s'est accompagnée d'une chute du « taux de mise en investigation[3] » par rapport à 2015. En 2016, à peine plus d'1 déclaration sur 10 a fait l'objet d'investigations par Tracfin alors que les critères de traitement par le Service sont restés constants sur la période (2015-2016) et que les capacités de traitement ont progressé[4].

C. La mobilisation des professions non financières en progression

Le partenariat institué avec les professions non financières a également permis une nette progression des résultats. En 2016, ces professions représentent 3 742 signalements à Tracfin (soit + 32 % par rapport à 2015). Avec 1 044 déclarations de soupçon en 2016, la profession du notariat demeure au 1er rang des professionnels déclarants du secteur non financier. En outre, les administrateurs judiciaires et mandataires judiciaires ont été fortement mobilisés avec 995 déclarations de soupçon transmises à Tracfin contre 528 en 2015. Les autres professionnels du chiffre se sont mobilisés en particulier par un ambitieux plan de formation qui produira des effets rapidement.

II. L'enquête de Tracfin : une analyse documentaire des flux financiers

Lorsque les informations reçues sont exploitables, les agents du Service contextualisent le soupçon en rapprochant les informations reçues de toute indication utile recueillie dans les fichiers informatiques auxquels ils ont accès. L'orientation est le premier acte d'analyse d'une information, elle débouche sur une enquête ou sur une mise en attente (lorsque l'information semble potentiellement inexploitable ou le soupçon peu clair, ou, après enquête, lorsque le doute est levé. Elle pourra néanmoins, au regard de nouvelles informations ultérieures reçues par le Service, être réactivée). Toutes les informations reçues par Tracfin sont analysées par le Service.

En 2016, 13 592 informations ont fait l'objet d'une analyse approfondie, 9 451 à partir d'informations reçues en 2015 et 4 141 informations reçues

antérieurement et réactivées.

Une déclaration ou une information de soupçon affectée en enquête fait alors l'objet de diverses investigations dont la profondeur est liée à la complexité du soupçon et à la compréhension des flux financiers. Les premières analyses réalisées visent à déterminer les éléments d'environnement des personnes déclarées. Ensuite, des éléments d'information supplémentaires permettant de mieux contextualiser le soupçon déclaré et/ou de l'enrichir. Ces recherches sont réalisées au moyen d'actes d'investigation.

Les actes d'investigation se traduisent notamment par la consultation directe ou indirecte de fichiers (fichier des comptes bancaires – Ficoba –, fichiers de l'administration fiscale ou des douanes, données sociales, fichiers de la gendarmerie ou de la police nationales), l'exploitation des bases ouvertes, l'interrogation des autres services de renseignement, des cellules de renseignement étrangères, ou encore d'autres administrations de l'État.

L'internationalisation des flux financiers, et donc des circuits de blanchiment, ont rendu nécessaire le développement de la coopération internationale. Les cellules de renseignements étrangères sont susceptibles d'être interrogées quand des liens financiers, voire juridiques (domiciliation de sociétés, etc.), sont mis en évidence afin de disposer de nouveaux éléments pouvant aider à la connaissance des bénéficiaires effectifs d'un flux financier.

Enfin, les agents recueillent et analysent, par l'exercice du droit de communication, tout document utile auprès des professionnels assujettis (relevés de comptes bancaires, actes notariés, statuts de société, documents d'expertise comptable, factures, documents d'ouverture de comptes, etc.).

Les 13 592 enquêtes réalisées par Tracfin (+ 28 % par rapport à 2015), issues d'informations reçues en 2016 ou antérieurement, confirment l'action du Service dans tous ses domaines de compétences en matière de lutte contre la fraude fiscale, douanière, sociale, la lutte contre la criminalité financière ainsi que les atteintes à la probité.

À l'issue de ses investigations, les informations sont externalisées, vers les cibles les plus pertinentes, sous forme de notes à l'autorité judiciaire, aux administrations partenaires ou aux cellules de renseignement financier étrangères.

III. L'externalisation des notes d'information

Le nombre de notes transmises par le Service à l'autorité judiciaire et aux administrations partenaires a connu une hausse de 16 % (1889 notes) en 2016. Plus précisément, 662 notes ont été adressées par Tracfin à l'autorité judiciaire en 2016 (595 en 2015) : 448 notes d'information portaient sur une présomption d'une ou plusieurs infractions pénales et 214 transmissions de renseignement ont été réalisées en direction des magistrats et aux services de police judiciaire.

Une transmission en Justice peut résulter d'une ou de plusieurs informations reçues par le Service. De nombreux dossiers découlent du croisement d'informations provenant de professionnels exerçant dans des secteurs distincts.

Les notes d'information transmises à l'autorité judiciaire mentionnent une qualification initiale des infractions à l'origine des flux observés. Cette qualification reste néanmoins indicative et ne lie pas l'autorité judiciaire, seule à même d'apprécier les orientations à donner aux informations transmises par le Service. Elle ne fait que traduire l'appréciation du Service au regard des éléments d'information à sa disposition au moment où les investigations sont effectuées.

En 2016 comme en 2015, les cinq catégories d'infractions sous-jacentes les plus représentées sont la fraude fiscale, l'abus de confiance, l'escroquerie (simple ou aggravée), le travail dissimulé, et l'abus de biens sociaux.

En sus des transmissions portant sur une présomption d'infraction pénale, Tracfin a la faculté d'adresser à l'autorité judiciaire toute information utile aux missions de celle-ci. Le Service peut ainsi porter à sa connaissance les éléments qu'il détient ne recelant pas en eux-mêmes une suspicion d'infraction, mais susceptibles d'abonder ou d'éclairer une enquête judiciaire en cours, notamment sur l'environnement financier des personnes mises en cause.

Tracfin est par ailleurs susceptible de pouvoir diffuser, dans le cadre de ses missions, des notes d'informations à certaines administrations partenaires, au premier rang desquelles les administrations fiscales, sociales, les autorités de contrôles et les cellules de renseignement étranger.

2016 marque d'ailleurs une nouvelle progression de l'activité de Tracfin en matière de lutte contre les fraudes sociales avec 165 notes transmises par le Service aux organismes de protection sociale soit une augmentation de 51 % par rapport à 2015 et le doublement du nombre de notes sociales émises par Tracfin sur deux ans.

IV. Tracfin, un service au sein de la communauté du renseignement

Tracfin est membre du Conseil national du renseignement (CNR) et du Centre national de contre-terrorisme[5] (CNRCT) depuis 2008 et en est un maillon essentiel par son expertise financière. Structurellement, les échanges entre Tracfin et les autres services de renseignement se reflètent par le développement de trois structures au sein du Service : le pôle prédation économique et financière (juillet 2015), la division de lutte contre le financement du terrorisme (octobre 2015), et le pôle renseignement (janvier 2016).

A. Lutter contre la prédation économique

En matière de prédation économique et financière, Tracfin a constitué dès juillet 2015 une cellule spécialisée au sein du Service. Celle-ci est chargée d'analyser et d'exploiter les informations concernant des faits, actes ou tentatives d'ingérences menaçant les capitaux, les savoir-faire, les ressources humaines et la recherche des entreprises françaises. Par le prisme de l'analyse financière et de recherches d'environnement, les invesigations portent notamment sur des cas de captation de clientèle, de manoeuvres frauduleuses ou d'infractions commises à l'occasion de rachats de sociétés en difficulté, d'atteintes au patrimoine intellectuel d'une entreprise et de toute atteinte aux intérêts économiques de la Nation. Enfin, depuis le 1er janvier 2017, Tracfin peut échanger des informations avec le Service de l'information stratégique et sécurité économiques (art. L561-31 8° du Code monétaire et financier), et participe aux réunions interministérielles organisées par le Service de l'information stratégique et de la sécurité économiques (SISSE) en matière de sécurité économique.

En 2016, la cellule a externalisé 9 transmissions judiciaires et 53 transmissions spontanées vers les services partenaires.

B. Tracfin se mobilise au service de la communauté du renseignement

L'activité « renseignement » du Service a quant à elle été marquée par la poursuite du développement des échanges d'informations financières avec les autres services de la communauté du renseignement. Le nombre de notes transmises à ces services a encore progressé passant de 349 en 2015 à 488 sur la période de référence. Ces notes ont porté sur des personnes physiques et morales soupçonnées d'activités terroristes, sur des activités financières et immobilières en France de Personnes Politiquement Exposées étrangères (PPE) et d'hommes d'affaires étrangers, sur le commerce/trafic d'armes, sur la prolifération et le contre-espionnage.

Enfin, le Service participe activement à la lutte contre le terrorisme et son financement en travaillant en étroite collaboration avec les services de la communauté du renseignement. Tracfin a accru sensiblement, en 2016, le nombre de notes de renseignement dédiées à la lutte contre le financement du terrorisme transmises ces services (+121% avec 396 notes). L'accentuation de la coopération de Tracfin avec les services du premier cercle de la communauté du renseignement se traduit également par la participation du Service dans le cadre de la cellule inter-agence de la DGSI.

V. De nouvelles prérogatives pour Tracfin en 2016 et en 2017

Le surcroit d'activité perçu en 2016 s'accompagne de l'impact des évolutions juridiques dont les effets se poursuivront en 2017 et 2018. En effet, les années 2016 et 2017 ont été marquées par l'introduction de nouveaux dispositifs qui sont venus renforcer les moyens d'action de Tracfin, codifiés dans le Code monétaire et financier[6]. Les missions de Tracfin ont également évolué à l'occasion de la transposition de la 4ème Directive européenne relative à la lutte contre le blanchiment et le financement du terrorisme[7].

En matière d'accès à l'information, le champ des personnes auxquelles Tracfin peut désormais demander communication d'informations s'est étendu à d'autres personnes privées : les Caisses Autonomes des règlements pécuniaires des avocats (CARPA), les entreprises de location de véhicules de transport

terrestre, maritime ou aérien, l'ensemble des plateformes de collecte de fonds en ligne[8]. Par ailleurs, Tracfin accède dorénavant au fichier Traitement des antécédents judiciaires (TAJ) pour l'ensemble des activités du Service et non plus seulement en matière de prévention du terrorisme[9] et a également un accès direct au fichier des personnes recherchées (FPR). Enfin, l'extension du nombre de professions assujetties[10] depuis le 1er janvier 2017 et la possibilité pour Tracfin, de diffuser des notes de renseignement au bénéfice de nouvelles autorités administratives[11] sont autant d'atouts en faveur d'une meilleure circulation de l'information en direction des autorités compétentes en matière de fraudes.

Enfin, s'agissant des pouvoirs de Tracfin, la loi n° 2016-731 du 3 juin 2016 a introduit un nouveau dispositif autorisant Tracfin à désigner aux entités déclarantes des opérations ou des personnes qui présentent un risque important de blanchiment de capitaux et de financement du terrorisme[12]. Cette prérogative sera effective courant 2018, des discussions sont actuellement en cours avec le secteur bancaire sur les modalités de mise en oeuvre. Par ailleurs, des mesures de vigilance confortée sont également mise en place. Si les personnes politiquement exposées (PPE) étrangères devaient déjà faire l'objet d'une vigilance particulière, c'est désormais également le cas pour les PPE nationales.

Les sanctions susceptibles d'être prononcées par les diverses autorités de sanction en cas de manquements aux obligations LCB/FT ont été harmonisées. Le principe de la sanction pécuniaire a par exemple été généralisé à l'ensemble des assujettis.

Enfin, Tracfin a désormais un droit d'opposition plus effectif. En application de l'article L.561-24 du Code monétaire et financier (anciennement article L. 561-25), Tracfin peut s'opposer à l'exécution d'une opération pendant une durée qui a été étendue de 5 à 10 jours ouvrables par l'ordonnance de transposition.

De nombreux enjeux stratégiques subsistent pour Tracfin veille à rester performant, anticiper et détecter les nouveaux risques, consolider les partenariats existants et imaginer de nouvelles formes de coopération entre les acteurs engagés dans la lutte contre le blanchiment et le financement du terrorisme. La mutation de Tracfin comme service de renseignement spécialisé dans le domaine financier se poursuit plus que jamais, bien engagé en 2017, 2018 sera l'année du défi du Big Data avec le déploiement d'un nouveau système de gestion de l'information au sein du Service.

Notes :

1. Cf. décret du 9 mai 1990 portant création d'une cellule de coordination chargée du traitement du renseignement et de l'action contre les circuits financiers clandestins.
2. Cf. article L. 561-15 du Code monétaire et financier.
3. Le taux de mise en investigation est le ratio entre le nombre de déclarations de soupçon envoyées en enquête (préliminaire ou approfondie) et le nombre total de déclarations de soupçon adressées par un déclarant. C'est un indicateur de suivi qui permet, parmi d'autres, d'apprécier la pertinence des signalements.
4. Le Service compte 132 agents au 31 décembre 2016. Le nombre d'agents du Service a augmenté de 27 % en 2 ans et de 57 % en 5 ans.
5. Le CNRCT est composé de 6 services : Direction générale de la sécurité extérieure (DGSE), Direction générale de la sécurité intérieure (DGSI), Direction du renseignement militaire (DRM), Direction du renseignement et de la sécurité de la Défense (DRSD), Direction nationale du renseignement et des enquêtes douanières (DNRED), TRACFIN.
6. Cf. articles L. 561-1 à L. 561-45 et R. 561-1 à R. 561-50 du Code monétaire et financier.
7. Cf. Parue au JORF le 2 décembre 2016, ordonnance n° 2016-1635.
8. Ordonnance n° 2016-1635 du 1er décembre 2016 – article L. 561-25-1 du Code monétaire et financier.
9. Loi n° 2016-731 du 3 juin 2016
10. Les nouveaux professionnels assujettis sont les personnes acceptant des paiements en espèces ou au moyen de monnaie électronique d'un montant supérieur à 1 000 euros et se livrant au commerce de biens suivants : pierres précieuses, métaux précieux, bijoux, objets d'ameublement et de décoration d'intérieur, produits cosmétiques, produits textiles, maroquinerie, produits gastronomiques, horlogerie, arts de la table ; les intermédiaires en opérations de banque et en services de paiement mentionnés lorsqu'ils agissent en vertu d'un mandat délivré par un client et qu'ils se voient confier des fonds en tant que mandataire des parties. Par ailleurs, l'assujettissement des agents immobiliers a été étendu à leurs activités de location et toutes les plateformes de financement participatif de don sont assujetties depuis le 1er janvier 2017.
11. Peuvent ainsi être destinataires des informations Tracfin : les juridictions financières, la Haute autorité pour la transparence de la vie publique (HATVP), l'Agence française anticorruption ou encore le Service de l'information stratégique et de la sécurité économiques (SISSE). Par ailleurs, si Tracfin et les autorités de contrôle pouvaient échanger toute information utile à l'accomplissement de leurs missions en matière de LCB/FT, il est apparu nécessaire de prévoir la possibilité pour Tracfin d'adresser à certaines de ces autorités des informations relevant d'autres missions. Ainsi, depuis le 1er janvier 2017, Tracfin peut adresser à l'Autorité de contrôle prudentielle et de résolution (ACPR), à la Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF), au Service central des courses et jeux (SCCJ) et à l'Autorité des marchés financiers (AMF) les informations utiles à l'exercice de l'ensemble de leurs missions.
12. Article L.561-26. du Code monétaire et financier Le décret n° 2016-1793 du 21 décembre 2016 est venu préciser les conditions d'application de cette mesure (article R. 561-37-1).

QUAND L'ARTISAN-CHEF PANEB SÉVISSAIT À DEIR EL-MÉDINA :

CONSIDÉRATIONS SUR LA CORRUPTION DANS L'ÉGYPTE DU NOUVEL EMPIRE (DÉBUT DU XII^{e} S. AV. NOTRE ÈRE)

CHRISTINE HUE-ARCÉ

DOCTEURE EN ÉGYPTOLOGIE (UNIVERSITÉ DE STRASBOURG)

Sauf indication contraire, les traductions de textes égyptiens présentés dans cet article ont été effectuées par l'auteure.

Si la corruption et le crime organisé semblent être des questions actuelles, ces préoccupations ne sont en réalité pas propres à nos sociétés occidentales modernes. La corruption et la volonté de lutter contre ce phénomène sont bien attestées dans l'antiquité, particulièrement sur les rives du Nil, comme le montre une affaire survenue dans l'Égypte du Nouvel Empire. Au début du règne du Pharaon Siptah[1] (XIXe dynastie, 1194-1188 av. notre ère), Deir el-Médina, le village des artisans travaillant à la construction des tombes et temples royaux à Thèbes Ouest, est secoué par un scandale d'ampleur : Paneb, artisan-chef – fonction d'importance au sein de la communauté –, est accusé de crimes nombreux et variés. Meurtre et tentatives de meurtres, adultères et possible viol côtoient détournements de biens, spoliations et corruption.

Le droit de l'Égypte pharaonique a cela de particulier qu'aucun texte théorique de législation ne nous est parvenu[2]. L'égyptologue doit alors se reposer sur les textes de la pratique quotidienne, qui nous renseignent sur des cas concrets et réels, pour dresser un tableau des crimes et des châtiments de l'Égypte antique. Pour le Nouvel Empire, le recours aux sources de Deir el-Médina est indispensable[3] : le climat désertique de ce village situé en bordure de désert, ainsi que le taux d'alphabétisation de ses habitants, supérieur à la moyenne de l'Égypte[4], ont permis la conservation d'une masse documentaire inédite sur la vie quotidienne d'une communauté d'artisans. Parmi ces documents, le papyrus P. Salt 124 (British Museum)[5] a conservé sur quatre colonnes de texte écrit en hiératique les accusations portées à l'encontre de Paneb dans une dénonciation adressée par l'artisan Imennakht au plus haut dignitaire du pays après Pharaon : le vizir.

I. Les délits de Paneb et le contexte de la dénonciation d'Imennakht

Parmi les méfaits reprochés à Paneb dans la plainte du P. Salt 124, plusieurs relèvent ainsi de la corruption, du détournement de biens publics et de l'abus d'autorité.

La charge d'artisan-chef détenue par Paneb lui a été octroyée par le vizir Prêemheb, après le décès de son précédent détenteur, Néferhotep, qui était le protecteur de Paneb et le frère du requérant Imennakht. Ce dernier accuse Paneb d'avoir encouragé la décision du vizir, en lui faisant don de cinq serviteurs (recto i 2-4). Il ne s'agit pas là de la seule accusation de corruption à l'encontre de Paneb : selon Imennakht, l'homme

aurait également offert « un petit quelque chose » au scribe de la Tombe[6] Qenherkhepeshef, afin que celui-ci taise un délit commis par l'artisan-chef (recto i 18).

Paneb se serait en outre rendu coupable de détournement de biens publics : les outils et le matériel utilisés lors du travail dans la Nécropole royale appartenaient à l'institution de la Tombe et donc, de facto, à l'administration pharaonique. Or, Paneb est accusé d'avoir dérobé du matériel, des biens et du mobilier funéraire dans la tombe du pharaon Séthi II, qui furent par la suite retrouvés dans sa demeure (recto i 14-16)[7]. Il aurait par ailleurs ordonné aux ouvriers sous sa responsabilité de tailler des pierres destinées à la tombe du Pharaon pour les employer pour sa propre tombe, utilisé (et endommagé) un ciseau, et volé une pioche pour travailler dans sa tombe (recto ii 5-9 ; verso i 9-10). Les ouvriers de Deir el-Médina ont ainsi été forcés de travailler sur les travaux personnels de Paneb, tandis que l'artisan-chef exigeait que leurs épouses tissent des vêtements pour lui (recto ii 19-20).

Ces délits dont Imennakht accuse Paneb ne sont pas les actes d'un individu isolé, mais d'un homme qui sait faire usage de coercition et d'un réseau d'influence développé. Nous avons pu voir que Paneb aurait activement corrompu non seulement le scribe de la Tombe Qenherkhepeshef, mais aussi le vizir Prêemheb, pour parvenir à ses fins. Lorsqu'un vizir tenta de mettre fin à ses agissements, l'artisan-chef parvint à le faire congédier, en s'adressant directement à Pharaon (recto ii 17-18), faisant ainsi montre d'un réseau développé jusque dans les plus hautes sphères du pouvoir. Paneb disposait par ailleurs d'un acolyte de choix dans ses méfaits : son fils Aâpehty, accusé par Imennakht d'avoir pris part aux détournements de biens orchestrés par son père. Peut-être faut-il voir ici l'indice d'une famille à l'influence criminelle bien implantée dans le village des artisans. En outre, l'homme bénéficiait de la complicité des ouvriers sous ses ordres : Imennakht dénombre ainsi 16 tailleurs de pierres qui travaillèrent au compte de Paneb (recto ii 10-12). La complicité des artisans de Deir el-Médina dans ces crimes était-elle forcée ou volontaire ? L'artisan-chef disposait d'indéniables moyens de pression sur eux. Outre son statut de supérieur hiérarchique, plusieurs méfaits dénoncés par Imennakht sont l'indice du ton menaçant de Paneb envers les hommes de la Tombe. Parmi de nombreux actes de violence, il est ainsi reproché à Paneb d'avoir battu « sans s'arrêter » des artisans durant une réunion nocturne (verso i 4-5). De surcroît, Paneb disposait peut-être d'un moyen de pression plus insidieux sur les hommes du village : un passage de la dénonciation l'accuse en effet d'avoir entretenu des relations sexuelles avec les épouses de certains artisans (recto ii 2-4). Ces adultères constituaient-ils de simples incartades d'un Dom Juan, ou des actes délibérés visant à faire pression sur les artisans pour s'assurer de leur complicité et de leur silence[8] ? Il n'est pas inconcevable que pour arriver à ses fins, Paneb ait menacé les époux des femmes adultères d'exposer publiquement leur déshonneur.

La dénonciation d'Imennakht nous livre ainsi l'image d'un homme d'influence, bénéficiant d'un réseau organisé, et non celle d'un simple délinquant commettant des crimes d'opportunité. Néanmoins, face à l'ensemble des accusations portées à l'encontre de Paneb, la prudence doit être de mise : le biais de l'auteur du document influence grandement le contenu de ce dernier, d'autant plus qu'il s'agit du seul texte qui nous renseigne de manière extensive sur les crimes de l'artisan-chef. L'auteur du P. Salt 124, Imennakht, considère en effet être le juste récipiendaire de la fonction d'artisan-chef détenue par Paneb. Aussi Imennakht finit-il sa plainte de la manière suivante : « Or, il n'est pas digne de cette fonction. Oh, il se porte bien, (mais) il est comme un fou. [...] Vois, j'ai renseigné le vizir sur sa nature » (verso ii) ». Le but premier de cette plainte est ainsi de réclamer la fonction d'artisan-chef ; les dénonciations de corruption, détournements de biens et autres violences ont avant tout pour objectif de dresser un portrait à charge contre Paneb[9].

Si cette plainte fut adressée au vizir, c'est parce que ce dignitaire était en charge de l'attribution des fonctions d'importance au sein du village, telle celle d'artisan-chef. C'est en réalité à l'instance en charge de l'institution de la Tombe que le conflit est présenté : le recours est ainsi administratif et hiérarchique, et non judiciaire. Ce document doit ainsi être compris comme une requête en destitution, plutôt

que comme une véritable plainte visant à dénoncer des infractions pénales[10].

II. Quelles sanctions pour Paneb ?

A. Les informations de la plainte et de la documentation de Deir el-Médina

Les conséquences des dénonciations d'Imennakht à l'encontre de Paneb ne nous sont pas connues : si sa requête a bien été transmise au vizir, aucun document qui atteste une prise de décision de la part du haut dignitaire ne nous est parvenu. Ce silence de la documentation ne doit pas nécessairement être interprété comme une absence de réaction de la part de l'administration vizirale : il est également possible qu'il soit dû à la perte des archives du vizir[11], ou à l'absence de mise à l'écrit[12].

Le papyrus de la requête d'Imennakht fait lui-même mention d'une intervention antérieure du vizir : Paneb a reçu un châtiment, dont la nature n'est pas explicitée, suite à quoi il s'est plaint au Pharaon Amenmès qui a congédié le vizir concerné (recto ii 17-18). L'artisan-chef a en outre dû prêter le serment suivant (verso i 6 -8) : « Si le vizir entend encore parler de moi, je serai chassé de ma fonction et je serai placé comme carrier »[13]. S'il trahissait son serment, l'artisan-chef belliqueux risquait ainsi d'être rétrogradé de son statut, marque d'infamie dans un village où les artisans-chefs étaient parmi les plus importantes personnalités, tandis que les carriers se situaient en bas de l'échelle sociale. Le principal complice de Paneb, son fils Aâpehty, est également concerné par ce serment : n'étant qu'un simple artisan, le jeune homme ne serait pas rétrogradé, mais directement exclu de la communauté d'artisans[14]. Cependant, ce serment et la menace subséquente concernaient les « vociférations » de Paneb (peut-être quelque diffamation lui était alors reprochée), et non les détournements de biens et autres actes de corruption. Le rappel par Imennakht de ce serment violé par Paneb vise certainement à remémorer au vizir la menace de son prédécesseur de démettre l'artisan-chef de ses fonctions – destitution qui profiterait alors sans doute à notre requérant.

De manière notable, Paneb disparaît de la documentation de Deir el-Médina après l'an 2 de Siptah, qui correspond à la période à laquelle la requête d'Imennakht fut déposée auprès du vizir. L'artisan-chef n'apparaît plus dans les textes du village, qu'il s'agisse de textes économiques, des registres d'absences du travail à la Nécropole, ou encore des registres de distribution des rations des artisans. Hasard de la conservation des documents ? Si tout argument ex silentio doit être envisagé avec prudence, il est possible de voir dans ce silence des sources un indice d'une destitution de Paneb de ses fonctions, voire même de son exclusion de la communauté des artisans de la Nécropole thébaine.

Le cas de Paneb est par ailleurs cité comme précédent dans une affaire postérieure concernant un vol de pierres, commis dans le cadre des grèves importantes des artisans de la nécropole thébaine, qui marquèrent le règne de Ramsès III[15]. Malheureusement, le texte ne fait pas état de la sanction infligée à l'artisan-chef.

B. Des cas similaires ?

La requête d'Imennakht ainsi que les autres documents de Deir el-Médina qui mentionnent Paneb ne nous apportent que de maigres informations sur les conséquences des dénonciations à son encontre. Néanmoins, d'autres documents du village des artisans rapportent des cas en partie similaires, et permettent ainsi d'établir un tableau plus complet des peines qui auraient pu sanctionner les méfaits de l'artisan-chef.

S'il n'existe pas, à Deir el-Médina, de parallèle exact à l'ampleur des crimes reprochés à Paneb, certains délits spécifiques sont attestés par des ostraca et papyri pour d'autres habitants du village. Ainsi, il est reproché à Paneb d'avoir dérobé un ciseau destiné au travail à la Nécropole à des fins personnelles. Or, deux autres cas analogues sont connus à Deir el-Médina. Sous le règne de Séthi II, Hérya est accusée par un artisan, devant la qnb.t (l'assemblée locale de Deir el-Médina), de lui avoir dérobé un outil en cuivre qui appartenait au temple d'Amon[16]. L'assemblée déclare Hérya « digne de mort » pour avoir commis ce crime, tandis qu'est cité un précédent judiciaire où une femme avait été « menée à la rive » pour un tel vol. À partir de ces informations, il a été supposé que Hérya risquait une mise à mort par l'eau pour avoir volé

l'outil en cuivre. Néanmoins, si la femme est dite « digne de mort » par l'assemblée locale du village, la décision finale est en réalité remise entre les mains du vizir, et ne nous est pas connue[17]. En outre, la mention d'une femme conduite à la rive par le vizir pour un vol semblable ne fait sans doute pas référence à la sanction infligée, mais au lieu du jugement par le haut dignitaire : l'administration vizirale était située sur la rive est de Thèbes, tandis que Deir el-Médina était à Thèbes Ouest ; il était donc nécessaire d'être mené à la rive pour traverser le Nil. En définitive, la sanction à l'égard de Hérya pour avoir détourné un bien du temple n'est pas connue, et ne peut donc pas servir à établir la peine risquée par Paneb.

Dans un autre cas analogue, pour un vol de ciseau accompagné de violence commis lors du travail dans la Vallée des Rois, Pairy est condamné par une assemblée d'artisans à recevoir 100 coups de bâton[18]. Cependant, ici le châtiment corporel ne sanctionne pas le vol du ciseau en lui-même, mais le ralentissement du travail à la Nécropole induit par la blessure infligée par Pairy à son collègue[19].

En dehors de la région thébaine, un scandale similaire à celui des crimes de Paneb a eu lieu dans le temple de Khnoum d'Éléphantine : plusieurs prêtres sont accusés de corruption, détournements de biens du temple, violences et adultères[20]. La plainte d'Éléphantine fut certainement adressée à l'administration cléricale, et non à l'appareil judiciaire étatique. Néanmoins, comme pour Paneb, les conséquences de la dénonciation ne sont pas connues.

C. Corruption au Nouvel Empire : principes généraux et édits royaux

Les principes théoriques qui régissaient les mentalités égyptiennes apportent un éclairage supplémentaire sur la manière dont les actes de corruption de Paneb peuvent avoir été appréhendés. Dans l'Égypte du Nouvel Empire, la corruption est condamnée, car considérée comme contraire à la Maât, la structure éthique qui régit les comportements dans la société nilotique. L'importance de la Maât est particulièrement notable dans les sagesses, ces textes sapientiaux qui édictaient des principes généraux de vie. L'auteur de *l'Enseignement d'Aménémopé*, daté de la fin du Nouvel Empire (xie s. av. notre ère), recommande ainsi à son lecteur : « Ne reçois pas de gratification d'un puissant pour débouter en sa faveur un faible ; quant à la Maât, c'est un grand présent du dieu, il la donne à qui il souhaite »[21]. La corruption constitue ainsi une transgression de la Maât. Qui transgressait la Maât s'exposait à un châtiment divin, peut-être à la privation d'une vie après la mort. Si le positionnement de la Maât face à la corruption est instructif sur la perception de ce délit dans la société du Nouvel Empire, il ne nous apprend néanmoins guère plus sur les sanctions judiciaires que risquaient ceux qui contrevenaient au principe divin.

Une autre catégorie de textes nous fournit des informations plus concrètes sur les sanctions face à la corruption : les édits royaux. Si nous n'avons pas conservé de législation à proprement parler pour l'Égypte du Nouvel Empire, les souverains ramessides nous ont laissé des édits, inscrits sur des stèles. Ces édits ne constituent en aucun cas des lois générales : il s'agit d'édits normatifs, de décisions ponctuelles qui visent à apporter une solution à des problèmes spécifiques[22].

Plusieurs édits royaux du Nouvel Empire assurent la protection des propriétés et des biens des principaux clergés, et font mention de corruption ou de détournements de biens appartenant à l'administration pharaonique ou cléricale. L'édit du temple de Karnak, promulgué par le pharaon Séthi II (1203-1194 av. notre ère) menace ainsi tant le supérieur ecclésiastique corrompu que le subordonné qui aurait essayé d'acheter ses faveurs d'une destitution de leurs fonctions, pour être réduits au rang de cultivateurs[23]. La corruption est ici punie sur un plan administratif, et non par des sanctions émanant du système judiciaire.

L'édit de Nauri de Séthi Ier ne fait pas mention de corruption dans son acception la plus stricte, mais concerne des détournements de biens et de matériel, des abus d'autorité, parfois accompagnés de violence. Les sanctions sont à la fois économiques, avec un remboursement de la valeur des détournements et des amendes en sus, mais aussi physiques, avec des châtiments corporels dont le plus commun est l'infliction de 100 ou 200 coups de bâton, parfois accompagnée de blessures

ouvertes ou de l'ablation du nez et des oreilles[24]. Les édits d'Hermopolis et d'Ermant, promulgués respectivement par Séthi Ier et Ramsès II, sont quant à eux plus intransigeants : tout membre du clergé qui détournerait la propriété ou les serviteurs du temple serait empalé sur le lieu de son méfait[25].

Conclusion

Il est difficile, à partir de la seule documentation concernant Paneb, de déterminer quelles ont pu être les conséquences de la plainte d'Imennakht à son encontre. Les cas parallèles et la comparaison avec les édits normatifs du Nouvel Empire indiquent néanmoins que la corruption et les détournements de biens appartenant au Pharaon ou au clergé pouvaient être sanctionnés par des châtiments corporels, des peines pécuniaires ou par une destitution des fonctions. La peine dépendait sans doute de l'instance de gestion du conflit : selon que ce dernier était géré par la justice – représentée par l'assemblée locale à Deir el-Médina – ou par la hiérarchie du contrevenant, la nature de la sanction n'était pas la même. Dans le cas de Paneb, le contenu et le contexte de la dénonciation indiquent que le recours au vizir a été effectué en tant que supérieur hiérarchique : le haut dignitaire est celui qui attribuait les plus hautes fonctions dans le village, notamment celle d'artisan-chef. Le serment de Paneb, où il est menacé d'être destitué de ses fonctions, fait écho à l'édit de Karnak, dans lequel la corruption des membres du clergé est punie par une telle sanction. La disparition de Paneb de la documentation postérieure à la dénonciation d'Imennakht, le serment prêté et le parallèle de l'édit de Karnak orientent ainsi les hypothèses vers une destitution de Paneb de sa charge d'artisan-chef.

Le cas de Paneb et les parallèles évoqués indiquent que la corruption était bien présente en Égypte, peut-être plus particulièrement à la fin du Nouvel Empire[26]. Si les édits royaux révèlent que la lutte contre la corruption faisait partie des priorités du pouvoir pharaonique, la gravité de la punition et son effectivité dépendaient des réseaux de soutien dont disposait le malfaiteur : Paneb est longtemps resté impuni grâce aux pressions exercées sur les artisans de Deir el-Médina, et à ses soutiens dans les plus hautes sphères du pouvoir.

Mais plus que la nature même du délit, ce qui compte dans l'affaire Paneb, et dans beaucoup de textes qui rapportent des délits au Nouvel Empire, c'est le choix du plaignant dans l'instance de dénonciation[27] : se plaindre à la hiérarchie pour des questions de fonctions, d'autorité ou de biens attribués par l'administration ; se plaindre à l'assemblée locale en cas de réelle volonté de sanction ou de résolution du conflit, le plus souvent pour des conflits de droit privé. Ainsi, la sentence de l'instance décisionnelle ne dépend pas réellement de la nature « pénale » ou « civile » de l'affaire[28], mais de l'intention du plaignant. Les délits de corruption et de détournement de biens n'échappaient pas à cette distribution des juridictions.

Notes :

1 Sur la date des dénonciations d'Imennakht, distincte de la datation du papyrus qui en conserve la copie, cf. A. Théodoridès, « Dénonciation de malversations ou requête en destitution ? », *Revue Internationale des Droits de l'Antiquité* 28, 1981, p. 75.

2 Cf. S. Allam, « Un droit pénal existait-il "stricto sensu" en Égypte pharaonique ? », *The Journal of Egyptian Archaeology* 64, 1978, p. 66. Cette absence de théorisation de la loi ne doit pas être interprétée comme l'indice d'une pensée juridique peu développée. Au contraire, l'analyse de l'édit d'Horemheb menée par Jean-Marie Kruchten indique « une conception de la justice qui paraît singulièrement avancée » (J.-M. Kruchten, *Le Décret d'Horemheb. Traduction, commentaire épigraphique, philologique et institutionnel*, Bruxelles, 1981, p. 209, 223).

3 Il faut pourtant garder à l'esprit que Deir el-Médina est un village atypique, construit et habité par des artisans : faute d'une documentation similaire pour d'autres communautés, il n'est pas possible de savoir si les interprétations des sources issues de ce microcosme sont valables pour le macrocosme que représente le reste de l'Égypte du Nouvel Empire (cf. A. G. McDowell, *Jurisdiction in the workmen's community of Deir el-Medîna*, Leiden, 1990 (*Egyptologische Uitgaven* 5), p. 9). Néanmoins, nous verrons que dans le cas de la corruption, la confrontation avec des sources extérieures au village procure une vision de ce phénomène qui n'est pas restreinte à la communauté des artisans.

4 Cf. J. Baines, Chr. Eyre, « Four notes on literacy », *Göttinger Miszellen* 61, 1983, p. 86.

5 Voir l'édition de J. Černý, « Papyrus Salt 124 (Brit. Mus. 10055) », *Journal of Egyptian Archaeology* 15, p. 243-258.

6 La communauté des artisans de Deir el-Médina est souvent désignée, dans les textes égyptiens, sous l'appellation de « la Tombe », en référence à la tombe du souverain régnant, qui était le principal chantier de construction de ces hommes.

7 Paneb s'est ainsi parjuré à ce propos, puisqu'il avait prêté serment de n'avoir « pas touché une pierre dans la Place de Pharaon » (P. Salt 124 recto i 16-17).

8 Ces comportements de Paneb sont d'autant plus ambigus que la terminologie égyptienne, en particulier dans ce passage de la plainte d'Imennakht, ne permet pas d'établir le consentement des femmes concernées.

9 Aristide Théodoridès a su montrer qu'Imennakht n'avait d'autre choix que de dresser un tel portrait de Paneb : faute

de pouvoir réclamer la fonction d'artisan-chef de droit, il lui fallait démontrer que Paneb avait transgressé à de nombreuses reprises les obligations incombant au porteur de la charge (A. Théodoridès, « Dénonciation de malversations ou requête en destitution ? », 1981, p. 63).

10 Cf. A. Théodoridès, « Dénonciation de malversations ou requête en destitution ? », 1981, p. 60-63.

11 Les archives de l'administration vizirale étaient conservées à Thèbes : en raison des crues du Nil, ces documents n'ont pas été conservés. À l'inverse, grâce aux conditions climatiques arides de Deir el-Médina, les textes de ce village en bordure du désert nous sont parvenus en grand nombre.

12 La mise à l'écrit des jugements n'était pas systématique à Deir el-Médina : elle relevait du choix d'une des parties, le plus souvent la partie gagnante afin de pouvoir prouver son bon droit en cas de contestation ultérieure. Cf. A. G. McDowell, *Jurisdiction in the workmen's community of Deir el-Medîna*, 1990, p. 188.

13 Traduction J. Winand, « Le serment de Paneb et de son fils ; Papyrus Salt 124, Vo 1, 6-8 », *Bulletin de la Société d'Égyptologie, Genève* 15, 1991, p. 110.

14 « (Si le vizir entend encore parler de moi), je serai chassé, je ne resterai pas dans la Tombe » (traduction J. Winand, « Le serment de Paneb et de son fils », 1991, p. 111).

15 Aux environs de 1166 av. notre ère. Cf. P. Vernus, *Affaires et Scandales sous les Ramsès : la crise des valeurs dans l'Égypte du Nouvel Empire*, Paris, 2001, p. 121.

16 O. Nash 1.

17 A. Théodoridès, « Dénonciation de malversations ou requête en destitution ? », 1981, p. 66.

18 O. BTdK 699.

19 Cf. Chr. Hue-Arcé, « The legal treatment of interpersonal violence in Deir el-Medina », dans A. Dorn, St. Polis (éd.), *Deir el-Medina and the Theban Necropolis in contact*, Liège (à paraître).

20 P. Turin 1887.

21 P.BM EA 10474 XXI 3-6

22 Sur ces édits royaux, cf. A. David, *Syntactic and lexico-semantic aspects of the legal register in Ramesside royal decrees*, Wiesbaden, 2006 (Göttinger Orientforschung IV. Reihe Ägypten 38), p. 3, P. Vernus, « The royal command (wḏ-nsw): a basic deed of executive power », dans Moreno Garcia J. C. (éd.), Ancient Egyptian Administration, Leiden – Boston, p. 259-340, et J.-M. Kruchten, Le Décret d'Horemheb, 1981, p. 214-223.

23 *Édit de Karnak*, l. 16-17. Cf. A. David, *The legal register in Ramesside royal decrees*, 2006, p. 138-140.

24 Cf. A. David, *The legal register in Ramesside royal decrees*, 2006, p. 56-98.

25 Cf. A. David, *The legal register in Ramesside royal decrees*, 2006, p. 108-109.

26 Cf. P. Vernus, *Affaires et Scandales sous les Ramsès,* 2001, p. 15.

27 Cf. Chr. Hue-Arcé, « The legal treatment of interpersonal violence in Deir el-Medina » (à paraître).

28 Sur la notion de droit pénal dans l'Égypte ancienne, cf. S. Allam, « Un droit pénal existait-il "stricto sensu" en Égypte pharaonique ? », 1978, p. 65-68. Voir également l'analyse menée par Andreas Helmis dans sa thèse d'État, restée inédite, à propos de la « pénalité » dans le droit ptolémaïque, qui soulignait avec justesse que la documentation papyrologique « plutôt que de nous permettre de reconstituer un système pénal homogène et aux structures bien précises, nous invite constamment à éclairer des zones d'obscurité que percent, par-ci par-là, quelques étincelles. Dans ces conditions, il s'agit moins de déceler une "pénalité", laquelle, jusque dans nos systèmes les plus évolués, n'a jamais bénéficié d'une réelle et totale autonomie, que de cerner les contours d'un modèle spécifique de réponse aux transgressions de la norme » (A. Helmis, *Crime et châtiment dans l'Égypte ptolémaïque : recherches sur l'autonomie d'un modèle pénal*, Thèse d'État, Université Paris Ouest Nanterre La Défense, Nanterre, 1986, p. 107). Le chercheur conclut à l'existence d'une pénalité multiple dans l'Égypte lagide (*Ibid.*, p. 126) : cette observation est également valable pour les sources néo-égyptiennes du Nouvel Empire.

FIRM

Forum on Islamic Radicalism and Management

En partenariat avec

ASIS INTERNATIONAL

Advancing Security Worldwide®

Chapitre 249 France

PRÉSENTE UN COLLOQUE INNOVANT

Le radicalisme islamique sur le lieu de travail

Jeudi 16 Novembre 2017

Le jeudi 16 novembre 2017 à Paris, FIRM et ASIS accueilleront les plus éminents spécialistes mondiaux du radicalisme islamique, ainsi que des responsables de grandes entreprises.

Ils se réuniront pour le premier colloque consacré au *Radicalisme Islamique sur le lieu de travail*. A cette occasion, une large gamme de sujets sera abordée.

- **De l'aménagement des pratiques religieuses, jusqu'à la détection de la radicalisation.**
- **Des attentats meurtriers contre les cibles vulnérables, jusqu'à la guerre juridique menée contre les employeurs.**
- **Du micro-financement du djihad, en passant par la sécurité, jusqu'à la protection des employés et des clients.**

Nous rassemblons un groupe impressionnant de personnalités qui œuvrent toutes, et sans relâche, pour trouver des solutions au fléau mondial que représente le radicalisme islamique. L'entrée au colloque s'effectuera uniquement sur inscription préalable, et tous les participants seront sélectionnés afin que seul un public choisi puisse participer et interroger notre panel d'experts et de spécialistes.

Conférences en anglais et français avec traduction simultanée

Participez a notre sondage

English:
https://www.surveymonkey.com/r/FIRM-ESCP

Français:
https://fr.surveymonkey.com/r/FIRM-ESCP-VF

ANONYMAT ASSURÉ

Tous les participants au colloque recevront un exemplaire du rapport

Pour vous inscrire :

1. Allez sur le site web **https://firmeurope.com/**

2. Envoyez nous votre adresse mail via la case « APPLY »

3. Nous vous enverrons des instructions

2008 2017
L'ODYSSÉE DU CYBERESPACE

Qui aurait imaginé en 2008 que les menaces auxquelles nous avons à faire face et qu'il nous faut prévenir face aux risques cyber auraient un développement exponentiel ?

Qui aurait pensé qu'un simple logiciel pourrait rançonner en quelques jours et en quelques clics des millions de particuliers, d'entreprises et de services publics sur toute la planète ?

Qui aurait prévu qu'internet pouvait aussi devenir l'outil d'un État pour influencer les élections présidentielles d'un autre ?

Qui aurait supposé que Google peut agir plus sur l'image d'une entreprise que le dirigeant de cette entreprise lui-même ?

Les frontières du cyberespace et donc des cybermenaces se développent quotidiennement.

Plus que jamais, connaitre et partager les enjeux, adopter et faire adopter les bons comportements et les bonnes actions à mettre en œuvre sont devenus des basiques vitaux.

C'est ce défi qui a été porté sur ces dix ans par les dix éditions des forums du Rhin Supérieur et exprimé par plus de 100 conférenciers sur l'ensemble des composantes techniques, juridiques, financières, philosophiques ou tout simplement humaines.

Cette dixième édition, portée par la Réserve Citoyenne et la Gendarmerie d' Alsace assurera, plus que jamais, son rôle de vigie face à ces enjeux auxquels les PME et PME d'Alsace ont à faire face.

Gilbert GOZLAN
LCL (RC) Gendarmerie d'Alsace
Président association AD HONORES Réseau Alsace

PLAN DE SITUATION

CCI ALSACE EUROMÉTROPOLE · Gendarmerie nationale · AD HONORES · CRCC · CLUSIR EST · l'ena · Atheo · KASPERSKY · AXA · Julien Bonfirtsch · LCR · SOCIETE GENERALE

FRC 2017
10ème édition

LA GENDARMERIE D'ALSACE
& LES OFFICIERS DE LA RÉSERVE CITOYENNE

AD HONORES Réseau ALSACE

10ème FORUM DU RHIN SUPÉRIEUR SUR LES CYBERMENACES
2008 - 2017 : L'ODYSSÉE DU CYBER

www.frc.alsace
@cybermenaces

7 Novembre 2017 à l'ENA de STRASBOURG



LA CYBERSÉCURITÉ OPÉRATIONNELLE — LES ATTEINTES À LA RÉPUTATION

DATE LIMITE D'INSCRIPTION LE 27/10/2017 (places limitées)

Réservation par e-mail : cabcom.rgals@gendarmerie.interieur.gouv.fr
En précisant :
Nom, prénom, fonction, entreprise, ville, téléphone, adresse e-mail.

PROGRAMME
ENTRÉE LIBRE
SUR RÉSERVATION

Salle de conférence de l'ENA

FRC 2017 10ème édition

13h00 — ACCUEIL DES PARTICIPANTS

13h30 — DISCOURS D'OUVERTURE

Général Stéphane OTTAVI
Commandant adjoint de la région de gendarmerie Grand Est.
Commandant le groupement de gendarmerie départementale du Bas-Rhin.

Monsieur Jean-Luc HEIMBURGER
Président de la CCI Alsace Eurométropole.

Monsieur François SCHRICKE
Adjoint au secrétaire général pour les affaires régionales et européennes auprès du préfet de la région Grand Est.

■ Animation
Monsieur Gilbert GOZLAN
Directeur de la Sûreté - la Poste Nord & Est.
Président de l'association AD HONORES Réseau Alsace.
Lieutenant-Colonel (RC) de la gendarmerie nationale.

14h00 — CONFERENCE PLENIÈRE

INTERNET : DE LA RECHERCHE A BIG BROTHER

Monsieur Louis POUZIN
Président Open-Root.
Inventeur du datagramme et concepteur du réseau à commutation de paquets.
Queen Elizabeth Prize for Engineering - 2013.

14h30 — TABLE RONDE #1

LA CYBERSECURITE OPERATIONNELLE

Monsieur Michel ROCHELET
Délégué ANSSI Région Grand-Est.

Monsieur Fabrice STALTER
Responsable Sécurité des Systèmes d'Information aux Hôpitaux Universitaires de Strasbourg.
Chargé d'enseignement à l'université de Strasbourg et à l'université d'Angers.

Monsieur Jean-Marc MISERT
Service PGCS – La Banque Postale.
Président du Clusir-Est.

Messieurs Kevin BROU BONI et Axel RIBON
Etudiants à l'Ecole Nationale Supérieur d'Ingénieurs Sud Alsace, université de Haute Alsace.

15h40 — PAUSE / DÉTENTE

10ème FORUM DU RHIN SUPÉRIEUR SUR LES CYBERMENACES

16h20 — TABLE RONDE #2

LES ATTEINTES A LA REPUTATION

Colonel Nicolas DUVINAGE
Chef du Centre de lutte Contre les Criminalités Numériques de la gendarmerie nationale (C3N) - Pôle Judiciaire de la Gendarmerie Nationale (PJGN).

Monsieur Daniel GUINIER
Expert en cybercriminalité et crimes financiers près la Cour pénale internationale de la Haye.
Colonel (RC) de la gendarmerie nationale.

Monsieur Ludovic HAYE
Maire de Rixheim, Délégué régional ANAJHEDN Alsace.
Chef d'escadron (RC) de la gendarmerie nationale.

Lieutenant-Colonel Gilles LE GAL
Officier professeur au Centre d'Enseignement Supérieur de la Gendarmerie (CESG) de l'Ecole des Officiers de la Gendarmerie Nationale (EOGN).

17h20 — CONFERENCE DE CLÔTURE

Général d'armée (2S) Marc WATIN-AUGOUARD
Ancien inspecteur des armées-gendarmerie,
Directeur du Centre de Recherche de l'Ecole des Officiers de la Gendarmerie Nationale (CREOGN).

18h30 — COCKTAIL

2008 2017
L'ODYSSÉE DU CYBERESPACE

www.frc.alsace
@cybermenaces

CEIFAC : UNE TABLE RONDE SUR LA CRÉATION DU PARQUET EUROPÉEN, LE VENDREDI 27 OCTOBRE 2017, À L'UNIVERSITÉ DE STRASBOURG

La France, l'Allemagne, la Belgique, la Bulgarie, la Croatie, Chypre, l'Espagne, la Grèce, la Finlande, la Lituanie, le Luxembourg, le Portugal, la République tchèque, la Roumanie, la Slovaquie et la Slovénie : ces 16 États membres de l'union européenne (UE) se sont accordés sur la création du Parquet Européen dont l'objectif premier est de protéger les intérêts financiers de l'UE en luttant contre les cas de fraude aux fonds structurels de l'UE et de fraude transfrontière de grande ampleur à la TVA.

Ce parquet permettra de donner aux enquêteurs et aux procureurs nationaux, les outils indispensables en matière pénale pour agir rapidement par-delà les frontières.

La création du Parquet Européen est une étape capitale dans la construction d'un espace judiciaire européen.

Ce Parquet sera composé d'un Procureur européen, qui aura la charge de la direction des enquêtes et de la coordination des actions judiciaires, ainsi que de procureurs européens délégués, qui exerceront l'action publique devant les juridictions nationales.

Le Parquet Européen travaillera également main dans la main avec l'Office Européen de Lutte contre la Fraude (OLAF), Eurojust, Europol et les autorités nationales.

La table ronde organisée par le CEIFAC a pour but de faire un état des lieux de la situation actuelle afin de formuler des préconisations pour une mise en oeuvre optimale du Parquet Européen.

PROGRAMME

08h15 – 08h30

Accueil des participants

08h30 - 09h15

OUVERTURE

LE PARQUET EUROPÉEN, AU SERVICE DE L'EUROPE, DE LA JUSTICE ET DU DROIT

Chantal CUTAJAR, Directrice générale du CEIFAC, Maître de conférences à l'Université de Strasbourg, Directrice du Groupe de recherches actions sur la criminalité organisée (GRASCO) (UMR DRES 7354)

09h15 - 10h00

L'ANALYSE DE LA FRAUDE AUX QUOTAS DE CARBONE DANS L'UE

Chris PERRYMAN, chef de projet, département Crime organisé, point contact EUROPOL pour les fraudes TVA intracommunautaire, EUROPOL, LA HAYE, PAYS-BAS

10h00 – 10h20

Pause-café

10h20 – 11h45

TABLE RONDE : « UN PARQUET EUROPEEN, POUR QUOI FAIRE ? »

animée par Chantal CUTAJAR, Directrice générale du CEIFAC **et Marc SIMON,** Commissaire divisionnaire, Chef de l'Unité centrale d'analyse criminelle opérationnelle, Direction de la lutte contre la criminalité grave et organisée, BRUXELLES, BELGIQUE

Débat avec :

Eliane HOULETTE,
Procureur national financier, PARIS, FRANCE
Michel CLAISE, Juge d'instruction financier, BRUXELLES, BELGIQUE
Bruno GONZALEZ-VALDELIEVRE,
Chef d'analyse de la dépense publique, Direction de l'Analyse Office antifraude de la CATALOGNE, BARCELONE, ESPAGNE

11h45 - 12h15

CLÔTURE

Nathalie GRIESBECK, députée européenne Grand EST, Présidente de la commission spéciale sur le terrorisme du Parlement Européen, Mouvement Démocrate, Alliance des démocrates et des libéraux pour l'EUROPE.