LA REVUE DU
GRASCO

www.grasco.eu
www.larevuedugrasco.eu

N°34 — juillet 2021

Parution trimestrielle
Gratuite

EDITORIAL

CHANTAL CUTAJAR

DIRECTRICE DU GRASCO

Depuis le 12 juillet 2021 le Professeur Jean Pradel n'est plus parmi nous.

Le professeur Pradel a été magistrat de 1959 à 1969, date à laquelle il obtint l'agrégation en droit privé et en sciences criminelles. D'abord affecté à la Faculté de droit de Tunis, il devint professeur à la Faculté de droit à Poitiers en 1972. Il était professeur émérite de l'Université de Poitiers depuis 2003. Directeur honoraire de l'institut de sciences criminelles de Poitiers, il a présidé l'Association française de droit pénal. Il a participé à de nombreux congrès internationaux et est l'auteur de nombreux ouvrages en Droit pénal général, Procédure pénale, Droit pénal comparé et Droit pénal spécial.

Il a fait l'insigne privilège à la revue du Grasco de partager notre aventure fidèlement et nous aider ainsi à essaimer les savoirs et les savoir- faire dans le domaine de la lutte contre la criminalité organisée.

Il avait en effet clairement conscience que ce champ devait être investi fortement et dans la durée. On soulignera ainsi, parmi tant d'autres, l'ouvrage collectif sur la criminalité organisée à la lumière du droit français, européen et international qu'il a dirigé avec Jacques Dallest et auquel il m'avait fait l'honneur de me solliciter pour y contribuer.

Le monde scientifique et la communauté des juristes, sont orphelins de son intelligence, de son humanité et de sa capacité à combiner et à marier les grands principes de la culture pénale avec le pragmatisme de la justice pénale au quotidien.

Il n'y a pas de grandes ou de petites délinquances mais des comportements qui doivent être appréciés à l'aulne de l'utile et du juste. C'est à la fois une méthode et une philosophie qu'il a pratiquées, analysées et qu'il nous a transmises.

Toute l'équipe du GRASCO adresse ses très sincères condoléances à sa famille et à ses proches. La grande humanité et le charisme du Professeur Jean Pradel le rendent immortel pour toutes celles et ceux qui l'ont aimé, admiré ou simplement rencontré.

SOMMAIRE

COMITÉ SCIENTIFIQUE DE LA REVUE DU GRASCO

FALLETTI François

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

LABORDE Jean-Paul

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

LEBLOIS-HAPPE Jocelyne

Professeur à L'Université de Strasbourg et chargée de cours à l'Université Albert-Ludwig de Fribourg-en-Brisgau (Allemagne). Elle est membre du groupe European Criminal Policy initiative.

MATHON Claude

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

PRADEL Jean

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

SORDINO Marie-Christine

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

STRICKLER Yves

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

STORCK Michel

Professeur émérite à l'Université de Strasbourg.

INTERVIEW

GÉNÉRAL ÉRIC FREYSSINET,

CHEF DU PÔLE NATIONAL DE LUTTE CONTRE LES CYBERMENACES (PNLC)

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

L.R.D.G. : Pour quelles raisons le pôle national de lutte contre les cybermenaces (PNLC) a été mis en place en 2019 et quelles sont ses missions ?

L'objectif de la création du PNLC en 2019 était de renforcer la gouvernance au niveau central du dispositif CyberGEND. Celui-ci s'est construit progressivement depuis la fin des années 90 et regroupait alors plus de 5 000 gendarmes, depuis les correspondants en technologies numériques (CNTECH) dans toutes les brigades de gendarmerie jusqu'au centre de lutte contre les criminalités numériques (C3N) à Pontoise.

La multiplication des affaires judiciaires d'ampleur, dans le champ de la cybercriminalité, l'imbrication de plus en plus forte de la dimension cyber dans la gestion des crises, ont amené le directeur général à rechercher un pilotage plus direct et plus réactif de ce dispositif. Cela s'est particulièrement ressenti pendant la crise épidémique, où dès le mois de mars 2020 des campagnes préventives ciblées étaient menées vers les publics les plus vulnérables ou ciblés : d'abord les pharmacies victimes d'escroquerie à la vente de produits sanitaires, puis plus tard de nombreuses collectivités locales, hôpitaux et entreprises ciblés par des attaques de rançongiciels opportunistes.

La mission première du PNLC était donc de conduire un plan d'action pour consolider le dispositif CyberGEND et d'assurer le pilotage national en temps de crise.

L.R.D.G. : Quels sont les axes du plan d'action que vous menez pour lutter contre les cybermenaces ?

Le plan d'action que nous menons depuis 2019 se décline en trois axes principaux qui s'inscrivent pleinement dans le plan GEND 20.24 du directeur général : la proximité, l'excellence technologique et les résultats opérationnels.

Ainsi, sous l'angle de la proximité, il s'agit de poursuivre la densification du réseau CyberGEND et d'améliorer sa réponse aux attentes des usagers.

Très concrètement, nous avons mené avec notre direction informatique (le service des technologies et des systèmes d'information de

la sécurité intérieure ST(SI)[2]) le rapprochement au niveau de chaque groupement de gendarmerie départementale des spécialistes des systèmes d'information (les gendarmes SIC) et des enquêteurs spécialisés dans l'enquête numérique et le traitement de la preuve sur les supports numériques (enquêteurs NTECH) pour constituer 102 sections opérationnelles de lutte contre les cybermenaces.

Au niveau régional, 11 groupes cyber de sections de recherches ont été renforcés pour constituer des antennes du C3N, en capacité de traiter des enquêtes de la même complexité au plus près des victimes et développer des échanges plus riches entre ces unités.

De même, nous poursuivons le renforcement de la formation des gendarmes, avec l'expérimentation cette année de compagnies d'élèves gendarmes numériques, donc identifiés dès leur recrutement pour renforcer les compétences techniques au sein de la gendarmerie. De nouvelles formations sont régulièrement créées pour nos enquêteurs, tel le stage FINTECH qui permet de former des enquêteurs aux méthodes de traçage et si nécessaire de saisie judiciaire des cryptoactifs rencontrés dans de plus en plus d'enquêtes judiciaires.

Nous avons aussi développé de nouveaux partenariats avec des acteurs académiques et par exemple rejoint la chaire de cybersécurité des grands événements publics de l'Université de Bretagne Sud ou expérimenté une formation à l'attention de nos enquêteurs départementaux et spécialistes de la prévention dans les entreprises avec l'ENSIBS (École Nationale Supérieure d'Ingénieurs de Bretagne Sud) à Vannes.

Enfin, le plan d'action développe une dimension opérationnelle, pour mieux mesurer l'impact des menaces cyber et conduire – en lien avec les plans d'actions européens EMPACT (European Multidisciplinary Platform Against Criminal Threats) soutenus par EUROPOL – des efforts sur les thématiques les plus prégnantes, depuis le trafic de stupéfiants sur le dark-web jusqu'aux botnets et rançongiciels en passant par les atteintes aux mineurs facilitées par Internet.

L.R.D.G. : Quels sont les liens entre le pôle national de lutte contre les cybermenaces (PNLC) et le Centre de lutte contre les criminalités numériques (C3N) et le commandement de la gendarmerie dans le cyberespace créé par arrêté du 25 février 2021 ?

Le PNLC et le C3N rejoindront le commandement de la gendarmerie dans le cyberespace qui constitue en quelque sorte la prochaine étape dans cette transformation pour une gouvernance plus dynamique et plus transverse de la réponse apportée par la gendarmerie aux enjeux de sécurité dans l'espace numérique.

L.R.D.G. : Quelles sont les principales menaces en matière de cybercriminalité et quel est selon vous le plus grand danger notamment au vu des nouveaux outils connectés ?

En volumétrie, les Français sont touchés par une délinquance numérique du quotidien qui se caractérise par des courriers électroniques malveillants ou des tentatives d'escroqueries par différents vecteurs, y compris notablement sur les plateformes sociales ou de petites annonces. Les atteintes aux mineurs sur Internet sont toujours très prégnantes malheureusement, qu'il s'agisse de harcèlement numérique ou de sollicitations sexuelles.

Sur l'ensemble des faits de criminalité purement informatique (les atteintes aux systèmes de traitement automatisé de données) on retrouve d'abord des accès ou des maintiens frauduleux dans des comptes (d'accès à des systèmes, des courriers électroniques ou encore des comptes de réseaux sociaux) pour faciliter la commission d'autres infractions (notamment des escroqueries et des diffusions de logiciels malveillants).

Et ce sont bien ces derniers qui ont l'impact le plus important, en particulier les rançongiciels. L'évolution la plus notable en la matière est qu'après différentes phases, ce sont aujourd'hui massivement les entreprises et les organisations au sens large (administrations, collectivités locales, établissements de santé) qui en sont victimes. L'importance de cette menace est liée à une véritable professionnalisation des acteurs cybercriminels et en particulier la mise à disposition de rançongiciels clés en mains sur des plateformes de type « crime as a service ».

Mais cette délinquance numérique très visible ne doit pas masquer d'autres réalités tout aussi préoccupantes comme le détournement de données personnelles, le vol de données dans les réseaux des

entreprises (d'ailleurs des rançons sont aussi demandées dans ces cas là sous menace de publication des données, opérations appelées communément « doxxing »), ou encore la fraude au faux support technique dont l'occurrence se multiplie ces dernières années.

Ce qui caractérise la délinquance numérique des années 2020 c'est qu'elle concerne désormais tout le monde, qu'elle ne cesse de croître en volume (10 à 20 % de faits supplémentaires traités par la gendarmerie chaque année selon les typologies) et qu'elle continue de s'appuyer systématiquement sur toutes les évolutions technologiques et toutes les nouveautés.

Et donc bien évidemment, les objets connectés – dans l'entreprise, les bâtiments, les routes ou à la maison – sont une préoccupation parce qu'ils seront systématiquement envisagés par les cyberdélinquants comme de nouvelles opportunités. Ce qui nous inquiète peut-être le plus en la matière c'est que trop souvent le maintien à niveau en termes de sécurité – au travers de mises à jour régulières – n'est pas toujours la priorité des fabricants ou des revendeurs de ces matériels. En témoigne, la faible sécurité souvent constatée pour les caméras de sécurité connectées.

L.R.D.G. : Comment s'organise la vente des attaques aux rançongiciels dont ont été victimes, notamment des hôpitaux courant 2021 ?

Les hôpitaux français ont vraisemblablement été des victimes par opportunité des délinquants, parfois parce qu'ils ont dû ouvrir leurs réseaux informatiques pour faciliter le télétravail. En effet, une grosse partie des attaques constatées en 2020 et 2021 étaient facilitées par des accès à distance mal sécurisés.

Les attaques par rançongiciel sont soit très ciblées, déclenchées à l'issue d'une longue période d'observation par les attaquants dans les réseaux de l'organisation ciblée, soit réalisées au hasard de la découverte d'une porte ouverte dans le système d'information d'une organisation de toute taille. Dans ce dernier cas, ce seront souvent des attaquants moins expérimentés ou en tous cas plus intéressés par la volumétrie que la qualité de la victime.

Il y a souvent plusieurs intervenants et outre le développeur du rançongiciel, l'attaquant d'un hôpital se sera d'abord inscrit comme « affilié » sur la plateforme de rançongiciels, puis aura envoyé des dizaines de courriers électroniques à des cibles potentielles ou aura ciblé des listes d'adresses IP sur lesquelles se trouvent des serveurs d'accès distant vulnérables ou en tous cas identifiés comme tels par d'autres groupes criminels. C'est donc toute une chaîne d'attaquants, mais pas forcément une démarche qui ciblait des hôpitaux.

L.R.D.G. : Existe-il un profil type des cybercriminels et quels sont leurs cibles privilégiés ?

Le profil dépend de la nature des infractions commises, et ce qui les caractérise le plus souvent est leur implantation géographique plus que leur âge ou leurs compétences techniques initiales. Ainsi, beaucoup d'attaquants mettant en oeuvre des rançongiciels sont d'origine russe ou russophones.

L.R.D.G. : Quels conseils donnez-vous pour se protéger des cyberattaques informatiques ?

Le premier conseil est de s'informer et d'être curieux. Le second est très certainement de prendre le temps de mettre en oeuvre les règles de base de l'hygiène informatique, telles qu'elles sont très souvent promues par l'ANSSI (https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/). Un guide plus spécifique pour les petites organisations, TPE et PME a été diffusé très récemment par l'ANSSI et cybermalveillance.gouv.fr (https://www.ssi.gouv.fr/guide/la-cybersecurite-pour-les-tpepme-en-douze-questions/).

Si je devais lister trois points clés importants :

- bien connaître son système d'information et où sont stockées et traitées les données sensibles ou à caractère personnel ;

- avoir un plan de continuité d'activité si un de ces systèmes venait à être compromis (notamment des sauvegardes régulières) ;

- enfin s'assurer de tenir à jour ses différents logiciels et systèmes d'exploitation, y compris sur les smartphones.

L.R.D.G. : Quel est votre avis sur la 5G qui, aux dires de certains, faciliteraient les échanges instantanés entre criminels et constitueraient un frein aux accès aux informations et discussions pour les forces de l'ordre ?

La technologie 5G apporte de nombreux bénéfices pour tous et d'excellentes opportunités pour le développement d'une industrie connectée ou les transports intelligents. Il faut que nous puissions prendre en compte ses spécificités pour être toujours en capacité de mener des enquêtes judiciaires, mais par principe nous ne sommes jamais opposés aux évolutions technologiques. Bien évidemment, nous devons rester conscients que toute nouveauté entraîne des risques supplémentaires, et la 5G, par le nombre de connexions plus important, continue de développer la surface d'attaque contre les organisations.

L.R.D.G. : Quelles réflexions vous incitent les deux décisions rendues par la Cour de justice de l'Union européenne (CJUE) le 6 octobre 2020 en matière de conservation des données, de renseignement et de surveillance étatique, selon lesquelles les États européens ne peuvent pas réclamer aux opérateurs une collecte massive des données de connexions à des fins judiciaires et de renseignement ?

Le Conseil d'État a pris en compte de façon très détaillée les différents enjeux que présentent ces décisions et nous suivons effectivement avec attention les suites qui seront données en droit interne et continuons de sensibiliser les autorités européennes sur les difficultés que cela peut poser.

Plusieurs aspects des décisions de la CJUE me posent question, que j'ai pu détailler dans un article de blog (https://eric.freyssi.net/2020/10/09/decision-de-la-cjue-du-06-10-2020-sur-les-donnees-de-connexion/). En particulier, la CJUE introduit une distinction entre les natures d'infractions selon leur gravité qui ne me semble pas pertinente.

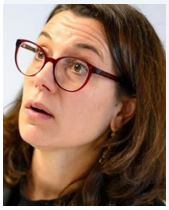
D'une part, parce qu'il n'existe aucune définition juridique internationale de cette notion de « délit sérieux » (serious crime) introduit par la CJUE, et en particulier aucune définition dans le droit de l'Union européenne. La Cour ne donne d'ailleurs aucune indication sur ce qui pourrait ou non entrer dans cette catégorie.

D'autre part, comme nous l'avons souvent expliqué, il y a un critère de nécessité qui ne doit pas être oublié et pour beaucoup d'infractions qu'on pourrait qualifier de « moins graves », s'il n'existe aucune trace sur les réseaux de communication électronique ou si on n'y a pas accès, il ne pourra pas y avoir d'enquête judiciaire. On pourrait citer par exemple, les insultes à caractère discriminatoire ou encore le spam qui sont des infractions moins sévèrement punies que d'autres.

L.R.D.G. : Sous l'impulsion du Président de la République, est prévue la création prochaine d'un Campus Cyber, qui rassemblera les principaux acteurs nationaux et internationaux des secteurs privé et public du domaine de la cybersécurité. Ce Campus, destiné à devenir l'homologue de ce qui se fait déjà depuis longtemps aux USA, en Chine ou encore en Israël, sera un point de contact fixe et identifié pour tous les partenaires européens et internationaux. Que pensez-vous de ce Campus Cyber et d'après-vous, sera-t-il le nouveau point de contact privilégié d'EUROPOL, et particulièrement du Centre européen de lutte contre la cybercriminalité (EC3) qui a été créé au sein de cette structure européenne dédiée à l'échange de renseignements opérationnels et au soutien des investigations transnationales ?

La gendarmerie, et plus généralement le ministère de l'Intérieur, soutiennent très activement la création du Campus Cyber et nous y serons présents pour participer aux échanges et à l'innovation qui sont nécessaires pour assurer une meilleure cybersécurité pour tous. Nous attendons avec impatience son inauguration.

LE TRAFIC DE STUPÉFIANTS : PREMIER MARCHÉ CRIMINEL EN FRANCE



STÉPHANIE CHERBONNIER

CONTRÔLEUR GÉNÉRAL, CHEFFE DE L'OFFICE ANTI-STUPÉFIANTS (OFAST)
DE LA DIRECTION CENTRALE DE LA POLICE JUDICIAIRE (DCPJ)

Premier marché criminel au monde, le trafic de stupéfiants est particulièrement actif sur le territoire français. Face à cette menace croissante, le Gouvernement a fait de la lutte contre les stupéfiants une priorité nationale de premier ordre. C'est dans ce contexte que le plan national de lutte contre les stupéfiants a été annoncé par les ministres de l'Intérieur, de la Justice et chargé des Comptes publics, à Marseille, le 17 septembre 2019.

Six axes, 55 mesures, ce plan porte une véritable politique publique de lutte contre les trafics de drogues, passant par une meilleure connaissance de la menace pesant sur notre territoire, mais favorisant également une approche globale de la lutte contre ces trafics. La mise en oeuvre de cette politique publique a été confiée à un acteur majeur, l'office anti-stupéfiants (OFAST), service à compétence nationale, créé le 1er janvier 2020. L'OFAST est le chef de file de la lutte contre les stupéfiants en France.

L'OFAST et son réseau territorial animent et coordonnent la lutte contre les trafics de stupéfiants, avec l'ensemble des acteurs français (partage du renseignement, identification de cibles d'intérêt prioritaire), mais aussi à l'international, en favorisant les liens avec les pays partenaires dans les zones de production et de rebond, en développant la coopération avec les pays hébergeant des trafiquants d'envergure.

L'état des lieux réalisé par l'OFAST durant ses 18 premiers mois d'activité met en exergue le fait que le marché de la drogue génère des profits considérables, souvent sous-estimés (I), que ce marché, dirigé par des groupes criminels d'envergure, utilise les codes des entreprises commerciales classiques (II), mais surtout que ce marché illégal est basé sur la violence, la corruption, tout en promouvant un contre-modèle (III).

I. Un marché illégal extrêmement lucratif

De nature criminelle, le trafic de stupéfiants est pourtant un « marché classique » où se rencontrent une offre et une demande : il repose sur une production, une consommation et des prix. L'activité criminelle du trafic de stupéfiants génère une véritable économique parallèle qui échappe au contrôle de l'État.

A. Un marché concurrentiel régi par la loi de l'offre et de la demande

L'offre en stupéfiants est caractérisée par une production soutenue qui tend désormais à se développer en dehors des zones traditionnelles de production, y compris en Europe et en France. La demande en stupéfiants est fortement liée au nombre de consommateurs qui a évolué en France au cours des deux dernières décennies. Quant aux prix des stupéfiants, ils reflètent la volonté des trafiquants de proposer des marchandises en cherchant à maximiser les profits.

i. Une offre de produits stupéfiants très abondante

Comme sur tout marché légal,

l'offre de stupéfiants se caractérise par la quantité de produits prêts à être vendus à un prix donné. Le marché atypique que constitue celui des stupéfiants dépend ainsi principalement des capacités de production des produits illicites et de la logistique permettant leur acheminement vers les zones de consommation.

Proche des zones de production des produits stupéfiants, voisine des portes d'entrée de la drogue en Europe et territoire de transit et de rebond, la France est géographiquement située au carrefour des trafics de stupéfiants. Dans ce contexte, l'offre de drogues sur le marché métropolitain et ultramarin est abondante.

La forte disponibilité de cannabis, cocaïne, héroïne et drogues de synthèse sur le marché français est assurée par une production mondiale maintenue à un niveau élevé durant la dernière décennie. Outre l'augmentation des surfaces cultivables et l'amélioration du rendement grâce à des techniques innovantes, la capacité à produire est renforcée par la localisation de certaines étapes de production au plus près des zones de consommation européenne et française. Que ce soit avec des laboratoires clandestins de conversion de cocaïne ou d'héroïne, ou bien avec la cannabiculture, la production de drogues s'exporte ainsi au-delà des zones traditionnelles que sont la région andine pour la cocaïne, l'Afghanistan pour l'héroïne ou le Maroc pour le cannabis. À cela s'ajoute la fabrication de drogues de synthèse historiquement bien implantée en Europe, notamment aux Pays-Bas et en Belgique.

Cette offre abondante de drogues en provenance de l'étranger est désormais complétée par l'herbe de cannabis issue de la cannabiculture pratiquée sur le territoire national. En plein essor depuis quelques années, et porté par l'image d'un « produit plus naturel », ce phénomène s'est accéléré depuis 2016 et place la France parmi les pays producteurs de ce produit illicite. En sont des indicateurs, les saisies de plus de 110 000 pieds de cannabis et le démantèlement de 3 148 sites de culture en 2020.

Avant leur diffusion sur le marché français, les produits stupéfiants provenant de l'étranger empruntent quotidiennement des routes et des vecteurs dont la diversité favorise la fluidité de l'approvisionnement.

Au-delà de leur multiplicité, les routes de la drogue se caractérisent également par leur constante évolution. La faculté des groupes criminels à s'adapter en permanence aux contraintes (instabilité géopolitique, conflits armés, mesures de restriction de circulation, contrôles renforcés, etc.) et aux opportunités (ouverture de nouvelles lignes aériennes ou maritimes, de nouvelles plateformes logistiques, etc.) participe fortement à l'entrée massive des produits stupéfiants en France. À titre d'exemple, pour acheminer le cannabis en France depuis le Maroc, les trafiquants mettent à profit la hausse significative des capacités du port de Tanger grâce au projet « Tanger Med II », de même que l'ouverture en 2017 d'une ligne directe « Morocco Express » reliant ce même port à celui de Marseille-Fos. Concernant la cocaïne, les trafiquants peuvent désormais atteindre directement le marché français depuis l'Amérique latine grâce à la nouvelle liaison maritime directe entre le Pérou, l'Équateur et Dunkerque.

En quête permanente d'efficacité et de profits, les trafiquants de stupéfiants adaptent les vecteurs d'acheminement aux quantités de produits stupéfiants transportées. Ainsi, le fret légal, maritime, routier et aérien, est privilégié pour acheminer de grosses quantités, la masse des échanges commerciaux internationaux limitant les risques de contrôle. À côté des caches classiques (coque du bateau, cache aménagée dans les camions, etc.), des techniques de dissimulation plus élaborées consistent à donner à la drogue la même apparence qu'une marchandise légale pour la rendre « invisible » et rendre nécessaire le recours à un test ou une analyse en laboratoire pour identifier formellement le produit stupéfiant. En outre, dans un but d'approvisionnement rapide et régulier du marché français, le recours à des moyens de transports dédiés et autonomes donne lieu à des modes opératoires variés : « *go-fast* » et « *go-slow* » avec des véhicules rapides roulant à vive allure sur le vecteur terrestre et maritime pour la première méthode et des véhicules classiques se noyant dans la masse en circulant à vitesse normale pour la seconde, utilisation d'avions privés empruntant des aérodromes secondaires moins contrôlés, etc. Enfin, des envois massifs de petites quantités de stupéfiants alimentent le marché français, via notamment des envois postaux ou des passeurs transportant la marchandise dans des bagages ou *in corpore,* principalement pour la cocaïne en provenance de Guyane et la résine de cannabis en provenance du Maroc. Les trafiquants adoptent ainsi la stratégie de saturation des

capacités de contrôle des services répressifs.

Malgré tous ces paramètres visant à complexifier la lutte contre le trafic de stupéfiants, les saisies de produits stupéfiants opérées sur le territoire national sont importantes, avec par exemple des saisies annuelles d'environ 100 tonnes de cannabis depuis 2017 et de plus de 10 tonnes de cocaïne depuis 2016.

ii. Une demande nourrie par une consommation généralisée

Dans un contexte de consommation des produits stupéfiants en France en forte progression depuis 20 ans, le nombre de consommateurs quotidiens de cannabis est actuellement de 900 000 personnes. C'est la drogue la plus consommée sur le territoire, en particulier chez les adolescents. Loin d'être négligeable, la consommation d'autres produits stupéfiants disponibles en France se constate toutefois dans des proportions moins importantes. La France compte ainsi 2,1 millions d'expérimentateurs de cocaïne dont 600 000 usagers dans l'année, 1,9 million d'expérimentateurs d'ecstasy/MDMA dont 400 000 usagers dans l'année, 500 000 expérimentateurs d'héroïne.

En plus de la généralisation tenant au panel des drogues disponibles sur le marché français, le phénomène de consommation généralisée recouvre aussi une réalité géographique et sociale. Elle n'est effectivement plus limitée aux grands centres urbains, l'usage des drogues s'étant progressivement développé dans les zones rurales et périurbaines, ainsi que dans les territoires ultramarins. En outre, cette consommation touche désormais toutes les catégories sociales, des plus précaires aux plus aisées, la livraison à domicile facilitant l'accès aux stupéfiants.

iii. Des prix soumis aux aléas du marché

Comme toute marchandise, les produits stupéfiants ont un prix de gros (le prix d'un kilogramme à l'entrée du produit stupéfiant sur le territoire national, pratiqué entre grossiste et détaillant) et un prix au détail (le prix de revente au consommateur final). La détermination de ces prix résulte du rapport d'équilibre entre l'offre et la demande, ainsi que de plusieurs autres variables. Le prix de gros varie en fonction des coûts de production et d'acheminement (distance parcourue, nombre d'intermédiaires), ainsi que du risque d'interception. Les variables de détermination du prix au détail sont quant à elles l'amortissement du prix de gros, la qualité et l'accessibilité au produit sur le territoire national (la faculté des consommateurs à l'acquérir, sans risque ou préjudice pour eux-mêmes sur le plan physique, matériel ou pénal) ainsi que le degré de concurrence entre trafiquants. D'autres paramètres peuvent également participer à la détermination du prix au détail. Il peut ponctuellement varier en fonction des politiques commerciales menées (réductions, promotions, déstockage) dans un contexte de concurrence accrue et une démarche de fidélisation de la clientèle. Le prix au détail peut aussi suivre les conjonctures de marché. Une augmentation des prix a par exemple été observée durant le premier confinement lié à la crise sanitaire, une pénurie au niveau national ayant été entraînée par une logistique fortement perturbée. Le cannabis s'est vendu plus cher, plus 40 à 60% en moyenne. De même, les prix moyens de la cocaïne et de l'héroïne ont augmenté d'environ 30%.

B. Un marché criminel constituant une économie alternative, source de déséquilibres économiques

En Europe et en France, le chiffre d'affaires annuel des stupéfiants est respectivement estimé *a minima* à 30 milliards et 3,5 milliards d'euros. La manne financière générée est considérable, les marges brutes dégagées étant particulièrement importantes. À titre d'exemple, le prix médian de gros de la résine de cannabis achetée au Maroc est d'environ 500 euros le kilogramme, soit 0,5 euros le gramme. Une fois importé en France, le même kilogramme vaut environ 3 500 euros, soit 3,5 euros le gramme. Le prix médian au détail de la résine de cannabis est de 8 euros le gramme.

En termes d'emploi, chaque point de revente implanté sur le territoire national représente plusieurs dizaines d'emplois illégalement rémunérés (transporteurs, grossistes, gérants de points de vente, revendeurs, guetteurs, nourrices, etc.). Avec un chiffre d'affaires quotidien estimé entre 20 000 à 80 000 euros, un point de deal peut s'avérer extrêmement lucratif[1]. Les activités liées à l'importation et à la redistribution des produits stupéfiants représenteraient au moins 21 000 emplois, et 240 000 personnes vivraient directement ou indirectement du trafic de stupéfiants en France.

Dans cette économie souterraine, des volumes considérables d'espèces sont échangés. Le trafic

de stupéfiants et le blanchiment de ses bénéfices sont des activités criminelles indissociables. La première procure des sources de revenus illicites, la seconde dissimule leur origine frauduleuse et assure leur réintroduction dans le circuit économique légal en France et à l'étranger. Différentes méthodes sont utilisées à cet effet : l'achat et la revente de biens de grande valeur (or, bijoux, articles de luxe, voitures, etc.), la réinjection de l'argent du trafic dans des commerces de proximité et des sociétés légales (restauration, boutique de téléphonie, BTP, etc.), le recours à des systèmes bancaires occultes aux ramifications internationales, etc. Cette introduction de l'argent de la drogue dans l'économie légale est alors source de déséquilibres économiques (fraudes sociales et fiscales, travail dissimulé, corruption, etc.) et de concurrence déloyale. Dans le contexte de crise sanitaire, le risque de blanchiment via les sociétés légales françaises est aggravé. Vulnérables économiquement, les entreprises en grande difficulté sont en effet plus enclines à accepter de « l'argent sale » de la criminalité organisée, notamment du trafic de stupéfiants.

II. Un marché dirigé par des groupes criminels employant les codes des entreprises commerciales légales

Le marché des stupéfiants est géré par des opérateurs économiques atypiques : les groupes criminels. Ces groupes criminels, telles des entreprises commerciales, sont de dimensions variées : auto-entrepreneurs, très petites entreprises (TPE), petites et moyennes entreprises (PME), organisations transnationales, etc.

Ces groupes criminels ont tous pour objectif de gagner des parts de marché et de générer le maximum de profits en diminuant les coûts et en prenant le minimum de risques. Ils présentent pour certains des niveaux de structuration et de professionnalisation très sophistiqués, fonctionnent comme une entreprise commerciale et agissent comme tout commerçant capable de s'adapter aux évolutions du marché, notamment grâce à la manne financière générée par les trafics de stupéfiants.

A. Agilité et adaptabilité des groupes criminels

Les groupes criminels adoptent le plus possible les modèles organisationnels des entreprises commerciales aux activités légales, en achetant, acheminant et distribuant de grandes quantités de produits stupéfiants de manière organisée, professionnelle et cloisonnée.

i. Division du travail

Grâce à leurs ressources humaines et financières et leurs moyens logistiques, les groupes criminels recourent, telles les entreprises commerciales, à la filialisation par activité. Ils organisent ainsi leur activité à travers un agrégat de structures en apparence distinctes les unes des autres, mais en réalité créées pour assurer le *continuum* entre la main d'oeuvre du bas de l'échelle et du point de vente (guetteurs, charbonneurs, nourrices, etc.) et le « chef d'entreprise » (commanditaire). La filialisation permet également aux commanditaires de gérer de loin ce trafic, sans risquer d'être repérés.

L'objectif de compartimenter les tâches se constate aussi bien dans les structures de taille moyenne que dans les plus puissantes. La spécialisation par branches, ou parfois le recours à de la sous-traitance pour une partie des activités, se traduisent fréquemment par une césure entre les filières d'approvisionnement et les filières de distribution. Avec pour but, à la fois de gagner en efficacité et de réduire les risques de détection, ces deux filières sont respectivement prises en charge par des « prestataires de service » spécialisés[2] et par une « main d'oeuvre », de type intérimaire, travaillant de façon occasionnelle et dédiée à des missions spécifiques (gérants des points de vente, revendeurs, guetteurs, nourrices, etc.).

ii. Alliances opportunistes et mise en concurrence des prestataires de services

Tout comme les entreprises commerciales, les groupes criminels ne sont pas figés dans leur organisation. Au contraire, ils fonctionnent de manière opportuniste dans leurs modes opératoires. Ainsi, ils ne recourent pas systématiquement aux mêmes prestataires ou partenaires. Les équipes de « petites mains », à titre d'exemple, sont fréquemment renouvelées et sont recrutées de façon variée : sur le territoire de vente de l'organisation ou à l'extérieur, via les réseaux sociaux ou directement sur place. Elles peuvent même être enrôlées au gré des alliances entre trafiquants et être mises à disposition d'autres groupes criminels opérant sur des territoires différents. De même, les groupes criminels n'hésitent pas à faire jouer la concurrence pour recruter les prestataires de services au moindre coût.

B. Résilience aux aléas

Grâce à leur agilité organisationnelle, les réseaux s'adaptent rapidement aux évolutions endogènes ou exogènes qui perturbent leurs activités (incarcération des têtes de réseau, situation géopolitique, contexte sanitaire, etc.).

Du fait de leurs moyens financiers et leur trésorerie, les réseaux deviennent résilients. La surface financière parfois très conséquente permet en effet aux plus importants groupes criminels de diversifier et multiplier les investissements. De plus, une perte de produit n'aura pas de conséquences importantes sur l'activité globale de l'organisation.

Ces ressources financières, conjuguées à la capacité logistique mise en place, permettent ainsi aux groupes criminels d'être en position de force vis-à-vis des producteurs et des distributeurs, de faire prospérer leur trafic extrêmement lucratif, mais aussi de se développer sur de nouveaux marchés. Comme une grande entreprise, la solvabilité du réseau et l'aura du chef, y compris à l'international, participent à la puissance des grands groupes criminels français.

Ainsi, durant la crise sanitaire en 2020, ce sont les groupes criminels les mieux organisés et disposant d'une importante surface financière qui ont pu s'adapter à la relative pénurie. Ils ont pu assurer la pérennité de leur activité, tant au niveau des importations que de la distribution. Les structures les mieux organisées, disposant à la fois d'un contact direct avec les fournisseurs étrangers et d'une capacité de stockage, ont dégagé une position de force pour asseoir leur emprise vis-vis des autres acteurs. À titre d'exemple, à Marseille, les équipes les plus importantes et les plus structurées qui recouraient au fret pour importer des stupéfiants depuis l'Espagne, ont pris l'ascendant sur les équipes qui fonctionnaient par rotation de transporteurs individuels.

C. Professionnalisation de la vente

Afin d'augmenter leurs profits et attirer de nouveaux clients, les groupes criminels adoptent les codes de l'entreprise commerciale.

i. Techniques de marketing pour attirer et fidéliser les consommateurs

À travers l'emploi de techniques de marketing et de vente, les trafiquants facilitent les achats de produits stupéfiants, de la commande à la livraison. Les groupes criminels peuvent également influencer les comportements d'achat des consommateurs en développant des besoins futurs ou déjà existants.

Les trafiquants cherchent ainsi à rendre les produits plus attrayants en améliorant l'esthétique des produits, l'emballage et le conditionnement. Les comprimés de drogues de synthèse ont, par exemple, des formes, des couleurs et des logos variés, avec nombre de références à la culture populaire (personnages de jeux vidéo, sigles de marques de vêtements, etc.). De même, la résine et l'herbe sont souvent conditionnées dans des boîtes de conserve colorées et des pochons attractifs avec parfois même des labellisations « bios », « éthiques », etc.

Au-delà de l'aspect visuel des produits, les trafiquants informent les clients sur les caractéristiques précises de la marchandise (prix, conditionnement, etc.), ainsi que sur les modalités d'achat/vente (moyen de paiement, mode de livraison, etc.). Ils proposent également des offres promotionnelles pour attirer et fidéliser les clients (cadeaux, soldes, cartes de fidélité, etc.). Ils utilisent ainsi des moyens traditionnels tels que des prospectus, affichettes ou encore des tags sur les murs d'immeubles, mais aussi des publications en ligne via les outils numériques.

ii. Vente en ligne : des transactions hors de l'espace public

Les outils numériques sont utilisés à toutes les étapes de la vente, de la commande au paiement en passant par la livraison, comme dans une boutique en ligne classique. Utilisés depuis plusieurs années dans la vente de produits stupéfiants, ces outils ont connu un développement spectaculaire lors de la crise sanitaire en raison des restrictions de circulation qu'elle a engendrées (confinement, couvre-feu). Cette tendance pourrait perdurer en raison des nombreux avantages qu'ils offrent : facilité, rapidité et discrétion, tant pour les vendeurs que pour les acheteurs.

Les outils numériques permettent ainsi les négociations et la commande de la marchandise. Les réseaux sociaux, sites internet, messageries chiffrées ou non et les centrales d'appels constituent alors des outils privilégiés par les trafiquants. Les commandes via le *darknet* sont plus

limitées mais tendent à se développer.

Une fois la commande enregistrée, les outils numériques servent à planifier les livraisons et assurer le paiement. Le client choisit l'adresse de livraison via les plateformes numériques, puis les produits peuvent être livrés à un point de *deal* traditionnel, mais aussi à domicile ou à des points dédiés plus discrets que les points de *deal* habituels. Lors des confinements, la livraison se déroulait ainsi près des centres commerciaux ou des lieux de restauration rapide à emporter, où la présence physique pouvait se justifier. Au-delà de la discrétion du trafic, le choix d'un autre lieu de livraison qu'un point de deal, satisfait certains consommateurs : ceux qui ne veulent plus se rendre dans les points de vente physiques, par souci de discrétion et de sécurité, et ceux qui ne peuvent pas s'y rendre du fait d'un éloignement géographique.

Traditionnellement, la livraison est effectuée soit directement par le trafiquant, soit par les services de transport classiques (colis). Pour renforcer la discrétion des livraisons, les trafiquants se sont tournés récemment vers une utilisation frauduleuse de l'équipement de célèbres enseignes de livraison (*Uber Eats*, *Deliveroo*, etc.), prenant ainsi l'apparence d'un transport légal.

S'agissant du paiement, outre les traditionnelles transactions en espèces entre le client et le vendeur, le paiement peut s'effectuer sur les réseaux sociaux (par des cartes prépayées, crypto-monnaies, etc.) ou sur le darknet (avec l'installation préalable d'une messagerie chiffrée et d'un porte-monnaie électronique, le *wallet*).

Les transactions en crypto-monnaie (*Bitcoin*, *Monero*, etc.) via le darknet permettent de garantir un certain anonymat aussi bien au vendeur qu'à l'acheteur et participent en grande partie à l'invisibilisation du trafic de stupéfiants en ligne. Néanmoins, en raison des connaissances et compétences nécessaires à l'utilisation des monnaies électroniques, les réseaux sociaux restent souvent privilégiés pour commander les produits stupéfiants, cette méthode laissant la possibilité de payer le produit lors de sa livraison.

D. Absence de contraintes administratives, fiscales et sociales

Même si les organisations criminelles se livrent à une véritable activité commerciale, elles s'affranchissent pourtant de toutes contraintes administratives, fiscales et sociales : elles ne sont pas redevables d'impôts et taxes, et ne sont pas soumises aux déclarations sociales et paiements de charges sociales. Par ailleurs, même si ces organisations s'affirment comme de vrais employeurs en recrutant, rémunérant et licenciant à leur guise leurs employés, elles se libèrent de toutes les obligations liées au droit du travail.

Cette absence de contraintes permet aux groupes criminels de limiter au maximum les coûts internes et de maximiser les profits. L'argent ainsi économisé est directement réinvesti et participe au caractère lucratif de cette entreprise criminelle.

III. Un marché reposant sur l'emploi de la violence et la promotion d'un contre-modèle social attractif

Un tiers des groupes criminels actifs en Europe sont impliqués dans le trafic de stupéfiants qui constitue le principal marché criminel en Europe et en France. Si le marché des stupéfiants fonctionne en grande partie comme un marché légal répondant aux composantes d'offre et de demande et empruntant les codes de l'entreprise commerciale légale, il s'en distingue par l'utilisation, par les groupes criminels, de méthodes violentes, de la corruption, ou encore en proposant un contre-modèle social et culturel.

A. Violences et corruption au service du marché des stupéfiants

Le caractère intrinsèquement criminel du trafic de stupéfiants se manifeste notamment par le recours à la violence. Pour garantir le maintien de leurs parts de marché ou en conquérir de nouvelles, les trafiquants usent en effet de la violence à plusieurs fins.

La manne financière générée par les trafics de stupéfiants suscite une concurrence féroce entre groupes rivaux qui emploient notamment la violence pour asseoir et étendre leur emprise territoriale. Ces faits de violence visant à éliminer ou à dissuader la concurrence (homicides, enlèvements, tortures, intimidations, incendies criminels, etc.) sont de plus en plus constatés dans les milieux narco-délinquants. À titre d'exemple, 262 faits de violences en lien avec le trafic de stupéfiants ont été recensés en 2020 contre 180 en 2019, soit une hausse de 45,5 %. En outre, 80% des règlements de comptes en France interviennent dans le cadre des trafics de stupéfiants. Ces règlements de comptes sont réalisés

par le biais d'actions de type « commando », que les narcotrafiquants accomplissent eux même ou sous-traitent à des équipes de « professionnels » ou de « mercenaires » notamment issus du grand banditisme. Dans ce contexte de protection ou d'appropriation d'un territoire dédié au trafic de stupéfiants, une forme de militarisation se développe avec des violences caractérisées par un usage accentué des armes à feu dont des armes de guerre.

Ces violences permettent aux trafiquants de nouer des complicités par la force afin de faciliter les trafics. Le recours à la violence s'observe dans certaines zones déterminantes pour le trafic afin de contourner l'action des services répressifs qui rend plus difficile pour les trafiquants la sortie des stupéfiants des zones portuaires. Dès 2017, les forces de sécurité ont constaté une augmentation des actions violentes (enlèvements et séquestrations) à l'égard des dockers, maillons essentiels de l'importation de cocaïne en France[3]. Ces derniers font l'objet de pressions répétées de la part de trafiquants désireux de s'adjoindre leurs services pour des « sorties » de drogue.

Les trafiquants cherchent aussi à protéger leur territoire de l'intervention des services répressifs, grâce au soutien d'individus recrutés pour faire diversion, par exemple avec des tirs de mortiers et des jets de projectiles. Le démantèlement d'un point de deal peut susciter des réactions violentes et des représailles (guet-apens, fonctionnaires menacés jusque dans leur vie privée[4], attaques de commissariats). Les dispositifs de vidéosurveillance gênant les trafics sont aussi ciblés par des actes de vandalisme, de même que des destructions d'éclairages publics sont recensées aux abords des points de deal.

Au-delà des violences envers les personnes et les biens, les trafiquants s'attaquent à la probité de tiers susceptibles de faciliter leurs trafics et d'assurer leur impunité. Les trafiquants procèdent via plusieurs modes opératoires pour corrompre leurs cibles. Ils parviennent à corrompre des agents en charge de la maîtrise des flux, afin qu'ils ne réalisent pas certains contrôles, falsifient des pièces de procédure, gênent la concurrence, etc. Il s'agit de policiers, douaniers, surveillants pénitentiaires, ou encore agents privés du secteur des transports notamment des dockers. À titre d'exemple, un docker a été interpellé lors d'une saisie d'1,4 tonne de cocaïne pour avoir participé à plusieurs récupérations de conteneurs contre rétribution. Cette corruption vise également des agents pouvant faciliter le sort des trafiquants en les renseignant sur les enquêtes en cours, en leur fournissant des papiers d'identité falsifiés ou encore en facilitant les échanges d'informations entre des détenus et le monde extérieur. Sont ainsi impliqués des membres des forces de sécurité mais aussi des institutions judiciaires et des administrations publiques en général. La corruption touche aussi les agents territoriaux en charge d'installations locales afin de faciliter les trafics. Des employés communaux permettent notamment l'approvisionnement et la gestion des stocks ainsi que l'encadrement des guetteurs et revendeurs. À titre d'exemple, un employé municipal a été interpellé en 2020 au volant d'une fourgonnette de la ville chargée de près de 100 kg de résine de cannabis.

La corruption de la sphère politique par des groupes criminels, très observée à l'étranger, constitue en France un point de vigilance. En ciblant des élus, notamment à l'échelle locale, les trafiquants cherchent à obtenir des contreparties permettant de faciliter leurs trafics. La contrepartie peut consister en une aide matérielle prenant la forme d'une mise à disposition de moyens ou de logements sociaux, par exemple, mais aussi de décisions et d'orientations politiques favorables au trafic. Pour les élus corrompus, peuvent être attendus en échange le financement de campagne électorale du candidat ciblé par les trafiquants, ainsi que du « lobbying » auprès des électeurs pour orienter leurs votes en sa faveur.

B. Un marché rendu attractif par le contre-modèle proposé

Comme tout marché, la pérennité du trafic de stupéfiants dépend de sa capacité à attirer de nouvelles recrues et à fidéliser la main-d'oeuvre déjà en place. Cependant, loin de véhiculer les valeurs traditionnelles du monde du travail et de favoriser l'intégration de cette main d'oeuvre dans l'activité légale, les trafiquants proposent un contre-modèle promouvant argent facile, rejet de l'autorité et de l'ordre social établi, et possibilités d'évolution et d'acquisition d'un statut élevé par le crime. Pour une population en quête d'ascension sociale,

notamment pour une jeunesse sans qualification professionnelle, refusant de s'insérer dans l'économie légale par des emplois non qualifiés (salaires très faibles, conditions de travail pénibles[5]), être dealer constitue un mode de vie alternatif attrayant. Afin de gravir l'échelle sociale du trafic de stupéfiants, l'usager-revendeur use de son ancrage territorial dans le quartier où il officie pour monter progressivement dans la hiérarchie du réseau et devenir un trafiquant d'envergure.

Parmi les contre-valeurs proposées par les trafiquants de stupéfiants, la promesse d'une rémunération élevée apparaît comme un élément majeur. Quel que soit le niveau de responsabilité dans la chaîne, pourtant hiérarchisée, chaque intervenant perçoit une rémunération supérieure à celle espérée au titre d'une activité licite, et s'assure un train de vie bien supérieur à celui auquel il pourrait prétendre. Même éloignées de celles des grossistes et des premiers intermédiaires, les rémunérations des intervenants au bas de l'échelle (guetteurs, barricadeurs, charbonneurs, nourrices, etc.) sont déjà très importantes. Si un grossiste peut gagner 400 000 euros par an[6], un jeune guetteur, souvent adolescent, gagne environ 90 euros par jour et un vendeur environ 150 euros. La nourrice, quant à elle, peut être rémunérée à hauteur d'un millier d'euros par mois[7]. Cette économie des « cages d'escalier » permet donc à ces délinquants de se procurer des revenus ou de les compléter pour faire face à leurs dépenses courantes et celles d'un foyer familial parfois élargi. L'argent de la drogue permet aux groupes criminels de mobiliser aussi bien les populations les plus précaires et vulnérables à la recherche d'une économie de survie, que des personnes simplement attirées par un niveau de vie plus élevé.

S'instaure une logique de « gagnant-gagnant » entre cette main-d'oeuvre très bien rémunérée pour occuper le terrain et prendre les risques, et les têtes du trafic gérant ainsi leurs affaires à distance, sans impacter la rentabilité de leur activité. La manne financière générée est telle que les coûts induits par le niveau élevé des rémunérations sont absorbés.

Notes :

1. Au 1er avril 2021, 3936 points de deal sont recensés sur le territoire national.
2. Ces équipes spécialisées peuvent grouper les importations de produits stupéfiants de plusieurs groupes criminels. Sur les sorties de conteneurs des équipes dédiées peuvent être sollicitées pour récupérer la cocaïne.
3. En juin 2020, homicide d'un docker mis en examen à la suite d'une saisie d'une tonne de cocaïne en 2017.
4. Les trafiquants obtiennent des informations nominatives issues des pièces de procédure, qu'ils complètent en suivant les policiers et en faisant des recherches sur internet.
5. Article « Génération scarface », *Déviance et Société*, Vol. 28, 2004.
6. Claire DUPORT, « De l'argent facile », *Mouvements*, n°86, 2016.
7. Étude « L'argent de la drogue en France : Estimation des marchés des drogues illicites en France », Institut national des hautes études de la Sécurité et de la Justice (INHESJ), 2016.

LA REVUE DU GRASCO

Numéro ISSN : 2272-981X

Université de Strasbourg, UMR-DRES 7354

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

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

Adresse mail : information@grasco.eu

Directrice de la revue du GRASCO : Chantal CUTAJAR

Rédactrice en chef : Jocelyne KAN

Rédacteur adjoint—Conception : Sébastien DUPENT

ET SI LA PROCHAINE PANDÉMIE ÉTAIT NUMÉRIQUE ?

VALÉRIE LAFARGE-SARKOZY

AVOCATE ASSOCIÉE, CABINET ALTANA, SECRÉTAIRE GÉNÉRALE DE LA COMMISSION CYBER RISK DU CLUB DES JURISTES

Couvrez ce risque que je ne saurais voir… serait-on tenté de penser en constatant, avec amertume, combien la prise de conscience de ce qui est sans conteste l'un des risques majeurs du 21ème siècle – le risque cyber – reste insuffisante. Depuis de nombreuses années, pas une semaine ne passe, parfois pas un jour, sans qu'un événement ne nous en rappelle la prégnance, illustrant parfois tragiquement à quel point entreprises, institutions, États et particuliers se trouvent désormais confrontés à un risque qui s'installe dans notre quotidien… et dont le coût, estimé à près de 10 000 milliards de dollars par an à l'horizon 2025, semble dépasser celui du risque climatique. La pandémie de Covid-19 a certes contribué à accélérer et faciliter certaines attaques, mais ces dernières ne disparaîtront pas avec elle. Le cyberespace, et ses dangers, se nourrit et se développe chaque jour. Il a pour cela le plus fertile des terreaux : une digitalisation croissante de nos usages, dans nos entreprises, chez les acteurs publics et jusque dans nos foyers.

Les cyberattaques inquiètent et pour cause, leur poids économique cumulé les positionne comme la 3e économie mondiale derrière celle des États-Unis et de la Chine. A été estimé ainsi à 6 000 milliards de dollars le coût de la cybercriminalité à travers le monde pour les entreprises et pour l'année 2021[1]. La sphère numérique est simultanément *« un levier économique, source de valeur (…), et source de cyberdélinquance »*[2]. Une ambivalence qui sous-tend une forme évidente de dépendance, et donc de vulnérabilité. Preuve en est qu'en France, en 2019, 90% des entreprises[3] et, en 2020, 18 millions de Français[4], ont été victimes d'un incident cybercriminel.

Face à l'ampleur de cette menace, les réponses sont à l'évidence multiples : des pratiques individuelles et collectives qui, pensées dans un écosystème global, permettent de se prémunir efficacement contre les cyberattaques, des moyens humains et techniques renforcés, des coopérations à une échelle supranationale, un arsenal législatif adapté, etc. Par-delà les réponses possibles, demeure une évidence : le fonctionnement en réseaux contraint à un éveil collectif des consciences, car nul ne peut se prétendre à l'abri, dans sa tour d'ivoire. La moindre faille, qu'elle soit humaine ou technique, interne ou liée à un fournisseur ou un partenaire, doit, à défaut d'être résolue, être connue, analysée et anticipée.

Tous ces constats ont renforcé une conviction ancienne : il est indispensable de faire collaborer acteurs publics et privés, qu'ils soient magistrats, enquêteurs, professeurs, représentants d'entreprises, assureurs et spécialistes des questions de cyberdéfense. Cela a été clairement rappelé par le Club des juristes, premier *think tank* juridique français, dans un rapport publié en avril dernier et intitulé « Le droit pénal à l'épreuve des cyberattaques ». Sur fond d'analyse des dernières menaces, ce rapport alerte sur une situation obérée, sans doute,

par la crise sanitaire mais qui ne saurait pour autant être regardée avec légèreté. Pour reprendre les mots du secrétaire général d'Interpol, la période aura effectivement été propice à la recrudescence des cyber infractions, « *exploitant la peur et l'incertitude causées par la situation économique et sociale* »[5].

I. Derrière le mot « cyber », une réalité éclatée

Définir précisément une réalité et ses conséquences est un exercice aussi délicat que nécessaire. Saint-Augustin s'y était essayé sur « le Temps » lorsqu'il confessait « Qu'est-ce que le temps ? Tant que personne ne me le demande, je le sais ; mais si je veux l'expliquer à qui me le demande, je ne le sais plus ». Et le parallèle est tentant avec le mot « cyber ». Chacun s'en forge une image, mais sans pour autant en comprendre avec précision la portée et la nature.

Aussi partons d'un constat simple, le risque cyber est évolutif et s'adapte extrêmement rapidement à l'environnement qui est le sien et aux résistances qu'on lui oppose. Nul ne peut nier que les « variants cyber » se sont multipliés et ont laissé place à une menace toujours plus diffuse et redoutable, s'ajustant au niveau de sécurité des cibles et à l'objectif poursuivi. On distingue ainsi un grand nombre d'infractions mais il nous paraît nécessaire de citer les sept principales décrites par le rapport IOCTA (Internet Organized Crime Threat Assessment) d'Europol paru en 2018 :

- le *ransomware* ou rançongiciel, qui rançonne le chiffrement des données d'un appareil ou d'un serveur ;

- le *DDoS* ou attaque par déni de service, qui par une saturation d'un réseau ou d'un service en ligne en rend l'accès impossible ;

- le *cryptojacking*, qui par infection oblige un ordinateur au minage d'une cryptomonnaie ;

- la fraude au faux support informatique ;

- le *phishing* ou hameçonnage, qui permet d'usurper l'identité numérique de la victime ;

- l'espionnage économique, qui vise à atteindre un patrimoine informationnel ;

- le sabotage, qui vise quant à lui la panne informatique pure et simple.

Et si ces assauts se nourrissent structurellement d'une économie toujours plus digitalisée, ils savent aussi être opportunistes. Le recours massif, et souvent de manière chaotique, au télétravail et à des outils digitaux peu maîtrisés, aura largement contribué à ce triste essor. Une situation nouvelle qui n'épargne désormais personne : du particulier au grand groupe en passant par l'administration et la PME, chacun est désormais exposé au risque cyber. Marqueurs d'une délinquance décomplexée, les hôpitaux, les collectivités locales et les écoles, pourtant mis à rude épreuve par la crise, auront eux aussi été la cible de ces délinquants surfant sur la vague de la pandémie numérique.

Ce qu'on ne peut désormais plus ignorer, ce qui doit être pour chacun un appel à la vigilance tient au caractère protéiforme de la menace cyber : certaines actions sont brutales, d'autres plus insidieuses. Les plus élaborées ciblent des acteurs majeurs (groupes internationaux, États, etc.), d'autres, moins évoluées, les plus vulnérables.

Quoi qu'il en soit, elles ont pour point commun de générer pour leur auteur un rapport risque/coût/gain à toute épreuve et inédit dans l'histoire de la criminalité. Le ticket d'entrée pour accéder à certaines technologies malveillantes (un kit pour hacker en quelque sorte) est de seulement 5 dollars sur le darknet, alors que le coût moyen d'une attaque pour une entreprise s'élève à 8,6 millions d'euros[6]. C'est sur ce point que chacun a un rôle à jouer. Seul le renforcement des dispositifs de lutte contre la cybercriminalité permettra de réduire ce juteux ratio pour les cybers délinquants.

II. Face au danger : la nécessaire prise de conscience de chacun

A. La crédulité, première source de danger

La cybercriminalité, définie comme « *les faits constituant des infractions pénales tentées ou commises à l'encontre ou au moyen d'un système d'information et de communication des données qu'il recèle* »[7] est clairement encadrée par le droit pénal. Mais elle se heurte encore parfois à l'impréparation, si ce n'est la crédulité, de certaines entreprises. On pourrait ici citer la pratique de la double extorsion, consistant en la subtilisation de données contre demande de rançon. Une pratique à laquelle les entreprises cèdent facilement ; on estime ainsi que

face à cette situation, deux entreprises sur trois cèdent au chantage[8], sans aucune garantie, pourtant, de récupérer les données confisquées…

Et la tentation est grande pour les criminels quand 80% des PME et ETI françaises n'ont pas de plan de sécurité adapté, laissant craindre que nombre d'entre elles ne dispose pas d'une connaissance fine des éléments vitaux de leur patrimoine informationnel : fichiers client, brevets, contrats, etc. À cet égard, il faut noter le souhait de la Commission nationale de l'informatique et des libertés (CNIL) de mener cette année un certain nombre de contrôles relatifs au niveau de sécurité des sites web parmi les plus utilisés dans différents secteurs.

Il faut pour autant agir vite devant un phénomène qui ne peut qu'alerter lorsque l'on sait qu'entre 2019 et 2020 le nombre d'attaques par rançongiciel a été multiplié par quatre. Ce qui n'empêche pas certaines petites entreprises de se penser à l'abri, alors que se multiplient les attaques dîtes « au chalut », qui ciblent de manière indifférenciée un grand nombre d'entreprises, peu important leur taille et leur secteur d'activité. En ce sens, le rapport du Club des juristes rappelle que la cybercriminalité n'épargne personne. Si les entreprises ont consacré près de 21% de leurs budgets informatiques à la cybersécurité en 2020 (contre un peu moins de 13% en 2019[9]), l'effort doit être accentué.

Certes, il serait tentant de penser que les risques changeront une fois la crise sanitaire passée… Mais ne nous y trompons pas, le retour à la vie normale et la reprise du travail en présentiel ne marqueront pas l'inversion de la tendance. La transition numérique engagée se poursuivra quoiqu'il arrive. Ainsi, la protection, l'hygiène informatique, la traque des délinquants et la coopération internationale seront déterminantes.

B. Prévenir, pour ne pas avoir à guérir

La nécessité d'une politique d'information et de sensibilisation est perçue au plus haut niveau de l'État, conduisant les pouvoirs publics à développer un certain nombre d'outils à destination de tous les publics ciblés. Une campagne dont la pierre angulaire, la plateforme gouvernementale « cybermalveillance.gouv.fr », est le porte-étendard. Face à l'importance de cette mission d'intérêt général, le Président de la République dévoilait en février dernier un plan d'un milliard d'euros pour renforcer la cybersécurité en France. Avec pour objectif, notamment, de doubler les emplois dans la filière à horizon 2025, en s'appuyant notamment sur la création d'un « Campus Cyber » fédérant les différents acteurs de l'écosystème et renforçant les synergies entre les acteurs clés du tissu industriel et de la filière.

Les acteurs institutionnels du secteur auront eux aussi tiré les enseignements de cette nouvelle vague d'infractions en renforçant leur collaboration. Ainsi, le ministère de la Justice et l'Agence nationale de la sécurité des systèmes d'information (ANSSI) ont élaboré conjointement un guide de bonnes pratiques dont on ne peut qu'inviter à la lecture, tant il rappelle des fondamentaux trop souvent méconnus.

Cette sensibilisation a aussi, et il faut en avoir pleinement conscience, un revers juridique puisque l'imprévoyance ou la négligence peuvent ouvrir des voies de droit contre celles et ceux qui auraient manqué à leurs obligations. Ainsi, le défaut de sécurisation des Systèmes de traitement automatisés de données (STAD) peut désormais entraîner de lourdes sanctions pour les entreprises. D'où, l'obligation de notification de toute violation de données à la CNIL qui va également dans ce sens et a vocation à sensibiliser les acteurs de l'écosystème cyber à l'engagement de leur responsabilité.

Reste un constat partagé par tous les spécialistes de la discipline : le coût de l'investissement dans la prévention est infiniment moindre que le coût à supporter en cas d'attaque d'ampleur. Investir, pour une entreprise, 5 à 10% de son budget IT dans la prévention des risques cyber est une nécessité pour prévenir cette menace.

III. Une criminalité organisée, opportuniste… loin de l'image d'Épinal du hacker solitaire

Si personne n'est épargné, le secteur public et les entreprises sont des cibles majeures de la cyberdélinquance. L'état de la cybermenace inquiète et pour cause, nous avons assisté ces dernières années à la multiplication des atteintes aux STAD. Chacun garde en mémoire les attaques d'EDF en 2011, d'Orange en 2014, de Saint-Gobain en 2017, d'Eurofins en 2019, de Google en 2020, de la mairie de la Rochelle la même année et de celle d'Amiens en 2021. Des atteintes d'envergure

qui, si on les ajoute à celles dirigées contre le secteur public, mettent en péril des acteurs économiques majeurs, et parfois la sécurité nationale.

Le rapport du Club des juristes définit le STAD comme « *un ensemble composé d'unités de traitement, de mémoire, de logiciels, de données, d'organes d'entrées-sorties et de liaisons devant être protégés par des dispositifs de sécurité (…). Concrètement, pour une entreprise, il s'agit de son patrimoine informationnel, de son savoir-faire et des données concernant son personnel, ses clients, ses prospects, ses fournisseurs. Ces données de l'entreprise constituent un bien à protéger, car ce sont elles qui sont convoitées par les cyberdélinquants* ». À l'heure ou « *presque tout, des appareils électroménagers aux véhicules, en passant par les jouets pour les enfants, est en passe d'être paré de la connectivité réseau et communication* », la prudence est de mise.

Au fantasme du *hacker* isolé, incarné autrefois par Néo dans *Matrix* ou par Stanley Jobson dans *Opération Espadon,* se substitue aujourd'hui la réalité d'une menace ciblée et industrialisée relevant de la criminalité organisée, à l'origine de 55% des attaques mises en oeuvre. La structuration de ces groupes criminels les conduit désormais à envisager des cibles de premier plan, plus lucratives. Une tendance confirmée par le vol d'outils de piratage à la CIA et au groupe de cybersécurité FireEye en 2017 et 2020 : des outils sophistiqués permettant de nuire aux systèmes même les mieux protégés.

À cette sophistication des moyens d'assaut, s'ajoute une approche *business* parfaitement mûrie. Philippe Cotelle, Head of Insurance Risk Management chez Airbus Defence and Space, rappelait récemment que « *les cybercriminels font des études de marché de leurs cibles. Lorsque celle-ci ont atteint un niveau supérieur de protection, ils concoctent des attaques sophistiquées via leurs intermédiaires plus fragiles en termes de cybersécurité* ».

Les risques encourus par les entreprises sont nombreux : vol de données personnelles, de secrets industriels et commerciaux, blocage des systèmes d'information, atteinte à la réputation, risque de sanction par manque de sécurisation des STAD, pertes financières, désorganisation… Les raisons de se protéger sont multiples, alors comment lutter efficacement ?

IV. Répondre à la menace cyber : un enjeu collectif

A. La mobilisation des moyens judiciaires

Avec la spécialisation du droit pénal pour rempart, la France s'avère techniquement au point dans la lutte contre les menaces informatiques. Par ailleurs, nos experts et enquêteurs, bien que trop peu nombreux, sont formés à la pointe des connaissances et des techniques modernes.

En appui à la spécialisation des magistrats, la spécialisation des services d'enquêtes a, elle aussi, contribué au déploiement d'une défense efficiente. À ce titre, la sous-direction de lutte contre la cybercriminalité (SDLC), l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC), les différentes brigades spécialisées dans le traitement du contentieux lié aux STAD et aux données et la Direction nationale du renseignement et des enquêtes douanières (DNRED) « *se sont fortement mobilisés ces dernières années pour relever les défis relatifs à la connaissance du cyberdélinquant, au développement des ressources humaines de renseignement, à la coordination des réseaux d'information et d'innovation, à la formation des enquêteurs en plus grand nombre et à la coopération internationale* »[10].

Au cours des dernières années, la France s'est dotée d'un corpus de textes spécifiques, parmi lesquels on peut citer la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, la loi Godfrain du 5 janvier 1988 ou loi relative à la fraude informative, la loi pour la confiance dans l'économie numérique du 21 juin 2004, la loi pour une République numérique du 7 octobre 2016 ou encore le contenu de la loi de programmation et de réforme de la Justice du 23 mars 2019. Un corpus solide qui témoigne de la densité de l'évolution de l'arsenal répressif pour le législateur. Un arsenal en appui duquel, les dispositions du Code de la propriété intellectuelle et du Code monétaire et financier achèvent de parfaire la couverture juridique française.

La variété des modes opératoires emporte aussi la grande diversité des qualifications juridiques en matière d'infraction cyber. En pratique, ces infractions sont souvent qualifiées

d'escroquerie (article 313-1 du Code pénal), de vol (article 311-1 et suivants du Code pénal) ou encore de faux et usage de faux (article 441-1 du Code pénal). Sans compter le recours à l'infraction spécifique d'atteinte aux STAD (article 323-1 et suivants du Code pénal).

Une lutte judiciaire qui, outre ses réponses fermes, doit aussi faire preuve d'adaptabilité et de réactivité dans son appréhension de ces nouvelles infractions. Raisons pour lesquelles le soutien aux enquêteurs, le développement des services d'enquête, les moyens qui leur sont alloués et les coopérations internationales doivent encore faire l'objet d'améliorations.

La volatilité de la preuve en matière cybercriminelle laisse toutefois apparaître plusieurs limites. Ainsi, « *en matière de preuve numérique, droit et techniques s'associent afin de garantir une efficience procédurale, conditionnée par la recherche d'un équilibre indispensable entre la préservation de la vie privée et la protection de l'ordre public* »[11]. La dématérialisation et l'extraterritorialisation de la preuve constituent des freins majeurs à l'exercice judiciaire, au même titre que le recours à certains outils d'anonymisation comme les *Virtual Private Networks* (VPN) et la technologie TOR, qui rendent plus ardue la tâche des enquêteurs.

Raison pour laquelle les techniques d'investigation ont été adaptées à la menace. Les officiers de police judiciaire peuvent le cas échéant, procéder à des réquisitions, perquisitions et saisies informatiques des données. La possibilité d'accéder aux correspondances stockées et d'enquêter sous pseudonyme est aussi de nature à faciliter l'enquête, au même titre que l'obligation de conservation des données par les opérateurs et les différents moyens d'accès aux données chiffrées.

Il faut aussi signaler l'exceptionnel travail de l'ANSSI qui coopère très efficacement au quotidien avec les services d'enquêtes et de renseignement et partage ses connaissances et ses méthodes.

La coopération judiciaire internationale fonctionne également de mieux en mieux et se développe très nettement en Europe.

Mais les moyens offerts au justiciable et notamment aux entreprises ne consistent pas seulement dans l'efficacité de la réponse judiciaire, se trouvent également entre leurs mains un certain nombre d'outils.

B. La mobilisation des acteurs économiques

Au-delà des préconisations formulées par le rapport – et sur lesquelles nous reviendrons – les entreprises se voient offrir un large panel « d'actifs » mobilisables dans la lutte contre la cybercriminalité.

Pour les entreprises, cela passe par l'instauration d'une indispensable culture transverse de cybersécurité et la définition d'une stratégie de gouvernance des données et du patrimoine informationnel. Un processus qui passe par des investissements humains, techniques et organisationnels, autour d'un plan d'action regroupant : l'identification des données sensibles à protéger ; la désignation des référents en charge de ces questions et la formation des collaborateurs ; la définition d'une politique de sécurité des systèmes d'information ; la mise en conformité avec le Règlement général sur la protection des données (RGPD) ; l'intégration de ces règles dans le règlement intérieur et la définition d'un plan de gestion de crises en cas d'attaque. L'intégration du risque cyber aux stratégies de *risk management* impose aux entreprises des audits réguliers, l'adoption de logiciels de protections et d'outils de sauvegarde.

D'un point de vue assurantiel, le coeur de notre économie, les moyennes entreprises, n'est en grande majorité pas protégé. En cas d'attaques, ces entreprises, qui n'ont pas les compétences internes et ont des trésoreries tendues, sont vulnérables. Or, en parvenant à atteindre ces cibles « faciles », les cyberattaques ont un impact majeur sur le fonctionnement des grandes entreprises, dont ces plus petites organisations composent l'écosystème. Cela génère une menace pour l'ensemble de l'économie française, pour autant, le recours à l'assurance ne doit pas éclipser les bonnes pratiques

Dans les affaires de criminalité, la réactivité étant la clé, la victime doit agir avec rapidité, tant dans la saisine et l'information de l'ANSSI que dans le dépôt de plainte. En dépend la sécurité de l'entreprise et la possibilité d'identifier rapidement les auteurs d'infractions. La constitution de « *Red Teams* », capables de déceler les failles de sécurité dans les systèmes informatiques, et le maintien de l'engagement individuel des collaborateurs à un niveau élevé sont autant de pratiques vertueuses

à encourager.

V. Dix préconisations pour mieux lutter contre la menace cyber

Au terme de son rapport, le Club des juristes formule dix préconisations à destination du Gouvernement, du ministère de la Justice, de l'ANSSI et des entreprises :

Selon ces prescriptions, l'attention portée par le Gouvernement au risque cyber devrait être celle d'une cause nationale, au risque de passer à côté d'un enjeu majeur de sécurité.

Le ministère de la Justice devrait s'engager plus encore dans la spécialisation des magistrats du siège et du parquet, au travers notamment de la formation continue. Ce qui pourrait nécessiter la création d'une filière de cyber magistrats ; le renforcement du pôle cyber du parquet de Paris ; la spécialisation d'une chambre du tribunal judiciaire en matière de droit du numérique ; la création d'un département numérique et cyber au niveau de la cour d'appel de Paris et la mutualisation de la formation des jeunes magistrats, des élèves avocats ainsi que des corps de Police, Gendarmerie et Douanes.

Les services de la Justice en matière de lutte contre la cybercriminalité devraient être étoffés au travers du recrutement de cadres et assistants spécialisés dans les questions de cybersécurité. Sans oublier le développement des échanges réguliers avec les compagnies d'experts judiciaires dont la nomenclature devrait être revue afin d'introduire une spécialité numérique et cybersécurité.

Il conviendrait également de veiller à renforcer la coopération public/privé, en orientant les investissements vers l'émergence d'une filière française et européenne d'excellence en matière de cyber technologie.

Les instances européennes, quant à elles, doivent oeuvrer pour l'adoption d'un régime européen uniforme de conservation des données, permettant de répondre aux besoins opérationnels des services répressifs et judiciaires.

Il faudrait enfin inciter les États sanctuaires, au sein desquels de nombreux cybercriminels trouvent refuge, à mettre fin à l'impunité de ces groupes cybercriminels sévissant depuis leur territoire. L'ANSSI travaille efficacement sur le sujet afin de contraindre ces États à une forme de solidarité contre la menace qui vise tous les États sans aucune exception. Un des objectifs étant une plus large adhésion à la Convention de Budapest du 23 novembre 2001 relative à la cybercriminalité.

Les entreprises quant à elles, et comme nous l'avons vu plus en détail, sont invitées à investir davantage dans la prévention des risques cyber.

La prévention intégrée dans un dispositif global de gestion des risques qu'ils soient faits à l'échelle internationale, étatique ou privée, reste l'outil de protection le plus efficace.

En conclusion, il est temps de se donner tous les moyens d'agir et de poursuivre la mobilisation de tous les acteurs (nationaux et internationaux) pour voir remporter d'autres victoires, à l'image de l'arrestation, en Ukraine, de plusieurs cybercriminels du groupe Egregor en février dernier et du démantèlement des réseaux Eramet et Gregor. La présidence française de l'Union européenne en 2022 sera là aussi l'occasion et une opportunité unique de consolider la coopération internationale, sous l'impulsion des initiatives tricolores et d'un exécutif résolu, aux côtés des entreprises, à prendre toute la mesure du risque cyber.

Notes :

1. Rapport annuel de Cybersecurity Ventures et de Herjavec Group, 2019 – https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf
2. Rapport du Club des juristes « Le droit pénal à l'épreuve des cyberattaques », avril 2021 – https://www.leclubdesjuristes.com/les-commissions/publication-du-rapport-le-droit-penal-a-lepreuve-des-cyberattaques/
3. Rapport du ministère de l'Intérieur « État de la menace liée au numérique en 2019 », février 2019 - https://www.interieur.gouv.fr/fr/content/download/117487/942458/file/rapport-cybermenaces2019-HD-web.pdf
4. Norton Cyber Safety Insights, 2021 – https://www.nortonlifelock.com/us/en/newsroom/press-kits/2021-norton-cyber-safety-insights-report/
5. Rapport d'Interpol « Cybercriminalité : impact du Covid-19 », août 2020 - https://www.interpol.int/fr/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-Design_02_FR.pdf
6. Rapport d'Accenture Security « The cost of cybercrime », 2019 – https://www.accenture.com/fr-fr/insights/security/etude-cout-du-cybercrime
7. Rapport du ministère de la Justice « Cybercriminalité », février 2014 -http://www.justice.gouv.fr/include_htm/pub/rap_cybercriminalite.pdf
8. Hiscox Cyber Readiness Report, 2021 - https://www.hiscox.co.uk/cyberreadiness
9. Hiscox Cyber Readiness Report, 2021 - https://www.hiscox.co.uk/cyberreadiness
10. Rapport du Club des juristes « Le droit pénal à l'épreuve des cyberattaques », avril 2021.
11. Rapport du Club des juristes « Le droit pénal à l'épreuve des cyberattaques », avril 2021.

BIENS MAL ACQUIS : VERS UN MODÈLE DE RESTITUTION ?

SARA BRIMBEUF

RESPONSABLE DU PLAIDOYER GRANDE CORRUPTION ET FLUX FINANCIERS ILLICITES À TRANSPARENCY INTERNATIONAL FRANCE

En octobre 2017, pour la première fois en France, un tribunal condamnait un haut dirigeant étranger pour avoir blanchi sur le territoire français des fonds publics détournés dans son pays, pour un montant estimé à plus de 150 millions d'euros. Prononçant la confiscation de ces fonds, le tribunal correctionnel de Paris concluait son jugement en appelant à une évolution du régime français des peines de confiscation en vue de l' « *adoption d'un cadre législatif adapté à la restitution des avoirs illicites*[1] ».

Près de quatre ans plus tard, cet appel semble enfin sur la voie d'être entendu. Dans le cadre du projet de loi de programmation relatif au développement solidaire et à la lutte contre les inégalités mondiales qui devrait être adopté dans le courant de l'été 2021, le Parlement français a adopté une série de dispositions portant création d'un mécanisme de restitution des avoirs illicites.

Ce dispositif, par son architecture et ses modalités, doit satisfaire l'objectif suivant : s'assurer que les fonds confisqués, une fois restitués, ne retombent pas dans les circuits de la corruption mais bénéficient aux populations dans les pays d'origine concernés.

Dépassant les normes multilatérales qui demeurent insuffisantes en la matière (I), le dispositif français s'inscrit dans une dynamique internationale qui a permis l'émergence de quelques principes de droit souple (II). Sous l'impulsion des organisations de la société civile française, certains de ces principes ont été pour la première fois incorporés dans un dispositif de restitution de droit interne (III). En faisant le choix d'inscrire ces principes dans le droit français, les parlementaires ont fait un choix ambitieux qui pourrait faire du dispositif français un modèle dans la matière. Pour ce faire, ce choix doit à présent s'accompagner d'une véritable politique française de restitution et de la mise en place de modalités règlementaires et budgétaires donnant à ces principes une portée contraignante (IV).

I. La restitution des avoirs : principe fondamental mais cadre juridique minimal

Érigée en principe fondamental de la Convention des Nations Unies contre la Corruption[2] (ci-après « CNUCC »), la restitution des avoirs illicites est pourtant l'un des articles de cette Convention dont la mise en oeuvre par les États signataires est la plus lacunaire[3]. La CNUCC pose un cadre juridique minimal en la matière, reflet d'un compromis résultant d'intenses négociations entre les États[4]. Ces règles succinctes couplées à de nombreux obstacles juridiques, politiques et matériels expliquent en grande partie pourquoi les avoirs illicites confisqués demeurent généralement si peu restitués.

Les règles de restitution prévues par la CNUCC ne jouent, en effet, que lorsque l'État *d'origine* des avoirs a engagé et mené à leur terme les procédures judiciaires nécessaires au recouvrement des avoirs illicites blanchis ou recelés à l'étranger. Qu'il s'agisse d'une requête aux fins d'exécution d'une décision de confiscation[5], d'une action aux fins de reconnaissance de son droit de propriété ou d'une action aux fins d'indemnisation de son préjudice[6], toutes ces actions nécessitent une démarche de l'État d'origine des avoirs.

Faute de requête émanant des États d'origine, rien n'impose aux États d'accueil ayant procédé à la confiscation des avoirs blanchis

ou recelés sur leur territoire, de les restituer. Or, par manque de volonté politique, en raison d'obstacles techniques, parce que leurs juridictions se trouvent empêchées d'agir par crainte de représailles ou parce qu'elles sont elles-mêmes sujettes à la corruption, les États d'origine font trop rarement la démarche d'exiger la restitution de leurs avoirs confisqués à l'étranger[7].

En dehors de cet aspect, le texte de la CNUCC est également laconique sur les modalités de mise en oeuvre et principes directeurs de la restitution. Ce texte se borne ainsi à rappeler, à titre préliminaire, que l'exécution de leurs obligations par les États parties au titre de la présente Convention doit se faire dans le respect des « *principes de l'égalité souveraine et de l'intégrité territoriale des États et celui de la non-intervention dans les affaires intérieures d'autres États*[8] ». La CNUCC prévoit, enfin, la possibilité pour les États parties de déduire des fonds confisqués des montants correspondant aux « *dépenses raisonnables encourues pour les enquêtes, poursuites ou procédures judiciaire ayant abouti à la restitution*[9] » ainsi que celle *« de conclure, au cas par cas, des accords ou des arrangements mutuellement acceptables pour la disposition définitive des biens confisqués*[10] ».

Dans ce contexte, quelques pays ont développé leurs propres mécanismes de restitution. Les succès et les échecs de ces différentes expériences de restitution ont progressivement permis de faire émerger, sous l'impulsion notamment de l'Office des Nations Unies contre la Drogue et le Crime (ONUDC) et de la Banque mondiale, certains principes directeurs en la matière.

II. L'émergence de principes de droit souple qui peinent à s'affirmer

Lors du Forum Mondial sur le Recouvrement des Avoirs qui s'est tenu à Washington D.C. en décembre 2017, à l'initiative des États-Unis et du Royaume-Uni et sous l'égide de la Banque mondiale et de l'ONUDC, furent adoptés les Principes pour la disposition et le transfert de actifs volés confisqués dans des affaires de corruption[11]. S'inspirant des expériences réussies en la matière, ces principes dépourvus de portée contraignante, prévoient notamment d'associer les organisations de la société civile au processus de restitution, d'encadrer les processus de restitution par des principes de transparence et redevabilité, et de veiller à ce que les avoirs restitués ne profitent pas aux personnes impliquées dans la commission des infractions sous-jacentes.

Certains de ces principes ont récemment été repris par la déclaration politique adoptée en juin 2021 par les États Membres des Nations Unies lors de la session extraordinaire de l'Assemblée générale dédiée à la lutte contre la corruption[12]. Cette déclaration politique souligne, par exemple, la nécessité que les mesures de restitution soient « *mises en oeuvre de manière transparente et responsable* » et de veiller à « *penser aux objectifs de développement durable au moment de décider de l'emploi des avoirs restitués*[13]». Enfin, elle évoque également différents modèles possibles pour la disposition et l'administration des avoirs confisqués tels que « *l'allocation de ce produit au Trésor public, le réinvestissement des fonds à des fins spéciales et l'indemnisation des victimes de l'infraction, ainsi que la réutilisation des avoirs à des fins sociales au bénéfice des communautés*[14]».

Accueillis positivement et complétés par la société civile[15], ces principes semblent être de plus en plus intégrés aux *Memorandums of Understanding*, ces accords passés entre États d'accueil et États d'origine, déterminant les modalités concernant la disposition, l'allocation et l'affectation des biens restitués[16]. De plus en plus repris par ces accords, ces principes peinent néanmoins encore à se généraliser et à s'imposer[17]. En témoignent par exemple les clauses intégrées dans la plupart des accords bilatéraux de restitution prévoyant que ces principes ne créent aucune obligation susceptible d'engager la responsabilité des pays signataires[18].

Preuve supplémentaire d'une certaine frilosité des États en la matière, ces principes n'ont pour l'instant pas été repris par les droits nationaux, cela même chez les pays les plus actifs en matière de restitution. Ainsi, la Suisse, qui a progressivement développé un dispositif de lutte contre les avoirs illicites de potentats et a déjà restitué près de deux milliards de dollars de fonds détournés[19], se borne seulement par exemple à rappeler dans sa loi sur les valeurs patrimoniales d'origine illicite la nécessité d'associer « *autant que possible les organisations non gouvernementales au processus de restitution*[20] ». Il en va de même pour le Royaume-Uni comme les États-Unis, pourtant à l'initiative de l'instauration de ces principes.

Sous l'impulsion des organisations de la société civile françaises, la France semble au contraire sur la voie de s'engager sur un tout autre chemin.

III. L'ancrage de ces différents principes dans le dispositif français

En précisant que les avoirs confisqués seront restitués *« dans les pays concernés au plus près des populations »* en vue de financer « *des actions de coopération et de développement dans le respect des*

principes de transparence et de redevabilité, et en veillant à l'association des organisations de la société civile », le législateur fait le choix de transposer dans le droit français certains des principaux principes directeurs portés au niveau international[21].

En pratique, des lignes budgétaires spécifiques seront créées au sein de la mission « Aide publique au développement » qui est placée sous la responsabilité du ministère des Affaires étrangères. Avec cette solution de fléchage budgétaire, le ministère des Affaires étrangères pourra décider, au cas par cas, la manière dont les fonds seront restitués[22]. Ce mécanisme de fléchage budgétaire devrait permettre d'assurer la traçabilité des fonds dès les premières étapes du processus de restitution. Les fonds seront non seulement isolés sur une ligne budgétaire spécifique au sein du budget général de l'État français, mais ils pourront également faire l'objet d'un contrôle annuel par le Parlement.

Ambitieux et avant-gardiste, le dispositif qui devrait être adopté par le législateur français dans le cadre du projet de loi de programmation relatif au développement solidaire et à la lutte contre les inégalités mondiales ne constitue néanmoins qu'une première étape dans la construction du dispositif final de restitution des avoirs illicites. Si cette première étape démontre qu'un modèle français de restitution peut progressivement émerger, elle demeure à elle seule insuffisante.

IV. Des modalités règlementaires et budgétaires en suspens et la nécessité d'une volonté politique ambitieuse

De nombreux points restent en effet en suspens. Les fonds restitués n'étant ni des dons ni des prêts, mais de l'argent détourné qui n'a jamais appartenu à la France, il est ainsi crucial qu'ils ne soient pas comptabilisés comme l'aide publique au développement française. Ces modalités qui devront être précisées dans le cadre du projet de loi de finances pour l'année 2022 devront également s'accompagner d'indicateurs précis permettant de mesurer avec précision l'effet d'additionnalité des fonds restitués.

Le ministère des Affaires étrangères s'octroyant la possibilité de définir les modalités de restitution « au cas par cas », il sera crucial d'instaurer des garanties permettant d'assurer l'effectivité, la transparence, l'intégrité et la redevabilité du processus afin d'éviter, pour chaque nouvelle affaire, que les intérêts politiques, économiques ou diplomatiques ne prennent le pas sur l'objectif premier de la restitution.

Les modalités de sélection et d'intervention des différents intermédiaires par lesquels transiteront les fonds confisqués destinés à être restitués, au premier rang desquels l'Agence Française de Développement, devront être clairement définis dans le cadre d'instruments règlementaires ou contractuels ultérieurs.

Le dispositif de restitution ne saurait donc suffire à lui seul et dans sa forme actuelle à poser un modèle en la matière. Outre l'instauration de garanties techniques et budgétaires, la solidité du futur mécanisme dépendra également de la volonté politique de la France de faire de son futur mécanisme de restitution un véritable outil au service de la lutte contre la corruption et pour le développement solidaire.

Notes :

1. Jugement rendu le 27 octobre 2017 par le tribunal correctionnel de Paris.
2. Article 51 de la CNUCC : « *La restitution d'avoirs en application du présent chapitre 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.* »
3. « *Most countries reviewed to date did not have practical experience with the return and disposal of assets.*", §20, Conference of the States Parties to the United Nations Convention against Corruption Implementation (UNCAC), Implementation of Chapter V (Asset recovery) of the UNCAC, Avril 2018 ; « *Bien que des condamnations pour blanchiment d'argent puissent être prononcées dans l'État dont les fonds publics sont détournés, la plupart de celles examinées […] ont eu lieu en dehors du pays où a eu lieu l'infraction d'origine de détournement de fonds. En analysant les affaires qui ont été examinées dans le rapport, la rareté des demandes de coopération internationale basées sur les ordres de confiscation dans l'État dont les ressources ont été détournées ou qui ont subi un préjudice est notable* », Digest of asset recovery cases, Office des Nations-Unies contre la Drogue et le Crime, Décembre 2013.
4. Travaux préparatoires of the negotiations for the elaboration of the United Nations Convention against Corruption.
5. En vertu de l'article 57.3 alinéas a) et b) de la CNUCC.
6. En vertu de l'article 53 de la CNUCC.
7. Sur ce point, voir « Le sort des biens mal acquis et autres avoirs illicites issus de la grande corruption – Plaidoyer pour une procédure adaptée, au service des populations victimes », p.9, Transparency International France, Octobre 2017.
8. Article 4 de la CNUCC.
9. Article 57.4 de la CNUCC.
10. Article 57.5 de la CNUCC.
11. GFAR Principles for Disposition and Transfer of Confiscated Stolen Assets in Corruption Cases
12. Déclaration politique « Notre engagement commun à nous attaquer efficacement aux problèmes posés par la corruption et à prendre des mesures pour la prévenir et la combattre et renforcer la coopération internationale » annexée à la résolution A/S-32/L.1 adoptée le 2 juin 2021 lors de la session extraordinaire de l'Assemblée générale des Nations Unies sur les problèmes posés par la corruption et les mesures visant à la prévenir et à la combattre et à renforcer la coopération internationale.
13. Ibid, §48.
14. Ibid, §49.
15. Civil Society Principles for Accountable Asset Return - Submission to the UNGASS against corruption
16. Voir par exemple le *Memorandum of Understanding* signé en décembre 2017 entre le Conseil Fédéral Suisse, la République du Nigéria et la Banque Mondiale qui prévoit l'association effective des organisations de la société civile nigériane au processus de restitution ainsi que la nécessité d'un processus transparent et redevable.
17. Voir par exemple la réaction de la société civile internationale vis-à-vis du premier accord de restitution signé entre l'Irlande et le Nigéria en septembre :"*Alors que le protocole d'accord souligne que les parties impliquées « reconnaissent l'importance de veiller à ce que les normes les plus élevées possibles en matière de transparence et de redevabilité soient appliquées pour le retour et la disposition des actifs », il comprend peu de dispositions spécifiques sur la transparence et la redevabilité et ne fait aucune référence de la société civile dans le suivi de l'utilisation des fonds restitués.* », 2020UNCAC Coalition, 28 septembre 2020.
18. Voir par exemple le *Memorandum of Understanding* signé en septembre 2020 entre le Conseil Fédéral Suisse et la République qui, tout en

rappelant expressément la nécessité de mettre en oeuvre les principes adoptés lors du Forum Mondial de Recouvrement des Avoirs, prévoit à l'article 7 que "*this memorandum is considered a basis for continued cooperation and does not create any legally binding rights or obligation between the signatories.*"

19. « Pour que le crime ne paie pas - L'expérience de la Suisse en matière de restitution d'avoirs illicites », 2017.

20. Loi sur les valeurs patrimoniales d'origine illicite du 18 décembre 2015, Article 18.

21. Le dispositif français de restitution fait, en outre, expressément référence aux principes adoptés lors du Forum Mondial sur le Recouvrement des Avoirs. Le Cadre de partenariat global annexé au projet de loi de programmation relatif au développement solidaire et à la lutte contre les inégalités mondiales dispose en effet que « « La *France restitue, en coopération avec les États étrangers concernés, et au plus près des populations de ces États, les fonds issus de la cession des biens dits « mal acquis », dans le cadre du mécanisme prévu à l'article 1er de la présente loi de programmation, et conformément à l'ODD 16 de l'Agenda 2030 et du programme d'action d'Addis-Abeba. Dans le respect des principes de transparence et de redevabilité, notamment rappelés lors du forum mondial sur le recouvrement des avoirs de 2017, la France veille à la bonne information du Parlement, des citoyens et des organisations de la société civile ainsi qu'à l'association de cette dernière au suivi de la mise en oeuvre du mécanisme prévu au même article 1er. Les actions de coopération et de développement financées dans les pays concernés, à partir des crédits ouverts concomitamment aux recettes issues de la cession des biens dits « mal acquis », ne sont pas comptabilisées au titre de l'aide publique au développement de la France.* »

22. Le projet de loi de programmation relative au développement solidaire et à la lutte contre les inégalités mondiales, Article 1er alinéa XI : « *À cette fin, les recettes mentionnées au premier alinéa du présent XI donnent lieu à l'ouverture de crédits budgétaires au sein de la mission « Aide publique au développement », placés sous la responsabilité du ministère des affaires étrangères, et financent des actions de coopération et de développement dans les pays concernés au plus près des populations, dans le respect des principes de transparence et de redevabilité, et en veillant à l'association des organisations de la société civile. Le ministère des affaires étrangères définit, au cas par cas, les modalités de restitution de ces recettes de façon à garantir qu'elles contribuent à l'amélioration des conditions de vie des populations* ».

OUVRAGES RÉCENTS

LA CONFISCATION DES AVOIRS CRIMINELS

NOUVEAU ENJEUX JURIDIQUES

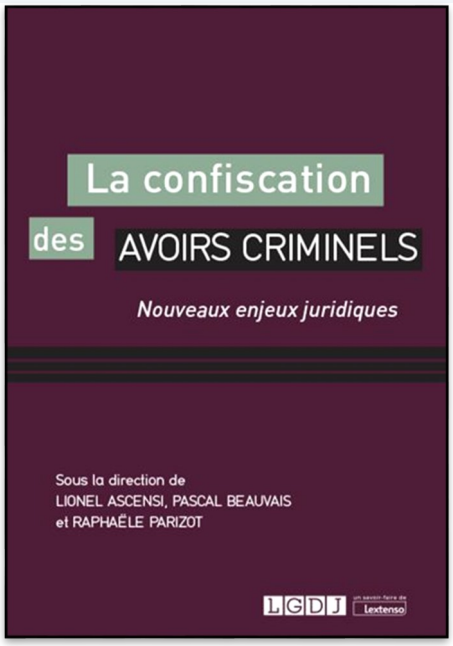
SOUS LA DIRECTION DE : LIONEL ASCENSI, PASCAL BEAUVAIS ET RAPHAËLE PARIZOT

ÉDITEUR : LGDJ

Résumé

Les saisies et confiscations pénales ont connu depuis quinze ans une succession de réformes fondamentales : le domaine d'application de la peine de confiscation s'en est trouvé considérablement étendu et son contenu diversifié, quand sont dorénavant mises en oeuvre de nouvelles procédures de saisies destinées à en garantir l'exécution.

Ces réformes ont immédiatement provoqué l'explosion d'un contentieux particulièrement technique pour les magistrats du siège et du parquet, avocats, enquêteurs, mais aussi pour les notaires, huissiers de justice ou encore établissements bancaires, tant la matière est à la confluence du droit pénal et de la procédure pénale, du droit civil des biens et des régimes matrimoniaux, des procédures civiles d'exécution et collectives.



Surtout, ces évolutions ont été porteuses d'enjeux nouveaux pour le droit pénal, la volonté des législateurs interne et européen d'assurer le recouvrement des avoirs criminels pour « garantir que le crime ne paie pas » se heurtant à la nécessité de respecter ces principes fondamentaux que sont la présomption d'innocence, le respect des droits de la défense, la personnalité et l'effectivité de la peine.

Ce sont ces enjeux que cet ouvrage collectif examine. Il est le fruit d'un colloque qui s'était tenu le 8 novembre 2019 sous l'égide de la chambre criminelle de la Cour de cassation et du Centre de droit pénal et de criminologie de l'Université Paris Nanterre, et la direction scientifique de Lionel ASCENSI, Pascal BEAUVAIS et Raphaële PARIZOT. Réunissant pour la première fois professeurs de droit, magistrats, avocats et membres de l'Agence de gestion et de recouvrement des avoirs saisis et confisqués (AGRASC), ce colloque, puis cet ouvrage, visent à stimuler une réflexion interdisciplinaire et de droit comparé, théorique et pratique, sur les nouveaux enjeux juridiques du recouvrement des avoirs criminels.

NOËL PONS

AUTEUR DU LIVRE *LA CORRUPTION COMMENT ÇA MARCHE ? FRAUDES, ÉVASION FISCALE, BLANCHIMENT*

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

L.R.D.G. : En tant qu'ancien inspecteur des impôts, ancien conseiller au Service Central de Prévention de la Corruption (SCPC), co-directeur pédagogique des certificats fraude et corruption de l'École Supérieure de la Sûreté des Entreprises (ESSE), quel constat faites-vous sur les pratiques frauduleuses ?

Depuis presque cinquante années, je décrypte les pratiques frauduleuses partagées entre initiés et j'atteste que l'adage latin « Fraus omnia corrumpit », la fraude corrompt tout, est plus que jamais valide. Elle a désormais intégré le coeur de l'économie et participe pleinement à la construction de la marge.

Les fraudes, dans leur acception la plus large, ont muté. En leur temps spécifiques, sectorielles, oeuvrant en silo, elles se sont déployées « à la ville et au monde », elles se sont métamorphosées en une véritable activité professionnelle très lucrative. Ses « mécanismes de l'ombre » ne se développent plus, depuis longtemps, à la marge des économies mais ont intégré leurs processus de fonctionnement. Elles engendrent l'un des secteurs les plus florissant et créent des masses d'argent occulte et autant de pertes pour les finances publiques.

L.R.D.G : Qu'avez-vous voulu exprimer dans votre dernier livre *LA CORRUPTION COMMENT ÇA MARCHE? Fraudes, évasion fiscale, blanchiment*, paru au mois d'avril 2021 ?

Cet ouvrage est fondamentalement disruptif. Il met en lumière les pratiques de l'ombre, il décrit les techniques couramment utilisées en les illustrant de cas réels dans lesquels bien des « premiers de cordée » pourraient se reconnaître. Il peut aussi être considéré comme un support d'investigation pour ceux qui désireraient analyser quelques dérives à leur porte, et à l'instar du livre de Jean Cosson *Les industriels de la fraude fiscale*, de mieux comprendre ces activités clandestines.

Il décline l'aphorisme suivant :

- Celui qui fraude doit blanchir ;

- Celui qui corrompt doit d'abord frauder puis blanchir ;

- Tous ont besoin d'argent sale dont les criminels disposent à foison !

L.R.D.G. : Quels sont les outils pour frauder que vous décrivez dans votre livre ?

L'écosystème des fraudes associe en tant que de besoin tous les participants à l'ingénierie du faux.

Le constat est attristant, le « consortium des magouilleurs » a réussi là où les administrations peinent souvent par manque de volonté politique. Il regroupe les savoirs et diffuse les métastases de ce cancer dans toutes les opérations économiques. Ces seigneurs de l'ombre, agents multicartes des manipulations, déploient leurs activités dans chacun des domaines analysés dans l'ouvrage : la fraude fiscale et sociale qui assassine la démocratie, évidemment la corruption intimement liée à la fraude, le truquage des marchés publics, un sujet rarement développé, l'inévitable intrusion de la criminalité dans l'économie et enfin l'irrésistible ascension des lanceurs d'alerte. Ces créateurs de fictions juridiques, grands détecteurs de failles, utilisateurs de faux documents, manipulateurs de comptes, véritables « couteaux suisses » des montages dont ils organisent l'installation et le suivi, puisent le savoir dans le sel des professions juridiques, comptables, bancaires et se complaisent dans les paradis fiscaux. Ce métier « moderne » s'est magnifiquement développé ! Des cohortes d'artistes du faux ont conçu et diffusé des montages sur mesure et sur étagère, s'articulant autour de paradis fiscaux, de pays « rebonds » et de réseaux constitués entre conseils et partenaires délinquants. Ils collent constamment aux besoins des clients considérant que la transparence est ontologiquement intolérable. C'est un meccano géant, fluide et réactif à l'échelle du monde qui s'est informatisé s'appuyant sur les failles et les blocages des diverses législations. Les manipulations se déclinent désormais à l'infini du fait du développement du numérique.

Toute cette organisation est structurée autour de chaînages de faux : sociétés écran, fausses factures, faux contrats, surfacturations et factures de complaisance entre autres. À cet égard l'actuel procès de « Bygmalion » peut tout à fait être utilisé comme support de formation pour des enquêteurs débutants tant il condense les typologies des fraudes comptables.

Le paradis fiscal est sans doute le plus connu des outils utilisés, une bonne moitié de son activité est composée par des opérations non frauduleuses mais pouvant attenter à la concurrence ou relevant de l'optimisation fiscale. Le reste implique la fraude ou le camouflage criminel. Un paradis fiscal réunit cinq opportunités, une fiscalité réduite, une opacité maximale couverte par le secret bancaire, une législation financière allégée, le refus de transmettre toute information et la création de structures écran. Tous les pays *utiles* ne possèdent pas ces opportunités, l'un des enjeux majeurs consiste à éclater les créations d'entités et les flux entre les pays mon-

nayant ces pratiques, les pays criminalisés et sans moyens de contrôle réel et ceux dans lesquels des failles discrètes peuvent être utilisées.

De nombreuses mesures ont été prises pour réduire ce potentiel nuisible dont l'exigence de déclaration des bénéficiaires effectifs, mais l'expertise des conseils permet de les contourner aisément.

Cette caisse noire des évadés fiscaux, ce réseau d'optimisation fiscale ou de gestion administrative des fonds provenant des activités criminelles se comportent comme une plateforme et comme une chambre d'enregistrement des droits de propriété et jouent un rôle central dans ces montages. Ils fonctionnent comme une comptabilité miroir. Quant à la liste officielle, c'est une farce, les pays les plus nocifs n'y figurant pas et nombre de ces confettis sont issus d'enjeux géopolitiques.

À la suite des « *Panama papers* », un seul pays a mis en place une législation efficace, ce sont les États-Unis avec la loi FATCA (Foreign Account Tax Compliance Act). Il est toujours surprenant de constater, dans les hautes sphères, le grand silence qui entoure les scandales liés aux paradis fiscaux, on se demande toujours si elles approuvent ou regrettent la situation.

Les grands cabinets de conseil, ont élaboré et élaborent sans doute bien des montages défiscalisant complexes multipliant les filiales offshores. Ils développent les montages dits « d'optimisation » enrichissant sans cause les « pique-assiette » européens entre autres.

La demande est si forte ! Adeptes du grand écart, ils ne rechignent pas à conseiller à la fois les États, dont l'Union européenne dans la mise en place des contrôles, et les entreprises cibles de ces derniers, c'est gênant et fleure bon le conflit d'intérêts.

Ces structures ont aussi un rôle de contrôle des entreprises dont on peut se demander si les multinationales ne sont pas finalement « too large to be effectively controlled ». Quelques scandales récents semblent en apporter la preuve, la chute de CARILLION en Grande Bretagne, l'immense scandale financier de Wirecard en Allemagne, près de deux milliards d'euros comptabilisés n'existaient pas, et chez nous la remarquable escroquerie de la célèbre « mamie cassoulet » dont l'entreprise a pu pendant des années déclarer 300 millions de faux produits.

L'activisme des intermédiaires répond aux demandes des clients, infinies, complexes, diversifiées et... tellement rémunératrices. Juste pour le plaisir, j'ai décrit quelques montages opérés par ces conseils si discrets au titre de leurs propres rémunérations. La mondialisation et l'internet ont été le facteur facilitateur de ces opérations en se jouant des frontières, des lois, en découplant le flux financier du flux documentaire et en fractionnant la propriété intellectuelle.

La demande est forte, on a constamment besoin des paradis fiscaux, des conseils, des sociétés écrans, d'un montage propre à l'oligarchie : la rétro commission, de banques et banquettes expertes dans l'art du blanchiment officialisant les flux douteux un moment invisibles et réapparaissant l'instant d'après purifiés.

En fait, qu'il s'agisse de manipuler les valeurs de transfert, de faire tourner les fausses factures, ou d'éviter le paiement de la TVA, l'opacité permet à qui le désire de disposer de fonds en franchise d'impôts. Ces derniers étant recyclés en partie sur les marchés après une succession complexe d'opérations à l'occasion desquelles les fonds criminels se mélangent aux produits de la fraude.

Le montage du retour sur commissions, ce « chocolat du troisième étage » des élites perverties oeuvrant dans les grands marchés internationaux est aussi décrit, analysé, on y relève souvent la présence de liens tissés avec la grande criminalité.

La réussite majeure de ces entités c'est d'avoir su créer et d'entretenir les réseaux utiles et les circuits de communication protégés à l'instar des groupes criminels.

L.R.D.G. : Quelle analyse faites-vous du développement des fraudes fiscales et sociales ?

Le développement des fraudes fiscales et sociales est une plaie ouverte dans le processus démocratique.

La fraude fiscale, sujet obsédant et complexe nous concernant tous, est l'objet de toutes les attentions. Érigeant en système l'appauvrissement collectif, pénalisant par trois fois les personnes acquittant leurs impôts. En effet, les personnes qui acquittent leur impôt sont pénalisées au cours de l'année où la fraude a lieu. Elles doivent compenser les gains cumulés des placements frauduleux évidemment non déclarés et les dettes d'État car les sommes fraudées se retrouvent sur les marchés créanciers des États endettés. La fraude fiscale utilise gaillardement tous les montages élaborés ci-dessus. Quelques avancées législatives ont, certes, été constatées, cependant la masse des fraudes, plus de cent milliards d'euros par an, près de onze milliards de fraudes sociales s'y ajoutent, nécessite des mesures exceptionnelles difficiles à prendre pour ceux qui visent une élection. L'ouvrage décrit d'abord une sorte de typologie du comportement des fraudeurs, chaque groupe présentant un profil adapté au type de secteur agressé depuis les gagne-petit jusqu'aux professionnels patentés. Quelques-unes des mille et une opportunités d'évitement utilisées par les personnes physiques ainsi que les techniques les plus utilisées sont ainsi décrites. Il démontre aussi que l'assise des escroqueries sociales est bien plus importante dans le secteur des cotisations (8 milliards environ) que dans celui des prestations (2,3 milliards).

Il en ressort une sorte d'inventaire des pratiques en vigueur chez les personnes physiques sur la base de faux documentaires.

Les techniques les plus utilisées par les entreprises pour minorer la base imposable et emplir leur caisse noire sont aussi disséquées par cycle comptable. L'évitement du paiement de la TVA et les attaques criminelles font aussi l'objet d'une analyse approfondie en particulier des structures

écrans et des plates-formes d'achat. Certains dirigeants de sociétés fraudent aussi, quelques pratiques particulièrement raffinées sont décortiquées, en particulier le fait de majorer considérablement les commissions versées par l'entreprise à un fournisseur qui finance ainsi l'activité d'une entreprise personnelle, les montants se comptant par millions d'euros, ce qui démontre que l'imagination est aussi au pouvoir dans ce domaine.

Cette étude des caisses noires est complétée par une description des comportements ordinaires, peu, voire pas du tout transparents (pas de publication du chiffre d'affaires dans les pays, dans le cloud, opacité des algorithmes etc.), et complexes à souhait des multinationales et des GAFAM camouflées sous la fiction de l'optimisation fiscale et posant le problème des oligopoles privés ne pouvant être régulés que par une réglementation ferme. Les propositions américaines dont on semble se féliciter en apparence préconisent la mise en place d'une taxation de 21 % réduite à 15 % semble acceptée, du bout des lèvres, mais un lobbying effréné est en cours. Les pays dont le taux d'imposition est moindre que le taux envisagé, l'Irlande, Chypre, la Pologne et la Hongrie, y sont évidemment opposés ce qui n'est pas une surprise.

Les entreprises devraient donc payer là où elles réalisent leurs profits et non au lieu de leur siège social. Pour ma part, j'estime que si la fixation d'un taux d'imposition fixe semble constituer un bon début, les effets peuvent cependant en être aisément limités par une manipulation de la base taxable. Les exonérations, des crédits d'impôts, des régimes de faveur (rescrits) et les fraudes (valeurs de transferts et montages tout aussi classiques destinés à réduire les bénéfices) ne manqueront pas d'impacter le processus engagé, et rien n'est précisé sur le régime de la propriété intellectuelle ! Attendons donc les aménagements finaux avant de nous réjouir, il ne faudrait pas que cela devienne un « emmental fiscal avec beaucoup de trous » ! selon l'expression du fiscaliste genevois Thierry Boitelle (Le Temps, 9 juin 2021, Sébastien Ruche).

L'analyse des dépenses de l'État largement incontrôlées qui sont l'objet des critiques des grands organismes de contrôle finalise cette partie.

En matière de fraudes et de « dépenses de l'État » c'est bien « un pognon de dingue » qui est perdu pour l'État et pas uniquement là où on le dénonce à grands cris.

L.R.D.G. : En quoi consiste l'hyper corruption dont vous faites mention dans votre livre ?

La globalisation, un monde multipolaire, de nouvelles hiérarchies économiques, les prouesses des techniciens du faux et la criminalisation des économies ont engendré une hyper corruption, facteur essentiel de l'aggravation des dérives frauduleuses qui s'accomplissent dans la rente des corrompus et jamais dans la redistribution. De plus les kleptocrates, ils sont nombreux, ne favorisent pas les dynamismes mais le conservatisme local.

Cette hyper corruption qui affecte l'élite comme les strates mineures, est susceptible de poser quelques problèmes relevant de l'éthique des gouvernants. L'ouvrage identifie les procédés généralement utilisés pour gommer les effets des procédures anticorruption et pour contourner les réglementations mises en place à la suite des directives OCDE et Onusiennes relatives à la corruption transnationale. Il précise comment, pour ces mêmes raisons, certains services baissent discrètement les yeux. Les entreprises, pour leur part, savent faire évoluer les montages protégeant le paiement de commissions voire de rétrocommissions en apprêtant des montages écrans aussi alambiqués qu'efficaces. Le but recherché étant de rendre le contrôle inopérant en l'absence de dénonciation, de contentieux inattendu ou d'intervention américaine. Ainsi, une organisation élaborée autour de structures ad hoc est établie afin que le flux versé aux commissionnés illégitimes, souvent « splittés » (prestataires et sous prestataires domiciliés dans des paradis fiscaux différents) et en provenance d'un cadre organisationnel peu contrôlable ne permettent pas d'atteindre les corrupteurs. Les flux corruptifs passent aussi par des faux investissements, par des paiements de facilitation et par tant d'autres pratiques frauduleuses bien connues et toujours efficaces.

Les États-Unis semblent avoir conçu la lutte anticorruption comme l'un des moyens de limiter le développement des multinationales souvent européennes avec ces « deals de justice » conclus avec les multinationales en

cause : de l'argent pour éviter un procès, après leur avoir fait payer les frais de l'enquête visant à les incriminer et engager une surveillance approfondie de ces dernières pendant trois ans. Ces poursuites engagées permettent effectivement de lutter contre la corruption en exigeant le paiement d'amendes sévères. Le ciblage est souvent pertinent, car il permet d'accéder aisément aux secrets des entreprises mises en cause lors de la procédure d'accompagnement et souvent de s'approprier par voie de fusion ou d'absorption tout ou partie de ces dernières comme ce fut le cas pour ALSTOM et TECHNIP entre autres.

C'est ensuite une balade assez affligeante dans la corruption ordinaire rencontrée en France comme dans tous les pays réputés développés qui est proposée au lecteur. Elle affecte tous les domaines depuis le gardien d'immeuble jusqu'aux plus hauts fonctionnaires publics et les responsables privés. Les divers moyens d'entretenir des rapports « friendly » avec des cibles corruptibles sont aussi décrits et quelques cas, significatifs il est vrai, illustrent ces comportements répréhensibles. À cet égard, la tendance actuelle, dont le principe a été conçu au cours des années soixante, tendant à multiplier le recrutement des contractuels dans l'administration, à généraliser le recours aux cabinets extérieurs et la réforme des grands corps ne pourra que multiplier les conflits d'intérêts et la corruption poussés par des intérêts privés ou de carrière. Le risque majeur reste cependant avec la création d'une élite « polyvalente » la perte de tout lien avec les « métiers » fort différents en laissant la main aux conseils extérieurs dont l'efficacité des tableurs reste à prouver.

L'ouvrage brosse aussi un tableau accablant des pratiques corruptrices dans le monde qui, on peut le dire, sont devenues endémiques. Ces dernières concernent d'abord la corruption des pauvres, qualifiée souvent de « corruption du ventre », celle générée par le système politique et enfin celle des kleptocrates qui est reproduite à l'identique dans tant de pays. Le scandale ODEBRECHT est exemplaire d'une situation hélas très fréquente.

Finalement, les constats décrits dans cette partie mettent en évidence le caractère endémique du développement de la corruption « urbi et orbi », il est donc possible de plagier Descartes en avançant le fait que « la corruption est la chose au monde la mieux partagée ! ».

L.R.D.G. : Qu'en est-il des marchés publics en France ?

Les marchés publics sont constamment affectés par les atteintes à la probité et ces dérives rongent le coeur même de la démocratie. Or leur importance n'est pas négligeable, plus de cent milliards d'euros pour la France et un potentiel de fraudes possibles évaluées entre 15 et 30 % d'après l'OCDE.

Dans ces montages, il est souvent fait fi des trois principes fondamentaux composant l'essence de la réglementation : la liberté, l'égalité d'accès et la transparence. Une parfaite transparence est requise dans ce domaine, or elle est sans cesse chicanée par les non-dits, par la mauvaise foi, par les faux documentaires, par les fraudes et les pratiques corruptrices qui constituent autant d'atteintes à la probité qu'aux finances. Cette partie permet au lecteur de pénétrer dans la boîte noire.

C'est une **cartographie** des dérives possibles pour chacune des phases du marché qui a été élaborée, ces dernières sont illustrées par de multiples exemples actuels mais aussi anciens qui démontrent que ce sont les mêmes typologies frauduleuses qui sont utilisées et qui s'adaptent à l'évolution technique et aux modifications réglementaires.

Chacune des phases des marchés est affectée par des types de montages particuliers parfaitement adaptés à la situation depuis des lustres. Les montages se développent donc dans les études, dans l'évaluation du besoin, dans l'évitement des appels d'offres, dans les fraudes au moment du choix du bénéficiaire, mais surtout dans l'exécution et en fin de parcours. Tout le cycle est couvert ! Les ententes et leurs tables destinées à majorer le coût des opérations en constituent le point d'orgue et de cela on ne parle guère. En fait, c'est une « génération Balkany » qui est décrite ici, elle est fort bien accompagnée par le bal des corrupteurs. Les contrôles internes sont récents et peuvent être exercés de manière peu systématique et pas encore approfondie. Le contrôle de légalité pratiqué par les services préfectoraux est limité par les moyens humains, par l'effet technicité, par l'effet volume et

par la pression du politique local. Les autres contrôles sont conçus comme des contrôles de conformité, aux textes, aux procédures, aux règles budgétaires, ils font pourtant remonter de nombreuses exactions mais elles ne peuvent souvent pas être poursuivies directement... Dans un tel dispositif, un montage savamment organisé présente de solides garanties d'impunité.

Ainsi, l'ouvrage expose les risques induits dans les études, appelés « marchés de prestations intellectuelles », ces prestations immatérielles sont particulièrement vulnérables aux fraudes de toute nature. Celui qui en maîtrise le fonctionnement peut s'en servir dans les situations requérant un besoin urgent et peu honorable de trésorerie, le champ d'action est vaste, il s'étend depuis la « pure » fausse facture émise pour « aider » un proche au téléguidage du choix d'un prestataire particulier, à des formations plus destinées à récupérer des fonds qu'à former qui que ce soit, à des expertises bidonnées, ou à des modifications des caractéristiques des besoins, la liste n'est évidemment pas close !

Les besoins peuvent aussi être manipulés, égo incommensurable, réseautage, pression des fournisseurs avec ou sans rétribution sont autant de moyens d'engager des dépenses au détriment des fonds publics. Nous ne sommes parfois pas très éloignés des célèbres éléphants blancs. S'il s'agit dans les cas précédents de manipulations plutôt intellectuelles, celles qui suivent sont plus factuelles, elles affectent l'évitement des appels d'offres et le saucissonnage, les analyses des offres, et surtout l'exécution des travaux. C'est là que se concentrent les multiples tours de mains frauduleux, largement utilisés par les fournisseurs avec ou sans la complicité des décideurs, d'autant plus que les dispositions éditées par le Code des marchés dans ce domaine ne constituent que moins de 10 % de l'ensemble des mesures réglementaires. Ce Code est fondé sur le principe de la bonne foi partagée des participants, alors que, depuis longtemps il n'est guère respecté. Les ententes sont particulièrement présentes dans tous les secteurs et en particulier dans l'immobilier et on n'y fait guère référence.

J'expose aussi l'articulation des pratiques frauduleuses auxquelles ont recours les corrupteurs pour transmettre leurs deniers aux corrompus. Un autre point est aussi identifié comme présentant des risques majeurs : les grands travaux en cours sont traités en urgence, le politique a fixé une date butoir, point n'est besoin d'être Cassandre pour penser que des dérives monstrueuses auront lieu, autant dans la gestion, déjà pressenties et dénoncées par la Cour des comptes et l'Inspection des finances car nombre de contournements de procédures ont déjà été identifiées. Au regard de l'éthique pure, même si les montants peuvent apparaître comme proportionnellement peu significatifs, il est nécessaire d'analyser les remboursements de frais engagés dans la période qui précède l'engagement des travaux. Elle est souvent propice à des dépenses notablement exagérées et parfois sans lien avec l'opération en cause. L'un des indicateurs de la présence d'un problème est le fait d'écarter et de remplacer les contrôleurs un peu trop « tatillons ».

L.R.D.G. : Quel comportement adoptent les organisations criminelles dans le monde économique ?

La criminalité organisée apparaît comme étant partie prenante au développement économique. Après avoir décrit les rouages essentiels de la criminalité financière, l'ouvrage dépeint la symbiose entre secteurs légaux et illégaux et le comportement des organisations criminelles qui s'intègrent aisément dans le monde économique du fait de leurs exceptionnelles et liquides disponibilités financières. Elles sont souvent présentes, directement ou le plus souvent indirectement dans des activités commerciales, en particulier dans le secteur touristique, dans l'immobilier, dans celui de la sous-traitance BTP, dans la gestion des ordures, dans la restauration et dans les transports entre autres sans jamais négliger les techniques nouvelles tout en développant leur business historique. Elles ont besoin d'entreprises officielles à des fins stratégiques, organisationnelles, financières pour blanchir toujours dans le dessein d'approcher au plus près le pouvoir. L'exemple du gang de la Brise de Mer le démontre, la plupart des gains était réintégré dans des entreprises « propres » et le gang disposait de relais dans les administrations. Quant au système bancaire, il facilite, certes en tordant quelques principes, le blanchiment des gains illégaux.

Les criminels disposent de fonds à foison, ils ont les moyens de se faire respecter mais sont en manque de reconnaissance. Les entreprises disposent de la reconnaissance mais peuvent manquer de trésorerie ou de moyens pour se développer. L'articulation de ces besoins constitue évidemment une opération « gagnant-gagnant » pour qui, poussé par l'obligation de majorer ses profits, ne dispose pas d'une éthique solide. De plus, de nombreux pays, on l'a vu, sont criminalisés et le modèle mondialisé facilite ces rapprochements.

L'ouvrage décrit quelques situations dans lesquelles la criminalité fait montre d'un savoir-faire tellement varié et met en évidence le fait qu'elle est bien présente chez nous comme dans tous les pays, surtout s'ils sont développés. Sont décrits ici les multiples agissements développés pour escroquer l'État dans le domaine de la TVA et dans celui des subventions octroyées, la pandémie restant un bon exemple de cette capacité, les montages savants élaborés avec les banques parallèles et les escroqueries aux entreprises.

La source de gains la plus importante de la criminalité dans le cybermonde réside dans les montages, souvent désignés comme étant « les quatre cavaliers de l'apocalypse » constitués par *les fuites de données, l'hameçonnage (phishing)*, *les agressions par rançongiciel* (*ransomware*) et *les faux ordres de virement* (FOVI/BEC). L'avènement cyber devient une source exceptionnelle de revenus. Il intègre dans les montages destinés à exécuter les attaques comme dans ceux affectés au blanchiment des sommes détournées, un remarquable système antique s'appuyant sur une sous-traitance technique et financière en cascade qui instrumentalise un système de chantage mondialisé. De plus, une sorte d'hybridation, d'intérêts bien compris entre les cybers criminels et la criminalité classique a permis de financer les contrefacteurs asiatiques et les cyber escrocs. La pandémie a, c'était prévisible, facilité cette évolution et ce type de cybercriminalité est devenue au moins pour la prochaine dizaine d'années le problème majeur de la sécurité des entreprises et des États.

L.R.D.G. : La dernière partie de votre livre est consacrée aux lanceurs d'alerte. Comme vous l'écrivez, sont-ils le dernier rempart de la démocratie ?

Les lanceurs d'alerte pourraient bien être le dernier rempart de la démocratie.

La dernière partie de l'ouvrage est dédiée à l'activité des lanceurs d'alerte. Les parties précédentes décrivent des forfaits en série. Les États, le secteur économique, tous les systèmes politiques financiers et religieux dissimulent des failles, des secrets et des dysfonctionnements inacceptables inhérents aux pouvoirs. Les manipulations, l'actualité le confirme, la fraude et la corruption sont couramment pratiquées pour s'enrichir, conquérir le pouvoir et s'y maintenir. Ceux qui sont en charge du problème ne se bousculent pas vraiment pour prévenir et sanctionner ces dérives mondialisées. Le lanceur d'alerte, trouve aisément sa place dans un tel milieu, lui qui cherche à faire reconnaître, souvent à contre-courant, l'importance d'un danger ou d'un risque en lien avec l'intérêt général. Paradoxalement les États affaiblis par les menées néolibérales sont amenés, souvent à reculons, à protéger les lanceurs d'alerte qui finalement ne révèlent que ce que les contrôles publics auraient, en bonne logique, dû mettre en évidence.

Les alertes se propagent dans tous les domaines. Hétéroclites, elles révèlent la prolifération des pratiques illégales ainsi que les systèmes de camouflage édifiés pour les protéger. Ces alertes peuvent être considérées comme des actions de « désobéissance civile » au sens où l'entend Hannah Arendt[1].

Les services répressifs nationaux courent après les fraudes systémiques professionnalisées, l'hybridation entre les montages d'habitude et les montages criminels, l'internationalisation et l'inventivité des nouvelles fraudes. Ils sont aussi affectés par l'idiotie libérale exigeant la réduction des fonctionnaires de contrôle des secteurs régaliens. Ceux qui restent, courent désespérément après les évolutions techniques et malgré leur engagement ne sont plus à même de réaliser correctement leur mission.

La société a dorénavant besoin de systèmes d'alarmes atypiques pour prévenir des situations néfastes ou scandaleuses qui se propagent insidieusement dans le domaine de la probité et des libertés individuelles. L'alerte devrait être une exception, elle se banalise ! Elle devient l'aiguillon et l'auxiliaire déterminée des services de contrôle lorsqu'ils s'en saisissent. Concomitamment, l'ouverture

sur le monde et les fuites internet facilitent l'accès à des informations jusque-là bien cachées et un besoin irrépressible de transparence se développe.

L'environnement favorable de la mondialisation, les évolutions techniques et les carences éthiques facilitent les manipulations alors que le développement du numérique permet à la fois un camouflage et une opportunité de transparence. La criminalité d'affaires s'appuie sur l'opacité structurelle juridique, comptable et géographique créant une économie de l'ombre prospérant dans les niches qui ont rendu l'arsenal juridique classique quasiment inopérant. Cette situation a été accompagnée par la perte de toute lecture éthique des situations puisque le risque est nul, seule compte la recherche du profit. Les agissements de la « criminalité en col blanc » engendrent un gisement infini de scandales à la portée des lanceurs d'alerte. Atteintes à la probité, à la libre concurrence, irrespect des textes, contournement des règles fiscales et camouflage savant des manipulations, tels sont les comportements habituels. Le « crime d'entreprise » prolifère car le risque est faible. La criminalité financière, complexe, « hyper technique » et internationale est mal identifiée et se dissimule dans l'entre-soi protecteur d'une élite. En France, les grands scandales décrits par la presse affectaient essentiellement les délits d'initiés jusqu'à ce que quelques magistrats accompagnés par l'incontournable « Canard enchaîné » aient clairement qualifié la criminalité d'affaires, « cet abîme insoupçonné » selon le mot de Maurice ROLLAND, président de la chambre criminelle de la Cour de cassation dans sa préface de l'ouvrage « Les industriels de la fraude fiscale ».

Un métier peu connu car extrêmement discret facilite le contournement des textes, fournit des « kits » de fraudes, édifie des montages sophistiqués, disperse les preuves dans divers pays, et vend des montages à la technique irréprochable mêlant le juridique et le comptable. Il organise une protection maximale pour les fraudeurs, rendant presque impossible les poursuites. L'utilisation de repentis bien au fait des opérations ou les lanceurs d'alerte permettent alors de mettre le doigt sur les montages si bien cachés.

Cet ouvrage donc, décrypte les opacités d'un système dont tous les promoteurs mettent volontiers en avant le fameux « il n'y a pas d'autre alternative » mieux connu sous l'anagramme « TINA » si chers à Thatcher, à Reagan et à tous les tenants des « réformes » dont le vicomte de Lampedusa dans « Le guépard » avait identifié l'essence : « il faut que tout change pour que rien ne change » ! Il démontre que cette mascarade est constituée par une succession de fictions : fiction de propriété, fiction d'éthique, fiction d'entreprises, fiction de nationalité, fiction de réussite économique qu'il serait aisé de réduire ! Le capital est désormais anonyme donc sans prise réelle, c'est devenu sa force. Les exemples multiples tirés de faits réels cités dans l'ouvrage suffiront à écarter l'argumentaire de ceux qui prétendraient que cette approche relève de la théorie du complot, ils devraient aussi pouvoir apporter un appui significatif à des investigateurs en manque de formation.

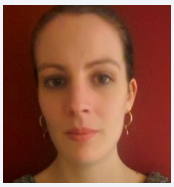
Notes :

1. « Il existe une différence essentielle entre le criminel qui prend soin de dissimuler à tous les regards ses actes répréhensibles et celui qui fait acte de désobéissance civile en défiant les autorités et s'institue lui-même porteur d'un autre droit. [...] Il lance un défi aux lois et à l'autorité établie à partir d'un désaccord fondamental, et non parce qu'il entend personnellement bénéficier d'un passe-droit ». Du mensonge à la violence, 1972.

CYBERSÉCURITÉ EN ENTREPRISE : LE RÔLE DU DPO

ALINE ALFER

AVOCATE AU BARREAU DE PARIS, MATHIAS AVOCATS



CHARLÈNE GABILLAT

DPO ADJOINTE, GROUPE SAINT-GOBAIN

AMANDINE KASHANI-POOR

DPO, AGENCE FRANÇAISE DE DÉVELOPPEMENT (AFD)

GARANCE MATHIAS

AVOCATE AU BARREAU DE PARIS ET DPO EXTERNE,
FONDATEUR DE MATHIAS AVOCATS

La fonction de délégué à la protection des données (ou data protection officer – « DPO ») est récente, puisqu'elle a été créée par le règlement général sur la protection des données (RGPD) entré en application le 25 mai 2018. Elle est devenue incontournable en raison notamment du niveau d'exigences réglementaires, de la nature des sanctions encourues, ainsi que de leurs impacts en termes d'image et de réputation. Ainsi, dans son classement des spécialités les plus recherchées en France publié en 2019, LinkedIn plaçait l'expertise de délégué à la protection des données en première place devant l'ingénieur en intelligence artificielle[1].

Le DPO a trouvé sa place à la frontière de plusieurs disciplines, que sont le juridique, la conformité et la cybersécurité. L'Agence nationale de la sécurité des systèmes d'information (ANSSI) définit cette dernière notion comme l'« [é]tat recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense[2]. » Ainsi, fait-elle partie du quotidien du DPO.

I. La cybersécurité : une composante essentielle de la gouvernance de la protection des données

La cybersécurité fait partie intégrante des principes fondamentaux de la protection des données personnelles, listés à l'article 5 du RGPD. Par ailleurs, le principe de sécurité est renforcé par l'article 32 du RGPD, qui définit une obligation d'assurer la sécurité des données libellée comme suit : « Compte tenu de l'état des connaissances, des coûts de mise en oeuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en oeuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque (...) ».

Dans ces conditions, le DPO doit s'enquérir des mesures de sécurité des données à caractère personnel mises en oeuvre au sein de l'organisme qui l'a désigné et, le cas échéant, les évaluer ou demander qu'elles le soient en fonction de la cible de sécurité, de la nature des données personnelles traitées et des risques générés par les traitements mis en oeuvre pour les

personnes concernées. Pour ce faire, il peut se référer aux bonnes pratiques en la matière, telles que relayées notamment dans la documentation de la Commission nationale de l'informatique et des libertés (CNIL)[3], de l'ANSSI[4] ou de l'Agence européenne de la cybersécurité (European Union Agency for Cybersecurity – ENISA)[5].

Le DPO trouve donc dans le domaine de la cybersécurité un allié naturel en la fonction de Responsable de la sécurité de l'information (RSSI).

II. DPO et RSSI : un pas de deux cadencé autour de la cybersécurité

Les missions respectives du DPO et du RSSI (responsable de la sécurité des systèmes d'information) sont assez proches, dès lors qu'elles consistent à conseiller, contrôler et mettre en place une documentation interne associée à leur périmètre d'action. Si ces deux fonctions renvoient à des domaines d'expertise voisins, il convient toutefois de les distinguer.

Le RSSI s'assure de la sécurité de tous types d'informations traitées dans les systèmes d'informations et s'attache ainsi à protéger tous les secrets manipulés au sein de son organisme. Le DPO se concentre sur la sécurité des données à caractère personnel, périmètre d'activité également très étendu en raison de la définition large de la notion de « données personnelles[6] ».

RSSI et DPO travaillent de concert mais ne partagent pas nécessairement la même perspective. Ainsi, le RSSI appréhende-t-il les impacts pour la personne morale au moyen de ses analyses de risques, quand le DPO s'intéresse à la protection des données des personnes concernées. Il demeure évident que ces deux fonctions sont complémentaires en matière de cybersécurité. Les actions de chacune d'elles oeuvrent à la définition, au maintien voire au renforcement du niveau de sécurité de l'organisme et, en conséquence, des données qu'il traite. En outre, ces deux acteurs enrichissent mutuellement leurs pratiques. À titre d'illustration, les constats résultant des audits réalisés en protection des données par le DPO peuvent améliorer la vision opérationnelle du RSSI, et inversement. Pour autant, si le RSSI s'intéresse uniquement à l'efficacité des mesures de sécurité, le DPO va également s'intéresser à leur proportionnalité, notamment au moyen d'une analyse de leur nécessité et des mesures alternatives existantes.

III. Le DPO au coeur de la mise en balance entre sécurité, proportionnalité et libertés

Dans la mesure où elle implique de prendre en compte les droits et libertés fondamentaux, la protection des données personnelles suppose nécessairement de mettre en balance des intérêts pouvant être divergents. Le RGPD précise ainsi que « (…) Le droit à la protection des données à caractère personnel n'est pas un droit absolu ; il doit être considéré par rapport à sa fonction dans la société et être mis en balance avec d'autres droits fondamentaux, conformément au principe de proportionnalité[7] (…). »

La cybersécurité ne fait pas exception à cet exercice de mise en balance d'enjeux opposés. Les mesures de journalisation mises en oeuvre dans les systèmes d'information en sont un exemple. Celles-ci ont pour objectif d'assurer une traçabilité des accès et des actions des utilisateurs des systèmes d'information. Cette traçabilité permet de prévenir les risques notamment en matière d'intégrité des données. Plus les enjeux de sécurité sont élevés, plus la granularité de traçabilité exigible doit être fine. Pour autant, les traces recueillies constituent des données à caractère personnel dans la mesure où elles sont associées à des utilisateurs identifiés. Le traitement de ces traces doit donc respecter les grands principes de la protection des données, dont le principe de proportionnalité.

À cet égard, le RGPD souligne que : « Le traitement de données à caractère personnel dans la mesure strictement nécessaire et proportionnée aux fins de garantir la sécurité du réseau et des informations, c'est-à-dire la capacité d'un réseau ou d'un système d'information de résister, à un niveau de confiance donné, à des événements accidentels ou à des actions illégales ou malveillantes qui compromettent la disponibilité, l'authenticité, l'intégrité et la confidentialité de données à caractère personnel conservées ou transmises, ainsi que la sécurité des services connexes offerts ou rendus accessibles via ces réseaux et systèmes, par des autorités publiques, des équipes d'intervention en cas d'urgence informatique (CERT), des équipes d'intervention en cas d'incidents de sécurité informatique (CSIRT), des fournisseurs de réseaux et de services de communications

électroniques et des fournisseurs de technologies et services de sécurité, constitue un intérêt légitime du responsable du traitement concerné. Il pourrait s'agir, par exemple, d'empêcher l'accès non autorisé à des réseaux de communications électroniques et la distribution de codes malveillants, et de faire cesser des attaques par « déni de service » et des dommages touchant les systèmes de communications informatiques et électroniques[8]. »

Ainsi, la légitimité de la sécurisation des systèmes d'information n'est nullement contestée. En revanche, la collecte de traces est susceptible de faire peser un risque de surveillance excessive des utilisateurs. C'est pour prévenir ce risque et encourager les responsables de traitements à s'en tenir à un niveau de journalisation et à une durée de conservation strictement nécessaire que la CNIL a publié un projet de recommandation relative aux mesures de journalisation, soumis à consultation publique[9]. Ce document vise à ménager un équilibre entre l'enjeu de sécurité et la préservation des droits et libertés des utilisateurs du système d'information, notamment eu égard à la surveillance systématique de ces derniers. La CNIL rappelle ainsi dans son projet « qu'il convient de veiller à limiter les risques portant sur ces catégories de personnes, en proportionnant la collecte, au sein des journaux, de données à caractère personnel relatives aux utilisateurs habilités, à la sensibilité des données à caractère personnel du traitement principal et aux risques qu'un mésusage de celui-ci ferait courir aux personnes concernées ».

Cet exercice de mise en balance et d'application du principe de proportionnalité conduit le DPO à une approche tout en nuances des mesures de sécurité à mettre en oeuvre. Le principe d'efficacité ne suffit pas à justifier une mesure. Celle-ci doit également être proportionnée et nécessaire. Cette approche s'applique à l'ensemble des actions associées à la sécurité de l'information. Ainsi, s'il est certain que l'accès aux serveurs physiques doit être très sécurisé, un contrôle d'accès biométrique ne sera pas nécessairement justifié pour un DPO. D'une part, cette modalité d'accès engendre des risques pour les personnes concernées et, d'autre part, le DPO doit s'assurer que des modalités de contrôles satisfaisants et moins invasifs ne peuvent pas être utilisées, à l'instar du contrôle d'accès par badge[10]. Cette appréciation doit bien entendu s'effectuer au regard du secteur d'activité et de la sensibilité de l'information, des locaux, applications ou appareils à protéger.

Le DPO aborde également la cybersécurité sous l'angle de la concrétisation des risques de sécurité, avec la gestion des violations de données.

IV. DPO et violations de données

La notification des violations de données généralisée à l'ensemble des acteurs est l'une des grandes innovations du RGPD. La violation de données se définit comme « une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données[11] ».

S'il n'est bien évidemment pas le seul acteur de la gestion d'une telle violation, le DPO a toute sa place et légitimité. En effet, l'article 38-1 du RGPD prévoit expressément qu'il soit associé aux questions relatives à la protection des données. L'Autorité de protection des données belge a ainsi sanctionné une entité du fait que le DPO qu'elle avait désigné n'était pas suffisamment associé à la gestion du risque relatif à une violation de données, en relevant que : « Le délégué à la protection des données du défendeur [était] uniquement informé du résultat de l'évaluation des risques. (...) la matrice RACI [indiquait que le DPO était] uniquement "informed" et non "consulted". L'article 38, paragraphe 1, du RGPD requiert toutefois que le DPO soit associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel[12]. »

Quel rôle le DPO doit-il jouer en cas de violation en définitive ?

En amont, en cas de recours à la sous-traitance au sens du RGPD, le DPO a tout intérêt à s'assurer que les contrats conclus stipulent une obligation de notification de tout incident de sécurité à la charge des cocontractants et pas uniquement des violations de données ; même si l'article 33-2 du RGPD limite la notification

due par le sous-traitant aux seules violations de données. De cette manière, le DPO permet à son entité de garder la maîtrise de la qualification des violations de données. Le DPO s'assure également, en concertation avec le RSSI, qu'une procédure et des outils robustes de détection et de gestion des incidents de sécurité susceptibles d'être qualifiés de violations de données sont mis en place, ainsi que des mesures organisationnelles (comitologie de gestion de crise, sensibilisation des acteurs de la gestion de crise, rôle et responsabilité de chacun, etc.).

En cas de violation de données, en fonction de l'organisation mise en place, le DPO procède à la qualification de l'incident en violation de données ou fait partie de l'instance qui procèdera à la qualification. Dans certaines hypothèses, le DPO peut être informé de la qualification retenue, charge à lui, le cas échéant, de la discuter et de donner son avis. Par ailleurs, le DPO s'assure que le délai de notification est respecté et, s'il ne peut pas l'être en raison des investigations à mener, il veille à ce que les motifs du retard soient précisément décrits. Dans tous les cas, il doit, en application du principe d'accountability, documenter la gestion de la violation de données ou veiller à ce qu'elle le soit s'il ne réalise pas lui-même cette action. Le DPO pourra s'appuyer sur cette documentation pour diffuser un éventuel retour d'expérience et ainsi rappeler aux collaborateurs les règles applicables au sein de l'organisme (procédure, saisine du DPO, mesures de confidentialité mises en oeuvre, traçabilité de l'origine de l'information, etc.).

La décision de notifier ou non ne revient pas au DPO mais bien au responsable de traitement, représenté en interne par une ou plusieurs fonctions de direction au sein de l'organisme. Cette décision de notifier intervient sur la base de l'analyse et des recommandations du DPO. La décision de procéder ou non à la notification peut être prise en cellule de crise si le responsable du traitement a estimé nécessaire d'en constituer une. Les critères selon lesquels une cellule de crise est activée peuvent être utilement listés dans la procédure de gestion des violations de données. Cela est par exemple le cas lorsque la violation concerne plusieurs entités ou des catégories particulières de données. Par ailleurs, le DPO doit participer à la cellule de crise. En revanche, il ne doit pas participer à la prise de décision, comme l'a rappelé l'Autorité belge de protection des données en affirmant que le DPO a un rôle de consultation à l'égard du responsable du traitement mais ne peut pas être « coresponsable de la décision finale conformément à l'article 38-1 du RGPD combiné à l'article 39-1, a) du RGPD[13] ».

Une fois cette décision prise, le DPO procède, le cas échéant, à la notification sur le site de la CNIL. Il devrait en outre être impliqué dans les démarches de communication aux personnes concernées si elles s'avèrent requises en raison des risques générés par la violation de données. À ce titre, il est recommandé que le DPO, voire le RSSI, soit préparé à ce type d'exercice.

À la suite d'une violation de données, le DPO peut décider de procéder à un audit du traitement de données impacté, ne serait-ce que pour vérifier que les mesures de remédiation ont été mises en oeuvre par la ou les directions métiers concernées, avec l'appui du RSSI et de son équipe. Il peut s'agir de mesures techniques mais également de mesures organisationnelles ou juridiques. Si la violation de données est survenue du fait d'un sous-traitant, ce peut être l'occasion pour le DPO de déclencher un audit, dans le cadre de sa mission de conseil. Le DPO pourra enfin s'interroger sur le besoin de réalisation d'une analyse d'impact relative à la protection des données éventuellement révélé par la violation de données compte tenu des risques auxquels les personnes concernées auront été exposées ou sur la mise à jour de celle qui avait été réalisée afin de prendre en compte les mesures de remédiation.

Conclusion

Face à l'inflation des menaces que nous avons pu connaître notamment dans le contexte de crise sanitaire, la cybersécurité des acteurs publics et privés devient une priorité nationale. Ainsi, la Direction générale du Trésor vient-elle de lancer une concertation au niveau national sur l'assurance du risque cyber[14]. Dans ce contexte, le rôle du DPO est primordial et essentiel au sein de l'entreprise. La CNIL souligne encore cette année, dans son plan de contrôle de 2021, la prédominance des enjeux de cybersécurité, deux des trois thèmes

de contrôle portant sur des enjeux de sécurité des données[15].

Notes :

1. Le monde informatique, « Selon Linkedin, le DPO en tête des professions IT les plus demandées », article de Véronique Arène, publié le 12 Décembre 2019.
2. ANSSI, Glossaire accessible à l'adresse URL : https://www.ssi.gouv.fr/administration/glossaire/c/
3. En particulier, les trois niveaux progressifs de sécurité des données accessibles à l'adresse URL : https://www.cnil.fr/fr/securite-des-donnees, les décisions de la Présidente de la CNIL et des délibérations de la formation restreinte de la CNIL relatives à l'obligation d'assurer la sécurité des données.
4. En particulier, le guide d'hygiène informatique accessible à l'adresse URL : https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/
5. L'ENISA propose notamment sur son site Internet des notes d'information (*cyber security info notes*) et des documents (*reports*) classés par thèmes, comme des guides pratiques (*handbooks*), études (*studies*) et lignes directrices (*guidelines*).
6. RGPD, article 4.1.
7. RGPD, Considérant 4.
8. RGPD, Considérant 49.
9. CNIL, Projet de recommandation relative à la journalisation, 29 avril 2021 accessible à l'adresse URL : https://www.cnil.fr/sites/de_fault/files/atoms/files/projet_de_recommandation_-_journalisation.pdf
10. CNIL, Délibération n°2019-001 du 10 janvier 2019 portant règlement type relatif à la mise en oeuvre de dispositifs ayant pour finalité le contrôle d'accès par authentification biométrique aux locaux, aux appareils et aux applications informatiques sur les lieux de travail.
11. RGPD, article 4.12.
12. Autorité de protection des données, Chambre contentieuse, Décision quant au fond 18/2020 du 28 avril 2020, Numéro de dossier : AH-2019-0013, p.12.
13. Autorité de protection des données, Chambre contentieuse, Décision quant au fond 18/2020 du 28 avril 2020, N° de dossier : AH-2019-0013, p.14.
14. DG Trésor, Lancement d'une concertation nationale sur l'assurance du risque cyber, accessible à l'adresse URL : https://www.tresor.economie.gouv.fr/Articles/2021/07/05/lancement-d-une-concertation-nationale-sur-l-assurance-du-risque-cyber
15. Cnil, Actions de contrôles prioritaires en 2021 accessibles à l'adresse URL : https://www.cnil.fr/fr/cybersecurite-donnees-de-sante-cookies-les-thematiques-prioritaires-de-controle-en-2021

OUVRAGES RÉCENTS

POURSUIVRE

AUTEUR : FABIENNE KLEIN-DONATI

ÉDITEUR : EQUATEURS

Résumé

« Quand on arrive en Seine-Saint-Denis pour exercer une fonction telle que la mienne, l'envie de prendre les choses en main vous saisit immédiatement. De même qu'une sorte de vertige en mesurant l'investissement nécessaire. » Procureure de la République de Seine-Saint-Denis, avec une équipe de cinquante-sept magistrats, Fabienne Klein-Donati livre un combat quotidien contre les faits de délinquance qui rongent le département. Les affaires dont son parquet a la charge nous font plonger avec effroi dans la criminalité rencontrée par d'autres villes, mais rarement de manière aussi concentrée et avec la même intensité : multiplication des agressions gratuites, violences faites aux femmes et aux enfants, rixes, trafic de stupéfiants et son cortège de nuisances, exploitation de la misère par les marchands de sommeil, délinquance des mineurs. Face à ces phénomènes, la procureure montre de façon inédite l'autorité judiciaire en action. Du plateau de permanence, où les dossiers en cours sont traités en temps réel, aux salles d'audience correctionnelle ou d'assises, des scènes de crimes aux réunions avec les partenaires publics et associatifs, elle décrit l'engagement des magistrats du parquet dans la répression, mais aussi dans la prévention des infractions. Deux enjeux fondamentaux. Poursuivre est un récit immersif, addictif, au coeur du plus important parquet de France, après celui de Paris. Un tableau vertigineux de la criminalité française.

LA RÉGULATION ET L'OFFRE ILLÉGALE DES JEUX D'ARGENT EN LIGNE DANS L'UNION EUROPÉENNE

JOHANNA JÄRVINEN-TASSOPOULOS

CHERCHEUSE SPÉCIALISÉE DANS L'ÉTUDE DES JEUX D'ARGENT À L'INSTITUT NATIONAL POUR LA SANTÉ ET LES AFFAIRES SOCIALES À HELSINKI (FINLANDE), MAÎTRE DE CONFÉRENCES EN POLITIQUE SOCIALE (UNIVERSITÉ D'HELSINKI)

L'avènement de l'Internet a permis aux États membres de l'Union européenne (UE) d'exploiter des technologies nouvelles et des connexions de plus en plus rapides dans l'opération des jeux d'argent. L'Internet leur a ouvert de nouvelles possibilités d'étendre les limites de leur marché national et de mettre à jour leurs produits et services relatifs aux jeux d'argent. Bien que la conquête de l'espace virtuel se soit faite à des périodes différentes compte tenu de la régulation de l'opération des jeux d'argent en ligne et du jeu des citoyens en ligne dans chaque État membre, le secteur des jeux d'argent virtuels est devenu une industrie lucrative en Europe ayant une valeur estimée à 24,7 milliards d'euros en 2020[1].

Actuellement, le secteur des jeux d'argent en ligne européen comprend différents types de marchés. Le marché légal se compose de modèles réglementaires de licences et de monopoles. La France, qui a adopté la loi relative à « l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne » le 12 mai 2010, a ouvert partiellement son marché national à des opérateurs de paris sportifs, de paris hippiques et de poker en ligne étrangers. La Suède, dont l'opérateur étatisé Svenska Spel a introduit le poker en ligne dès 2006, a ouvert son marché en ligne en 2019 à trois parties qui sont les opérateurs nationaux, les opérateurs étrangers agréés et le secteur des organisations non-gouvernementales. En revanche, la Finlande continue à maintenir son modèle monopolistique ayant un seul opérateur étatisé offrant des jeux d'argent hors ligne et en ligne. Le marché « gris » se compose d'opérateurs qui ont une licence dans un État membre ou sur une île à législation autonome dans l'UE, mais dont l'offre n'est pas forcément autorisée ou légale dans les États membres. Enfin, le marché « noir » désigne les opérations de jeux d'argent en ligne sur des sites illégaux qui offrent leurs produits et services aux citoyens des États membres[2].

Le problème le plus difficile au sein de l'UE est de lutter contre la criminalité relative à l'opération des jeux d'argent en ligne et l'offre illégale de ces jeux. Comme cette opération n'est pas légiférée au niveau européen, les États membres sont obligés de lutter contre le blanchiment d'argent, la fraude, la manipulation des compétitions et des paris sportifs et l'offre illégale en ligne par leurs propres moyens. Malgré la modification de la législation relative aux jeux d'argent en ligne, les États membres comme la France ou la Belgique ont vu la proportion de l'offre illégale diminuée d'une manière claire, mais sans disparaître complètement. La criminalité et l'offre illégale des jeux d'argent en ligne mettent en péril les efforts de protection des joueurs, des mineurs et des personnes vulnérables. En raison de cela, il est important d'étudier la régulation des jeux d'argent en ligne dans l'UE et d'analyser comment lutter contre les risques criminels et de l'offre illégale pour mieux protéger les différents citoyens des conséquences négatives associées aux jeux d'argent.

I. De la régulation des jeux d'argent en ligne dans l'UE

La régulation des jeux d'argent en ligne dans les États membres dépend de la législation nationale, mais elle est assujettie à l'application des articles 49 et 56 du traité sur le fonctionnement de l'UE (TFUE) relatifs à la liberté d'établissement et à la libre prestation des services[3]. Cependant, les jeux d'argent en ligne ne sont pas une forme de « commerce ordinaire » ou de « service ordinaire », car ils représentent en même temps des bénéfices économiques et des coûts sociaux[4]. Les bénéfices économiques peuvent se composer du développement économique dans le secteur des jeux d'argent, des revenus financiers aux niveaux individuel et communautaire et des recettes fiscales aux niveaux régional et national, mais les coûts sociaux sont liés à la criminalité, à l'endettement et à la faillite des joueurs et au traitement des joueurs excessifs et dépendants[5]. Chaque État membre est donc libre de fixer ses objectifs réglementaires et politiques en matière de protection des joueurs et de lutte contre la criminalité[6].

Bien que la régulation des jeux d'argent (hors ligne et en ligne) n'ait pas été harmonisée dans l'UE, il existe plusieurs circonstances qui ont poussé les États membres à reconsidérer leur modèle réglementaire monopolistique dans les années 2000. En 2006, la Commission européenne (CE) a engagé à l'encontre de plusieurs États membres (entre autres la France, le Danemark, la Suède et la Finlande) une procédure d'infraction concernant les jeux d'argent (e.g. les paris sportifs). D'abord la France (en 2010) et ensuite le Danemark (en 2012) ont abandonné leur modèle réglementaire monopolistique pour pouvoir ouvrir partiellement leur marché en ligne aux opérateurs étrangers[7]. En revanche, la libéralisation des autres marchés nordiques n'a pas été aussi rapide. La Suède a ouvert son marché en ligne aux opérateurs agréés en 2019 et la Finlande maintient toujours son modèle réglementaire monopolistique malgré la forte concurrence de la part des opérateurs illégaux[8].

En 2011, la CE a publié un Livre vert sur les jeux d'argent et de hasard dans le marché intérieur. Dans ce Livre, la CE note la croissance rapide des jeux d'argent en ligne sur le marché global et souligne que « l'essor de l'Internet et l'offre accrue de services de jeux d'argent et de hasard en ligne ont rendu plus difficile la coexistence des différents modèles de réglementation nationaux[9] ». La même année, le Parlement européen (PE) a publié sa résolution sur le même sujet : il constate que « ce secteur [des jeux d'argent en ligne] ne constitue pas un marché comme les autres en raison des risques qu'il comporte en matière de protection des consommateurs et de lutte contre la criminalité organisée », en ajoutant que ce secteur « n'est pas réglementé de manière identique dans les différents États membres et que cela permet difficilement aux opérateurs autorisés de proposer des services transfrontaliers et légaux de jeux d'argent et de hasard, mais aussi aux autorités de réglementation de protéger les consommateurs et de lutter contre les jeux d'argent et de hasard en ligne illicites et contre le risque connexe de criminalité au niveau de l'Union[10] ».

La CE a ensuite traité le cadre européen des jeux d'argent en ligne dans une communication dans laquelle elle recense les défis et les difficultés liés à la coexistence de différents modèles réglementaires nationaux au sein du marché intérieur. Ces défis et difficultés concernent surtout l'offre transnationale au sein du marché européen, la protection des consommateurs et des citoyens, la protection des mineurs, l'encouragement des pratiques publicitaires responsables, la prévention du jeu pathologique ou de l'addiction au jeu et la prévention des actes criminels (comme le blanchiment d'argent, la fraude, la cybercriminalité, la sauvegarde de l'intégrité des sports et la lutte contre le trucage des matchs[11]). Enfin, la CE a pris une décision d'exécution le 4 avril 2018 concernant les jeux d'argent en ligne. Cette décision d'exécution entame la procédure de la « normalisation européenne » faisant référence à la demande faite à la CE à rédiger une norme ou des normes européennes « sur les déclarations aux autorités de réglementation des jeux de hasard des États membres aux fins de la surveillance des services de jeux de hasard en ligne[12]».

Au sein de l'UE, les circonstances ont été propices pour la disparition des monopoles en matière des jeux d'argent en ligne. Les prises de position de la CE, les arrêts de la Cour de justice de l'UE (CJEU) et l'envahissement des marchés nationaux par une offre de jeux transnationale illégale, ont préparé le terrain pour la libération du secteur des jeux d'argent en ligne[13]. Cependant, il reste à voir ce que la CE décidera en matière de l'harmonisation des dispositions nationales dans

le futur : est-il question de la protection des consommateurs (ou des joueurs et des personnes vulnérables) et de la lutte contre la criminalité ou de la libéralisation totale du secteur des jeux d'argent en ligne[14] ?

II. La criminalité relative aux jeux d'argent et leur offre illégale sur Internet

Pour lutter contre la criminalité sur Internet, il faut d'abord reconnaître les formes qu'elle peut prendre et les parties qu'elle peut toucher. Le blanchiment des capitaux, la fraude et la manipulation des compétitions sportives (et des paris sportifs) sont des formes de criminalité qui nuisent les États membres, les opérateurs étatisés et agréés et les joueurs en ligne. L'offre illégale des jeux d'argent en ligne est un défi réglementaire dans l'UE, car elle est souvent organisée par des opérateurs en ligne installés sur des îles européennes (e.g. Malte ou les îles Åland) ou dans desdits « paradis fiscaux » en dehors l'UE[15].

A. Les différentes formes de criminalité virtuelle

Le blanchiment des capitaux est une des activités les plus caractéristiques du crime organisé[16]. La 4ème Directive anti-blanchiment et financement du terrorisme de l'UE prend en compte tous les jeux d'argent et traite de l'obligation des opérateurs du secteur des jeux d'argent d'appliquer des mesures de vigilance à l'égard de leur clientèle[17]. Le but du blanchiment est d'injecter des capitaux d'origine criminelle dans un circuit légal. Le blanchiment peut se faire en accord entre les joueurs et l'opérateur : les joueurs misent de l'argent sale sur un site qui peut être une « véritable plateforme de blanchiment[18] ». Les organisations criminelles qui se sont spécialisées dans la vente illégale des paris blanchissent aussi des capitaux[19]. Les loteries peuvent aussi être utilisées pour blanchir de l'argent sale, mais il s'agit d'un moyen coûteux et pas forcément fiable[20]. Les mesures pour lutter contre le blanchiment en ligne sont peu nombreuses : les autorités de régulation peuvent limiter l'usage des comptes bancaires ou des institutions de crédit afin de restreindre les transactions douteuses[21].

La fraude est un phénomène complexe. L'opération illégale des jeux d'argent en ligne est une forme de fraude qui touche les États membres, car les opérateurs exploitent la demande nationale sans licence et sans contribuer aux recettes fiscales[22]. Il existe aussi des sites de jeux en ligne qui sont des falsifications créées par des groupes criminels : ces faux sites peuvent ressembler à des sites authentiques, mais leur but est de recueillir des données sur les joueurs, offrir des jeux d'argent en ligne et ensuite disparaître avant de payer les gains aux joueurs[23].

Le joueur peut aussi être victime d'un vol de données personnelles, d'un détournement de données bancaires ou du piratage de son compte d'utilisateur, comme Neteller[24]. Par la méthode « phishing », les criminels s'emparent du code PIN d'une carte bancaire ou d'une carte de crédit ou même du code d'accès pour accéder à un compte bancaire[25]. Au Danemark, seulement les joueurs enregistrés peuvent jouer et parier sur Internet. Or, en ouvrant un compte de jeu personnel chez l'opérateur, les joueurs doivent donner leur code d'identité que l'opérateur peut ensuite vérifier de la base des codes d'identité nationale[26]. Cependant, le joueur peut aussi détourner des fonds et donc commettre une fraude en utilisant le compte bancaire ou la carte de crédit d'une autre personne sans sa permission[27]. Pour la plupart du temps ce type de délinquance est associée à la dépendance au jeu.

La manipulation des compétitions sportives (ou le « match-fixing ») et des paris sportifs est une forme de criminalité transnationale qui touche différentes parties, comme les gouvernements, les organisations sportives (nationales et internationales) et les opérateurs de jeux d'argent[28]. La marchandisation du sport, l'explosion du marché des paris sportifs en ligne et les facteurs sociaux et institutionnels (cf. la pression exercée sur les sportifs, les difficultés financières des clubs sportifs) sont les causes principales de ce problème transnational[29]. Les organisations criminelles, qui vendent des paris illégalement, blanchissent des capitaux et manipulent les compétitions sportives, créent des risques importants pour l'exploitation des paris sportifs[30]. En Finlande, il existe un système d'identification aux points de vente et en ligne, semblable à celui du Danemark, qui permet de lutter contre les paris illégaux et le blanchiment des capitaux[31].

Enfin, il est possible de jouer avec de la « monnaie virtuelle » qui se distingue de la « monnaie électronique ». La « monnaie virtuelle » (cf. le « bitcoin ») est utilisée sur Internet : les transactions ne peuvent

se rattacher à aucune zone géographique déterminée et les flux de monnaies ne sont pas détectables par un organe de régulation. La « monnaie virtuelle » permet des transactions anonymes sans plafond et sans identification entre particuliers ou par l'intermédiaire des services spécialisés. Les transactions peuvent aussi se faire dans des réseaux clandestins en ligne[32]. L'usage de la « monnaie virtuelle » pour payer la participation aux jeux d'argent en ligne est déjà permis en Espagne et en Estonie[33].

B. Lutter contre l'offre illégale des jeux d'argent en ligne

Une des raisons principales qui ont poussé plusieurs États membres à modifier leur législation relative à l'opération des jeux d'argent en ligne est la concurrence de la part des opérateurs non agréés. En 2005, il a été estimé que l'activité illégale en ligne représentait entre 300 et 400 millions d'euros annuels de Produit Brut de Jeux (PBJ) en France où l'activité légale ne représentait que 110 millions d'euros[34]. La proportion du jeu des Français sur les sites illégaux a ensuite diminué de 75% en 2008 à 10% en 2013[35]. Pour que cette diminution ait eu lieu, il a fallu créer une infrastructure nouvelle pour lutter efficacement contre l'offre illégale et des mesures pour empêcher les joueurs de naviguer sur les sites illégaux.

La France et la Belgique possèdent un système de régulation fort en matière d'opération des jeux d'argent en ligne. Bien que la législation belge ne distingue pas les jeux d'argent hors ligne des jeux en ligne comme fait la législation française de 2010, les deux États membres ont créé des autorités pour lutter contre l'offre illégale en ligne : l'Autorité de Régulation des Jeux en Ligne (ARJEL) en France et la Commission des Jeux de Hasard (CJH) en Belgique. L'Autorité nationale des jeux (ANJ), qui a remplacé l'ARJEL depuis octobre 2019, et la CJH possèdent pourtant des moyens différents pour lutter. Un an après l'entrée en vigueur de la loi du 12 mai 2010, plus de 70 sites illégaux ont été dénoncés par l'ARJEL au procureur de la République de Paris. Aussi, certains opérateurs auparavant illégaux ont adopté la légalité et certains autres se sont retirés du marché français[36]. La CJH belge peut rendre public le nom de domaine des sites illégaux, mais la diffusion de ces listes n'est pas prévue par la législation française. Pourtant la publication des « listes noires » a permis de diriger des joueurs belges vers le marché légal en ligne[37].

La Finlande est en train de modifier sa législation relative aux jeux d'argent pour répondre, entre autres, au défi de l'offre illégale en ligne. Comme en Belgique, la législation finlandaise ne différencie pas les jeux d'argent hors ligne et en ligne. Depuis plusieurs années, le moyen principal de lutte contre cette offre a été la canalisation, c'est-à-dire le fait de diriger la demande finlandaise vers le site légal national tout en protégeant les joueurs des opérateurs illégaux qui n'offrent pas de dispositifs « responsables[38] ». Canaliser la demande n'est pas facile dans un environnement tel que l'Internet, car les opérateurs concurrents ont les moyens d'attirer les joueurs finlandais vers leurs sites en leur offrant des taux de redistribution intéressants, des bonus et des jeux gratuits. Il est donc difficile à un opérateur étatisé (et ayant le monopole de tous les jeux d'argent) de lutter contre l'offre illégale sans renouveler l'offre de ses produits et services en ligne en la rendant plus attractive ou sans développer son marketing[39].

À part la canalisation, le blocage des sites en ligne peut restreindre l'offre illégale des jeux d'argent en ligne. En France, un décret précise les modalités de blocage des sites illégaux. Le moyen de restreindre l'accès aux sites illégaux est d'exiger un blocage par les fournisseurs d'accès à Internet (FAI)[40]. Le blocage des transactions financières entre les opérateurs illégaux et les joueurs est aussi un moyen de lutte contre l'offre illégale. Les États membres peuvent légiférer sur le blocage et obliger les banques à refuser ces transactions. Cependant, l'efficacité de ce blocage peut être atténuée par l'usage des monnaies virtuelles[41].

Les opérateurs illégaux et non agréés persistent à répondre à la demande des joueurs en ligne. Les mesures de blocage ne sont pas utilisées dans les États membres d'une manière identique et l'idée de la canalisation semble peu encourageante dans la lutte contre l'offre illégale. Malgré les prohibitions nationales, les opérateurs illégaux et non agréés ont trouvé des moyens de faire la publicité dans certains États membres. L'Internet, les chaînes de télévision câblées établies à l'étranger, les fréquences de radio et surtout les réseaux sociaux (cf. Facebook, YouTube, Instagram, Twitter) sont utilisés par les

opérateurs pour promouvoir leurs produits et services en ligne[42]. En outre, le rôle des « influenceurs » des réseaux sociaux est important, car les jeunes générations les suivent[43].

III. La protection des joueurs, des mineurs et des personnes vulnérables des conséquences négatives associées aux jeux d'argent en ligne

La protection des consommateurs (ou des joueurs, des mineurs et des personnes vulnérables) est primordiale dans les documents de la CE, mais compte tenu de la nature technologique de l'Internet (sans localité et sans temporalité unique), du manque de législation harmonisée au niveau européen et de l'ubiquité de la publicité en ligne, il est difficile de trouver des moyens efficaces de protection. Les mineurs sont les premiers à être protéger par les législations nationales. Les personnes vulnérables (comme les personnes âgées ou celles ayant des problèmes de santé mentale) doivent aussi être protégées de l'offre de jeux en ligne et de la publicité tendancieuse. La protection des joueurs, des mineurs et des personnes vulnérables des dommages liés aux jeux d'argent en ligne les abrite aussi de l'exclusion sociale et de la précarité économique.

Les risques en ligne sont nombreux pour les joueurs. Tout d'abord, il est possible que tous les joueurs ne sachent pas qu'ils jouent sur des sites considérés comme illégaux. Cela peut arriver quand l'opérateur est de même nationalité que les joueurs (cf. l'affaire Partouche en France)[44], l'adresse IP de l'opérateur semble légal et l'opérateur communique en langue maternelle des joueurs[45]. Pour se faire connaître par les joueurs de différentes nationalités, les opérateurs non agréés et illégaux peuvent utiliser des sites de promotion (ou de sites « aspirateurs »)[46] qui font la publicité de leurs jeux et services en ligne tout en promettant aux joueurs que la participation est légale ou encore des célébrités qui sont employés pour parler des jeux d'argent en ligne à leurs abonnés sur les réseaux sociaux[47].

Les États membres et les opérateurs en ligne ont des moyens de prévention des risques liés au jeu excessif et à la dépendance au jeu. La prohibition du jeu des mineurs (cf. l'identification et l'enregistrement obligatoires des joueurs et le contrôle d'âge), la limitation du jeu en ligne et l'interdiction de la participation aux jeux d'argent en ligne sont des moyens de protection des joueurs, des mineurs et des personnes vulnérables que les États membres peuvent inclure dans leur législation relative aux jeux d'argent en ligne[48]. Les opérateurs peuvent, à leur tour, proposer aux joueurs des outils de jeu responsable comme la possibilité de s'exclure pour une période limitée, des limites de mises et de pertes, un programme d'évaluation du comportement du joueur (tel Playscan qui est un outil de contrôle des mises développé par la Française des jeux), des tests d'auto-évaluation ou encore une limitation de la publicité provenant de l'opérateur[49]. En France, les opérateurs agréés doivent avoir des mesures de protection à offrir aux joueurs. La Suède exige des opérateurs agréés qu'ils avertissent activement les joueurs quand leur comportement devient risqué et qu'ils les informent de l'aide apportée aux joueurs excessifs (une « obligation de soin »)[50].

La responsabilité de la protection des joueurs, des mineurs et des personnes vulnérables appartient aux États membres et aux opérateurs étatisés et agréés. Les joueurs doivent être informés et avertis des risques liés au jeu excessif et à la dépendance au jeu en ligne et les outils de jeu responsable proposés doivent être efficaces et obligatoires. La responsabilité des États membres ne s'arrête donc pas à la lutte contre l'offre illégale, car cette lutte peut cacher un objectif financier comme celui de percevoir des impôts ou de financer des « bonnes causes »[51]. D'autre part, les opérateurs étatisés ne peuvent pas se déclarer plus responsables que les opérateurs agréés ou même illégaux, puisqu'ils n'offrent pas des jeux d'argent à haut risque ou ne cherchent pas à maximiser leur profit[52]. Les États membres et les opérateurs agréés doivent prendre activement la responsabilité de l'opération des jeux d'argent en ligne en créant un contexte de jeu où tous les joueurs se sentent protégés.

Conclusion

Les États membres ont choisi des parcours différents dans la régulation des jeux d'argent en ligne. Le secteur des jeux d'argent en ligne est particulièrement difficile à réguler, car un grand nombre d'opérateurs s'y trouvent sans qu'ils respectent les législations nationales ou les avis de la CE et sans qu'ils prennent en compte les questions d'éthique ou de responsabilité. D'autre part, jouer en ligne peut être un défi pour les joueurs qui

ne sont pas forcément au courant de la différence entre l'offre légale et illégale. Il existe des loteries transnationales, comme l'EuroMillions (organisé dans 12 pays européens) ou le Vikinglotto (organisé dans les pays nordiques et baltes, en Slovénie et en Belgique), auxquelles les citoyens de plusieurs États membres ont droit de participer[53]. En outre, l'offre illégale peut se faire en plusieurs langues et même les services d'aide proposés aux joueurs excessifs sur les sites illégaux peuvent sembler familiers et authentiques[54].

Bien qu'il existe plusieurs moyens de lutter contre la criminalité et l'offre illégale des jeux d'argent en ligne, ils ne sont pas les mêmes dans tous les États membres de l'UE. Les moyens de lutte utilisés dans les États membres sont le blocage des sites illégaux, le blocage des transactions financières, la régulation de la publicité et l'usage des sanctions contre les opérateurs, les joueurs et les intermédiaires[55]. Pour savoir si ces moyens sont efficaces et protègent les joueurs, les mineurs et les personnes vulnérables, les États membres devraient, entre autres, organiser des enquêtes de prévalence sur la pratique des jeux d'argent (en ligne) et sur les dommages liés au jeu excessif et à la dépendance au jeu, commissionner des études sur la criminalité, sur l'offre illégale et sur le jeu en ligne et exiger des opérateurs nationaux et agréés qu'ils aient des mesures de jeu responsable et un plan éthique. En outre, les États membres devraient suivre de manière constante le développement technologique des jeux en général (e.g. les « loot-boxes »), le marketing de l'offre illégale (cf. surtout sur les réseaux sociaux et les applications des opérateurs), l'évolution de la cybercriminalité et l'usage des monnaies virtuelles[56].

Notes :

1. Hojnik J. (2018), "Online Gambling under EU Law : Strolling Between Controlled Expansion and Genuine Diminution of Gambling Opportunities", Lexonomica, 10, pp. 67-102.
2. Commission européenne (2011), Livre vert sur les jeux d'argent et de hasard en ligne dans le marché intérieur, SEC(2011 321 final, Bruxelles, le 24 mars 2011, p. 3.
3. Kalb C. (2018), « Réguler les paris sportifs modernes : quel équilibre entre demande, attractivité de l'offre et maîtrise des risques ? », in J-B. Vila (dir.) Régulation et jeux d'argent et de hasard, Issy-les-Moulineaux, LGDJ/Lextenso éditions, pp. 197-212.
4. Monteils J-F. (2018), « Introduction aux réflexions sur la notion de la régulation », in J-B. Vila (dir.) Régulation et jeux d'argent et de hasard, Issy-les-Moulineaux, LGDJ/ Lextenso éditions, pp. 17-19 ; Hojnik, ibid., pp. 70-71.
5. Hojnik, ibid., pp. 70-71.
6. Escande M. (2013), Droit des jeux d'argent et de hasard. Les mutations de l'ordre public, Paris, L'Harmattan, p. 384.
7. Escande, 2013; Kristiansen S. & Trabjerg, C.M. (2017), « Legal gambling availability and youth gambling behaviour: A qualitative longitudinal study », International Journal of Social Welfare, 26, pp. 218-229.
8. Cisneros Örnberg J. & Hettne, J. (2018), « The Future Swedish Gambling Market : Challenges in Law and Public Policies », in M. Egerer, V. Marionneau & J. Nikkinen (dir.) Gambling Policies in European Welfare States, Cham, Palgrave Macmillan, pp. 197-216; Littler A. & Järvinen-Tassopoulos J. (2018), « Online Gambling, Regulation, and Risks: A Comparison of Gambling Policies in Finland and the Netherlands », Journal of Law and Social Policy, 30, pp. 100-126.
9. Commission européenne, ibid., p. 3.
10. Parlement européen (2011), « Résolution du Parlement européen du 15 novembre 2011 sur les jeux d'argent et de hasard en ligne dans le marché intérieur (2011/2084(INI)) », Journal officiel de l'Union européenne, C 153 E, pp. 36-37.
11. Commission européenne (2012), Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions. Vers un cadre européen global pour les jeux de hasard en ligne, SWD(2012) 345 final, Strasbourg, le 23 octobre 2012.
12. Commission européenne (2018), Décision d'exécution de la Commission relative à une normalisation adressée au Comité européen de normalisation en ce qui concerne l'élaboration d'une norme européenne en matière de déclaration à l'appui de la surveillance des services de jeux de hasard par les autorités de réglementation des jeux de hasard dans des États membres, C(2018) 1815 final, Bruxelles, le 4 avril 2018, p. 4.
13. Van Baeveghem P. (2018), « Régulation et économie des jeux – Le cas particulier de la Belgique », in J-B. Vila (dir.) Régulation et jeux d'argent et de hasard, Issy-les-Moulineaux, LGDJ/Lextenso éditions, pp.119-124 ; Malgorn, B. (2018), « Pour une régulation nationale globale et indépendante », in J-B. Vila (dir.) Régulation et jeux d'argent et de hasard, Issy-les-Moulineaux, LGDJ/Lextenso éditions, pp. 241-246.
14. Van Baeveghem, ibid., p. 121.
15. Trespeuch M. (2013), « L'île de la tentation. Malte ou la construction d'un cyber-district des jeux d'argent », Réseaux ,180, pp. 123-156 ; Spapens T. (2008), « Crime Problem Related to Gambling: An Overview », in T. Spapens, A. Littler & C. Fijnaut (dir.) Crime, Addiction and the Regulation of Gambling, Leiden et Boston, Martinus Nijhoff Publishers, pp. 19-54; Lerkkanen T. & Hellman M. (2021), « Resilience and autonomy at stake: The public construct of the Paf gambling company in the Åland Islands community », Journal of Island Studies, pp. 1-22.
16. Delrue G. (2014), « L'état des lieux de la lutte contre la cybercriminalité en rapport avec la lutte contre le blanchiment des capitaux. L'argent criminel voyageant sur la Toile », in M. Trannois & B. Vincendeau (dir.) La réglementation des jeux d'argent en ligne en Europe. État des lieux et perspectives, Collection Laboratoire d'études juridiques et politiques, Université Cergy-Pontoise, p. 75.
17. Tracfin (2015), « Les principales innovations de la 4e Directive anti-blanchiment et financement du terrorisme en 12 points », La Lettre d'information de Tracfin, numéro spécial, octobre 2015.
18. Degermann V. & Alezra J-P. (2011), « Le droit pénal du jeu », Pouvoirs, 139, p. 113.
19. Kalb, ibid., p. 209.
20. Spapens, ibid., p. 45.
21. Spapens, ibid., p. 33.
22. cf. Albanese J.S. (2018), « Illegal gambling businesses & organized crime: an analysis of federal convictions », Trends in Organized Crime, 21, p. 262.
23. Banks, J. (2012), « Edging your bets : Advantage play, gambling, crime and victimisation », Crime Media Culture, 9, p. 178.
24. Hoekx N. (2014), « Les spécificités du droit des jeux d'argent en ligne en Europe », in M. Trannois & B. Vincendeau (dir.) La réglementation des jeux d'argent en ligne en Europe. État des lieux et perspectives, Collection Laboratoire d'études juridiques et politiques, Université Cergy-Pontoise, p. 17 ; Bauer A. (2009), Jeux en ligne et menaces criminelles, Paris, La Documentation Française, pp. 14, 36.
25. Delrue, ibid., p. 76.
26. Littler A. (2013), « Ensuring Internet Gaming that is Free from Fraud and Cheating », in A. Cabot & N. Pindell (dir.) Regulating Internet Gaming. Challenges and Opportunities, Las Vegas, UNLV Gaming Press, pp. 310-311.
27. Järvinen-Tassopoulos J. (2016), « Problem gambling and drinking among Finnish women », Nordic Studies in Alcohol and Drugs, 33, pp. 27-42.
28. Robert-Cuendet S. & Prezas M.I. (2014), « La convention du Conseil de l'Europe sur la manipulation de compétitions sportives : prélude à un régime global de lutte contre un nouveau fléau des relations transnationales », Annuaire français de droit international, 60, pp. 707-730 ; Littler, ibid.
29. Robert-Cuendet & Prezas, ibid., pp. 709-710.

30. Kalb, ibid., p. 209.
31. Kalb, ibid., p. 211.
32. Delrue, ibid., pp. 76-77.
33. Hömle J., Littler A., Tyson G., Padumadasa E., Schmidt M-J. & Ibosiola D.I. (2018), Evaluation of Regulatory Tools for Enforcing Online Gambling Rules and Channeling Demand towards Controlled Offers. Final Report, Bruxelles, Commission européenne, p. 78.
34. Bauer, ibid., p.10.
35. Marionneau V. & Järvinen-Tassopoulos J. (2017), « Consumer protection in licensed online gambling markets in France: the role of responsible gambling tools », Addiction Research & Theory, 25, p. 441.
36. Degermann & Alezra, ibid., pp. 114-115.
37. Marique É. (2013), « Défis de la régulation belge des jeux d'argent sur Internet », in M. Trannois & B. Vincendeau (dir.) La réglementation des jeux d'argent en ligne en Europe. État des lieux et perspectives, Collection Laboratoire d'études juridiques et politiques, Université Cergy-Pontoise, pp. 90.
38. Papineau É. & Leblond J. (2011), « Les enjeux de l'étatisation du jeu en ligne au Canada : une analyse de santé publique », Revue canadienne de santé publique, 102, p. 418.
39. Marique É. (2010), « Limites de la notion de jeu responsable à travers l'expérience du dispositif de régulation belge et son analyse juridique », in C. Dunand, M. Rihs-Middel & O. Simon (dir.) Prévenir le jeu excessif. D'une approche bio-psycho-sociale à la définition d'une politique de santé publique, Genève, Éditions Médecine & Hygiène,p. 262.
40. Escande, ibid., p. 319.
41. Hörnle et al., ibid., p. 55.
42. Rydman E. & Tukia J. (2019), Rahapelilainsäädäntöä koskeva esiselvitys [Étude préliminaire de la législation relative aux jeux d'argent], Helsinki, Sisäministeriö (Ministère de l'Intérieur).
43. Hörnle et al., ibid., p. 156.
44. Le droit français ne permet aucune extension virtuelle de l'activité des casinos « physiques » établis en France. Le groupe Partouche a été sanctionné par le TGI de Nanterre (le 15 mars 2007) et la Cour d'appel de Versailles (le 4 mars 2009) pour avoir rendu accessible un site de jeux en ligne depuis l'île de Bélize (Escande, ibid., pp. 315-316).
45. Escande, ibid., pp. 316, 409-410 ; Nadeau L., Dufour M., Guay R., Kairouz S., Ménard J.M. & Paradis C. (2014), Le jeu en ligne. Quand la réalité du virtuel nous rattrape, Montréal (Québec), Groupe de travail sur le jeu en ligne, p. 36 ; Järvinen-Tassopoulos J. (2020), « Les espaces de jeux d'argent : une analyse sociologique de la production de l'espace, du risque et de la prévention du jeu problématique », Sciences du jeu, 13.
46. Bauer, ibid., p. 9.
47. Järvinen-Tassopoulos J. & Marionneau V. (2021), « Licensed vs. unlicensed online gambling : What features make foreign-based gaming sites attractive to customers ? », manuscrit.
48. Hoekx, ibid., pp. 29-32.
49. Marionneau & Järvinen-Tassopoulos, ibid., p. 437.
50. Marionneau & Järvinen-Tassopoulos, ibid.; Forsström, D. & Cisneros Örnberg J. (2018), « Responsible gambling in practice: A case study of views and practices of Swedish oriented gambling companies », Nordic Studies on Alcohol and Drugs, p. 3.
51. Marique (2013), p. 93.
52. Forsström & Cisneros Örnberg, ibid., p. 14.
53. Järvinen-Tassopoulos J. (2010), « Les jeux d'argent : un nouvel enjeu social ? », Pensée plurielle, 23, pp. 65-76.
54. Järvinen-Tassopoulos (2020); Banks, ibid.
55. Hörnle et al., ibid.
56. Vila J-B. (2021), « Jeux d'argent et régulation : les risques et les droit », La revue du Grasco, 33, pp. 23-31 ; Hörnle et al., ibid. ; Delrue, ibid.

OUVRAGES RÉCENTS

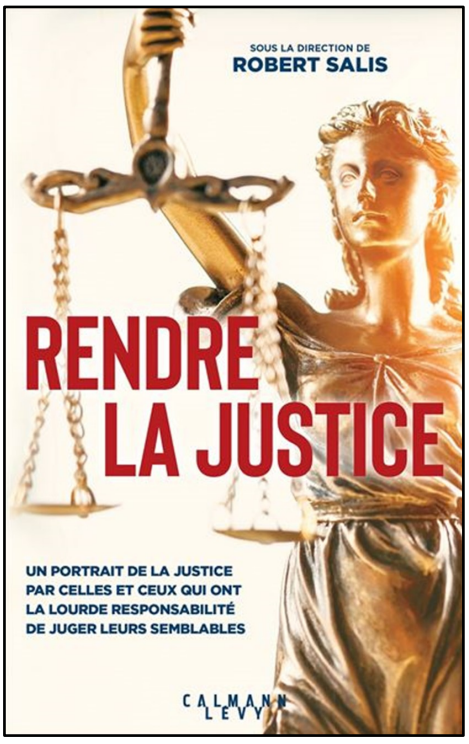
RENDRE LA JUSTICE

SOUS LA DIRECTION DE : ROBERT SALIS

ÉDITEUR : CALMANN LEVY

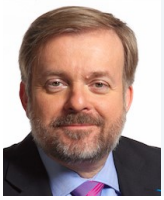
Résumé

Soixante-cinq des plus grands noms de la magistrature, parmi lesquels François Molins, procureur général près la Cour de cassation, ou Jean-Michel Hayat, premier président de la cour d'appel de Paris, mais aussi des juges des enfants, des avocats généraux, des procureurs, des membres du Conseil constitutionnel, du Conseil d'État, du Conseil supérieur de la magistrature, qui officient aussi bien dans des tribunaux de commerce que dans l'antiterrorisme, à Paris en province et en outre-mer, prennent la parole et nous disent ce qu'est rendre la Justice au quotidien... Comment ? Avec quels moyens ?



Chacune de leurs voix se propose de comprendre un pan des rouages de la machinerie judiciaire et de saisir toute la difficulté d'un métier où l'impartialité, l'intégrité, la recherche perpétuelle de ce qui est juste, font loi. Mais nos gardiens de la justice restent des hommes, faillibles parfois, sensibles – car l'humain n'est jamais loin, et s'il peut être la source de cas de conscience cornéliens, il est aussi ce qui permet d'apporter un peu de lumière dans une profession labyrinthique.

DROITS ET INTELLIGENCE ARTIFICIELLE : UN CODE INFORMATIQUE PEUT-IL SE SUBSTITUER AUX CODES JURIDIQUES ?



NICOLAS LERÈGLE,

AVOCAT AU BARREAU DE PARIS, AUDITEUR DE L'INHES (19ÈME SESSION),
CONFÉRENCIER EN SÉCURITÉ ÉCONOMIQUE LABÉLISÉ EUCLÈS

L'intrusion de l'Intelligence Artificielle dans notre monde, nous n'en sommes qu'au début, commence à questionner quant au degré d'autonomie qui doit être laissée aux objets qui en sont dotés. Ces objets, civils ou à usage militaire, ont vocation à interagir avec des humains les questions de responsabilité, de gestion des conséquences de leurs actions. Le rôle des programmateurs et autres tendent à avoir comme plus petit dénominateur commun le droit et ses notions complémentaires que sont l'éthique et la morale. Et s'il a fallu plusieurs centaines d'années pour que les animaux se voient reconnaître des droits, on peut penser que cela sera nettement plus rapide pour les androïdes que nous serons amenés à côtoyer dans un futur (très) proche. Sommes-nous à l'aube d'un temps où le droit ne serait plus rédigé par des législateurs mais par des informaticiens, voire des machines artificiellement intelligentes ?

Cette question amène à se demander si l'Intelligence Artificielle est une intelligence, comment le droit est rédigé et s'applique, s'il faut à l'Intelligence Artificielle un droit spécifique, si l'Intelligence Artificielle peut être créatrice de droit, si les notions de morale et d'éthique peuvent s'appliquer à des androïdes. Enfin, nous regarderons ce qui se fait dans le domaine militaire qui est, dans ce domaine, à la pointe, peut-être un peu trop, des applications concrètes.

I. Quel droit pour l'Intelligence Artificielle ?

A. L'Intelligence Artificielle est-elle une intelligence ?

Il convient de ne pas faire de l'Intelligence Artificielle une intelligence équivalente à celle des hommes. Et comparaison ne vaut pas raison. À ce stade elle n'est encore que le produit d'une programmation et d'une volonté humaines et part d'un postulat différent. Là où l'intelligence humaine repose sur un organe vivant, le cerveau, et met en jeu la clairvoyance, l'imagination et l'analyse élargie des champs du possible, l'Intelligence Artificielle se fonde sur un programme informatique permettant l'enregistrement de données, une analyse de correspondances avec une situation et la sélection optimisée d'une solution. Si à deux énoncés la solution peut être identique cela ne présage pas que, parfois, il y aura des différences.

L'Intelligence Artificielle est, aujourd'hui encore, le fait d'une intelligence humaine. Ce qui compte plus que l'intelligence ce sont donc les intentions de celui qui produit une norme et, si Rousseau pensait l'homme comme naturellement bon et Hobbes en faisait un loup pour l'Homme, dans tous les cas c'est le droit et la crainte qu'inspire son application ou le non-respect de celle-ci qui permet de réguler nos penchants et caractères.

L'intelligence peut-elle être artificielle ? Qu'un ordinateur puisse battre Kasparov aux échecs témoigne surtout d'une capacité de mémorisation de parties et de calcul des combinaisons plus que d'une réflexion stratégique pouvant induire une dose d'irrationalité pour déstabiliser son adversaire.

En effet, les qualités émotionnelles et d'adaptation qui sont le

propre de l'intelligence humaine ne sont pas, a priori, encore présentes dans ce que l'on nomme communément Intelligence Artificielle.

Maintenant les progrès de cette dernière, en attendant les évolutions qui seront rendues possibles par les ordinateurs quantiques, sont tels qu'elle tend à se rapprocher de l'intelligence humaine et donc à se poser de vraies questions quant à sa capacité, par son autonomie, à créer des usages, des obligations, des sanctions et donc du droit. Essayons de toujours avoir à l'esprit que les ordinateurs, les androïdes et l'Intelligence Artificielle sont des créations humaines et non l'inverse.

B. Le droit humain est artificiel

Si nous nous rappelons que l'être humain est un mammifère et donc un animal comme les autres, les règles de droit ont, depuis l'origine une fonction artificielle, à savoir encadrer des comportements naturels qui pourraient nuire à la vie en société et permettre à cette dernière de se pérenniser.

Donc, dès l'origine, le droit a été et est encore artificiel au sens où il vise à canaliser des penchants naturels dont l'expression n'est pas compatible avec une vie communautaire équilibrée dite civilisée. Le droit est donc une construction humaine, fruit d'une réflexion sur l'état de la société et ce dans toutes ses composantes, allant du rapport au divin à la préservation des espèces ou de la nature en passant par le politique, la liberté ou la sécurité.

Il évolue au gré des époques et des mentalités et donc de facto de l'acceptation qu'une société ou un pouvoir peut avoir d'un équilibre entre les libertés individuelles et collectives et leur expression plus ou moins autorisée. Mais cette évolution est aussi le fruit d'influences généralement liées au développement des connaissances, des techniques, des moeurs qui amène, périodiquement, à reconsidérer la formulation du droit et de son application.

Il est donc tout à fait envisageable de penser que le développement d'androïdes disposant d'une grande autonomie de fonctionnement pourrait amener, à terme, à la création d'un droit dédié spécifique. Dans un premier temps, il serait lié aux droits et obligations qui s'appliquent aux propriétaires d'objets meubles mais qui pourrait évoluer au gré de l'autonomie laissée à ces androïdes.

C. Quel droit créer pour des systèmes gérés par l'Intelligence Artificielle ?

La question du droit applicable se pose dès lors qu'une idée devient une réalité tangible. Ce droit existe-t-il déjà ou doit-on envisager sa création, son évolution, son application ? Cela implique la définition d'une morale qui permet de distinguer ce qui est et ce qui doit ou devrait être, puis d'une éthique, à savoir une distinction entre ce qui est bon et juste et ce qui ne l'est pas. Viennent simplement ensuite le droit qui définit le permis et l'interdit et la déontologie qui assure une conformité avec les règles d'éthique définies.

Ce droit doit être le garant moral de la pertinence de ce qui est proposée comme place de l'Homme dans la société et son rapport à la société et au pouvoir en place.

La dimension démocratique, dans l'acceptation occidentale que nous vivons, ne doit jamais être perdue de vue. Car le droit a aussi sa place pour corriger les éventuels manquements d'usage qui ne manqueront pas de se produire du fait d'un recours massif à une technologie qui ne sera pas toujours humainement contrôlée. Or, ce contrôle est nécessaire ; on estime, depuis 1965, a une cinquantaine les occurrences où un conflit nucléaire aurait pu se déclencher du fait d'une mauvaise information technique ou interprétation informatique et, seul le facteur humain a empêché d'appuyer sur le bouton rouge.

La problématique de l'Intelligence Artificielle c'est que l'humain tend à s'éclipser et qu'il n'y a plus d'interrupteur sur lequel il peut ou non appuyer, c'est une machine qui s'en charge.

i. Le droit peut-il être le fait d'une Intelligence Artificielle ?

Posé de la sorte le propos amène une succession de questions quant à l'artificialité du droit, son rapport à l'Intelligence Artificielle et le rapport de cette dernière avec le droit et la place de l'Homme. Questions dont les réponses, pour autant qu'elles puissent être données, seront des marqueurs de la relation, dans un rapport risque/attrait, entre cette Intelligence Artificielle et les préoccupations de nos sociétés en termes de liberté/sécurité-sûreté.

En somme, Objets artificiels, avez-vous donc une âme et cette âme vous donne-t-elle la force de protéger nos libertés ?

Si aujourd'hui la réponse peut sembler être encore négative, elle mérite d'être nuancée et surtout d'anticiper ce que sera demain. Nous sommes dans un syllogisme digne d'Anouilh dans son Antigone : si le droit est

intelligent et que l'intelligence peut être artificielle, alors le droit peut être artificiel. C'est tout autant imparable que discutable.

Pour l'essentiel de la population mondiale le droit n'est pas d'origine humaine mais d'inspiration divine. Le décalogue apporté par Moïse depuis la montagne est gravé par Dieu ; la Mishna est le recueil des règles de droit issues de la Torah ; les principes de Bouddha ; le Coran qui pose le respect de la Charia. Quant aux catholiques, le Nouveau testament a défini des règles morales qui ont irrigué notre droit, romain, depuis le règne de Constantin. Donc divin, humain, naturel aussi quand mère Nature impose ses règles à nos usages, le droit peut donc être aussi, demain, artificiel au sens informatique ou algorithmique du terme.

Le droit sert à organiser, autant que possible, une vie harmonieuse en société en substituant par exemple à la loi du Talion des normes et des règles en accord avec la vision de la civilité des sociétés successives. Un droit issu d'une Intelligence Artificielle, sur le principe, n'aurait pas vocation, en théorisant que les concepteurs du programme informatique idoine adoptent cette vision, à être en contradiction avec cet objectif.

ii. L'application informatisée du droit fait déjà appel à l'Intelligence Artificiel

La norme de droit est avant tout un exercice d'observation, de réflexion, de solutions, d'écriture et d'adoption en vue de son application. Il en est de même d'un programme informatique avec lequel la différence est faible puisque c'est seulement au stade de son application pratique que l'on pourra avaliser la pertinence de la solution proposée avec les observations initiales.

Hier, Dieu donnait la Loi, aujourd'hui les législateurs la votent, demain les informaticiens pourraient la programmer. Cette évolution peut surprendre ou choquer mais le droit est à l'image de notre société. Dans une société théocratique le droit émane du divin et du religieux, dans une société civile des législateurs – qui ne sont pas des juristes mais des politiques –, dans une société informatisée à outrance, le droit pourrait être inspiré par des usagers, élaboré par des informaticiens, avalisé par des législateurs et mis en oeuvre au travers d'installations autonomes.

Le saut technique n'est d'ailleurs pas énorme, certains cabinets d'avocats dotés des outils informatiques idoines telles des technologies de type *blockchain* sont en mesure d'analyser, pour un cas soumis, toutes les décisions rendues par les juridictions concernées et de produire une probabilité de succès ou d'échec quant à l'application de la norme de droit au cas proposé. Remonter à rebours le mécanisme pourrait permettre d'analyser les décisions, de les coupler avec la volonté du législateur ou les raisonnements des magistrats et proposer de nouvelles rédactions des règles en vue de les rendre plus « efficaces ». L'essence du droit ne serait plus alors un raisonnement fruit d'expériences mais le traitement informatique d'expériences et de probabilités.

D'ailleurs nous sommes déjà dans une ère où l'application du droit, au-delà du calcul de probabilités, relève d'ores et déjà de systèmes informatiques autonomes. La question n'est pas morale à savoir celle du bien ou du mal mais plutôt de savoir si nous sommes dans une application contradictoire, automatique ou autonome de la norme. Ces deux derniers adjectifs sont les plus adaptés à un droit « artificiel ». Nous en avons déjà un exemple avec les radars autoroutiers qui flashent, vérifient et expédient les PV sans intervention humaine. Les systèmes type bracelets de surveillance ou d'anti-rapprochement fonctionnent de la même façon et leurs alertes déclenchent une réponse automatique sous la forme d'un appel aux forces de police concernées. Ils existent bien évidemment des voies de recours mais elles sont souvent plus dissuasives qu'intuitives, c'est la conséquence d'une croyance absolue dans l'infaillibilité de la technologie en place.

iii. De l'application du droit à la création d'un droit « artificiel », la frontière est mince

Il n'y pas de raison que certaines de nos sociétés n'empruntent pas la voie d'un droit artificiellement créé, de sa création à son application.

Insistons, le droit est le marqueur de notre société ou de ce que nous voulons qu'elle soit. Des différences existent. Dans certaines parties du Monde le droit n'a pas évolué depuis des siècles car la force théologique prime sur le progrès technologique ou scientifique. Ce n'est pas un jugement de valeur mais un constat. Mais si pour des raisons techniques, budgétaires, d'efficacité voire de neutralité on souhaite un droit artificialisé car considéré comme moins subjectif ou sujet à interprétation, les outils existent pour cela.

La Chine est un bel exemple de pays *Big Brother* qui doit regarder

avec condescendance notre règlement général sur la protection des données (RGPD). Les outils mis en place par le gouvernement permettent de savoir combien de feuilles de papier toilette vous utilisez, les programmes télévisés que vous regardez ou les sites Internet consultés, où vous êtes, avec qui et pour combien de temps. Autant dire que créer un algorithme qui croiserait les informations pour définir des interdictions n'est pas très compliqué et les sanctions en conséquence seraient automatiques du fait de cette prééminence technologique, les Ouïghours sont idéalement placés pour savoir que cela existe et fonctionne.

Tant dans le domaine civil que militaire le barycentre entre l'envie d'encadrer, la création d'un droit et l'application de celui-ci est l'éthique, plus que la morale, conditionnant l'Intelligence Artificielle et que l'on souhaite voir présente et suivie.

Prenons l'exemple des voitures autonomes, qui est certainement une excellente application de l'Intelligence Artificielle au plus grand nombre et qui peut être appréhendée au travers d'un prisme éthique car un « droit artificiel », pour être accepté, doit d'abord être en phase avec l'éthique de la société. Dans le cas de la voiture, en cas de souci, qui doit être sauvé, le conducteur ou les piétons qui sont sur son chemin ? Certains constructeurs expliquent que le conducteur étant leur client et payant cher sa voiture, sa sécurité est la priorité absolue, d'autres ont une position plus ambigüe, peut-on froidement expliquer à son client que sa vie sera sacrifiée au profit d'autres de lui inconnus ? Le prix de la voiture n'est pas étranger à ces prises de position.

Nous savons déjà que des ordinateurs peuvent appliquer des normes de droit dès lors qu'ils ont été programmés pour cela, mais de la création à l'application il y a un monde.

C'est clairement l'enjeu des décennies futures. Des machines peuvent-elles développer des normes de droit sans que leur concepteur/fabricant/utilisateur en soit informé ou impliqué ?

Sur le papier rien n'interdit une telle évolution. Il existe aujourd'hui des programmes informatiques qui donnent aux ordinateurs une capacité créative qui leur permet d'écrire des romans, de peindre, de corriger des photos ou des textes alors pourquoi pas d'édicter des règles de droit.

On peut toujours se rassurer en se disant que si cette tendance devenait réelle et potentiellement dangereuse il suffirait de débrancher les équipements pour y mettre un terme.

On peut aussi s'inquiéter en se rappelant qu'il est parfois difficile de trouver l'interrupteur et la personne qui sait l'utiliser, en cas de tensions pouvant avoir des incidences militaires par exemple. Celles-ci ont leur propre logique et les moyens utilisés ne sont pas toujours proportionnés à une menace réelle mais plutôt à une menace perçue. Dans ce domaine, le recours à l'Intelligence Artificielle pourrait être compris comme un moyen de compléter l'intelligence humaine ou de pallier aux défaillances de celle-ci. Mais de quel droit agir de la sorte ?

II. Les usages militaires de l'Intelligence Artificielle

A. Les armes connectées et les armes autonomes

La question du rôle de l'Intelligence Artificielle dans notre rapport au duo sûreté/sécurité ne relève pas que de la science-fiction même si cette dernière est très porteuse de réflexion en la matière. Progressivement, l'ordinateur doué de sa raison comme HAL dans « 2001 Odyssée de l'espace » cède la place à des entités artificielles de plus en plus humaines, y compris dans leur intelligence, sur le modèle des Replicants de Blade Runner. Or le roman d'Arthur Clarke date de 1968 la même année que celui de Philip K Dick « *les androïdes rêvent-ils de moutons électriques ?* » dont a été tiré le film de R. Scott.

En somme, il y a plus de 50 ans deux auteurs ont anticipé des révolutions technologiques que nous sommes en train de vivre actuellement. Dans le domaine militaire, qui préfigure généralement ce qui se mettra en place dans le civil, l'explosion présentielle des drones de combat volants, marins, terrestres et sous-marins, commandés, comme des jeux vidéo, depuis des bases éloignées n'est pas sans rappeler la thématique de « la stratégie Ender » ouvrage de Orson Scott Card écrit en deux temps entre 1977 et 1985. À partir des années 60, l'ordinateur et ses dérivés sont entrés de plain-pied dans ce type d'ouvrages au point de susciter l'intérêt de la NASA ou de la DARPA (Defense Advanced Research Projects Agency) aux États-Unis, du CEA (Commissariat à l'énergie atomique et aux énergies alternatives), de l'Armée ou du CNES (Centre national d'études spatiales) en France qui recrutent des auteurs de ce genre pour analyser et se confronter à la faisabilité de leurs idées.

L'anticipation d'hier tend à devenir notre présent ce qui amène à se poser la question de la place du droit – humain croyons-nous

– pour encadrer des outils dotés d'une intelligence – artificielle créons-nous – disposant de leur propre autonomie d'action.

En France, nous sommes certainement à l'aube d'une révolution dans le domaine militaire. Elle n'est pas mineure, même si présentée avec un luxe de précautions pour en atténuer la portée, car elle va faire cohabiter, dans un futur très proche, hommes et robots dans les mêmes combats.

Selon le comité d'éthique de la défense qui, en décembre 2020, avait approuvé le principe du « soldat augmenté », celui-ci s'est prononcé fin avril 2021 en faveur des systèmes d'armes létaux intégrant de l'autonomie (SALIA). On ne doit pas minorer l'importance de ce « I » qui distingue une arme autonome mais commandée et activée par l'homme du « robot tueur » qui agit de sa propre autonomie sur la base de son programme. Il ne faut pas cependant y voir une opposition éternelle dans la mesure où la France se doit de disposer d'une armée qui ne soit pas sous-équipée par rapport à de potentiels ennemis.

Toute la difficulté, typiquement française, car d'autres pays ne s'embarrassent pas de tels prévenances, est donc de faire accepter une première étape (SALIA) en attendant la seconde, à terme, d'armes complétement autonomes (SALA).

Passer du soldat augmenté, c'est-à-dire doté de technologies ou de médicaments le rendant plus performant, ce qui se fait depuis l'aube des temps, aux robots tueurs n'est pas sans conséquence sur notre rapport à la guerre et à son déroulé. Au siècle dernier, avec les drones, se posait la question de leurs pilotes qui, au début, confondaient quelque peu le maniement de leurs armes et un jeu vidéo. Si on s'affranchit de l'humain dans la gestion opérationnelle du combat on se placera dans une opposition hommes/machines poussée à l'extrême qui ne sera pas sans effet sur notre rapport à l'ennemi.

B. L'usage des armes autonomes et la question de la responsabilité juridique

Toute déshumanisation du combat est source de dérives, dès lors que se battre et neutraliser un ennemi se fait de façon désaffecté ou désincarné. Il y a dans ce constat un paradoxe effrayant.

Mener une guerre sans se doter des moyens de son ennemi c'est assurément la perdre (exemple récent du conflit dans le Haut-Karabakh), la faire avec les mêmes armes ne signifie pas pour autant gagner (Iran/Irak), disposer d'un armement supérieur c'est une chance de victoire (Hiroshima) en acceptant de franchir un cap dans les pertes infligées.

Il y a là une comptabilité morbide qui rappelle que le vainqueur a toujours raison !

Dans cette question de multiples angles de réflexion vont se développer.

Éthique, déontologie, philosophie, droit, économie et tant d'autres qui vont nous interpeller sur cette évolution inévitable convient-il de souligner.

Sans trop s'avancer, ce qui a été possible avec le nucléaire et les traités de non-prolifération ne sera certainement pas de mise pour des armes qui ne sont pas, à ce stade, vues comme de destruction massive.

Aux robots tueurs ou plutôt militaires on peut penser que les lois de la robotique d'Asimov ne seront assurément pas programmées, elles seraient un contresens.

Bien au contraire leur but sera de neutraliser un ennemi humain et paradoxalement de laisser à des humains informaticiens le soin de neutraliser, de leur côté, les robots militaires informatisés du camp opposé. Révolution copernicienne de l'art de la guerre qui ne se voudra plus seulement asymétrique dans les équipements mais aussi dans les "duels".

Il y aura, peut-être, dans le futur des évolutions des "lois de la guerre" pour encadrer l'usage de tels équipements et leurs conséquences en évitant de penser qu'ils puissent franchir la frontière entre autonomie et indépendance. Mais les progrès sont extrêmement rapides en la matière, ils sont assurément plus véloces que la rédaction de la règle de droit.

Ne nous trompons pas, il ne s'agit pas, bien au contraire, d'armes « du pauvre » que ces robots militaires. On peut même penser qu'ils vont faire l'objet d'une compétition de même nature que celle qui a prévalu dans les années 80 avec la « guerre des étoiles » initiée par R.Reagan. Et que le gagnant marquera notre monde de son empreinte tant militaire que diplomatique mais aussi technologique et économique.

Malheur au vaincu aujourd'hui (ou demain) comme hier en somme.

Bien entendu la question du droit et donc de son rapport à l'Intelligence Artificielle embarquée et agissante constitue un filigrane intéressant de ces nouvelles

armes.

À la différence des SALIA, rester dans la logique de la responsabilité d'un individu ne semble pas applicable à des robots totalement autonomes. Assumer que chaque conflit, qui ferait intervenir de façon massive ces types d'armes au risque de dommages collatéraux importants, doit déboucher sur un tribunal de Nuremberg ou un tribunal pénal international (TPI) ne semble pas non plus une option viable.

Si nous sommes dans une approche d'armes intégrant de l'autonomie, les règles actuelles de droit ont vocation à s'appliquer puisqu'il y a l'assurance d'avoir un humain derrière la console qui commande le robot.

Si nous évoquons les armes totalement autonomes, la responsabilité ne peut pas être celle de l'opérationnel mais devra être recherchée au niveau hiérarchique supérieur soit à celui du politique qui, théoriquement, engage un conflit et autorise l'usage de tel ou tel équipement. Et ce dernier devra donc en accepter les responsabilités, ce qui peut être une forte barrière à leur usage inconsidéré.

Maintenant le choix n'existe pas vraiment de mettre en place SALA ou SALIA, c'est juste une question de temps et de moyens et non de volonté car ces armes sont conventionnelles et ont vocation à être utilisées sur un théâtre d'opération classique. On peut espérer qu'à défaut d'avoir une âme ces objets animés auront un programme fondé sur une Intelligence Artificielle intégrant des règles, *a minima*, d'éthique.

On peut craindre que cela soit un voeu pieux car il apparaît selon un rapport de l'ONU de mars 2021 (mentionné dans un article de Courrier International du 02/06/2021) que des « *drones auraient attaqué des humains de leur propre initiative* » et ce, en Libye. Il s'agit de drones turcs fonctionnant « *de façon autonome dotés d'une intelligence artificielle qui repère et identifie les cibles* ».

Bienvenue dans le meilleur des mondes !

En conclusion, aujourd'hui nous sommes dans l'interaction entre deux mondes celui d'avant où le droit et son application relèvent de l'intelligence humaine et celui de demain où le droit comme son application peuvent relever d'une intelligence artificielle, considérant cependant qu'un informaticien n'est pas un législateur. Ce qui est valable pour un véhicule civil l'est autant pour un système d'arme ou des robots humanoïdes qui pourraient développer une conscience propre de leur existence, de leur rapport à notre monde et de la volonté d'y trouver une place qui ne soit pas nécessairement celle à laquelle nous souhaiterions les cantonner.

Aujourd'hui ces deux mondes cohabitent. Celui que nous fréquentons quotidiennement guidé par nos habitudes, nos réflexes et nos erreurs, en somme un libre arbitre, et celui fondé sur une rationalité algorithmique qui laisse moins, pour ne pas dire pas de place, au libre arbitre. Les forces en présence ne sont pas équilibrées et ce depuis longtemps.

L'histoire est là pour nous montrer que la cohabitation entre ces deux mondes n'a jamais été douce et pacifique. La technique bénéficie d'un avantage indéniable sur le raisonnement logique, elle ne s'embarrasse pas de sentiments et méconnaît les cas de conscience.

C'est tout l'enjeu d'un droit « artificiel », en acceptant cette terminologie ; la dose d'humanité qui lui sera instillée par son concepteur.

Soit il est conçu en vue d'une société pour laquelle l'humain, et sa liberté d'être, ne sont que des sujets à encadrer et à réprimer dès qu'ils sortent du cadre fixé. Dans ce cas nous sommes dans le *1984* d'Orwell et l'artificialisation du droit sera une manière de disposer d'un outil autonome de contrôle des populations et de prévenir toute velléité de changer les choses.

Soit il est conçu par et pour des sociétés démocratiques, pour lesquelles l'humain et sa liberté sont des principes fondamentaux essentiels à respecter pour que, justement, puissent s'exprimer toutes les différences d'être et de penser. Dans ce cas, l'artificialisation du droit doit être pensée comme répondant à des critères éthiques qui peuvent amener justement à limiter cette évolution de peur d'en perdre le contrôle.

Dans quel monde serons-nous demain ? Être ou ne pas être dans un meilleur des mondes guidé par la croyance aveugle dans la technologie telle est la question à laquelle nous aurons à répondre.