LA REVUE DU
GRASCO

www.grasco.eu
www.larevuedugrasco.eu

N°45 — Août 2025

Parution trimestrielle
Gratuite
ISSN 2272-981X

ÉDITORIAL

CHANTAL CUTAJAR

DIRECTRICE LA RDG, DIRECTRICE DU GRASCO
UMR DRES 7354

Le 13 juin 2025, la loi n° 2025-532 « visant à sortir la France du piège du narcotrafic » a été promulguée dans un climat d'urgence politique et sociale, nourri par les violences meurtrières liées aux trafics de stupéfiants. Si les commentaires se sont majoritairement concentrés sur les aspects répressifs du texte, son Titre II, consacré à la lutte contre le blanchiment, constitue un tournant structurel dans l'outillage juridique de l'État.

En rupture avec les paradigmes traditionnels de l'action pénale, cette partie de la loi repose sur une méthode de prévention et de désorganisation financière des économies criminelles. Elle traduit une ambition claire : tarir les flux financiers du narcotrafic, qu'ils circulent dans l'économie visible ou par les canaux numériques de la finance opaque.

À l'économie du narcotrafic, une économie sous contrôle. Une innovation majeure réside dans le renforcement des pouvoirs de fermeture administrative. Désormais, le représentant de l'État peut ordonner la fermeture de tout commerce ou établissement ouvert au public lorsqu'il facilite la commission de délits graves, notamment de blanchiment. En cas de fermeture maximale (six mois), les autorisations commerciales sont automatiquement abrogées. Le ministre de l'Intérieur peut prolonger la mesure. Cette faculté de sanction administrative évite les lenteurs de la justice pénale mais pose une question d'équilibre entre efficacité et garanties fondamentales. Le Conseil constitutionnel, dans sa décision n° 2025-885 DC du 12 juin 2025 (Cons. const., déc. n° 2025-885 DC, JO, 13 juin 2025, texte n° 58), a validé ce dispositif, tout en émettant des réserves d'interprétation garantissant le respect de la liberté d'entreprendre et de la proportionnalité des atteintes. Il a censuré d'autres dispositions du texte, notamment en matière d'accès aux données personnelles ou de traitements algorithmiques non encadrés, rappelant que l'État de droit ne peut être un dommage collatéral de la sécurité.

Au-delà des fermetures, la loi élargit la liste des professionnels soumis aux obligations de LCB-FT : promoteurs immobiliers, marchands de biens, vendeurs ou loueurs de véhicules ou d'aéronefs, clubs de football. Ces acteurs doivent suivre une formation obligatoire sur leurs obligations. Le paiement en

SOMMAIRE

espèces est interdit pour la location de véhicules, et les greffes peuvent radier d'office les sociétés qui ne déclarent pas leurs bénéficiaires effectifs (art. L. 561 -47 et L. 561-47-1 CMF).

Crypto-actifs : l'anonymat comme indice de culpabilité. L'article 7 de la loi prévoit une présomption de dissimulation frauduleuse dès lors qu'une opération est réalisée via un crypto-actif comportant une fonction d'anonymisation (Monero, Zcash, Tumblers). Le texte assimile ainsi l'anonymat technologique à une intention blanchisseuse, ce qui inverse la charge de la preuve pénal. Cette disposition n'a pas été censurée par le Conseil constitutionnel.

En outre, certains professionnels (mentionnés à l'article L. 561-2 du CMF) ne peuvent plus proposer de services permettant l'anonymisation ou l'opacification des transactions (art. L. 561-14-1 A CMF). La loi renforce ainsi la traçabilité numérique, dans une logique alignée sur les réglementations internationales (règlement MiCA, recommandations du GAFI).

Gel, saisie, radiation : le droit administratif comme bras armé. Le gel administratif des avoirs, possible sur simple décision conjointe des ministres de l'Intérieur et de l'Économie (art. L. 562-2-2 CMF), s'étend jusqu'à 48 mois (6 mois renouvelables 7 fois), à l'égard de toute personne ou entité liée au trafic de stupéfiants, sans condamnation judiciaire préalable. Les agents des douanes peuvent saisir, sur autorisation du procureur puis validation par un juge, les comptes bancaires ou actifs numériques dès le stade de l'enquête (art. 323-12 C. douanes).

En outre, le pouvoir est donné au greffier du registre du commerce de radier d'office les sociétés qui ne respectent pas les obligations de transparence sur les bénéficiaires effectifs. Le texte donne ainsi une arme de désorganisation rapide des structures de blanchiment, au prix d'un recours judiciaire qui n'est pas toujours suspensif.

La tentation d'une « république du soupçon » ? Dans sa volonté d'assécher les flux financiers du narcotrafic, le législateur bascule vers une prévention extrêmement proactive, quitte à remettre en cause certains standards juridiques. Ainsi, les atteintes portées aux droits de la défense, à la présomption d'innocence et à la liberté d'entreprendre sont réelles. Le droit de la transparence risque de se transformer en droit à la surveillance généralisée, si les contrepoids ne sont pas consolidés.

La décision du Conseil constitutionnel joue ici un rôle de régulateur, validant l'essentiel tout en censurant certaines surenchères normatives. Elle appelle implicitement à une vigilance renouvelée des juridictions administratives et judiciaires dans l'application de ces dispositions. La simplification des voies de recours, la publicité des motivations administratives, et la protection du contradictoire sont des exigences minimales si l'on veut éviter un basculement de la justice vers l'exception permanente.

Pour une stratégie durable du démantèlement financier. Ce Titre II opère un changement de paradigme profond. L'État ne se contente plus de sanctionner le blanchiment : il cherche à le préempter par le droit administratif, la contrainte financière et la transparence forcée. Cette stratégie peut produire des résultats, à condition de respecter l'équilibre des droits fondamentaux. La guerre contre l'argent sale ne doit pas devenir une guerre contre les garanties de l'État de droit. La vigilance conjointe de la doctrine de la jurisprudence et de l'administration est la condition de sa légitimité.

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 : Emilie EHRENGARTH

Rédacteur adjoint—Conception : Sébastien DUPENT

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 ».

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 dont il est le référent éthique et intégrité scientifique et le président du Comité d'éthique de la recherche. Membre du Haut Conseil de la Magistrature de la Principauté de Monaco et Directeur scientifique de l'Institut monégasque de formation aux professions judiciaires. Il est juge ad hoc à la Cour européenne des droits de l'homme.

STORCK Michel

Professeur émérite à l'Université de Strasbourg.

Inscription à la revue du GRASCO

Par mail : abonnement@larevuedugrasco.eu

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

Par mail : information@grasco.eu

1 après validation de la rédaction

INTERVIEW

MADAME LISE CHIPAULT CHEFFE DE LA DÉLÉGATION FRANÇAISE AU GROUPE D'ÉTATS CONTRE LA CORRUPTION (GRECO) DU CONSEIL DE L'EUROPE.

PROPOS RECUEILLIS PAR EHRENGARTH ÉMILIE RÉDACTRICE EN CHEF DE LA REVUE DU GRASCO

Née en 1985, titulaire d'un diplôme de master « carrières juridiques et judiciaires » de l'Institut d'Etudes Politiques de Paris obtenu à l'issue d'un cursus de premier cycle franco-allemand, Lise Chipault a obtenu le concours de l'Ecole Nationale de la Magistrature en 2008. Magistrate de l'ordre judiciaire depuis 2011, elle a occupé successivement des fonctions de substitute du procureur près le tribunal judiciaire d'Evreux, de juge aux affaires familiales au tribunal judiciaire de Meaux puis de substitute à l'administration centrale du ministère de la Justice, d'abord au bureau du droit de l'Union européenne et de l'entraide civile à la direction des affaires et du sceau puis au bureau de l'entraide pénale internationale à la direction des affaires criminelles et des grâces. Elle a également exercé les fonctions de secrétaire générale adjointe au Conseil supérieur de la Magistrature.

Actuellement en détachement à la direction des affaires juridiques du ministère de l'Europe et des affaires étrangères, elle est cheffe de la délégation française au Groupe d'Etats contre la corruption (GRECO) du Conseil de l'Europe.

Elle effectue régulièrement des missions d'expertise dans le cadre de projets de coopération pilotés par Expertise France dans les domaines de la lutte contre la corruption, de la promotion de l'Etat de droit et de la réforme des systèmes judiciaires, notamment en Ukraine, en Bosnie-Herzégovine, et en Macédoine du Nord et en Moldavie

L.R.D.G. : Chère Madame Chipault, pourriez-vous présenter la direction des affaires juridiques du ministère de l'Europe et des affaires étrangères ? Quelle est son organisation et quelles sont ses principales activités ?

La direction des affaires juridiques du MEAE est chargée par décret de la représentation de l'État devant toutes les juridictions internationales, y compris européennes et arbitrales, et de conseiller le ministre de l'Europe et des affaires étrangères, ainsi que l'ensemble du gouvernement, en droit international et européen. Elle représente notamment la France devant la Cour internationale de justice, la Cour européenne des droits de l'homme ou encore la Cour de justice de l'Union européenne.

Elle compte 58 agents aux expériences et profils très variés (diplomates, contractuels universitaires ou avocats, magistrats de l'ordre judiciaire et de l'ordre administratif en détachement).

Elle est composée de quatre sous-directions (sous-direction des droits de l'homme, sous-direction du droit de l'Union européenne et du droit international économique, sous-direction du droit de la mer, du droit fluvial et des pôles, sous-direction du droit international public) ainsi que d'une mission accords et traités.

Elle compte également deux chargées de mission magistrates de l'ordre judiciaire, placées sous l'autorité du directeur des affaires juridiques et travaillant en étroite collaboration avec la directrice adjointe. L'une est compétente pour traiter des questions de justice pénale internationale. L'autre (moi) a des attributions

transversales centrées autour de la coopération judiciaire en matière civile et pénale.

L.R.D.G. : Quelle est votre principale mission au sein de la direction des affaires juridiques ? En quoi consiste-t-elle exactement ?

J'ai pris mes fonctions à la direction des affaires juridiques des affaires étrangères le 1er octobre 2023.

Ma principale attribution est d'être cheffe de la délégation française au Groupe d'Etats contre la corruption (GRECO) du Conseil de l'Europe. Dans ce cadre, j'assure l'élaboration de la stratégie de défense de la situation française dans le cadre des procédures d'évaluation et de suivi concernant la France, en lien avec l'ensemble des ministères et autorités nationales concernées (principalement, le ministère de la Justice, le ministère de l'Intérieur, la Haute Autorité pour la transparence de la vie publique et l'Agence française anticorruption). Par ailleurs, je participe aux procédures d'évaluation et de suivi des autres Etats membres.

J'assiste à toutes les réunions plénières du GRECO, lesquelles se déroulent trois fois par an à Strasbourg.

Au mois de novembre 2024, le bureau du GRECO a été intégralement renouvelé. La France a été élue pour y siéger, de sorte que depuis le 1er janvier de cette année, je siège également au bureau du GRECO. Le bureau a notamment pour mission de préparer l'ordre du jour des réunions du GRECO, de formuler des propositions à l'attention du GRECO concernant l'avant-projet de budget et la composition des équipes d'évaluation, d'organiser les visites dans les pays, sur la base des décisions prises par le GRECO ou encore de représenter le GRECO au niveau institutionnel.

L'élaboration de la position française au GRECO s'effectue bien-sûr en cohérence avec la position soutenue par la France dans d'autres enceintes internationales s'intéressant à la lutte contre la corruption (OCDE, ONUDC, OSCE, G20, Union européenne). Je participe donc à de nombreux travaux au sein ou en lien avec ces enceintes. J'ai notamment composé la délégation française à la 10eme Conférence des États parties à la Convention des Nations-Unies contre la corruption du 9 décembre 2003 (dite Convention de Mérida) qui s'est déroulée à Atlanta (États-Unis) du 9 au 16 décembre 2023 et ai ainsi pris une part active à la négociation de plusieurs résolutions. J'espère pouvoir faire partie de la délégation qui se rendra à Doha (Qatar) en décembre prochain pour la 11eme Conférence des Etats-parties, l'expérience à Atlanta s'étant avérée extrêmement enrichissante.

L.R.D.G. : Quels sont les travaux actuellement en cours au GRECO concernant la France ?

Fin 2023 s'est achevé pour la France le quatrième cycle d'évaluation, relatif à la prévention et la lutte contre la corruption ainsi qu'à la promotion de l'intégrité des parlementaires ainsi que des juges et des procureurs.

Le cinquième cycle d'évaluation, relatif à la prévention et la lutte contre la corruption ainsi que la promotion de l'intégrité des personnes exerçant de hautes fonctions exécutives et des forces répressives, lancé en 2019 pour la France, est toujours en cours.

Pour l'heure, le niveau de conformité atteint est encore relativement faible.

Le prochain rapport de conformité de la France sera examiné à la réunion plénière de novembre 2025. Cet examen constituera une occasion pour la France de faire valoir les avancées réalisées depuis la publication du dernier rapport le 10 avril 2024. Je ne peux pas dévoiler le contenu de nos observations que nous allons transmettre au GRECO début juillet mais nous avons d'ores et déjà effectué un certain nombre de progrès.

Nous nous situons à un moment particulièrement intéressant dans la réflexion autour de la corruption au sein des forces répressives notamment. En effet, les débats autour de la loi visant à sortir la France du piège du narcotrafic, promulguée le 14 juin 2025, ont fait ressortir le lien entre ce phénomène caché qu'est la corruption et la criminalité organisée. J'espère que certaines des mesures adoptées auront des effets tant sur la prise de conscience de l'existence d'un phénomène corruptif au sein de l'administration (pour l'heure non systémique mais bel et bien présent) que sur le renforcement de notre dispositif de prévention et de lutte contre la corruption.

Par ailleurs, comme vous le savez, le GRECO a lancé cette année un sixième cycle d'évaluation relatif à la prévention de la corruption et la promotion de l'intégrité au sein des entités infra-nationales. Il s'agit d'une thématique assez peu explorée jusqu'alors, alors même que le phénomène corruptif est au moins aussi intense au niveau local qu'au niveau national. Les défis de méthodologie sont de taille pour le GRECO, notamment compte tenu de la disparité administrative entre les États membres du GRECO, certains, comme la France, étant très centralisés et

d'autres d'organisation fédérale ou confédérale. La France ne sera pas évaluée en 2025 et ne figure pas sur la liste des États qui seront évalués en 2026 mais nous nous préparons d'ores et déjà à l'organisation de ce cycle inédit et nous l'attendons avec grand intérêt.

L.R.D.G. : Outre les questions de lutte contre la corruption, quelles sont vos autres attributions ?

Comme indiqué précédemment, j'ai en réalité des missions très transversales.

Au mois de mars 2023, le ministère de l'Europe et des Affaires étrangères et le ministère de la Justice ont lancé une stratégie conjointe d'influence par le droit.

J'assure, au sein du ministère, le suivi de la mise en oeuvre de cette stratégie, conjointement avec mes collègues de la mission de la gouvernance démocratique. Nous coordonnons notamment chaque année le dispositif de la Journée du droit dans le réseau diplomatique, inspiré de celui de la Nuit du droit instauré par le Conseil Constitutionnel.

Par ailleurs, je copilote, avec la cheffe du bureau du droit comparé de la délégation des affaires européennes et internationales du ministère de la Justice, le groupe de travail diffusion des conceptions juridiques français, qui réunit plusieurs directions du ministère de la Justice, le Conseil Constitutionnel, la Cour de cassation, le Conseil d'Etat, la cour d'appel de Paris (chambre de commerce internationale), plusieurs fondations et universitaires, plusieurs éditeurs juridiques ainsi que des représentants des professions juridiques (avocats, notaires…). Les travaux de ce groupe de travail, qui se réunit plusieurs fois par an, sont principalement axés sur les outils de diffusion ainsi que sur les enjeux liés à la traduction des sources juridiques françaises. A ce jour, la principale réalisation de ce groupe de travail est la conclusion, au mois d'août 2024, d'une convention de partenariat entre le ministère de l'Europe et des affaires étrangères (direction des affaires juridiques), le ministère de la Justice (délégation aux affaires européennes et internationales) et l'Institut de management et de communication interculturels (ISIT) qui forme notamment des juristes-linguistes. Dans le cadre de ce partenariat, nous avons confié à un groupe d'étudiantes de l'ISIT pour l'année universitaire 2024-2025 la traduction en langue anglais et en langue espagnole d'une fiche-pays élaborée par le ministère de la Justice (décrivant l'ensemble des institutions françaises et les principales caractéristiques de notre organisation judiciaire) ainsi que la constitution de glossaires juridiques dans ces deux langues. Ces travaux auront ensuite vocation à alimenter une plateforme collaborative, à disposition des institutions actrices de la stratégie d'influence par le droit.

Travailler sur la stratégie d'influence par le droit m'a fait prendre conscience de l'intérêt de la communication institutionnelle, de sorte que quelques mois après mon arrivée, j'ai créé la page LinkedIn de la direction des affaires juridiques (intitulée « direction des affaires juridiques du MEAE »). Elle compte désormais presque 18 000 abonnés. Nous y relayons des informations sur nos activités, sur certaines jurisprudences, certains colloques ainsi que nos offres de stages, de postes de contractuels ou d'apprentissages. Je profite également de cet espace pour faire connaître le GRECO au plus grand nombre et pour partager des contenus en lien avec la lutte contre la corruption lorsque le contexte s'y prête.

En parallèle, je suis sollicitée pour avis ou expertise sur des sujets relevant de la coopération judiciaire internationale en matière civile et en matière pénale. Je relis notamment toutes les conventions d'entraide aux fins d'enquête, d'extradition ou de transfèrement de personnes condamnées détenues conclues par la France à l'international.

Il s'agit de missions très variées et passionnantes qui exigent toutefois une grande capacité d'adaptation. Les journées se suivent mais ne se ressemblent jamais.

L.R.D.G. : Vous effectuez des missions de coopération à l'étranger en matière de prévention et de lutte contre la corruption. Pourriez-vous nous en dire un peu plus ?

J'interviens en effet en qualité d'experte dans le cadre de projets de coopération pilotés par Expertise France i est l'agence publique française de conception et de mise en oeuvre de projets internationaux de coopération technique (pas uniquement dans le domaine juridique mais également dans de très nombreux autres secteurs comme la santé, les transports…). J'ai commencé en 2022 par participer au projet EU4Justice en Bosnie-Herzégovine en effectuant plusieurs missions d'appui au Conseil de justice de Bosnie-Herzégovine, en charge de la nomination, de la discipline et de la déontologie des juges et des procureurs. Je me suis déplacée plusieurs fois à Sarajevo pour participer à des conférences ou des formations sur des thématiques comme l'entretien professionnel de recrutement des juges et des procureurs ou encore sur le conseil confidentiel en matière

d'éthique (qui correspond d'ailleurs à une des recommandations traditionnellement formulées par le GRECO dans le cadre du 4eme cycle d'évaluation)

Depuis le début de cette année, j'interviens également en qualité d'experte dans le cadre du projet Pravo Justice en Ukraine. Je me suis d'ailleurs déplacée à Kyiv en janvier dernier pour intervenir à l'occasion de la formation des nouveaux inspecteurs disciplinaires au Conseil de justice ukrainien.

Enfin, je me suis engagée dans des action menées dans le cadre du Fonds de lutte contre la corruption d'Expertise France, auprès du Conseil de justice de Macédoine du Nord et normalement bientôt auprès de l'Agence Nationale d'intégrité de Moldavie (ANI).

Ce que j'apprécie particulièrement dans ces missions, c'est qu'elles constituent un peu entre mes fonctions actuelles au GRECO et mon expérience antérieure de secrétaire générale adjointe au Conseil supérieur de la magistrature.

J'en ressors à chaque fois riche d'expériences, de bonnes pratiques mais aussi de rencontres avec des personnes résolument engagées dans la lutte contre la corruption dans leurs pays respectifs.

Chère Madame Chipault , un grand merci pour ces explications très intéressantes et ô combien éclairantes.

OUVRAGES RÉCENTS

CONCOURS COMMISSAIRE DE POLICE ET OFFICIER DE POLICE 2026-2027- TOUT-EN-UN

ÉDITEUR : VUIBERT

Résumé

Ce livre permet de se préparer efficacement à toutes les épreuves des concours de commissaires et d'officiers de police (lieutenants, capitaines, commandants) (externe, interne).L'officier de police assure les fonctions de commandement opérationnel des services et d'expertise supérieure en matière de police et de sécurité intérieure. Il peut être responsable de la sécurité d'un secteur de sécurité publique, en charge de missions de renseignement ou d'enquête, responsable de services de maintien de l'ordre. Officier de police...

L'OREO INDEX, LE NOUVEL INDICE DE MESURE DE L'OPACITE DANS LE SECTEUR IMMOBILIER

CHARLOTTE PALMIERI

CHARGÉE DE CONTENTIEUX ET PLAIDOYER AU SEIN DU PÔLE FLUX FINANCIERS ILLICITES DE TRANSPARENCY INTERNATIONAL FRANCE. DIPLÔMÉE D'UN MASTER II EN DROIT PÉNAL INTERNATIONAL ET DES AFFAIRES À LA SORBONNE AINSI QUE DU PROGRAMME GRANDE ECOLE DE L'EMLYON BUSINESS SCHOOL, CHARLOTTE A INTÉGRÉ TRANSPARENCY INTERNATIONAL FRANCE DÉBUT 2024. FORTE DE SON EXPÉRIENCE AU SEIN DU MINISTÈRE DE LA JUSTICE, CHARLOTTE A ÉTÉ AMENÉE À PARTICIPER AUX TRAVAUX DU GROUPE D'ACTION FINANCIÈRE (OCDE), À LA MISE EN OEUVRE DES SANCTIONS ÉCONOMIQUES PRISES À L'ENCONTRE DE LA RUSSIE ET AU SUIVI DES CRIMES DE GUERRE COMMIS EN UKRAINE.
AU SEIN DE TRANSPARENCY, ELLE EFFECTUE DES MISSIONS DE PLAIDOYER POUR LE RENFORCEMENT DE LA TRANSPARENCE FINANCIÈRE ET CONTRIBUE AUX CONTENTIEUX INITIÉS PAR L'ONG.

Entre 2015 et 2021, environ 2,3 milliards de dollars auraient été blanchis dans le secteur immobilier aux Etats Unis[1]. Ce chiffre vertigineux rappelle que l'investissement immobilier est devenu un vecteur de blanchiment privilégié pour les délinquants financiers. Ces investissements sont facilités par des cadres juridiques lacunaires et par la mise en place de montages financiers d'une extrême complexité favorisant une opacité complète des chaînes de détention des biens. Dans une étude menée en 2023, Transparency International France révélait ainsi que 70% des biens immobiliers détenus par des sociétés en France l'étaient de manière anonyme, malgré l'obligation de déclaration des bénéficiaires effectifs des sociétésFace à un mur d'opacité, Enquête sur les propriétaires réels des sociétés et des biens immobiliers en France, 2023 – Transparency International France et l'ACDC[2].

Ces premiers constats alertent, à l'heure où la majorité des produits du crime échappe aux autorités de poursuite et que 98% des avoirs criminels ne sont pas identifiés au sein de l'Union européenne[3].

Pour endiguer le phénomène, l'accès aux données relatives à la propriété, telles que les données sur les bénéficiaires effectifs, les données historiques sur la propriété ou la valeur et la date d'achat, peut aider les autorités, les journalistes et les organisations de la société civile à identifier les principaux signaux d'alerte. Dans le même temps, les agents immobiliers, les avocats et les notaires, entre autres, occupent des fonctions privilégiées pour identifier les transactions suspectes et empêcher le blanchiment de capitaux par l'intermédiaire de l'investissement immobilier.

Face à l'ampleur du défi, les standards européens et internationaux – comme ceux du Groupe d'action financière (GAFI) ou plus récemment, les dispositions de la 6ème directive européenne anti-blanchiment[4] - ont progressivement renforcé les dispositifs en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme (LCB-FT) en prenant en considération le risque spécifique attaché au secteur immobilier.

Si ces évolutions sont notables, les efforts restent considérables. C'est ce que révèle le nouvel indice d'opacité de la propriété immobilière (Opacity in real estate ownership index – OREO index) publié par Transparency International en partenariat avec l'Anti-Corruption Data Collective (ACDC) en mars 2025[5]. Cet indice classe 24 pays - principalement les pays du G20 et plusieurs autres centres financiers, tels que les Émirats arabes unis - en fonction de la solidité de leur cadre de prévention et de détection des flux financiers illicites dans le secteur immobilier. En évaluant deux piliers (la disponibilité et l'accessibilité des données immobilières dans un premiers temps ; la portée du cadre juridique de LCB-FT au sein du secteur immobilier dans un second temps), le rapport identifie les failles persistantes et porte plusieurs recommandations d'actions prioritaires pour les gouvernements et les organisations internationales.

La France se classe en troisième position, avec une note moyenne de 7.16 / 10 sur l'évaluation des deux piliers, après l'Afrique du Sud et Singapour. Les trois pays les moins bien notés sont les États

Unis, la Corée du Sud et l'Australie. Les résultats sont d'autant plus inquiétants que parmi les pays les moins bien classés – plusieurs sont devenus les destinations privilégiées pour l'investissement immobilier, comme les Émirats Arabes Unis (5ème pays le moins bien noté)[6].

L'analyse montre également que même dans les juridictions performantes, des lacunes importantes subsistent, qu'il s'agisse de l'exhaustivité et de l'accès aux données sur la propriété immobilière (I) ou de la mise en oeuvre de la réglementation LCB-FT (II), ce qui appelle à une série de réformes urgentes (III).

I. L'exhaustivité, l'accessibilité et la transparence des données immobilières, des paramètres à renforcer pour mieux prévenir les risques de blanchiment de capitaux

Alors que l'accès à des données qualitatives sur la propriété immobilière est indispensable pour favoriser la détection précoce d'infractions financières, le score moyen des pays évalués sur ce pilier dans l'OREO index est de 5.53/10. En étudiant l'exhaustivité des données enregistrées sur la propriété immobilière, les conditions d'accès à ces informations ainsi que les possibilités de réutilisation des données, l'étude déplore l'insuffisance des récoltes de données sur la propriété immobilière pour détecter les transactions illicites (1) ainsi qu'un accès encore imparfait aux données immobilières (2).

A. Une récolte de données sur la propriété immobilière insuffisante pour détecter les transactions illicites

68% des groupes et réseaux criminels au sein de l'Union européenne utilisent des méthodes de blanchiment d'argent de base, telles que l'investissement dans l'immobilier ou l'acquisition de biens de grande valeur[7]. Dans le même temps, selon l'OCDE, la quasi-totalité des délits économiques et financiers implique l'utilisation de sociétés anonymes[8].

Alors que les montages financiers mis en oeuvre aujourd'hui pour blanchir des fonds - notamment dans le secteur immobilier – sont d'une extrême sophistication, il est nécessaire que le recueil d'informations dans les registres dédiés soit le plus granulaire et exhaustif possible. Cela implique de recourir à l'enregistrement d'informations allant au-delà des données primaires sur la propriété, pour recueillir également des informations sur l'historique des données immobilières, les garanties encadrant l'acquisition immobilière ou encore les intermédiaires impliqués dans la signature des actes de vente.

Si l'ensemble des pays évalués a globalement obtenu des notes satisfaisantes sur la granularité des informations recueillies, un point de l'étude menée par Transparency International est particulièrement notable : le manque d'informations recueillies sur les bénéficiaires effectifs dans les différents pays étudiés au moment de l'enregistrement d'un bien immobilier. Seuls Singapour, l'Angleterre, certains États fédéraux de l'Argentine et le Canada collectent cette information, dans des conditions qui ne permettent toutefois pas toujours l'effectivité de la mesure.

En France, si l'information n'est pas directement enregistrée dans le fichier immobilier, au moins 11% des parcelles sont détenues par des sociétés dont les bénéficiaires effectifs doivent être déclarés au registre des bénéficiaires effectifs (RBE)Face à un mur d'opacité, Enquête sur les propriétaires réels des sociétés et des biens immobiliers en France, 2023 – Transparency International France et l'ACDC[9], ce qui permet de recouper les informations.

Restriction de l'accès du grand public au registre des bénéficiaire effectifs au sein de l'UE

La 6ème directive anti-blanchiment a récemment restreint l'accès du grand public au RBE en prenant acte d'une décision de la CJUE du 22 novembre 2022. Les entités ou personnes souhaitant accéder au registre devront désormais démontrer l'existence d'un intérêt légitime à accéder à ces informations – ce qui réduit de fait la possibilité pour la société civile d'identifier des transactions illicites. La France a fermé son RBE au grand public en juillet 2024. Parmi les pays étudiés dans le rapport de Transparency International, seuls le Canada, le Royaume Uni et l'Indonésie ont un registre des bénéficiaires effectifs ouvert au public.

L'étude révèle également que d'autres informations indispensables ne sont pas non plus enregistrées dans les registres immobiliers de certains pays, comme le prix de la transaction ou encore les informations fiscales grevées au bien susceptibles de révéler une surévaluation ou sous-évaluation du prix du bien. Ces informations doivent souvent être croisées entre différents registres, ce qui complexifie le travail d'enquête. Par ailleurs, les informations sur les intermédiaires impliqués dans les transactions ne sont pas toujours enregistrées. Si certains pays comme l'Argentine, l'Allemagne, le Panama, l'Afrique du Sud ou la France enregistrent des données sur les notaires ou avocats impliqués dans les transactions, les agents immobiliers ne sont pas toujours identifiés. Alors que de nombreuses professions assujetties aux obligations de LCB-FT sont aujourd'hui les premiers facilitateurs de la corruption et du blanchiment, leur identification est indispensable

pour rechercher leur responsabilité pénale parallèle.

B. Une accessibilité aux données sur la propriété immobilière encore réduite

Au-delà de l'exhaustivité des données récoltées, l'accessibilité de ces dernières doit également être garantie au plus grand nombre d'acteurs afin de favoriser les possibilités de détection d'infractions, ou simplement à des fins de documentation et d'éclairage pour le grand public. Selon l'étude menée par Transparency International, les données immobilières présentent un potentiel maximal de réutilisation lorsque l'information est accessible gratuitement, dans un format lisible par machine, librement disponible et téléchargeable en masse.

A cet égard, cinq pays étudiés (Argentine, Chine, Allemagne, Turquie et UAE) ne rendent pas leurs registres sur la propriété immobilière accessibles au public, mais seulement aux autorités compétentes ou aux personnes disposant d'un intérêt légitime à accéder à ces informations, étant précisé que la définition et l'appréciation de l'intérêt légitime est susceptible de varier considérablement d'un pays à l'autre. Certains journalistes, activistes ou chercheurs pourraient donc se voir refuser l'accès à certaines bases de données dans des pays adoptant une lecture restrictive de l'intérêt légitime. Les 19 pays restants évalués ont rendu la grande majorité de leurs données immobilières accessibles en ligne, à l'exception de certaines données historiques sur la propriété d'un bien précis où des demandes spécifiques doivent être faites dans plusieurs pays, comme en France[12].

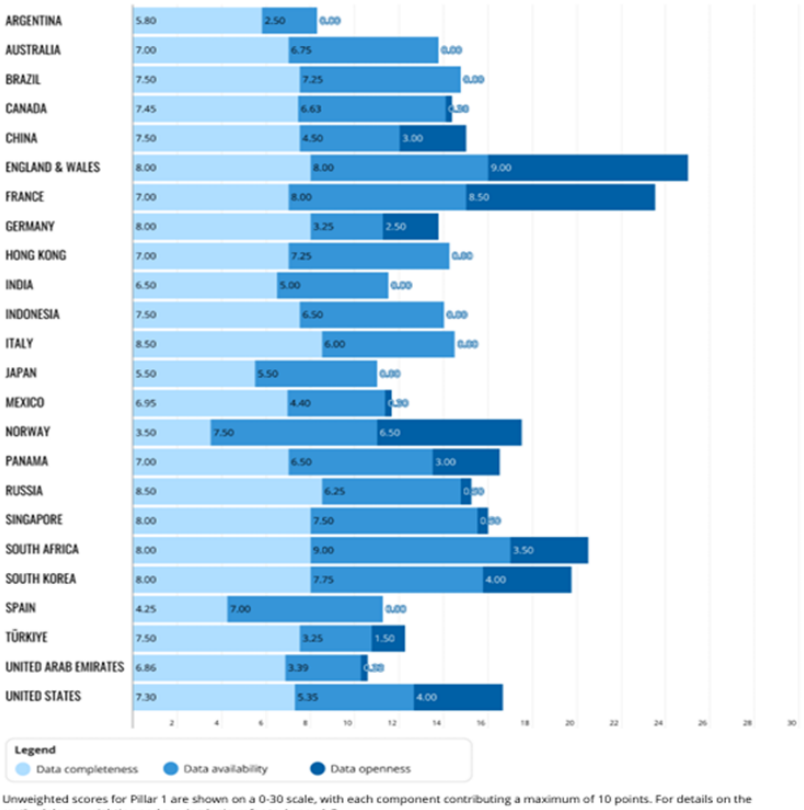
Il est utile de souligner par ailleurs que l'accessibilité de certaines données en ligne ne garantit pas toujours une exploitation immédiate et effective de ces informations. En cela, il est également intéressant d'analyser la possibilité de croiser des informations en provenance de plusieurs registres accessibles au public, comme les registres des bénéficiaires effectifs des sociétés enregistrées, les données sur les prix des transactions immobilières ou les informations sur la propriété foncière. D'après les résultats de l'étude menée par Transparency International, le Royaume-Uni se distingue à cet égard en étant la seule juridiction où l'ensemble des données citées plus haut sont non seulement disponibles, mais également accessibles au public. Un autre exemple positif souligné dans le rapport est celui de la France, qui fournit des informations collectées sur les transactions immobilières - date d'achat et prix de chaque bien - au cours des cinq dernières années (« demandes de valeurs foncières »). Cette base de données est publique, sous licence ouverte et lisible par machine[13].

Par ailleurs, l'étude révèle que 12 des 24 pays étudiés exigent un paiement pour consulter le registre immobilier et obtenir des certificats officiels; certains pays comme le Canada ou l'Australie ayant mis en place des montants potentiellement dissuasifs. Ces procédures ne permettent pas non plus le téléchargement en masse de données, pourtant indispensable pour la production de rapports susceptibles de faire émerger des tendances sur les principaux risques identifiés.

A ce titre, la France et l'Angleterre sont les seuls pays qui permettent le téléchargement en masse de données sur la propriété immobilière détenue par les personnes morales directement sur des bases de données en ligne[14]. En France, ces données sont également disponibles en licence ouverte, ce qui avait permis à Transparency International France, en croisant ces informations avec celles contenues dans le RBE, de mener une étude en 2023 révélant des données inédites sur la part de biens immobiliers détenus de manière anonyme[15].

Cela étant dit, aucune des juridictions évaluées ne classe explicitement toutes les données

FIGURE 3: DATA COMPLETENESS, AVAILABILITY AND OPENNESS



Unweighted scores for Pillar 1 are shown on a 0-30 scale, with each component contributing a maximum of 10 points. For details on the methodology, weighting and scoring logic, refer to Annex 1-3.

immobilières sous une licence ouverte, ni n'autorise clairement la réutilisation sans restriction de ces données.

II. Une mise en oeuvre lacunaire de la réglementation LCB-FT au sein des professions du secteur immobilier

Malgré un renforcement des standards internationaux en matière de réglementation LCB-FT dans le secteur immobilier, le score moyen des pays évalués pour ce second pilier par l'OREO index est de 5.52/10. En étudiant par différents canaux le champ d'application des dispositions LCB-FT au sein du secteur immobilier, l'étude déplore l'absence d'assujettissement de certaines professions clés (1) ainsi que la mise en oeuvre encore parcellaire des procédures de vigilance adaptées (2).

A. Des failles persistantes concernant l'assujettissement à la LCB-FT des professions du secteur immobilier

Un large éventail d'intermédiaires du secteur financier et non financier sont susceptibles de participer à des transactions immobilières, en fonction des spécificités juridiques du pays concerné. Dans le secteur non financier, chaque profession peut jouer un rôle distinct à différents stades de la procédure (les avocats peuvent acquérir des biens en tant que mandataires de leurs clients, les notaires doivent authentifier et certifier les actes, les comptables peuvent conseiller leurs clients sur le volet financier ou fiscal, etc.). Si ces professionnels se trouvent dans une position privilégiée pour empêcher l'argent illicite d'infiltrer le marché immobilier, ils peuvent aussi, par inadvertance ou délibérément, faciliter de telles activités.

L'étude de Transparency International a révélé que les régulateurs peinent à étendre les exigences de vigilance et les dispositions relatives à la LCB-FT à l'ensemble des professionnels et des entreprises non financières impliqués dans les transactions immobilières.

A cet égard, un point commun à plusieurs pays particulièrement notable est l'absence d'assujettissement des promoteurs immobiliers à la LCB-FT, comme par exemple en Argentine, au Royaume-Uni, en France[16], à Hong Kong, en Italie, en Norvège et aux EAU. Cette faille est d'autant plus inquiétante quand on connaît le rôle joué par les promoteurs immobiliers, qui peuvent commercialiser les biens immobiliers ayant fait l'objet d'une construction préalable.

La même lacune se retrouve aussi du côté des avocats, qui sont soit écartés du dispositif de LCB-FT, ou partiellement inclus, comme par exemple au Brésil, au Canada et au Panama, notamment pour des raisons de respect de la confidentialité, en contradiction avec les recommandations du GAFI.

Ainsi, 14 des 24 juridictions analysées échouent totalement à réglementer les professionnels impliqués dans des transactions immobilières ou bien présentent de sérieuses lacunes. L'étude de Transparency International révèle même que les transactions immobilières peuvent avoir lieu sans l'intermédiaire d'une profession assujettie dans de nombreux pays étudiés (Australie, Chine, Royaume-Uni, Japon, Turquie et EAU).

De même, lorsque les professions sont bien assujetties, la formation aux obligations de vigilance n'est pas toujours obligatoire. Dans presque tous les pays étudiés, les superviseurs développent des recommandations pour appuyer les professions concernées mais dans 5 pays, les professions assujetties n'ont toujours pas à se soumettre à des formations. Pourtant, au-delà de la mise en place des règlementations, c'est souvent l'enjeu de la compréhension des risques qui est au coeur du défi. L'Afrique du Sud en est un exemple criant : bien que toutes les professions immobilières soient couvertes par la législation relative à LCB-FT, les évaluateurs du GAFI ont conclu en 2021 qu'ils n'avaient pas encore une compréhension suffisante des risques de blanchiment d'argent dans le secteur immobilier et que les professionnels du droit n'étaient pas suffisamment supervisés[17]. A cet égard, l'étude souligne la nécessité de développer instances de supervision centralisées, indépendantes et disposant des capacités suffisantes pour contrôler les professions assujetties.

B. La mise en place parcellaire des procédures de vigilance dites « Know Your Customer »

Si elles sont effectivement mises en oeuvre, les obligations de vigilance à l'égard de la clientèle permettent aux professionnels de détecter les transactions suspectes, d'identifier les signaux d'alerte et d'atténuer les risques liés aux flux

financiers illicites. Dans les transactions immobilières, les obligations de vigilance doivent porter à la fois sur l'acheteur et le vendeur afin de garantir une évaluation complète du risque. L'étude menée par Transparency International s'est penchée sur la mise en oeuvre de quatre piliers des obligations de vigilance : l'identification du client, les motivations à l'origine de la transaction, la source des financements et le suivi de la relation client.

Les résultats ont démontré que la majorité des pays impose seulement des obligations de vigilance primaires, comme l'identification et la vérification du client. La vérification de l'origine des fonds n'est pas systématiquement requise, alors qu'il s'agit d'une mesure absolument indispensable pour détecter des transactions illicites, comme rappelé par les recommandations du GAFI. Ainsi, seulement 15 des 22 pays évalués appliquent ces vérifications seulement en cas d'obligations de vigilance renforcées (transactions impliquant des personnes politiquement exposées - PEPs, des arrangements de paiement inhabituels ou des transactions dans des juridictions à haut risque)[18]. Même dans les pays qui mettent effectivement en oeuvre des mesures de vigilance renforcées, seulement la France, Hong Kong et les EAU exigent que le premier paiement pour les transactions immobilières soit effectué par l'intermédiaire d'une institution financière.

Un autre point notable est l'absence d'obligation de déclaration de soupçon pour les avocats dans certains pays clés (Brésil, Canada, Panama). Même lorsque l'obligation de déclaration de soupçon existe, il a pu être rappelé à plusieurs reprises que celle-ci était encore trop partiellement mise en oeuvre par certaines professions particulièrement à risque. A cet égard, il est important que les autorités publient des statistiques sur le nombre de déclarations de transactions suspectes reçues chaque année. Dans l'étude menée par Transparency International, les statistiques fournies par près de la moitié des juridictions comprennent des informations détaillées sur le nombre de déclarations effectuées par chaque catégorie de professionnels. Certaines indiquent également le nombre de déclarations ayant donné lieu à une enquête des services répressifs. Ce type d'informations permet d'évaluer plus clairement si l'obligation de déclaration est effectivement appliquée aux différentes catégories de professionnels.

Déclarations de soupçon reçues par Tracfin dans le secteur immobilier

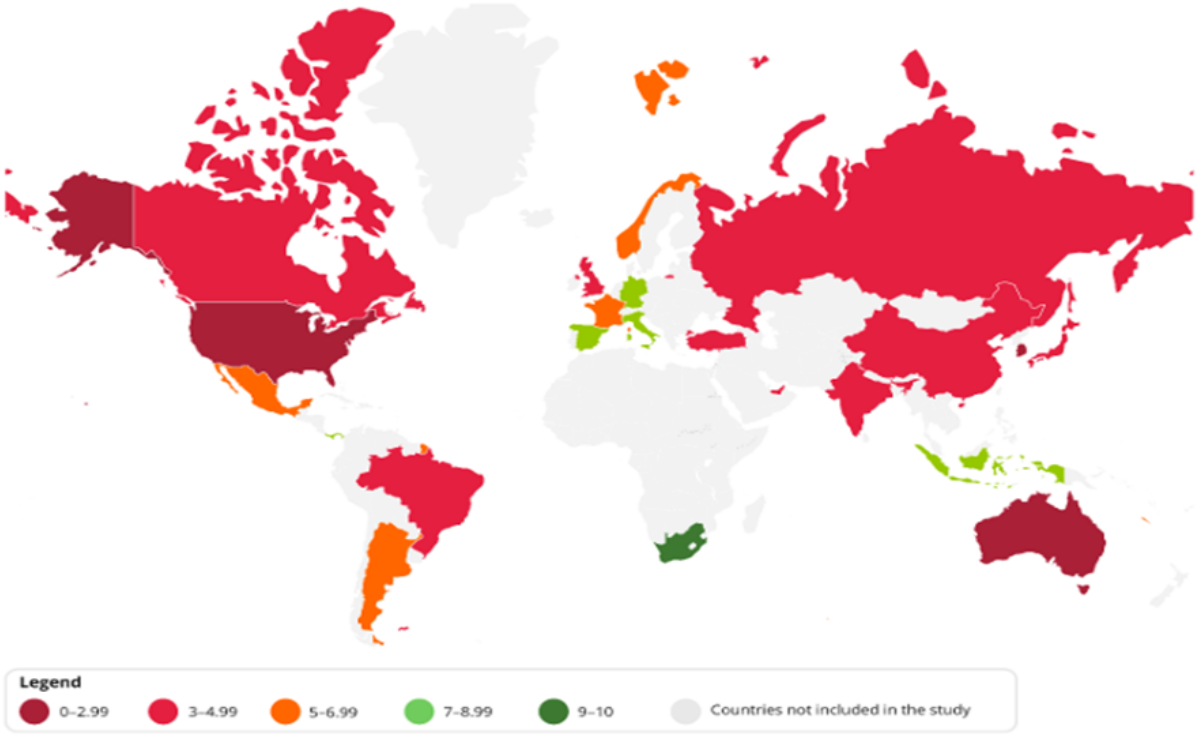
En France, les déclarations de soupçon en provenance des professions susceptibles d'être impliquées dans les transactions immobilières ont augmenté sur les dernières années, avec toutefois un niveau d'implication inégal d'une profession à l'autre.

En effet, les déclarations de soupçon effectuées par les notaires ont évolué progressivement sur les dernières années avec 3 242 déclarations de soupçons reçues en 2023, soit une augmentation de 21% depuis l'année 2022. En revanche, bien qu'en évolution, les déclarations de soupçon des avocats demeurent marginales, avec 35 déclarations pour l'année 2023, en augmentation de 25% depuis l'année 2022. Selon Tracfin, l'appropriation du dispositif LCB-FT par les avocats demeure ainsi significativement perfectible.

L'ensemble des professionnels de l'immobilier (agences immobilières, négociateurs, mandataires, etc.) ont quant à elles effectué 505 déclarations de soupçon en 2023, en évolution de 15% depuis 2022. Si ce chiffre est en augmentation depuis 3 ans, il reste selon Tracfin en deçà de ce qui pourrait être attendu alors que l'année 2022 à elle seule comptabilisait 1,3 million de transactions immobilières.

Enfin, dans presque tous les pays évalués, l'étude de Transparency International a montré que la collecte et la vérification des données sur les bénéficiaires effectifs était requise pour les sociétés qui achètent des biens immobiliers. Certaines juridictions comme Hong Kong ou les Émirats Arabes Unis, permettent toutefois des délais dans l'identification des bénéficiaires effectifs, afin de ne pas perturber l'activité de l'entreprise. Les exigences du Mexique en la matière sont les plus faibles, car sa législation oblige seulement les professionnels à demander des informations sur les bénéficiaires effectifs à leurs clients, sans les collecter et les conserver activement. Enfin, l'étude révèle que 11 des 24 pays étudiés – dont la France - n'exigent pas qu'une entreprise étrangère déclare ses bénéficiaires effectifs quand

FIGURE 6: OREO PILLAR 2 RESULTS – ANTI-MONEY LAUNDERNG FRAMEWORKS



elle achète un bien dans le pays concerné. Cela crée une lacune particulièrement préoccupante, permettant à des entités anonymes d'acheter des biens immobiliers à l'étranger sans contrôle. A noter que la mise en oeuvre de la 6ème directive anti -blanchiment doit contraindre les pays européens à combler cette faille.

III. Quelles priorités de réforme ?

L'OREO index montre que les principaux centres financiers restent vulnérables au blanchiment de capitaux par le biais de l'immobilier. A ce titre, l'Australie et les Etats Unis présentent des résultats particulièrement faibles. Si le placement sur liste grise du GAFI de certains pays comme l'Afrique du Sud, le Panama ou les EAU ont favorisé le renforcement de leurs dispositifs, des efforts importants demeurent attendus. Dans un contexte globalisé, où les transactions ne connaissent plus de frontières, les failles non comblées dans certains pays seront exploitées demain par les délinquants financiers souhaitant blanchir leurs fonds dans des juridictions aux réglementations plus souples, ou non appliquées.

Un travail de renforcement et d'harmonisation des standards au niveau international est donc indispensable. A ce titre, l'étude menée par Transparency International porte quelques recommandations visant à lutter contre l'opacité des chaînes de détention des biens immobiliers, renforcer les obligations de vigilance pour les professions susceptibles d'être impliquées dans les transactions immobilières et favoriser l'accès à des données immobilières exhaustives.

En premier lieu, l'étendue et la quantité des données sur la propriété immobilière devraient être améliorées. Ainsi, par exemple, les personnes morales nationales et étrangères qui achètent et vendent des biens immobiliers devraient être tenues de divulguer leurs bénéficiaires effectifs aux autorités. La 6ème directive européenne anti-blanchiment impose désormais aux sociétés et fiducies étrangères effectuant des investissements immobiliers dans les pays de l'UE de divulguer les informations relatives à leurs propriétaires effectifs[21]. En outre, elle exige que les pays enregistrent des informations historiques détaillées relatives aux biens immobiliers dans des registres immobiliers et qu'ils permettent aux autorités d'accéder à ces registres par l'intermédiaire d'un point d'accès unique.

Si ces évolutions sont particulièrement bienvenues au niveau européen, il n'existe toutefois actuellement aucune norme internationale qui traite les lacunes

identifiées. Les recommandations du GAFI sur la transparence des bénéficiaires effectifs pour les personnes morales et les constructions juridiques n'ont pas encore conduit à une transparence accrue sur les biens immobiliers détenus par les entreprises. A ce titre, il est urgent que des registres sur les bénéficiaires effectifs puissent être mis en oeuvre dans tous les pays, avec un accès garantit au plus grand nombre. Les instances internationales telles que celles du G20 ou du GAFI pourraient également jouer un rôle accru consistant à définir des normes minimales pour la collecte de données sur les biens immobiliers et la manière dont ces informations pourraient être partagées entre les pays. A cet égard, afin d'éviter que les pays ne reposent exclusivement sur des demandes d'entraide pénale pour partager des informations, les normes internationales devraient permettre de faciliter l'accès direct et non filtré des autorités compétentes nationales et étrangères à ces informations clés.

Par ailleurs, les pays devraient veiller à ce que les transactions immobilières requièrent l'intervention d'au moins une profession de garde-fou, à fortiori pour les biens de grande valeur ou les biens détenus par des personnes morales. De plus, tous les professionnels susceptibles d'être impliqués dans la vente ou l'achat d'un bien immobilier doivent être soumis à la réglementation LCB-FT. Les normes du GAFI exigent déjà que les pays étendent leurs obligations en matière de LCB-FT aux professionnels tels que les notaires, les agents immobiliers et les avocats lorsqu'ils effectuent des transactions liées à la vente ou à l'achat de biens immobiliers. De même, plusieurs directives européennes ont exigé des États membres qu'ils soumettent aux règles de lutte contre le blanchiment les professionnels généralement impliqués dans les transactions immobilières. Ainsi, les pays de l'UE obtiennent des résultats relativement satisfaisants dans le cadre du deuxième pilier. Si une série d'efforts sont particulièrement notables dans la mise en oeuvre des dispositifs LCB-FT par les différents pays évalués, de nombreuses professions, comme les promoteurs immobiliers ou les avocats, restent toutefois encore trop souvent écartées du dispositif. Transparency International appelle ainsi les pays du G20 à envisager d'élaborer des principes autonomes de haut niveau sur la réglementation et la surveillance des professions dans le secteur non financier, notamment pour assurer une supervision efficace et centralisée des professions concernées.

Alors que la France est bien connue pour être une destination privilégiée des délinquants financiers souhaitant blanchir leurs fonds dans le secteur immobilier du vice-président de Guinée équatoriale, Teodorin Obiang[22], des réformes ont été engagées récemment pour favoriser la transparence dans le secteur immobilier, répondant à une partie importante des lacunes précédemment identifiées.

En France, les données immobilières peuvent être recoupées avec celles sur les bénéficiaires effectifs quand les biens immobiliers concernés ont été acquis par l'intermédiaire d'une entreprise. Ainsi, lorsque les données sont enregistrées au sein du RBE, il est indispensable que celles-ci soient les plus exhaustives possibles, afin de favoriser le démantèlement de chaînes de propriétés opaques. La loi portant diverses dispositions d'adaptation au droit de l'Union européenne en matière économique, financière, environnementale, énergétique, de transport, de santé et de circulation des personnes (ci-après « projet de loi DDADUE ») promulguée le 22 avril 2025 instaure en son article 4 - et conformément aux recommandations de Transparency International France - de restaurer l'obligation de déclaration des chaînes de propriété au RBE, ainsi que l'historique des données[23].

Au défi de l'exhaustivité des données s'ajoute celui du taux de complétude du registre[24]. En effet, l'actuel taux de complétude du registre sur les bénéficiaires effectifs l'empêche d'être un outil véritablement effectif en matière de détection de la criminalité économique et financière. A cet égard, et alors même qu'il s'agit d'une obligation légale, il est très préoccupant de constater que, selon les dernières analyses de Transparency International, 31 % des personnes morales n'ont toujours pas encore déclaré de bénéficiaire effectif[25].

Afin de favoriser les sanctions en cas de non-déclaration des bénéficiaires effectifs, deux véhicules législatifs récents ont proposé des mesures inédites. Le projet de loi simplification de la vie économique adopté par le Sénat le 22 octobre 2024 et en cours d'examen à l'Assemblée nationale propose de considérablement renforcer le taux

de l'amende infligée en cas de non-déclaration des bénéficiaires effectifs[26]. Au-delà des sanctions pénales, la proposition de loi visant à sortir la France du piège du narcotrafic adoptée le mardi 29 avril 2025 par l'Assemblée nationale ajoute plusieurs mesures essentielles à disposition des greffiers des tribunaux de commerce visant à procéder à la radiation d'office d'une entreprise en cas de non-déclaration des bénéficiaires effectifs après relances[27].

Cette même proposition de loi prévoit, notamment en réaction aux résultats parus dans l'OREO index, d'assujettir de nouvelles professions à la LCB-FT, à savoir les personnes se livrant à titre habituel à la location ou à la vente de véhicules, de navires de plaisance et d'aéronefs au-delà d'un certain seul fixé par décret, ainsi que les promoteurs immobiliers et les marchands de biens.

Si ces quelques démarches sont encourageantes, elles ne doivent pas appeler au relâchement des efforts. Des améliorations sont encore possibles, notamment en ce qui concerne l'interopérabilité des différents registres sur la propriété. Dans un monde de plus en plus globalisé, les engagements en faveur de plus de transparence ne peuvent rester cloisonnés. Alors que la France a joué un rôle pionnier en matière de transparence des bénéficiaires effectifs et sur les données immobilières, il est à espérer que ces nouvelles propositions puissent inspirer au renforcement des standards au sein des instances internationales et des gouvernements.

Notes :

1. Kumar, L. and de Bel, K. (August 2021). Acres of Money Laundering: Why U.S. Real Estate is a Kleptocrat's Dream. (Global Financial Integrity). https://gfintegrity.org/report/acres-of-money-laundering-why-u-s-real-estate-is-a-kleptocrats dream

2. Face à un mur d'opacité, Enquête sur les propriétaires réels des sociétés et des biens immobiliers en France, 2023 – Transparency International France et l'ACDC

3. Europol, The changing DNA of serious and organised crime, EU Serious and organized crime threat assessment, 2025

4. Directive - UE - 2024/1640 - EN - EUR-Lex

5. Opacity in real estate ownership index, Transparency International et l'ACDC, mars 2025

6. Il convient de préciser que cet indice se limite à l'analyse du cadre juridique en place et n'évalue pas la mise en oeuvre effective de ce cadre.

7. https://www.europol.europa.eu/cms/sites/default/files/documents/socta2021_1.pdf, p.21.

8.https://www.oecd.org/daf/ca/43703185.pdf

9. Face à un mur d'opacité, Enquête sur les propriétaires réels des sociétés et des biens immobiliers en France, 2023 – Transparency International France et l'ACDC

10. Directive antiblanchiment : la disposition prévoyant que les informations sur les bénéficiaires effectifs des sociétés constituées sur le territoire des États membres soient accessibles dans tous les cas à tout membre du grand public est invalide

11. Transparency International France a eu l'opportunité, à plusieurs reprises, de déplorer la fermeture du RBE au grand public. L'accès au RBE s'est en effet révélé essentiel pour permettre à Transparency International France de mener ses travaux. C'est en s'appuyant sur ce registre que Transparency International France a pu dresser un inventaire du patrimoine immobilier en France de plusieurs oligarques et proches du régime russe dans la perspective d'actions judiciaires, identifier les chaînes de propriétés mises en place à cet effet, et réunir un faisceau d'indices sur l'origine illicite des ressources ayant permis l'acquisition de ces patrimoines.

12. Les demandes sont effectuées auprès du Service de la publicité foncière (SPF). Les SPF enregistrent les actes de vente, de donation, et autres transactions immobilières. Ils tiennent à jour les informations sur la propriété et la situation juridique des biens immobiliers. Ils fournissent des renseignements sur les biens immobiliers, tels que les différents propriétaires, les dates d'achat, etc. Ils perçoivent les impôts relatifs aux transactions immobilières.

13. Consulter les dernières transactions immobilières (demande de valeurs foncières) | Service-Public.fr

14. Pour la France, ce sont les fichiers des locaux et parcelles des personnes morales

15. Face à un mur d'opacité, Enquête sur les propriétaires réels des sociétés et des biens immobiliers en France, 2023 – Transparency International France et l'ACDC

16. Cette lacune a récemment été comblée en France, voir dans les développements en infra

17. MUTUAL EVALUATION REPORT OF SOUTH AFRICA

18. A noter que le Mexique n'impose même pas la mise en oeuvre d'obligations de vigilance renforcées dans ces cas précis

19. Rapport sur l'activité des professions déclarantes de la cellule de renseignement financier, Tracfin, 2023

20. Les pays sont notés de 0/10 sur chaque piliers. Les pays performants le moins bien sur le second pilier sont en rouge foncé sur la carte et les pays performants le mieux, en vert foncé.

21. Directive - UE - 2024/1640 - EN - EUR-Lex

22. Plusieurs affaires dites des « biens mal acquis » ont d'ores et déjà abouti à des condamnations et à des confiscations à hauteur de plusieurs millions, notamment à l'encontre du vice-président de Guinée équatoriale, Teodorin Obiang. Transparency International France est constitué partie civile dans plusieurs de ces affaires.

23. Ce projet de loi vient transposer plusieurs directives européennes ou adapter le droit français à plusieurs règlements européens récents dans différents domaines.

24. Transparency International France et le CNGTC ont notamment porté des recommandations conjointes sur le RBE dans un livre blanc publié en juillet 2024

25. Face à un mur d'opacité, Enquête sur les propriétaires réels des sociétés et des biens immobiliers en France, 2023 – Transparency International France et l'ACDC

26. Projet de loi de simplification de la vie économique (Dossier législatif en version dépliée) - Assemblée nationale

27. Narcotrafic Proposition de loi sortir du piège du trafic de drogue | vie-publique.fr

IMMUNITÉS, COOPÉRATION ET INDÉPENDANCE : LE PARQUET EUROPÉEN FACE À LA COUR DES COMPTES, UN TEST POUR LA POLITIQUE PÉNALE DE L'UNION

ÉMILIE EHRENGARTH,

PH.D., RÉDACTRICE EN CHEFFE DE LA REVUE DU GRASCO , DIRECTRICE DE L'AGENCE FIAT LUX-CONSEILS ET FORMATIONS . FORMATRICE SPÉCIALISÉE EN DROIT PÉNAL, EN DROIT DES AFFAIRES ET EN TECHNIQUES DE MANAGEMENT. CHARGÉE DE MISSION AUPRÈS DE L'UNIVERSITÉ DE STRASBOURG ET DE LA CHAMBRE DES SALARIÉS DU LUXEMBOURG.

Le recours introduit par le Parquet européen contre la Cour des comptes européenne révèle, au-delà d'un différend ponctuel, une faille structurelle dans la coopération interinstitutionnelle face aux exigences croissantes de protection des intérêts financiers de l'Union. Le 10 février 2025, le Parquet européen (PE) a introduit un recours (Affaire T-99/25) devant le Tribunal de l'Union européenne contre la Cour des comptes européenne (CCE). Par cette procédure, le PE conteste le refus de la CCE de lever la confidentialité de ses agents et de certains documents pour permettre l'audition de fonctionnaires de l'Union dans le cadre d'une enquête pénale sur des fraudes aux intérêts financiers de l'UE, constituant à son sens, une entrave grave à l'exercice de ses missions d'enquête et de poursuite des infractions portant atteinte au budget de l'Union européenne. Le Parquet européen affirme que la CCE, en refusant de lever l'immunité et d'autoriser l'audition de ses agents comme témoins, l'empêche de recueillir les éléments de preuve nécessaires pour établir la réalité d'éventuelles infractions pénales. Ce refus bloque ainsi le bon déroulement de l'enquête et la manifestation de la vérité. A l'appui de ce recours, le PE avance cinq arguments tenant au détournement de la procédure d'immunité, à la violation du principe de coopération loyale, à la violation de la confidentialité des enquêtes pénales, à la violation de l'indépendance du Parquet dans la conduite des affaires et à l'application erronée du protocole n°7 sur les immunités et les privilèges[1].

La procédure ouverte soulève une question de procédure relative à une demande de levée d'immunité des fonctionnaires de la Cour des comptes européenne.

Un contexte de tensions institutionnelles révélateurs de manques dans les instruments de coopération inter-entités

Conformément à l'article 19 du statut des fonctionnaires de l'Union, le PE avait sollicité le 26 septembre 2024 l'autorisation d'auditionner des fonctionnaires de la Cour des comptes comme témoins dans une enquête sur des soupçons de fraudes aux subventions européennes. La Cour des comptes a opposé un refus le 9 décembre 2024, estimant notamment que l'affaire devait être classée sans suite.

Selon le Statut des fonctionnaires européens de 2004, le recueil préalable d'une autorisation de l'autorité de provenance de la personne sujet de la mesure est une condition nécessaire destinée à assurer la protection des personnes compte tenu du risque de divulgation d'informations sensibles. La levée de l'immunité doit alors être étudiée au regard des « intérêts de l'Union » (CJUE). Or, le Parquet européen, organe indépendant est en charge de la poursuite des infractions pénales portant atteinte aux intérêts financiers de l'Union, il participe donc à la même mission que la Cour de comptes, à savoir protéger et défendre les intérêts financiers de l'Union européenne. Il paraît donc, a priori,

étonnant d'opposer ce principe comme obstacle à la participation de l'entité à une enquête pénale.

Compte tenu du refus, en empêchant ses membres d'être entendus à titre de témoin, le Parquet européen considère que les faits constituent une entrave dans sa capacité à mener à bien sa mission prévue par les traités, notamment l'article 86 TFUE et forme un recours devant la Cour de Justice de l'Union européenne, en charge de trancher les litiges entre organes de l'Union et de contrôler la légalité de la position de la Cour des comptes. Cinq moyens sont invoqués alors par le Parquet européen devant la Cour.

1. Détournement de pouvoir

Tout d'abord, le Parquet européen estime que la Cour des comptes européenne s'est fondée sur des motifs étrangers à la protection des intérêts de l'Union, détournant la finalité de l'article 19 du statut.

En effet, selon le Parquet, la CCE fonde sa décision sur des motifs étrangers à ceux inscrits dans l'article 19, visant à la protection des intérêts financier de l'Union.

Selon l'article 19, « le fonctionnaire ne peut faire état en justice, à quelque titre que ce soit, des constatations qu'il a faites en raison de ses fonctions, sans l'autorisation de l'autorité investie du pouvoir de nomination. Cette autorisation ne peut être refusée que si les intérêts des Communautés l'exigent et si ce refus n'est pas susceptible d'entraîner des conséquences pénales pour le fonctionnaire intéressé. Le fonctionnaire reste soumis à cette obligation même après la cessation de ses fonctions.

Les dispositions de l'alinéa précédent ne s'appliquent pas au fonctionnaire ou ancien fonctionnaire témoignant devant la Cour de justice des Communautés européennes ou devant le conseil de discipline d'une institution, pour une affaire intéressant un agent ou un ancien agent des trois Communautés européennes ».

Par ce texte, les auteurs ont voulu assurer la protection des agents européens en interdisant la divulgation d'informations sans autorisation préalable de l'autorité de rattachement, empêchant toute circulation non contrôlée d'informations sensibles ou confidentielles, sauf en cas de témoignage devant la Cour de justice de l'Union européenne (CJUE) ou devant le Conseil de discipline de son institution.

On peut donc conclure que l'article 19 instaure un filtre qui vient limiter la circulation de l'information acquise dans le cadre de fonctions, garantissant la confidentialité des travaux des fonctionnaires européens, sauf lorsque l'intérêt supérieur de l'Union ou la justice européenne l'exige.

Relevons alors que le Statut des fonctionnaires européens a été adopté par le Règlement n°31 (CEE), n°11 (CEEA) en juin 1962[2], qu'il a été modifié à plusieurs reprises mais dans une époque antérieure à la mise en oeuvre du Parquet européen. Il est donc à relever une certaine carence dans le dispositif et il semble alors intéressant de proposer ici une révision du texte pour permettre au Parquet européen de bénéficier du même régime d'exception que celui instauré pour la CJUE, à savoir, une levée de l'immunité des fonctionnaires européens lorsque le PE a besoin de les entendre dans le cadre d'une enquête pénale, les intéressés gardant intact leurs différents droits procéduraux (droit à l'assistance d'un conseil, à un recours effectif devant la CJUE, ….).

2. Violation du principe de coopération loyale

Dans un deuxième argument, le PE estime qu'en bloquant l'accès aux témoignages nécessaires à l'enquête, la Cour des comptes entraverait sa mission de collecter des preuves pertinentes à charge et à décharge. Il explique que la CCE, depuis le début de la procédure, adopte des décisions qui visent toutes à « priver le PE de la possibilité d'accomplir sa mission au titre des traités (art. 86 TFUE) »[3]. Selon le Parquet , les refus de la CCE l'empêche d'accomplir sa mission de recueil des éléments pertinents et utiles à l'enquête, que ces éléments soient à charge ou à décharge. Pour le PE, cette attitude ne peut s'interpréter qu'en une « ingérence indue » dans ses pouvoirs, entraînant une « violation de son obligation » de coopérer loyalement.

Rappelons que, selon les statuts, la Cour des comptes est la gardienne des finances de l'Union européenne et dans ce but, elle encourage ses agents « à promouvoir une culture de l'intégrité et de la probité dans leur relation avec les collègues, les partenaires et les entité auditionnées ». A ce

titre, suivant ce qui est inscrit sur le site de la Cour des comptes européenne, ses représentants ont pour mission de « montrer » l'exemple et de coopérer en toute bonne foi avec le Parquet européen lorsque ce dernier requiert son assistance dans une enquête qu'il diligente. Par ailleurs, au titre de l'Accord administratif signé avec le Parquet européen en septembre 2021, nous ne pouvons que nous étonner de la position de la Cour des comptes qui, par ce document, s'est engagé à faciliter l'accès du Parquet à ses bases de données lorsqu'il en fait la demande et qu'il agit dans le cadre d'une enquête[4] Plus encore, selon ce même document, la Cour des comptes a l'obligation de coopérer avec le Parquet lorsqu'il demande des documents ou des informations. Dans ce cas, la CCE doit répondre sans délais ou l'en informer du retard en motivant ce dernier. L'adoption de ce document, tout comme la signature de l'arrangement administratif du 22 mai 2019, vise à rendre efficiente et efficace la lutte contre la fraude, la corruption ou toute autre infraction pénale portant atteinte aux intérêts financier de l'Union. Il est donc étonnant de constater les réticences et le silence de la CCE face aux demandes du Parquet. Pourquoi une telle réticence ? Quels intérêts priment alors dans la position de l'entité ? Comment justifier ces refus ? Pourquoi entraver le cour de la justice ?

3. Violation de la confidentialité des enquêtes

Par ailleurs, le Parquet européen reproche à la Cour des comptes d'avoir tenté d'obtenir un accès illimité aux informations couvertes par le secret de l'enquête, en dépassant le cadre de sa compétence. En effet, dans le cadre de son enquête, le PE a envoyé une demande d'autorisation de levée de la confidentialité en vue d'une audition de témoins ainsi qu'une demande d'accès aux archives. Dans ces démarches, le Parquet a fourni à la CCE les informations nécessaires pour qu'elle puisse vérifier que les intérêts de l'Union ne sont pas gravement lésés. Malheureusement, la CCE n'autorise pas la levée de la confidentialité et refuse l'accès au témoin ainsi qu'aux archives de l'entité.

Par ailleurs, le Parquet européen reproche à la CCE de vouloir s'immiscer dans l'enquête en tentant d'obtenir à plusieurs reprises des informations couvertes par le secret de l'enquête (Règlement 2014/1939, art. 108). Pour le Parquet, de tels agissements outrepassent les limites de la mission de contrôle de la CCE dans l'étude de la recevabilité des demandes de levées des immunités de ses fonctionnaires. En agissant de la sorte, la CCE violerait ses obligations.

Se pose ici la question de l'étendue du contrôle exercé par l'organe chargé d'assurer la protection des fonctionnaires relevant de son autorité. Quelles mesures sont possibles ? Quels actes sont-ils acceptables ? Quand est-il possible de conclure au dépassement du cadre de la mission qui était allouée ?

Pour répondre à ces interrogations, il est possible de se tourner vers les principes entourant les contrôles exercés dans ces cas précis et , en premier lieu, poser le principe de légalité. En effet, l'action du Parquet européen intervient dans un cadre très strict qu'est celui de la légalité tel qu'il est posé par le paragraphe 66 du Règlement l'ayant institué. Suivant ce principe, il n'agit que lorsqu'une enquête est ouverte suite à un signalement d'infraction. Il agira alors en respectant les principes cardinaux de proportionnalité, d'impartialité et d'équité (§65) vis-à-vis des suspects ou de toute personne mise en cause dans la procédure. En contrepartie, dans le cadre d'une coopération loyale, l'entité d'appartenance chargée de vérifier la légalité de la levée de l'immunité devra respecter le cadre de son intervention et se limiter aux cas de refus que sont le risque de divulguer une information sensible et/ou de mettre en danger ledit fonctionnaire, la levée de l'immunité lui faisant alors grief. Pour réaliser sa tâche, la CCE a besoin d'informations tenant à la nécessité et à la proportionnalité de la mesure envisagée mais non à l'ensemble de la procédure laquelle est protégée par le secret de l'enquête. La levée de l'immunité ou l'accès aux archives ne requièrent en rien une étude approfondie du dossier d'enquête ; seule la proportionnalité et la nécessité d'une telle mesure devant être analysées.

4. Atteinte à l'indépendance du Parquet européen

Un autre argument soulevé par le parquet européen, réside dans la violation de l'indépendance de ce dernier dans la conduite des enquêtes. En effet, selon le PE, la conduite des enquêtes pénales relève

exclusivement de sa compétence et des autorités nationales, sans ingérence d'autres institutions de l'UE. Il ajoute que l'article 19 des Statuts ne donnent en aucun cas un droit de regard à la CCE sur les enquêtes menées par le Parquet, même si son concours est demandé.

Ainsi, lorsque la CCE , à l'appui de son refus de levée les immunités, conclut à l'inexistence d'une infraction pénale et au nécessaire classement sans suite, elle substitue son appréciation à celle du Parquet européen, cherchant alors, selon le Parquet, à influer sur la conduite des enquêtes pénales, outrepassant alors entièrement le champ de sa mission et de ses compétences.

Par ailleurs, le Parquet européen rappelle que, dans l'Union européenne, la protection des intérêts financiers de l'UE est primordiale et que le Parquet est précisément l'autorité indépendante chargée de cette mission (Règlement n°2017/1939, art. 4). Son efficacité repose sur la capacité de recueillir librement tous les éléments de preuve pertinents, y compris des témoignages de fonctionnaires européens, lorsque ceux-ci sont susceptibles d'éclairer des faits faisant l'objet d'une enquête pénale. Dans son recours, le PE précise alors que la CCE, en demandant l'organisation des réunions de travail en présence de fonctionnaires autorisés à connaître de l'enquête pénale, a cherché à plusieurs reprises à obtenir un accès , direct ou indirect, aux informations contenues dans le dossier de la procédure, outrepassant sa mission et le cadre de ses compétences telles qu'elles ont été fixées par l'Union.

5. Erreur d'application du protocole sur les privilèges et immunités

Enfin, dans un dernier argument, le PE soulève plusieurs erreurs commises par la CCE tenant à l'interprétation du régime d'immunité des fonctionnaires.

Ainsi, il rappelle, tout d'abord, que les témoins ne bénéficient pas d'immunités empêchant leur audition, contrairement à ce qu'a laissé entendre la Cour des comptes. En effet, qu'il s'agisse du Règlement ou du Protocole, seuls sont visés dans les autorisations préalables les personnes suspectées ou mises en causes dans une procédure (§85 du Règlement), il n'est, en revanche, jamais fait mention des témoins. Ce statut juridique est totalement inexistant dans les textes et semble avoir été oublié par les rédacteurs du Règlement n°2017/1939.

Ainsi, serait-ce à conclure qu'il est possible d'auditionner un fonctionnaire européen sous le régime juridique du témoin, sans qu'il soit nécessaire de requérir une levée d'immunité auprès de son organisme de rattachement ? Ou, au contraire, un tel régime serait inenvisageable dans les procédures menées par le Parquet ?

Rappelons qu'en droit, un témoin est une personne qui vient apporter son concours à une enquête en fournissant toute information qu'il a en sa possession. En procédure, le témoin est une personne libre de ses mouvements et de ses déplacements, sur laquelle ne pèse aucun soupçon ; dans le cas contraire, si des soupçons pèsent sur cette dernière, il faudra modifier son statut et passer sous un autre régime juridique. Donc, en toute logique, rien n'empêcherait le Parquet européen d'entendre des membres de la CCE sous le statut de témoin, ces derniers restant libres de ne pas répondre aux questions s'ils estiment que l'information est couverte par leur immunité et qu'ils violeraient leur obligation statutaire en révélant ladite information, l'action du PE restant soumise à un contrôle juridictionnel effectif. Dans ce contexte, la levée de l'immunité ne prive pas les fonctionnaires de leurs droits procéduraux, elle permet simplement à la justice d'effectuer son travail dans l'intérêt général de l'Union.

Ensuite, dans son recours, le Parquet européen ajoute que les demandes d'audition des témoins sont différentes de celles envoyées à la CCE pour la levée des immunités. En effet, les demandes formulées par le PE relatives aux auditions de personnes ne sont pas les mêmes que les demandes de levées d'immunités. Pour le PE, il n'y a donc pas de contradiction dans sa démarche et il n'est à soulever aucune atteinte à ce régime protecteur pour les membres visés de la CCE.

Mais, au-delà de cette affaire, la question de la levée d'immunité interroge dans le cadre aussi précis que celui d'une enquête pénale diligentée par le Parquet européen. En effet, le Parquet tout comme la CCE (et tout autre organisme européen) ont pour mission de défendre les intérêts financiers de l'Union européenne par leurs compétences respectives dans le but commun d'assurer l'effectivité d'un espace européen sécurisé pour l'ensemble des citoyens

européens. Pourquoi alors ses positions et ses entraves de la part de la CCE ? Quel est le but rechercher ? L'immunité des fonctionnaires européens ne devrait-elle pas s'effacer lorsqu'il est question de défendre les intérêts financiers de l'Union en participant à l'enquête pénale ?

Il est en effet, étonnant ici qu'un organe qui oeuvre, en principe, pour un but commun, semble entraver la bonne marche d'une enquête en détournant, a priori, un mécanisme qui a pour but de protéger le système.

Il semble ici utile de rappeler que la CJUE a déjà eu à connaître de la question des levées d'immunité en rappelant sans discontinuer que l'immunité des fonctionnaires européens ne relève pas d'un privilège personnel mais constitue l'une des garanties de l'indépendance des institutions. Par exemple, dans l'affaire C - 831/18P en date du 18 juin 2020, la Cour a statué sur la levée d'immunité d'un fonctionnaire de l'OLAF. Elle rappelle à l'attendu 47 que « les privilèges et immunités, reconnus par l'Union dans le Protocole n°7, revêtent un caractère fonctionnel en ce qu'ils visent à éviter qu'une entrave soit apportée au fonctionnement et à l'indépendance de l'Union, ce qui implique, en particulier , que les privilèges, immunités et facilités accordées aux fonctionnaires et autres agents de l'Union le sont exclusivement dans l'intérêt de cette dernière (rappelant ainsi l'ordonnance du 13 juillet 1990, Zwartveld e.a., C-2/88[5]). En conséquence, l'immunité accordée aux fonctionnaires européens ne doit intervenir que pour assurer la protection des intérêts de l'Union et non pour assurer un avantage personnel[6]. Elle ne doit pas être utilisée pour faire obstacle à la manifestation de la vérité ou à la poursuite d'infractions graves contre les intérêts financiers de l'UE.

Ainsi, le Parquet européen soutient que la CCE aurait dû apprécier si la levée de l'immunité portait réellement atteinte à l'intérêt de l'Union, ce qui n'était pas le cas en l'espèce, la demande visant uniquement à entendre des témoins dans une procédure impartiale, poursuivant justement ce but, à savoir vérifier la véracité des faits allégués dans le cadre d'une enquête pénale qui comporte, par essence, les garanties de protection des droits des personnes quel que soit le statut sous lequel elles sont entendues, y compris au stade d'une simple audition de témoin[7].

Compte tenu de la position de principe de la CJUE, qui opère un contrôle strict en matière de levée d'immunité en subordonnant cette dernière à la seule protection des intérêts de l'Union tout en garantissant le respect des droits de la défense des personnes concernées[8], il paraît choquant qu'un organisme européen semble se servir d'un mécanisme destiné à assurer la protection des intérêts de l'Union à des fins plus particuliers tenant à la retenue d'informations potentiellement cruciale pour une enquête pénale relative à des faits venant porter atteinte aux intérêts financiers de l'Union.

Un enjeu de gouvernance européenne et de protection des intérêts financiers de l'UE

Cette affaire illustre les tensions entre le Parquet européen et d'autres institutions de l'UE lorsque des fonctionnaires de ces dernières peuvent détenir des informations essentielles dans le cadre d'enquêtes pénales. Elle pose également la question des limites entre le respect des obligations institutionnelles et la préservation du secret des enquêtes pour garantir l'efficacité des poursuites.

Elle s'inscrit dans un contexte où la CJUE a récemment rappelé (affaire C-292/23[9]) que les actes du Parquet européen affectant la situation juridique des personnes doivent pouvoir faire l'objet d'un contrôle juridictionnel, tout en laissant aux États membres le soin de définir les modalités de ce contrôle.

Notons également que cette affaire fait suite à la publication du rapport d'activité du Parquet européen en 2024, dans lequel Laura Kovesi, cheffe du Parquet, avait déjà certains dysfonctionnements dans la prévention et la détection des infractions inscrites dans la Directive PIF (directive (UE) 2017/137) par certaines entités alors que cette mission relevait des prérogatives du Parquet .

Rappelons que, sur le fondement de l'article 86 du Traité sur le fonctionnement de l'Union européenne[10] et par application du Règlement (UE) 2017/1939 du 12 octobre 2017, instituant cette nouvelle entité, le Parquet européen est compétent pour diligenter les enquêtes, effectuer les actes de poursuite et exercer l'action publique devant les juridictions compétentes des États membres participants[11] A ces fins, il traite des « infractions PIF » telles qu'elles sont énumérées

dans la directive de 2017. Y figurent notamment, les fraudes transfrontalières à la TVA entraînant un préjudice d'un montant total d'au moins 10 millions d'euros ; les fraudes aux dépenses et les fraudes douanières ; les corruptions portant atteinte aux intérêts financiers de l'Union européenne ; le détournement de fonds ou d'avoirs européens par un agent public ; le blanchiment de capitaux et toutes infractions indissociablement liées à l'une des catégories susmentionnées. Dans ses missions, le Parquet poursuit également tout auteur d'infraction en lien avec une organisation criminelle lorsque l'objectif du groupement est de commettre une infraction PIF.

Pour réussir sa mission, le Règlement (UE) 2017/1939 a fixé une obligation de coopération des organes européens et nationaux[12] basée sur le mécanisme de la « coopération loyale ». Ainsi, au titre du §69, le texte impose à chaque organe et organismes compétents de l'Union de « soutenir activement les enquêtes et les poursuites menées » par ce dernier dès « qu'un soupçon d'infraction est signalé (...) et jusqu'à ce que ce dernier détermine s'il y a lieu d'engager des poursuites ou de procéder à un classement sans suite »[13]. Si le texte vise expressément EUROJUST, OLAF et EUROPOL, il mentionne que « chaque organe et organisme » européen participe à cette tâche, la Cour des comptes européennes faisant partie de ces organes et étant donc soumise à ces obligations en participant activement aux enquêtes par la communication des pièces demandées, l'audition de personnes disposant d'information et en évitant de constituer un obstacle à la bonne administration de la justice.

L'issue de ce recours sera déterminante en, espérons-le, clarifiant les modalités de levée de confidentialité par les institutions de l'Union lorsqu'il s'agit de simples témoins et non de personnes mises en cause dans une procédure ; en rappelant l'impératif respect de l'indépendance du Parquet européen et en rappelant l'indispensable équilibre entre protection des droits de la défense et efficacité des enquêtes pénales pour lutter contre la fraude aux finances de l'UE.

La décision de la CJUE renforcera ainsi ou réajustera les pratiques de coopération interinstitutionnelle dans la mise en oeuvre effective de la politique pénale européenne au service de l'intérêt financier de l'Union.

Quelle que soit l'issue du contentieux, cette affaire mettra la Cour de justice face à une exigence : affirmer, ou redéfinir, l'équilibre entre les garanties statutaires des fonctionnaires européens et l'exigence d'une justice pénale efficace au service de l'intégrité budgétaire de l'Union.

Notes :

1. Protocole n°7 sur les privilèges et immunités de l'Union européenne, C310/261, 16 décembre 2004, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2004:310:0261:0266:FR:PDF.

2. Règlement (Euratom, CECA, CEE) n° 1473/72 du Conseil, du 30 juin 1972, modifiant le règlement (CEE, Euratom, CECA) n° 259/68 fixant le statut des fonctionnaires des Communautés européennes ainsi que le régime applicable aux autres agents des Communautés, JO L 160 du 16.7.1972, p. 1–16.

3. Recours C/2025/2403, 2ème Moyen.

4. Accord administratif entre la Cour des comptes européenne et le Parquet européen, 3 septembre 2021, https://www.eca.europa.eu/ContentPagesDocuments/Public_scrutiny_of_EU_finances/EPPO-ECA_Working-arrangement_EN.pdf.

5. https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:61988CO0002(01)_SUM.

6. Protocole n°7, art.17 (qui relève du chapitre VII, intitulé « Dispositions générales ») : dispose que les privilèges, immunités et facilités sont accordés, notamment, aux fonctionnaires de l'Union exclusivement dans l'intérêt de cette dernière. En vertu de l'article 17, second alinéa, chaque institution de l'Union est tenue de lever cette immunité dans tous les cas où l'institution concernée estime que cette levée n'est pas contraire aux intérêts de l'Union, Protocole sur les privilèges et immunités de l'Union européenne, C310/261, 16 décembre 2004, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2004:310:0261:0266:FR:PDF.

7. Rappelé par exemple dans : CJUE , Conclusion de l'avocat général Mme E. Sharpston, présentées le 19 décembre 2019., Commission européenne contre RQ., 19/12/2019, C-831/18. Règlement n° 2017/1939, §85 ; Traité sur le fonctionnement de l'Union, art. 114 ; Charte des droits fondamentaux de l'Union, art. 41.

8. La décision de lever l'immunité constitue un acte faisant grief au fonctionnaire concerné, lequel doit donc bénéficier du droit d'être entendu, conformément à l'article 41 de la Charte des droits fondamentaux de l'Union européenne, https://fra.europa.eu/fr/eu-charter/article/41-droit-une-bonne-administration.

9. https://curia.europa.eu/juris/document/document.jsf;jsessionid=8DC92084A870A7161CD0808C6035A47A?text=&docid=297672&pageIndex=0&doclang=FR&mode=req&dir=&occ=first&part=1&cid=377015.

10. Traité sur le fonctionnement de l'Union européenne (version consolidée), art. 86, JO C 202 du 7.6.2016, p. 1-388, https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv%3AOJ.C_.2016.202.01.0001.01.FRA&toc=OJ%3AC%3A2016%3A202%3ATOC#C_2016202FR.01004701.

11. https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-public-prosecutors-office-eppo_fr.

12. Règlement (UE) 2017/1939 du 12 octobre 2017, propos introductifs, § 49 et § 69.

13. Ibid, §69

HACKER ÉTHIQUE ET CYBERSÉCURITÉ

MYRIAM QUÉMÉNER
MAGISTRAT HONORAIRE , DOCTEUR EN DROIT

Les hackers éthiques sont des individus encore méconnus, parfois perçus comme des pirates informatiques qui suscitent fascination ou angoisse. A l'heure où les cyberattaques explosent, il est pertinent de s'intéresser à tous les acteurs pouvant voir un rôle actif de vigilance face à ces incidents de sécurité qui peuvent nuire aux entreprises et aux organisations. Tel est le cas du hacker éthique qui est en quelque sorte une sentinelle de cybersécurité, publié chez Lextenso. proposent une analyse juridique originale pour décrypter l'éthique des hackers et leur contribution essentielle à la cybersécurité

Réglementation actuelle

Soumis à un régime juridique encore non stabilisé , le travail des hackeurs éthiques fait face à plusieurs défis, que ce soit en matière de droit pénal, droit de la propriété intellectuelle, droit des contrats ou encore de droit des données personnelles. En France, pour l'instant, le signalement spontané de vulnérabilités à l'Autorité Nationale de la Sécurité des Système d'Information (ANSSI) par les hackers éthiques est encadré par l'article L.2321-4 du code de la défense. Cet article réserve l'appréciation de la bonne foi du hacker ayant effectué un signalement aux collaborateurs du CERT de l'ANSSI (Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques) sans toutefois en connaître précisément les critères.

Le panorama de la cybermenace de l'année 20241 de l'Anssi indique que les signalants de vulnérabilités bénéficiant de cette protection prévue à l'article L. 2321-4 du Code de la défense (CD) 4] lorsqu'ils agissent de bonne foi ont transmis au CERT-FR 236 signalements de vulnérabilités en 2024. Ces signalements sont transmis par le CERT -FR au propriétaire du service vulnérable (dans le cadre d'une vulnérabilité affectant un service en production, comme un site Web) ou à l'éditeur lorsque la vulnérabilité concerne un produit, en protégeant l'identité du signalant et les circonstances de sa découverte. Pour les vulnérabilités produit, le CERT-FR peut proposer son service de coordination du traitement de la vulnérabilité

Plusieurs propositions législatives ont été réalisées sans avoir été retenues. Deux amendements notamment retiennent l'attention. Le premier, dit "Bluetouff" date de 2016. L'idée était d'ajouter un alinéa à l'article 323-1 du Code pénal pour "protéger les lanceurs d'alerte informatique lorsqu'ils veillent à avertir les responsables du traitement des failles dans leur systèmes". Jugé trop flou, notamment concernant le canal de la remontée d'information ou les suites à donner à cet avertissement, il a été rejeté. D'autant qu'il instaurait une exemption de peine, mais il aurait surtout pu être considéré comme une immunité pénale pour tous les hackers. Le second

amendement déposé dans le cadre de la loi dite “Sapin 2”, prévoyant une exemption de poursuite pour tous les hackers de bonne foi qui aurait averti immédiatement l’autorité administrative ou judiciaire, ou le responsable du système de traitement automatisé de données, a lui aussi été rejeté au motif que l’exemption de poursuite était illégitime face au risque de commission d’infractions annexes, comme par exemple l’extraction frauduleuse de données. Deux refus qui reflètent la difficulté à concilier d’un côté la défense face aux risques d’abus par les hackers d’un cadre juridique trop protecteur, et de l’autre le manque de garantie d’une absence de sanction pour les hackers en cas de signalement. Si aujourd'hui les cybermenaces sont grandissantes, visant aussi bien les entreprises, les collectivités que les hôpitaux, un cadre juridique clair et adapté à la réalité des hackers éthiques pourrait ouvrir la voie à une cyber résilience globale.

Hackers et justice

Les hackers identifiés au terme d’une enquête peuvent faire l’objet de poursuites, notamment sur le fondement des infractions d’atteinte au fonctionnement et aux données contenues dans un système de traitement automatisé de données (STAD). L’entreprise victime de l’acte malveillant pourrait également se prévaloir, selon les circonstances, d’un abus de confiance commis à son préjudice. Selon l’article 323-1 du Code pénal : « Le fait d’accéder ou de se maintenir, frauduleusement, dans tout ou partie d’un système de traitement automatisé de données est puni de trois ans d’emprisonnement et de 100 000€ d’amende. » Lorsqu’il en résulte soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de cinq ans d’emprisonnement et de 150 000 € d’amende.

Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l’encontre d’un système de traitement automatisé de données à caractère personnel mis en oeuvre par l’État, la peine est portée à sept ans d’emprisonnement et à 300 000 € d’amende. Ainsi, le simple fait d’accéder ou de se maintenir frauduleusement dans un système de traitement automatique de données peut être sanctionné par la loi pénale. Or, l’activité du hacker éthique consiste à s’introduire dans un système informatique sans droit d’accès afin de découvrir les éventuelles failles du système. En revanche, tous les hackers éthiques n’agissent pas forcément dans le cadre d’un bug bounty ou d’un audit de sécurité.

Aux termes de l’article 323-3-1 du Code pénal : « Le fait, sans motif légitime, notamment de recherche ou de sécurité informatique, d’importer, de détenir, d’offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l’infraction elle-même ou pour l’infraction la plus sévèrement réprimée ». Les hackers éthiques ne sont pas toujours à l’abri de poursuites sur cette base juridique, par exemple s’ils diffusent des failles de sécurité sans respecter une procédure bien définie avec le client afin d’éviter de nuire à sa réputation numérique.

L’infraction de collecte frauduleuse des données personnelles, punie par l’article 226-18 du Code pénal, a parfois été retenue cumulativement soit avec l’accès frauduleux dans un système de traitement automatisé de données soit avec l’extraction de données visée par l’article 323-3 du Code pénal.

Encadrement et bonnes pratiques

Des solutions juridiques existantes permettant de garantir un minimum d’encadrement pour les hackers éthiques, notamment lorsqu'ils agissent par exemple dans le cadre de contrats de pentests (tests d'intrusion) et de bug bounty, un programme organisé par une entreprise ou une organisation invitant des hackers éthiques à identifier et signaler des vulnérabilités (ou bugs) dans leurs systèmes informatiques, applications, ou sites web. En échange, ces chercheurs reçoivent des récompenses financières ou autres avantages en fonction de la gravité des failles découvertes. L’entreprise organisatrice de ces tests de sécurité devra alors déterminer les services que les hackers pourront explorer. Ces derniers sont soumis, dans leurs contrats, à une

obligation stricte de confidentialité pour ne pas nuire à la réputation de l'entreprise en cas de failles découvertes. Mais attention, ces solutions ne couvrent cependant pas le signalement spontané de vulnérabilités.

Perspectives

Les hackers éthiques ont désormais une place de choix à prendre en matière de vigilance de cybersécurité, à la condition de s'inscrire dans un dispositif contractuel bien défini pour rassurer les organisations et inspirer la confiance. En effet, l'activité des hackers éthiques consistant à signaler les vulnérabilités des systèmes informatiques afin de les corriger, elle renforce la cybersécurité de manière générale. L'intérêt grandissant pour l'activité des hackers éthiques se reflète notamment avec le développement considérable des programmes de bug bounty. Face à la complexification technique des cybermenaces, se passer des hackers éthiques semble être un risque pour la protection des systèmes informatiques. Il n'est donc pas dans l'intérêt public de restreindre l'activité de ces véritables lanceurs d'alerte informatique.

L'ouvrage « Hackers éthiques et cybersécurité – Opportunités et défis » propose ainsi une véritable doctrine de cybersécurité pour les hackers éthiques qui ont toute leur place dans la protection des systèmes d'information des organisations, des entreprises et des collectivités territoriales. Les préconisations suggérées résultent d'idées de différents professionnels de la cybersécurité interrogés et de l'analyse de réglementations étrangères comme la Belgique et la Suisse. La loi suisse prévoit que la détection de failles de sécurité sans mandat explicite et sans consentement est punissable dès lors qu'est franchie la protection d'accès d'un système tiers ou que l'on tente de le faire. Mais, le hacking éthique n'est pas considéré comme une infraction si l'état de nécessité licite est invoqué. En 2023, le Conseil fédéral de la République Helvétique est allé plus loin encore, adoptant un rapport visant à institutionnaliser le hacking éthique. En France, fixer un cadre juridique précis au hacker et hacking éthique apparaît essentiel pour que cette pratique puisse se développer de façon sécurisée en toute confiance pour les entreprises y ayant recours. La promotion par des acteurs institutionnels de hackathons contribue également à renforcer cette confiance.Compte tenu du contexte actuel où la vigilance doit redoubler , les hackers éthiques peuvent apporter une véritable plus value dans les stratégies de cybersécurité des entreprises et des organisations.

Notes :

1.https://www.cert.ssi.gouv.fr/uploads/CERTFR-2025-CTI-003.pdf

Sommaire du livre

Hackers éthiques et cybersécurité

Opportunités et défis

LES GOLDEN VISAS À L'ÉPREUVE DE LA VIGILANCE EUROPÉENNE : LE REGARD D'UN EX-AVOCAT EXTRA-EUROPÉEN

MARCUS SWENSON DE LIMA
ANCIEN AVOCAT BRÉSILIEN, DIPLÔMÉ EN MASTER DE DROIT, ÉCONOMIE, GESTION MENTION DROIT DES AFFAIRES PARCOURS TYPE INVESTIGATIONS FINANCIÈRES À L'ÉCHELLE EUROPÉENNE – UNIVERSITÉ DE STRASBOURG

Introduction

La citoyenneté, un droit ou une marchandise de luxe ?

Ce n'est pas nouveau dans l'histoire de l'humanité qu'il existe une formule d'échange entre l'argent et l'acceptation dans une caste privilégiée. Cette pratique remonte à la Rome antique, mais j'oserais dire qu'on peut aller plus loin même, jusqu'à la création de la monnaie, environ 2.000 a. J.C.

L'Union européenne, entité politique fondée sur la libre circulation, la coopération et la solidarité entre ses États membres, est confrontée à une tension structurelle : le combat à « la vente de citoyenneté européenne » par le biais des programmes dits de "résidence ou citoyenneté par investissement". Ces programmes ont ouvert la porte à des investisseurs non-européens — souvent fortunés — en échange d'un apport économique substantiel. Ces mécanismes, appelés communément "Golden Visas" ou « Golden Passeport », soulèvent des profondes interrogations de la part de l'opinion publique et les couloir du parlement à Bruxelles.

Peut-être qu'avez-vous, lecteur, entendu parler de cette question dans un passé récent, notamment dans la période entre crise économique de 2008 à crise sanitaire de 2020. Mais comme d'autres questions ont surgi et ont dominé (ou dominent encore) les titres de la presse, peut-être que vous pensez que ces programmes ont disparu… Désolé, mais non!

Ils sont toujours là ! Quasi comme le nom du film brésilien qui a gagné l'Oscar cette année. Et pour continuer dans le même secteur, la vigilance de l'Union Européenne sur ce sujet jusqu'à maintenant est digne d'un scénario de film comique.

Les étudiants en Droit, apprennent dès que leur entrée en étude que le droit n'est pas une science exacte, comme la Mathématique par exemple. Selon les règles de la science de Descartes 2 + 2 deviennent 4. Selon le Droit, 2 + 2 peuvent être 4, ou 22, ou même 2 + 2, tout simplement. Je me permets cette petite digression philosophique dans cette introduction pour illustrer qu'entre la théorie et la réalité dans l'univers juridique, il existe une énorme variété de possibilités. Un excellente illustration réside dans ces programmes de golden visa/golden passeport.

S'ils peuvent servir à une stratégie d'attractivité légitime pour les États en quête d'investissements, ils peuvent également servir d'instruments pour dissimuler la criminalité, lorsque le processus est conduit d'une façon obscure. C'est dans ce contexte que la question sur la vigilance, thématique centrale de cette réflexion, se manifeste.

Quelle vigilance les États-membres exercent (ou doivent exercer) lorsqu'ils ouvrent leur passeport à l'achat ? Quelle est (ou doivent être) le rôle de l'Union Européenne dans ce contexte ?

Grâce à une caractéristique unique de ces programmes (ou produit), ou son producteur exclusif et son régulateur utilise la même casquette, sans aucune obligation de transparence et… voilà ! vous avez un produit très

approprié pour servir d'instruments pour la corruption, blanchiment et ses délits assimilés.

Et puisque rien n'est si mauvais qu'il ne puisse empirer, si la nouvelle vague de memecoins créés par des présidents qui se croient au-dessus de tout et de tous prend de l'ampleur, comme nous l'avons vu récemment en janvier de cette année, nous pourrions atteindre le point absurde de créer un marché des passeports avec des prix stipulés en memecoins. S'il y a une chose que j'ai apprise tout au long de ma vie professionnelle, c'est de ne jamais douter de la créativité des êtres humains pour aggraver ce qui est déjà mauvais. Le réchauffement climatique parle pour lui-même.

Loin de vouloir ni trancher dans un débat trop introspectif sur ce sujet, ni d'avoir la prétention de dire aux européens comment ils doivent se protéger, cet article propose d'explorer — à travers le regard critique d'un citoyen extra-européen — les contradictions que ces programmes font peser sur la cohérence européenne. En effet, au-delà des règles de droit et des chiffres, c'est bien la notion de confiance, l'un des piliers du projet européen, qui est en échec.

I. Une stratégie d'attractivité aux limites de la souveraineté et de la coopération loyale

Les programmes de citoyenneté ou de résidence par investissement ne sont pas le fruit d'une opportunité, d'un hasard. Leur généalogie remonte dans l'occident aux années 1980, avec les professionnalisations des initiatives émanant de pays non-européens (notamment dans les Caraïbes et l'Amérique du Nord) qui proposaient des droits de séjour ou la nationalité contre un investissement[1].

C'est curieusement en Europe, le créateur de l'État moderne et l'inventeur contemporain du modèle de citoyenneté supranationale unique au monde, qu'une nouvelle génération de programmes centrée sur l'argent avant tout a commencé à apparaitre et à gagner de la force pendant la crise économique de 2008 (plus précisément de 2007 à 2009). Pour donner un exemple, en 2016, chaque État membre de l'UE avait adopté au moins un mécanisme légal pour faciliter la migration basée sur ces programmes.

Notons tout de même que si, aujourd'hui, plusieurs d'entre eux ont déjà déclaré d'avoir arrêté leurs programmes, il n'est pas difficile de trouver les mêmes offres sur internet, après une euphémisation de l'ancien nom. Comment ces programmes fonctionnent-ils effectivement ?

Le mécanisme est assez simple : une personne non européenne décide d'investir un montant significatif dans un pays de l'UE qui offre ces programmes et obtient en retour le droit de séjourne, ou directement un passeport, de ce pays. Normalement, les demandes se font dans le domaine de l'immobilier, ou dans celui des fonds de l'État. La principal différence entre les programmes entre ceux qui offre un droit de séjour (Golden Visa) et celui qui offre directement le passeport (Golden Passeport) est le facteur temps.

Dans le premier cas, il est nécessaire d'attendre quelques années avant de pouvoir demander son passeport. N'oublions pas que le temps est un facteur primordial mais il s'accompagne d'une autre considération, celui du prix. La nécessité d'obtenir directement un passeport a bien évidemment son prix.

Du point de vue d'un expatrié, la démarche semble rationnelle pour les «investisseurs», qui auront accès à une libre circulation dans presque tout l'Europe, exception de visas pour aller dans d'autre pays développés, ou même de s'assurer contre l'instabilité politique ou la tyrannie de son pays d'origine. En d'autres termes, c'est une espèce de « plan B ».

Cette solution pourra sembler avantageuse aussi aux États, qui pourront attirer des capitaux et générer de l'investissement direct de l'étranger . C'est également, pour certains acteurs, une manière de relancer un secteur économique ou une région en tension. Au premier regard, cela ressemble à une situation gagnant-gagnant, sauf que, dans la « réalité », la « théorie » est toute autre.

En effet, avec tous ces manquements de vigilance et de transparence, ou de corruption, la réalité est qu'il s'agit d'une véritable situation perdant-perdant que ce soit pour l'Union ou pour la société. Aujourd'hui, les vrais gagnant sont des criminels qui se présentent comme des « investisseurs ». Les corrompus profitent alors du manque de transparence de ces programmes pour s'enrichir à leur tour.

Il est alors légitime de s'interroger sur la position de l'Union européenne qui semble accepter une telle situation. Il est vrai que le bloc se caractérise par une organisation très particulière rendant plus complexe son système juridique mêlant règles et principes hiérarchisés.

Dans ce contexte, le Traité sur L'Union Européenne[2] contient deux principes juridiques que s'opposent : le principe de souveraineté de chaque pays lui permettant de décider de sa politique d'immigration et le principe de la coopération loyale entre ces membres, imposant le respect et l'assistance mutuellement dans l'accomplissement du bien commun de l'Union.

Alors, si le pouvoir de décider la politique immigratoire appartient à chaque État mais que la sécurité implique que tous les membres agissent de concert, quel est le principe faire prévaloir ?

La réponse la plus logique serait la suivante : si vous voulez appartenir à une groupe, une communauté, un bloc ou n'importe quel nom vous voulez donner à ce type d'association, la première règle doit être le bien-être commun avant le bien-être d'un individu considéré séparément. Dans le cas contraire, ce n'est pas une association, une union, c'est un cauchemar. Néanmoins, la réponse juridique n'est pas aussi simple qu'il n'y paraît.

II. Pour une vigilance, une transparence et une gouvernance partagées

Les institutions européennes n'ont pas ignoré les déviations de ces programmes. La Commission, le Parlement et plusieurs agences européennes ont régulièrement appelé à la suppression ou à la réforme des dispositifs existants, au nom de l'intérêt commun. Des rapports, des résolutions, des recommandations ont été émis, notamment après l'invasion de l'Ukraine par la Russie ou des affaires de corruption liées à certains programmes[3].

Toutefois de fortes résistances persistent. Pour certains États, la compétence exclusive en la matière a été décidée, notamment pour les pays de petite taille car ces programmes représentent un levier budgétaire non négligeable. Dans ce contexte, toute tentative d'harmonisation ou suppression de ces programmes apparaît une menace à sa souveraineté ou même une ingérence inacceptable à leurs yeux.

Serait-ce alors à dire que le devoir de vigilance des États-membres et/ou du bloc devrait être perçu comme une entrave ? ou la vigilance doit-elle être identifiée comme une nécessité, pour la confiance entre les membres ?

Pour donner un exemple, un rapport publié début 2019 de la Commission au Parlement Européen[4], adressé au Conseil, a exposé les principaux risques pour l'UE liés à ces programmes, spécialement, contre la sécurité du bloc ou liés au blanchiment de capitaux ou la fraude fiscale.

Sur la question de la sécurité du bloc, le rapport mentionne que « l'absence de contrôles aux frontières intérieures de l'espace Schengen rend particulièrement importante la mise en oeuvre de contrôles préventifs de sécurité adéquats et convenus d'un commun accord », mais qui n'ont pas encore été créées. Tout ce qui existe se résume en « des dispositions législatives ou des lignes directrices très limitées ».

La défaillance est si importante qu'elle permet aux demandeurs de comparer et choisir les pays présentant les conditions moins strictes, puisqu'il n'y a pas d'un service centrale de renseignement et d'enquêtes au sein de l'Union pour l'échange des informations ; « les États membres ne s'informent pas mutuellement des demandeurs rejetés », même s'ils ont été refusés pour un motif de risques pour la sécurité. Ainsi, un requérant dont la demande de citoyenneté a été refusée sur un territoire avait la possibilité de présenter une nouvelle demande dans un autre État membre.

Selon le rapport, la situation est un peu meilleure en ce qui concerne les visas. Pour assurer qu'ils ne constituent pas une menace à l'ordre et la sécurité publics de ces membres, les accords européens prévoient déjà certaines obligations concernant les contrôles de sécurité qui doivent être effectués avant la délivrance d'un visa aux investisseurs étrangers, comme la consultation dans un système central d'information à propos des prétendants, le système d'information Schengen – SIS (et à partir de 2013 SIS II, deuxième génération)[5].

Si cette personne a été refusée et signalée par un autre pays dans le système, les pays sollicités qui veulent donner le visa doivent prendre en compte les intérêts aussi du pays qui a refusé en premier lieu. Malgré cela, il y a encore un manque d'informations

disponibles et une marge de manoeuvre importante dans la manière dont les États membres abordent ces problèmes. Mais c'est déjà un début.

Il est alors légitime de se demander pourquoi les États-membres n'utilisent pas, au moins, le même système pour les demandes de citoyennetés. Dans un espace de libre circulation de personnes et marchandises, le minimum que s'espère d'un groupe qui est le 3ème PIB du monde est qui ils fassent face au challenge du monde moderne en matière de vigilance, transparence et gouvernance partagées, avec une base commune de due diligence renforcée et échange des informations.

Il existe également des contrôles postérieurs pour vérifier que les conditions dans lesquelles les droits de séjour ont été accordés sont toujours respectées, mais seulement dans un nombre limité de cas. Toutefois, comme les titulaires peuvent résider dans un autre État membre et pas nécessairement dans l'État qui a accordé le visa (même après une période de séjour minimale dans le pays d'accueil), cette vérification s'avère très difficile dans la pratique.

III. Vigilance collective compromise : profits privés, risques partagés

Si des progrès ont été réalisés dans la lutte contre le blanchiment d'argent avec les directives du Parlement européen et du Conseil de 2015 et 2018, concernant les fraudes fiscales il reste quand même la possibilité pour les acquéreurs de la deuxième nationalité de bénéficier de ces programmes pour choisir les règles fiscales les plus souples d'un pays voisin pour pouvoir dissimuler presque tranquillement leurs opérations frauduleuses d'évasion fiscale en contournant les accords de coopération entre les administrations fiscales.

Les progrès qui ont été réalisés par les directives dans le domaine LCB/FT[6]– avec notamment les signalements des transactions suspectes pour les entités assujetties privés (banques, agents immobiliers, PSAN etc.) à la cellule de renseignement financier de leur pays, le contrôle préalable renforcé sur les ressortissants de pays tiers à haut risque et plus spécifiquement pour les investisseurs de programmes de golden visas, en exigeant une vigilance renforcée dans tous les transactions des transferts de capitaux pour ces programmes – ne sont pas suffisantes, car elles ont « oublié » d'inclure les organisations et agences gouvernementales comme entités assujetties. Qui sont les responsables pour analyser et traiter les dossiers des candidats à un golden visa/passeport ?

Si les agents gouvernementaux ne sont pas considérés comme entités assujetties, il ne leurs est pas fait obligations de signaler des transactions suspectes. Ceci démontre que les directives ont permis une avancée mais incomplète et parfois elles peuvent même être contre-productives, en transférant la responsabilité de vigilance et contrôles vers les particuliers, aux banques et autres intermédiaires, qui n'analyseront jamais les prétendants (et souvent leurs futurs clients) dans la même perspective de risque que les autorités publiques. In fine, les directives finissent par être perçues comme une simple « check the box ».

Toutes ces risques pourraient être réduites si les membres de l'UE choisissaient d'être plus vigilants et plus transparents, en créant une gouvernance centralisée et partageant des informations entre eux.

Dans de nombreux cas, les données sur les bénéficiaires, les montants, les contrôles effectués, voire les décisions finales, ne sont ni centralisées ni publiques. Certains pays avaient même confié la gestion quasi intégrale de ces programmes à des entités privées affaiblissant (ou qui a affaibli) encore les exigences de vigilance publique.

L'espace européen repose sur la confiance mutuelle entre ses membres. Lorsque l'un d'eux ouvre sa porte d'entrée, c'est l'ensemble de l'Union qui en assume les conséquences. Dans un tel système, l'absence de vigilance d'un seul maillon peut compromettre la chaîne tout entière.

Au-delà de l'enjeu symbolique, la difficulté m'apparaitre de faire comprendre aux États membres offrant ce programmes que la privatisation des profits et la mutualisation des risques — probablement le principe le plus important dans le monde capitaliste d'aujourd'hui — n'est pas la meilleur choix pour l'Union au long terme.

Conclusion

Comme il n'y a pas de base de compétence assez claire pour

une action législative de l'UE - qui devra nécessairement passer par une révision des traités selon les juristes européens - il me semble que le combat doit se joue sur le terrain des principes : solidarité, coopération loyale, intégrité du marché intérieur, pour n'en citer que quelques-uns, car sont là que le devoir de vigilance prend tout son sens, comme devoir politique, exigence juridique et responsabilité collective.

Ce qui est en jeu n'est pas simplement un conflit entre la souveraineté d'un État membre de décider de sa politique d'immigration et la politique de sécurité de l'Union européenne, c'est le concept qui est en jeu, un concept de la solidarité, de la citoyenneté européenne et, in fine, de l'Union européenne elle -même.

Ça fait plus de 30 ans - depuis le traité de Maastricht de 1992, qu'a créé ce premier concept de la citoyenneté européenne liée à la nationalité des États membres - qu'il existe une controverse et une confusion entre les deux termes, citoyenneté et nationalité, qui sont souvent utilisés comme synonymes.

La nationalité exprime une relation entre un État et un individu, conformément aux principes de droit international adoptés par la Cour de justice de l'Union européenne, tandis que la citoyenneté européenne c'est un mécanisme qui s'ajoute automatiquement à la nationalité des États membres, une espèce de citoyenneté supranationale.

La controverse existe, sûrement. Il y a ceux qui disent que l'idée d'un citoyen européen est politiquement et juridiquement faible, qu'elle est de nature dérivée (elle dérive justement des nationalités des États membres). Ainsi cette idée de citoyenneté de l'Union est plus un concept économique que juridique. D'autres qui affirment que cette idée de la citoyenneté européenne est fondamentale pour l'Union Européenne, pour représenter elle-même la loyauté entre les État-membres et la principale raison d'existence de l'UE.

En attendant une action législative du Parlement européenne, le seul contrôle qu'existe déjà et les États membres ont choisi pour pragmatisme d'accepter, est le contrôle judiciaire, en accord avec les traités et principes internationaux. Mais le problème d'utiliser du contrôle judiciaire pour réguler ce système est que, par définition, le contrôle judiciaire est exercé à postériori.

Un récent arrêt de 29 d'avril de 2025, de la Cour de justice de l'Union européenne CJUE), dans l'affaire C-181/23 - Commission/Malte (Citoyenneté par investissement), a indiqué que « si la définition des conditions d'octroi et de perte de la nationalité d'un État membre relève de la compétence nationale, cette compétence doit être exercée dans le respect du droit de l'Union. Le lien de nationalité avec un État membre repose sur un rapport spécifique de solidarité, de loyauté et de réciprocité des droits et devoirs entre l'État et ses citoyens ».

Il poursuit « Lorsqu'un État membre accorde la nationalité, et donc automatiquement la citoyenneté de l'Union, en échange direct d'investissements ou de paiements prédéterminés via une procédure transactionnelle, il viole manifestement ces principes. Une telle « commercialisation » du statut de citoyen est incompatible avec la conception fondamentale de la citoyenneté de l'Union définie par les traités. Elle enfreint le principe de coopération loyale et met en péril la confiance mutuelle entre États membres concernant l'attribution de leur nationalité ».

Le signal de la CJUE est donc clair adopter une vigilance active et collective s'impose. C'est refuser que la liberté de circulation devienne un privilège achetable. C'est protéger l'intégrité du projet européen face à la vente de leur nationalité qui menace ses fondements.

La confiance se gagne, mais surtout elle se garde. Mieux vaut agir avant qu'il ne soit trop tard.

Notes :

1. BRILLAUD L., MARTINI M., European getaway : Inside the murky world of golden visas, Transp. Int., 2018, p. 08.

2. https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0002.02/DOC_1&format=PDF.

3. Recommandation C(2022)/2028/UE du Conseil de L'Union Européenne du 28 mars 2022 concernant sur les mesures immédiates à prendre dans le contexte de l'invasion russe de l'Ukraine en ce qui concerne les programmes de citoyenneté des investisseurs et les programmes de résidence des investisseurs. https://data.consilium.europa.eu/doc/document/ST-7916-2022-INIT/en/pdf.

4. Rapport de la Commission au Parlement Européen, au Conseil, au Comité Économique et Social Européen et au Comité des Régions. Programmes de citoyenneté et de résidence par investissement dans l'Union européenne, https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52019DC0012.

5. Ibid.

6. 4è Directive (UE) 2015/849 et 5è Directive (UE) 2018/843, du Parlement européen et du Conseil

SILK ROAD :
LE PREMIER GRAND MARCHÉ NOIR DU DARK WEB
ÉPISODE 1 :
LA NAISSANCE D'UN EMPIRE CLANDESTIN (2011-2012)

SÉBASTIEN DUPENT

PROFESSEUR AGRÉGÉ D'ÉCONOMIE ET GESTION, OPTION SYSTÈMES D'INFORMATION, ENSEIGNANT LA CYBERSÉCURITÉ AU LYCÉE RENÉ CASSIN À STRASBOURG ET AU CNED.
FORMATEUR ACADÉMIQUE EN SCIENCES NUMÉRIQUES ET TECHNOLOGIE (SNT) AINSI QU'EN CYBERSÉCURITÉ. INTERVENANT SUR LES THÉMATIQUES DES FRAUDES INFORMATIQUES ET DE L'UTILISATION DES OUTILS NUMÉRIQUES DANS LES ENQUÊTES FINANCIÈRES AUPRÈS DES ÉTUDIANTS EN MASTER JCCO ET IFEE À L'UNIVERSITÉ DE STRASBOURG.
RÉSERVISTE CITOYENNE AU SEIN DE LA GENDARMERIE NATIONALE

Introduction : Le contexte et les motivations

A. Présentation de Ross Ulbricht : son parcours universitaire (physique et cristallographie) et ses idéaux libertariens

Ross Ulbricht naquit le 27 mars 1984 à Austin, au coeur du Texas, dans une famille américaine ordinaire. Rien, dans les premières années de son existence, ne laissait présager qu'il deviendrait un jour l'architecte d'un empire clandestin défiant les lois et les institutions. Élevé dans une maison où régnaient la discipline et les valeurs traditionnelles, il grandit entre les collines verdoyantes et les vastes plaines de son État natal, nourrissant une curiosité insatiable pour le monde qui l'entourait.

Dès ses jeunes années, Ross se distingua par son esprit brillant et sa soif de savoir. Élève studieux, il obtint des résultats exceptionnels au SAT Reasoning Test, ce qui lui ouvrit les portes de l'Université du Texas à Dallas. Là-bas, il s'immergea dans l'étude des sciences physiques, explorant les mystères de l'univers avec la rigueur d'un chercheur en quête de vérité. Diplômé en 2006 avec les honneurs, il poursuivit son chemin vers l'Université d'État de Pennsylvanie, où il se spécialisa en cristallographie. Ses travaux scientifiques, précis et méthodiques, témoignaient déjà d'un esprit analytique hors du commun.

Ce fut toutefois à Penn State que Ross Ulbricht connut une transformation profonde. Au-delà des équations et des structures cristallines qu'il étudiait avec passion, il découvrit un univers idéologique qui allait bouleverser sa vision du monde : le libertarianisme. Inspiré par les écrits de Ludwig von Mises et les discours enflammés de Ron Paul, il embrassa cette philosophie prônant la liberté individuelle absolue et dénonçant la coercition exercée par les gouvernements. Pour Ross, l'État n'était qu'un obstacle à l'épanouissement humain, un oppresseur masqué derrière des lois et des institutions..

Dans ses réflexions nocturnes, il rêvait d'un monde affranchi des chaînes de la violence systémique et de la surveillance étatique. « Je veux abolir toute forme d'agression entre les êtres humains », écrivait-il sur sa page LinkedIn, comme un manifeste adressé à ceux qui partageaient ses idéaux. Il imaginait une société où chacun pourrait commercer librement sans crainte ni entrave – une utopie anarchique où l'économie serait le terrain d'expression ultime de la liberté.

Ainsi germa dans son esprit l'idée qui allait changer sa vie : créer une plateforme numérique incarnant ses principes libertariens. Ce projet ne serait pas seulement un outil technologique ; ce serait une révolution silencieuse contre l'ordre établi. En janvier 2011, sous le pseudonyme énigmatique de « Dread Pirate Roberts », inspiré du film « The Princess Bride », Ross Ulbricht donna vie à « Silk Road », un marché clandestin niché dans les profondeurs du

réseau Tor. Mais derrière cette création audacieuse se cachait un homme complexe – à la fois idéaliste et pragmatique –, prêt à défier les puissances du monde pour donner corps à ses rêves libertaires.

B. Sa vision philosophique : un marché libre basé sur l'anonymat et la cryptomonnaie, permettant aux individus de commercer sans restrictions ni violence

Ross Ulbricht, ce jeune homme à l'esprit ardent et à l'intelligence acérée, n'était pas seulement un scientifique ; il était, en son for intérieur, un penseur, un rêveur, un architecte d'idées. Ses études en physique et cristallographie lui avaient appris à décomposer les structures les plus complexes pour en révéler la pureté des formes élémentaires. Mais ce qu'il voulait déconstruire désormais, ce n'était plus un cristal ; c'était le grand édifice de la société moderne, ce colosse oppressant qui pesait sur les libertés individuelles.

Dans les méandres de ses réflexions philosophiques, Ross concevait une vision audacieuse et radicale : celle d'un marché libre, affranchi des chaînes de l'autorité étatique et des contrôles oppressifs. Ce marché ne serait pas un lieu physique, mais une agora numérique où chaque individu pourrait commercer selon ses désirs, sans entraves ni jugements. Il rêvait d'un espace où la main invisible de l'économie pourrait enfin s'exprimer dans sa forme la plus pure, sans être ralentie par les lourdes mains des gouvernements et des institutions.

Pour Ross, le commerce n'était pas seulement une transaction ; c'était une expression de la liberté humaine. Il croyait fermement que chaque homme et chaque femme avait le droit naturel de choisir ce qu'il achetait ou vendait, sans avoir à rendre compte à quiconque. Mais comment créer un tel sanctuaire dans un monde où les regards indiscrets des autorités scrutaient chaque mouvement ? La réponse lui vint sous la forme d'une technologie révolutionnaire : le Bitcoin.

Cette monnaie numérique, encore méconnue en 2011, était pour lui une clé ouvrant les portes d'un nouveau monde. Grâce à sa nature décentralisée et son anonymat intrinsèque, elle permettait aux individus de réaliser des transactions sans laisser de trace. Associée au réseau Tor, qui masquait l'identité des utilisateurs derrière des couches de cryptage impénétrables, elle offrait une promesse presque mystique : celle de l'invisibilité totale. Ross voyait dans cette combinaison le fondement d'un marché libre où chacun pourrait commercer sans peur ni violence.

Son rêve, toutefois, dépassait largement l'aspect technique. Il voulait bâtir un lieu où les principes libertariens triompheraient sur les lois coercitives des nations. Dans ses écrits et ses pensées solitaires, il décrivait un monde où la liberté individuelle serait sacrée, où nul ne serait contraint par la force ou par la peur. Ce marché numérique serait une révolution pacifique contre les systèmes oppressifs qui régnaient depuis des siècles.

Ainsi naquit *Silk Road*, non pas comme une simple plateforme de commerce clandestin, mais comme une utopie numérique façonnée par un idéaliste convaincu. Sous le pseudonyme mystérieux de Dread Pirate Roberts, Ross Ulbricht devint le capitaine d'un vaisseau virtuel naviguant dans les eaux obscures du dark web. À ses yeux, il ne faisait pas que vendre des produits ; il offrait aux hommes et aux femmes un refuge contre la tyrannie du monde moderne. Toutefois, à l'image des songes démesurés, celui-ci portait en lui les germes de sa propre chute.

C. Création de *Silk Road* en janvier 2011 : une plateforme révolutionnaire utilisant Tor et Bitcoin.

En ce mois de janvier 2011, alors que l'hiver étendait son voile glacé sur les rues d'Austin, une révolution silencieuse prenait forme dans l'esprit d'un homme. Ross Ulbricht, jeune idéaliste aux ambitions démesurées, s'apprêtait à poser la première pierre d'un édifice numérique qui allait bouleverser les fondements mêmes du commerce et de la justice. Dans la pénombre d'une chambre modeste, éclairée par la lueur vacillante d'un écran d'ordinateur, il donna vie à *Silk Road*, un marché clandestin niché dans les profondeurs insondables du réseau Tor.

Le projet était audacieux, presque utopique. Ross avait imaginé un lieu où l'anonymat serait absolu,

où chaque transaction s'accomplirait dans le secret le plus total grâce à Bitcoin, cette monnaie numérique encore balbutiante. Tor, avec ses labyrinthes cryptés et ses portes invisibles, serait le rempart contre les regards intrusifs des autorités. Le commerce y serait libre, affranchi des lois et des jugements moraux. Seules les violences extrêmes – assassinats et pédophilie – y seraient bannies, car même dans son anarchisme radical, Ross croyait en une éthique fondamentale.

Il choisit pour pseudonyme Dread Pirate Roberts, nom emprunté à un personnage fictif du film The Princess Bride. Ce choix n'était pas anodin : il symbolisait l'idée que le pouvoir pouvait être transmis sans révéler l'identité réelle de son détenteur. *Silk Road* ne serait pas seulement un site ; ce serait une idée, une philosophie incarnée par un nom qui pourrait survivre au-delà de son créateur.

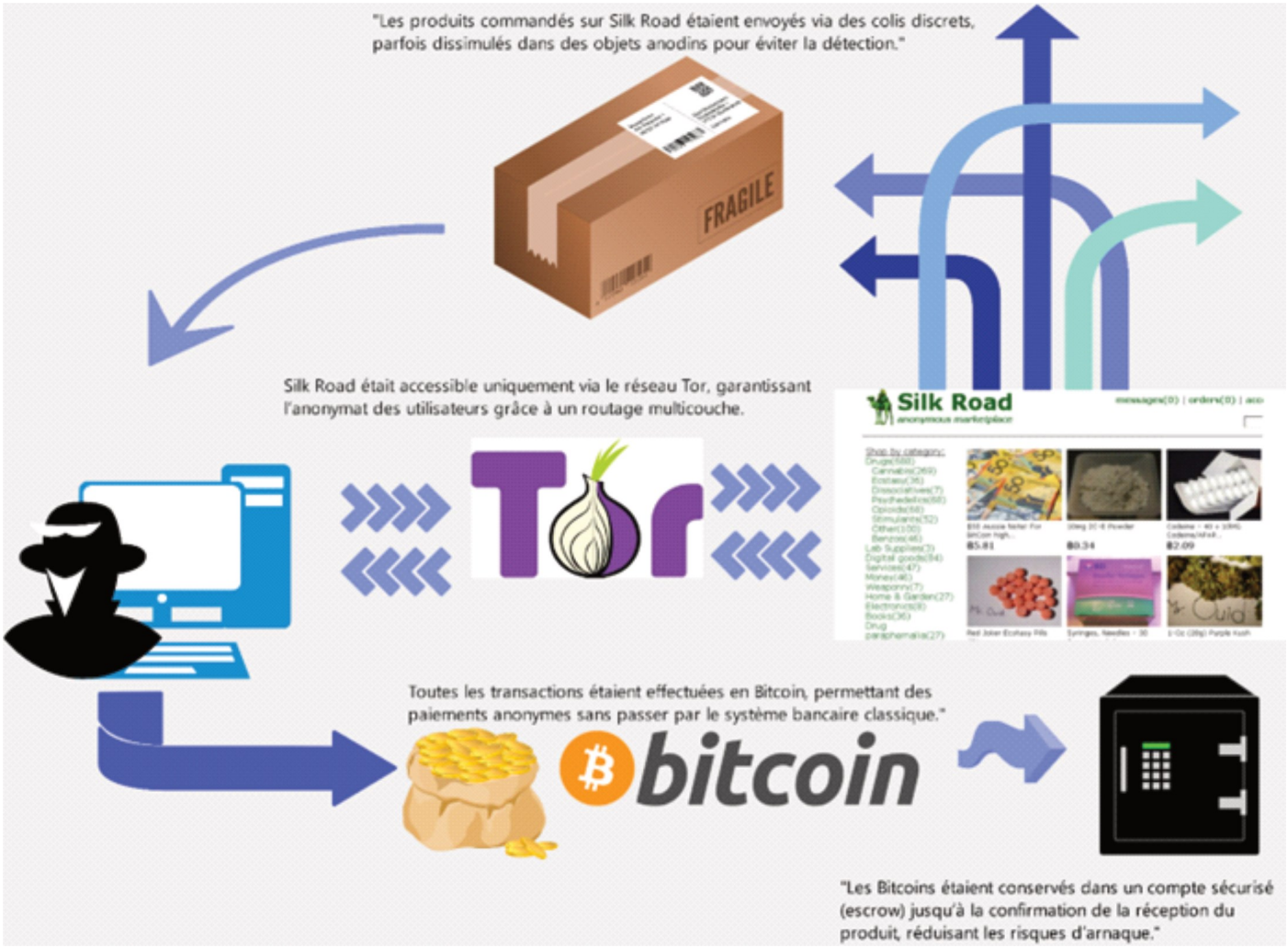
Lorsque Ross mit en ligne *Silk Road*, il savait qu'il pénétrait dans un territoire inconnu. Ce marché numérique était une oeuvre d'art clandestine, un défi lancé aux institutions et aux normes établies. Les premiers utilisateurs furent des pionniers eux-mêmes : hackers, libertariens et trafiquants en quête de discrétion. Rapidement, les échanges se multiplièrent. Drogues rares, faux papiers et logiciels interdits circulaient dans cet espace virtuel comme autant de marchandises sur une route ancienne reliant des mondes éloignés.

Ainsi naquit *Silk Road*, non pas dans le fracas des révolutions traditionnelles mais dans le silence feutré du dark web. Ross Ulbricht venait de créer une plateforme révolutionnaire où se mêlaient technologie et idéologie, anonymat et liberté. Mais derrière cette façade brillante se cachait une ombre grandissante – celle des autorités qui bientôt découvriraient ce marché clandestin et entameraient leur chasse à l'homme contre celui qui se faisait appeler Dread Pirate Roberts.

Chapitre 1 : Les débuts d'une idée audacieuse

A. Silk Road : anonymat via Tor, paiements en Bitcoin, interdiction des actes violents (assassinats, pédophilie)

Dans les méandres insoupçonnés du réseau Tor, où l'obscurité numérique se mêle aux ambitions humaines, un marché singulier vit le jour en janvier 2011. Baptisé « *Silk Road* », il n'était pas seulement une plateforme clandestine ; il était le reflet d'une idée audacieuse, presque utopique. Ross Ulbricht, son créateur, dissimulé sous le pseudonyme énigmatique de



« Dread Pirate Roberts », rêvait d'un espace où la liberté individuelle et l'anonymat absolu aboliraient les contraintes imposées par les institutions. Ce projet, à la fois visionnaire et troublant, allait bouleverser à jamais l'histoire de l'internet et des cryptomonnaies.

Le fonctionnement de *Silk Road* reposait sur deux piliers technologiques novateurs : le réseau Tor et la cryptomonnaie Bitcoin. Tor, ce réseau aux allures d'oignon dont les couches successives de chiffrement protégeaient les utilisateurs comme une armure impénétrable, permettait à chacun de naviguer sans laisser de trace. Les adresses IP des acheteurs et vendeurs disparaissaient dans les méandres des noeuds intermédiaires, rendant impossible toute identification. Ce voile d'anonymat était essentiel pour garantir la sécurité des transactions et préserver l'identité des protagonistes.

Le Bitcoin, quant à lui, jouait le rôle de monnaie universelle dans ce marché clandestin. Cette cryptomonnaie naissante, encore méconnue du grand public, permettait des paiements pseudonymes inscrits sur la blockchain mais dissociés de toute identité réelle. Chaque transaction était une danse silencieuse entre deux adresses numériques, invisibles aux yeux des autorités. Les fonds circulaient comme des ombres insaisissables dans un monde où la lumière ne pénétrait jamais.

Silk Road n'était pourtant pas un chaos anarchique ; il avait ses règles, ses principes. Ross Ulbricht avait interdit catégoriquement tout acte violent sur sa plateforme. Les assassinats et la pédophilie y étaient proscrits avec une fermeté absolue. À ses yeux, son marché devait être un sanctuaire pour le commerce libre, non une enclave pour les ténèbres humaines. Les stupéfiants, les faux papiers et les logiciels interdits y circulaient certes en abondance, mais toujours dans le respect d'une éthique libertarienne qui rejetait la coercition et la brutalité.

Ainsi fonctionnait *Silk Road*, ce bazar numérique niché dans l'ombre du dark web. Pour ses utilisateurs, il était un refuge contre les lois oppressives ; pour ses détracteurs, il était une menace contre l'ordre établi. Mais dans cette dualité résidait toute l'ambition de Ross Ulbricht : créer un espace où l'anonymat serait roi et où chaque individu pourrait commercer librement sans peur ni jugement. Pourtant, derrière cette façade d'idéal libertarien se profilait déjà l'ombre des autorités qui guettaient ce royaume clandestin avec une patience implacable.

B. Premiers utilisateurs et premières transactions : drogues, faux papiers, logiciels illégaux

Dans les recoins invisibles du réseau Tor, là où la lumière vacille et où les chemins numériques s'entrelacent comme les racines d'une forêt profonde, un marché singulier prit forme en janvier 2011. *Silk Road*, ainsi nommé en hommage à l'antique route des épices et des soieries, n'était pas qu'un simple espace de commerce clandestin. C'était une idée, un défi lancé aux structures établies, un rêve porté par Ross Ulbricht, caché derrière le masque énigmatique de Dread Pirate Roberts. Ce lieu virtuel, à la fois fascinant et redoutable, promettait à ses premiers visiteurs une liberté totale, affranchie des regards intrusifs et des chaînes de la régulation étatique.

Ils étaient des hommes et des femmes aux motivations diverses, mais tous partageaient un même désir : celui de trouver refuge dans un espace où leurs transactions ne seraient ni observées ni jugées. Parmi eux se trouvaient des trafiquants de drogues, cherchant à écouler leurs marchandises sans risquer les pièges tendus par les autorités ; des faussaires habiles, proposant des papiers d'identité falsifiés avec une précision presque artistique ; et des hackers ingénieux, vendant des logiciels interdits capables de déjouer les systèmes les plus sécurisés.

Les premières transactions furent modestes, presque timides, comme si chaque acheteur et chaque vendeur testait la solidité du système. Des grammes de cannabis changèrent de mains virtuelles, suivis bientôt par des substances plus rares et plus dangereuses : cocaïne, LSD, MDMA. Les faux papiers firent leur apparition dans cette agora numérique, offrant à leurs acquéreurs une nouvelle identité pour échapper aux griffes du monde réel. Les logiciels illégaux, eux, promettaient des outils puissants pour contourner les barrières technologiques et s'aventurer plus loin dans l'univers clandestin.

Chaque échange était enveloppé dans le mystère et l'obscurité. Les acheteurs utilisaient Bitcoin pour payer leurs commandes, transférant leurs fonds avec la discrétion d'un voleur glissant dans la nuit. Les vendeurs expédiaient leurs produits dans des emballages soigneusement préparés, souvent dissimulés dans des objets anodins : livres creusés, jouets d'enfant ou boîtes alimentaires. Les colis traversaient le monde entier sans révéler leur contenu ni leur origine.

Rapidement, *Silk Road* devint une ruche bourdonnante d'activité. Les utilisateurs affluaient en nombre croissant, attirés par la sécurité offerte par Tor et Bitcoin. Le marché s'élargissait chaque jour, accueillant de nouvelles catégories de produits illicites. Des forums s'organisèrent au sein du site pour échanger des conseils sur les transactions ou discuter des idéaux libertariens qui sous-tendaient cette révolution numérique.

Pour Ross Ulbricht, ces premières transactions étaient bien plus qu'un simple commerce ; elles étaient la preuve que son idée audacieuse pouvait fonctionner. Il voyait en *Silk Road* la réalisation concrète de ses principes philosophiques : un espace où chacun pouvait exercer sa liberté sans crainte ni contrainte. Mais derrière cet enthousiasme naissant se cachait une vérité inéluctable : plus le marché grandissait, plus il attirait l'attention des forces de l'ordre. Et dans ce jeu dangereux entre anonymat et surveillance, le rêve libertarien de Ross Ulbricht allait bientôt rencontrer les limites imposées par le monde réel.

C. Adoption rapide par la communauté du dark web

L'idée de *Silk Road*, née dans le secret d'une chambre obscure, se répandit comme une rumeur dans les corridors silencieux du dark web. Au début, seuls quelques initiés, des pionniers des profondeurs numériques, osèrent s'aventurer sur cette route de soie virtuelle. Mais bientôt, comme un feu de prairie attisé par un vent invisible, la nouvelle se propagea : un marché libre, affranchi des lois et des regards indiscrets, avait vu le jour. Une place où l'or numérique – le Bitcoin – circulait sans entrave, et où l'anonymat était une promesse tenue.

La communauté du dark web, cette assemblée disparate d'idéologues libertariens, de hackers ingénieux et de commerçants clandestins, accueillit *Silk Road* avec un mélange d'émerveillement et de prudence. Certains y voyaient une utopie réalisée, un espace enfin libéré des chaînes de la surveillance étatique. D'autres, plus pragmatiques, y décelèrent une opportunité inédite : celle d'écouler leurs marchandises interdites sans risquer les pièges tendus par les autorités.

Le bouche-à-oreille numérique fit son oeuvre. Sur des forums cachés et dans des salons cryptés, on murmurait le nom de *Silk Road* comme celui d'un sanctuaire. Les utilisateurs partageaient leurs expériences : la simplicité des transactions en Bitcoin, la sécurité offerte par le réseau Tor, l'efficacité presque irréelle avec laquelle les colis arrivaient à destination. Chaque témoignage renforçait la réputation du marché et attirait de nouveaux adeptes.

En quelques mois à peine, *Silk Road* devint une véritable ruche bourdonnante d'activités. Des vendeurs venus des quatre coins du globe s'y installèrent comme des marchands sur une place médiévale. Ils proposaient leurs marchandises avec une audace croissante : drogues rares et exotiques, faux papiers d'une précision troublante, logiciels capables de déjouer les systèmes de sécurité les plus sophistiqués. Les acheteurs affluaient en masse, séduits par l'anonymat absolu et la promesse d'un commerce sans entrave.

Ce qui distinguait *Silk Road* des autres marchés clandestins n'était pas seulement son efficacité technique ; c'était aussi son esprit communautaire. Sous l'égide du mystérieux Dread Pirate Roberts, un véritable forum s'organisa au sein du site. Les utilisateurs y débattaient avec passion des idéaux libertariens qui animaient ce projet révolutionnaire. On y discutait librement de philosophie politique, d'économie décentralisée et des moyens de résister à ce qu'ils percevaient comme l'oppression étatique.

Ainsi, *Silk Road* devint bien plus qu'un simple marché clandestin : il devint un symbole. Pour ses partisans, il représentait la promesse d'un monde nouveau où la liberté individuelle triompherait des contraintes imposées par les gouvernements. Pour ses détracteurs – qui commençaient déjà à se manifester – , il incarnait une menace grandissante contre l'ordre établi.

Pourtant, dans cette ascension fulgurante se dessinait déjà l'ombre d'un danger imminent. Plus *Silk Road* gagnait en popularité, plus il attirait l'attention non seulement des utilisateurs mais aussi des autorités. Ross Ulbricht, caché derrière son pseudonyme énigmatique de Dread Pirate Roberts, observait cette croissance avec une fierté teintée d'inquiétude. Chaque nouvelle transaction, il le savait, rapprochait un peu plus son rêve libertarien de la collision inévitable avec la réalité implacable du monde extérieur.

Chapitre 2 : L'expansion fulgurante

A. Popularité croissante de *Silk Road* malgré les dénonciations publiques, notamment celle d'un sénateur américain en juin 2011

En ce début d'année 2011, *Silk Road* n'était encore qu'un murmure dans les recoins obscurs du web, un secret chuchoté entre initiés. Mais le destin, ce maître d'oeuvre des grandes ascensions comme des

chutes tragiques, s'apprêtait à propulser ce marché clandestin sous les feux d'une notoriété inattendue. Le 1er juin 2011, un article publié sur le site Gawker par le journaliste Adrian Chen fit l'effet d'une étincelle dans une poudrière. Intitulé Le site web souterrain où vous pouvez acheter n'importe quelle drogue imaginable, il exposait au grand jour l'existence de cette plateforme révolutionnaire, tout en la présentant sous un jour presque fascinant.

L'article dépeignait *Silk Road* comme une prouesse technologique et un refuge pour ceux qui cherchaient à commercer loin des regards intrusifs. On y lisait ces mots provocateurs : « Et si vous pouviez acheter et vendre des drogues en ligne comme on achète des livres ou des ampoules ? Maintenant vous pouvez : Bienvenue sur *Silk Road*. » Ces phrases, simples et percutantes, firent le tour du monde numérique en quelques heures, attirant l'attention non seulement des curieux mais aussi des autorités.

Les réactions furent immédiates et contrastées. Tandis que les utilisateurs du dark web affluaient en masse pour explorer ce marché singulier, certains hauts responsables politiques s'indignèrent publiquement. En tête de cette croisade se trouvait le sénateur américain Chuck Schumer, qui dénonça avec véhémence l'existence de *Silk Road* et appela à sa fermeture immédiate. Il qualifia la plateforme de « supermarché numérique de la drogue » et exhorta les agences fédérales à agir sans délai pour mettre fin à ce commerce qu'il jugeait scandaleux.

Ces dénonciations, loin de freiner l'essor de *Silk Road*, semblèrent au contraire renforcer son attrait. Chaque critique publique devenait une publicité involontaire pour ce marché clandestin, attirant toujours plus d'utilisateurs désireux de tester cette route de soie numérique où l'anonymat et la liberté semblaient régner en maîtres. Les forums du dark web s'enflammèrent ; on louait la simplicité du système, la sécurité offerte par Tor et Bitcoin, et l'efficacité redoutable avec laquelle les transactions étaient exécutées.

Cependant, dans l'ombre, les premières fissures apparaissaient. Les agences fédérales commencèrent à surveiller de près ce phénomène grandissant. À Chicago, les agents du département de la Sécurité intérieure remarquèrent une augmentation inhabituelle des saisies postales contenant de petites quantités de drogue. Ces colis discrets portaient la signature invisible d'un commerce organisé qui échappait encore à leur compréhension.

Ainsi, tandis que *Silk Road* gagnait en popularité et consolidait sa place comme leader incontesté du commerce clandestin en ligne, ses ennemis se rassemblaient dans l'ombre. Mais pour Ross Ulbricht, caché derrière son pseudonyme de Dread Pirate Roberts, ces dénonciations publiques n'étaient qu'un bruit lointain. Loin de s'inquiéter, il voyait dans cette attention croissante une validation éclatante de son projet : *Silk Road* n'était plus un simple marché ; c'était désormais un symbole vivant d'une rébellion contre les institutions étatiques. Pourtant, comme tout astre brillant qui attire irrésistiblement les regards, il s'approchait chaque jour un peu plus du moment où il serait consumé par sa propre lumière.

B. Commissions sur les ventes (entre 8 % et 15 %), générant des millions de dollars

Dans les méandres du réseau Tor, où l'ombre et le silence régnaient en maîtres, *Silk Road* ne se contentait pas d'être un marché clandestin ; il était une machine économique d'une redoutable efficacité. Sous l'apparence d'un bazar numérique anarchique, il dissimulait une organisation méthodique et un modèle économique savamment conçu par son créateur, Ross Ulbricht, alias Dread Pirate Roberts.

Chaque transaction effectuée sur *Silk Road* rapportait une commission à la plateforme, un prélèvement subtil mais constant, qui s'opérait dans l'obscurité des échanges numériques. Le système était ingénieux : les vendeurs, pour avoir le privilège d'exposer leurs marchandises – drogues, faux papiers ou logiciels interdits –, acceptaient de céder une part de leurs gains à la plateforme. Cette commission était calculée selon un barème dégressif : entre 8 % et 15 % des ventes selon leur montant. Ainsi, plus la transaction était importante, plus le pourcentage prélevé diminuait, encourageant les échanges massifs tout en garantissant un flux constant de revenus pour *Silk Road*.

Ce n'était pas tout. Les nouveaux vendeurs désireux de rejoindre ce marché florissant devaient également payer un droit d'entrée, sous forme de frais fixes ou d'enchères, pour obtenir un compte vendeur. Ces barrières financières servaient à filtrer les participants et à renforcer la sécurité du site en limitant l'accès aux plus déterminés.

Les transactions étaient réalisées exclusivement en Bitcoin, cette

monnaie numérique encore naissante mais déjà auréolée d'un mystère fascinant. Les paiements transitaient par un système d'escrow – une sorte de garde-fou numérique – qui retenait les fonds jusqu'à ce que l'acheteur confirme la réception de sa commande. Ce mécanisme inspirait confiance aux utilisateurs tout en permettant à la plateforme de prélever ses commissions avec une précision implacable.

En moins de deux ans, *Silk Road* devint une véritable mine d'or numérique. Entre février 2011 et juillet 2013, plus de 9,5 millions de bitcoins transitèrent par ses serveurs, générant des ventes équivalentes à environ 1,2 milliard de dollars et des commissions estimées à 80 millions de dollars selon la valeur du Bitcoin à l'époque. Ces chiffres vertigineux témoignaient du succès fulgurant de ce marché clandestin, qui attirait chaque jour davantage d'utilisateurs venus des quatre coins du monde.

Pour Ross Ulbricht, ces revenus colossaux n'étaient pas seulement une récompense financière ; ils représentaient la validation éclatante de son idée révolutionnaire. Chaque bitcoin collecté était une preuve supplémentaire que son rêve libertarien pouvait prospérer dans les ténèbres du dark web. Mais cette prospérité insolente ne tarda pas à attirer l'attention des autorités fédérales, qui voyaient dans ces flux massifs de cryptomonnaie un défi direct à leur pouvoir.

Ainsi, tandis que *Silk Road* engrangeait des millions dans le secret des transactions anonymes, les forces de l'ordre affûtaient leurs armes dans l'ombre. Car si cette route numérique semblait infinie pour ses utilisateurs émerveillés, elle menait inexorablement vers une impasse où l'attendaient les griffes implacables de la justice.

C. Étude d'août 2012 révélant le succès du site et son rôle central dans le commerce illicite

En cet été de l'année 2012, alors que le soleil d'août baignait les rues en une lumière éclatante, dans les profondeurs invisibles du dark web, une autre lumière, plus sombre, brillait intensément : celle de *Silk Road*. Ce marché clandestin, né à peine un an et demi plus tôt, avait déjà conquis un empire numérique. Mais ce n'est qu'à travers une étude révélée en août de cette même année que la véritable ampleur de son succès fut mise au jour, frappant d'étonnement autant ses partisans que ses détracteurs.

Les chiffres étaient vertigineux, presque irréels. En seulement dix-huit mois d'existence, *Silk Road* avait généré près de 1,2 milliard de dollars en ventes illicites. Plus de 9,5 millions de bitcoins avaient transité par ses serveurs anonymes pendant toutes l'existence du site, chaque transaction laissant derrière elle une commission prélevée par le site, oscillant entre 8 % et 15 %. Ces prélèvements avaient permis à la plateforme d'amasser une fortune estimée à 80 millions de dollars en bitcoins, une somme qui semblait appartenir à un autre monde.

L'étude dévoilait également la diversité des biens échangés sur ce marché numérique. On y trouvait des drogues venues des quatre coins du globe : héroïne et cocaïne d'une pureté exceptionnelle, cannabis soigneusement cultivé, LSD et MDMA aux cristaux scintillants. Ce n'était pas tout : faux papiers, logiciels illégaux et autres produits interdits complétaient cette pharmacopée moderne. Les vendeurs venaient de plus de dix pays européens – Pays-Bas, Royaume-Uni, France et Espagne – ainsi que des États-Unis et du Canada. Les colis traversaient les océans et les frontières comme des spectres insaisissables..

Ce succès phénoménal ne reposait pas seulement sur l'offre abondante ou la qualité des produits ; il était également le fruit d'un système rigoureux et ingénieux. Les transactions étaient sécurisées par un mécanisme d'escrow qui retenait les fonds jusqu'à ce que l'acheteur confirme la réception de sa commande. Les vendeurs étaient évalués par leurs clients, créant un système de confiance semblable à celui des marchés légaux comme eBay ou Amazon. Cette combinaison d'anonymat absolu et de professionnalisme irréprochable avait fait de *Silk Road* un modèle unique dans l'histoire du commerce clandestin.

Cette étude ne se contentait pas de célébrer le génie technologique ou économique du site ; elle mettait également en lumière son rôle central dans l'économie illicite mondiale. *Silk Road* n'était plus seulement un marché noir parmi d'autres : il était devenu le coeur battant d'un réseau global reliant acheteurs et vendeurs au-delà des frontières et des lois. Pour les libertariens qui voyaient en lui une utopie numérique, ces chiffres représentaient la victoire éclatante de la liberté individuelle sur les institutions étatiques. Pour les autorités, ils étaient la preuve accablante d'un défi qu'il fallait relever à tout prix.

Ainsi, en cet été 2012, *Silk Road* atteignait l'apogée de sa gloire. Mais comme tout astre brillant qui

s'élève trop haut dans le ciel, il attirait aussi l'attention des puissances terrestres prêtes à tout pour éteindre sa lumière. Ces chiffres triomphants dissimulaient une autre réalité : celle de l'étau fédéral qui se resserrait lentement autour du mystérieux Dread Pirate Roberts.

Chapitre 3 : Les premières menaces

A. Premiers soupçons des autorités américaines : mobilisation du FBI, DEA et autres agences fédérales

Dans les vastes corridors feutrés des agences fédérales américaines, une rumeur commença à circuler, d'abord discrète, puis insistante, comme un murmure qui se fait cri. Un marché clandestin, niché dans les profondeurs du réseau Tor, prospérait dans l'ombre, défiant les lois et les institutions. Son nom était *Silk Road*, et il promettait à ses utilisateurs anonymat et liberté absolue. Mais pour les autorités, il représentait une menace insidieuse, une hydre numérique dont les ramifications s'étendaient bien au-delà des frontières visibles.

Les premiers soupçons prirent forme en juin 2011, lorsque le sénateur Chuck Schumer dénonça publiquement l'existence de *Silk Road*, qualifiant ce site de « supermarché numérique de la drogue ». Ses paroles résonnèrent comme un appel aux armes pour les agences fédérales : FBI, DEA, IRS, Homeland Security et même l'Inspection postale américaine se mobilisèrent pour traquer ce marché illégal. Mais la tâche s'avérait ardue. *Silk Road* était protégé par le réseau Tor, ce labyrinthe crypté qui dissimulait les adresses IP derrière des couches de chiffrement impénétrables. Les transactions financières étaient réalisées en Bitcoin, une monnaie virtuelle dont la traçabilité échappait aux outils traditionnels.

Dans des salles de réunion éclairées par des néons blafards, des équipes d'agents fédéraux se réunirent pour élaborer leur stratégie. Leurs discussions étaient ponctuées par des rapports inquiétants : des colis contenant des drogues d'une pureté exceptionnelle avaient été interceptés dans plusieurs centres de tri postal à travers le pays. Ces paquets discrets portaient la marque d'un commerce organisé qui semblait insaisissable. Les agents savaient qu'ils ne pouvaient compter sur leurs méthodes traditionnelles – interroger des témoins ou surveiller des lieux physiques – pour infiltrer ce réseau numérique.

L'enquête prit alors une tournure technologique. Des spécialistes en cybersécurité furent mobilisés pour tenter de percer les mystères de Tor et de Bitcoin. Des agents sous couverture commencèrent à opérer sur *Silk Road*, se faisant passer pour des vendeurs ou des acheteurs afin de collecter des informations sur le fonctionnement interne du site. Pendant ce temps, les autorités islandaises furent sollicitées pour récupérer l'historique d'un serveur suspect hébergé dans leur pays. Ce serveur, identifié grâce à une adresse IP révélée par un coup de chance extraordinaire, contenait des volumes massifs de trafic crypté lié à *Silk Road*.

Mais malgré ces efforts acharnés, le fondateur du site – cet énigmatique Dread Pirate Roberts – restait introuvable. Était-il un homme seul ou un collectif ? Était-il caché dans une maison anonyme ou derrière un écran dans une bibliothèque publique ? Ces questions hantaient les enquêteurs tandis que leur frustration grandissait face à l'ingéniosité du système mis en place par Ross Ulbricht.

Ainsi débuta une chasse à l'homme sans précédent dans l'histoire numérique. Les autorités américaines mobilisèrent leurs meilleurs agents et leurs technologies les plus avancées pour démanteler ce marché clandestin qui semblait défier toutes les lois établies. Mais dans cette lutte entre anonymat et surveillance, entre liberté et contrôle, *Silk Road* continuait de prospérer dans l'ombre, comme une étoile noire brillait au coeur du dark web.

B. Tensions croissantes entre l'idée libertarienne de Ross Ulbricht et les critiques dénonçant un outil facilitant le crime organisé

Dans les profondeurs du réseau Tor, là où les ombres numériques se mêlaient aux idéaux les plus audacieux, *Silk Road* s'élevait comme un phare pour ceux qui cherchaient à échapper aux chaînes de la surveillance étatique. Ross Ulbricht, son créateur, voyait en cette plateforme bien plus qu'un simple marché clandestin. Pour lui, elle incarnait une philosophie libertarienne pure, un sanctuaire où chaque individu pouvait exercer sa liberté de commercer selon ses propres choix, sans entrave ni jugement. « Donner aux gens la liberté de faire leurs propres choix », avait-il écrit dans une lettre poignante adressée au juge avant sa condamnation.

Tandis que *Silk Road* prospérait dans l'obscurité, attirant des milliers d'utilisateurs anonymes à

travers le monde, ses détracteurs s'organisaient dans la lumière. Les critiques se faisaient de plus en plus virulentes, dénonçant un site qui, sous couvert de liberté individuelle, facilitait le crime organisé à une échelle jamais vue auparavant. Des drogues d'une pureté exceptionnelle circulaient librement ; des faux papiers et des logiciels interdits étaient échangés sans crainte ; et tout cela se faisait sous le voile protecteur de Tor et du Bitcoin. Pour les autorités et les médias, *Silk Road* n'était pas un bastion de liberté mais une menace directe contre l'ordre établi.

Le sénateur Chuck Schumer fut l'un des premiers à monter au créneau. En juin 2011, il qualifia *Silk Road* de « supermarché numérique de la drogue », appelant publiquement à sa fermeture immédiate et exhortant les agences fédérales à agir sans délai4. Ses paroles résonnèrent comme un coup de tonnerre dans les cercles libertariens qui soutenaient Ross Ulbricht. Pour ces défenseurs du libre marché, cette condamnation publique était une attaque contre leurs idéaux fondamentaux : la liberté individuelle et le droit de commercer sans intervention étatique.

Cette tension entre idéologie et réalité ne se limitait pas aux discours politiques. Elle était inscrite au coeur même de *Silk Road*. Ross Ulbricht avait interdit catégoriquement les actes violents sur sa plateforme – assassinats et pédophilie y étaient proscrits avec une fermeté absolue – mais il ne pouvait ignorer que son marché servait aussi à alimenter des dépendances destructrices et des activités criminelles. Dans une lettre écrite depuis sa cellule, il déplora ce paradoxe : « *Silk Road* était censé donner aux gens la liberté de poursuivre leur propre bonheur [...] Ce qu'il est devenu, c'est en partie un moyen pratique pour les gens d'assouvir leur dépendance à la drogue »..

Ainsi, *Silk Road* devint le théâtre d'un affrontement idéologique entre deux visions du monde : celle d'une liberté absolue prônée par Ulbricht et ses partisans libertariens, et celle d'un ordre social où la régulation était nécessaire pour protéger les citoyens des dangers du commerce illicite. Tandis que Ross Ulbricht rêvait d'un avenir où chacun pourrait vivre selon ses propres règles, ses ennemis voyaient en lui un criminel facilitant des activités dangereuses à grande échelle.

Dans cette lutte entre lumière et ténèbres, entre idéaux libertariens et réalités criminelles, *Silk Road* continuait de croître inexorablement. Tandis que Ross Ulbricht défendait son rêve avec une ferveur presque romantique, l'étau des autorités se resserrait autour de lui, prêt à écraser ce symbole ambigu d'une révolution numérique.

C. Début des enquêtes sous couverture

Dans les vastes bureaux anonymes du FBI, où la lumière blafarde des néons semblait éternellement suspendue dans un crépuscule artificiel, une réunion d'une gravité particulière se tint à la fin de l'année 2011. Les agents fédéraux, réunis autour de dossiers épais et de moniteurs scintillants, faisaient face à un défi inédit : traquer et démanteler *Silk Road*, ce marché clandestin qui défiait ouvertement les lois et les institutions. L'heure n'était plus aux conjectures ; il fallait agir.

Le réseau Tor, ce labyrinthe numérique conçu pour garantir l'anonymat, protégeait *Silk Road* comme une forteresse invisible. Mais si les murs de cette citadelle étaient impénétrables, les agents savaient que la clé pour y entrer résidait dans l'infiltration. Ainsi débuta l'une des opérations les plus audacieuses de l'histoire du FBI : des agents sous couverture furent déployés dans les méandres du dark web, se glissant parmi les utilisateurs de *Silk Road* comme des ombres silencieuses.

Jared Der-Yeghiayan, un agent de la Homeland Security Investigations (HSI), fut l'un des premiers à s'immerger dans cet univers clandestin. Depuis son bureau situé à l'aéroport de Chicago, il avait remarqué une augmentation inhabituelle des saisies postales contenant de petites quantités de drogue. Ces colis discrets, soigneusement emballés et souvent dissimulés dans des objets anodins, portaient la marque d'un commerce organisé et sophistiqué. Intrigué, il traça leur origine jusqu'à *Silk Road* et rejoignit bientôt une équipe spécialisée en cybercriminalité du FBI à New York.

Les agents infiltrés adoptèrent des pseudonymes soigneusement choisis et commencèrent à interagir directement avec les vendeurs et les acheteurs sur le site. Ils passèrent des commandes fictives – échantillons de drogues, faux papiers – qui furent livrées avec une précision troublante. Chaque transaction leur permettait de collecter des informations précieuses sur le fonctionnement interne de *Silk*

Road. Ces données furent croisées avec celles obtenues par d'autres moyens : analyses des flux Bitcoin, saisies postales et témoignages d'utilisateurs arrêtés.

L'opération prit le nom évocateur d'Onion Peeler – littéralement « éplucheur d'oignons » –, une référence directe au réseau Tor dont les couches successives de cryptage devaient être patiemment décortiquées pour révéler l'identité des utilisateurs. Parmi ces agents infiltrés se trouvait Carl Force, membre expérimenté de la DEA, qui opérait sous le pseudonyme Nob. Force gagna rapidement la confiance des utilisateurs et parvint à dialoguer directement avec Dread Pirate Roberts, le mystérieux administrateur du site.

Cette infiltration n'était pas sans danger. Les agents savaient que le moindre faux pas pouvait trahir leur couverture et compromettre l'enquête entière. Ils évoluaient dans un monde où chaque mot pouvait être analysé, chaque transaction surveillée par ceux qu'ils cherchaient à piéger. Pourtant, leur patience fut récompensée : en juillet 2013, grâce aux informations collectées par ces agents sous couverture, les serveurs principaux de *Silk Road* furent localisés en Islande et saisis par les autorités locales.

Ainsi commença la longue traque qui mènerait à la chute de Ross Ulbricht. Mais dans ces premiers mois d'infiltration, alors que les agents fédéraux s'immisçaient lentement mais sûrement dans l'univers opaque du dark web, Dread Pirate Roberts restait insaisissable. Tel un capitaine défiant les tempêtes sur un navire fantôme, il continuait à diriger son empire numérique sans soupçonner que ses propres murs commençaient déjà à se fissurer sous le poids de l'enquête fédérale.

Conclusion : Une révolution controversée

A. Évaluation de l'impact de *Silk Road* sur le commerce illicite et l'utilisation de Bitcoin

Dans l'histoire tumultueuse des révolutions modernes, rares sont celles qui naissent dans l'obscurité et s'épanouissent dans le secret. *Silk Road*, ce marché clandestin niché dans les profondeurs du réseau Tor, fut l'une d'elles. Comme une étoile noire brillant au coeur du dark web, il transforma à jamais le paysage du commerce illicite et des cryptomonnaies, laissant derrière lui un héritage aussi fascinant qu'inquiétant.

Lorsque Ross Ulbricht donna vie à *Silk Road* en 2011, il ne se doutait pas qu'il allait inaugurer une ère nouvelle pour le commerce illégal. En combinant l'anonymat offert par Tor et la discrétion des transactions en Bitcoin, il créa un sanctuaire numérique où les vendeurs et acheteurs pouvaient échanger sans crainte d'être identifiés. En moins de trois ans, ce marché devint une plaque tournante mondiale pour le trafic de drogues, les faux papiers, les logiciels interdits et bien d'autres marchandises illicites. Les chiffres parlent d'eux-mêmes : plus de 1,2 milliard de dollars en ventes, près de 10 millions de bitcoins échangés, et des commissions atteignant 80 millions de dollars.

Silk Road ne fut pas seulement un marché ; il fut aussi une révolution technologique. En popularisant l'usage du Bitcoin comme monnaie exclusive pour les transactions anonymes, le site donna à cette cryptomonnaie une visibilité sans précédent. Avant *Silk Road*, Bitcoin était une curiosité réservée aux passionnés de technologie ; après lui, elle devint un outil incontournable pour ceux qui cherchaient à échapper aux régulations étatiques. L'impact fut tel que même après la fermeture du site en 2013, les successeurs comme AlphaBay ou Dream Market continuèrent à utiliser Bitcoin comme pilier central de leurs opérations.

Cependant, cet héritage est marqué par une dualité profonde. D'un côté, *Silk Road* démontra la puissance des technologies décentralisées et anonymes pour libérer les individus des contraintes imposées par les gouvernements. Il incarna pour certains une utopie libertarienne où la liberté individuelle triomphait des lois coercitives. De l'autre côté, il révéla les dangers inhérents à ces mêmes technologies : facilitation du crime organisé, propagation de drogues mortelles et mise en péril des structures sociales.

Enfin, l'impact de *Silk Road* sur le commerce illicite dépasse largement son existence éphémère. En créant une plateforme où les vendeurs pouvaient atteindre un public mondial sans jamais se rencontrer physiquement, Ross Ulbricht révolutionna le trafic de drogues et autres produits interdits. Les risques associés au commerce traditionnel – arrestations lors d'échanges physiques ou conflits violents – furent remplacés par des transactions numériques sécurisées et anonymes. Ce modèle inspira toute une génération de marchés noirs

numériques qui continuent aujourd'hui à défier les autorités malgré leurs efforts incessants pour les démanteler.

Ainsi, *Silk Road* demeure un symbole ambigu : celui d'une révolution technologique qui libéra autant qu'elle détruisit. Et tandis que son créateur, Ross Ulbricht, passa des rêves libertariens aux murs froids d'une cellule fédérale avant d'être gracié en 2025, son oeuvre continue de hanter le monde numérique comme un spectre insaisissable, un rappel que chaque progrès porte en lui la promesse du bien comme celle du mal.

B. Les premières investigations qui mèneront à la chute de Ross Ulbricht

Dans l'ombre du succès éclatant de *Silk Road*, une tempête se préparait. Tandis que Ross Ulbricht, caché derrière le pseudonyme énigmatique de Dread Pirate Roberts, dirigeait son empire numérique avec une confiance grandissante, les autorités fédérales affûtaient leurs armes. Les premières fissures dans l'anonymat de cette forteresse virtuelle apparurent comme des éclats de lumière dans une nuit sans lune, annonçant la fin d'une utopie libertarienne et le début d'une traque implacable.

Les enquêteurs, déterminés à démanteler ce marché clandestin, commencèrent par infiltrer ses profondeurs. Des agents sous couverture se glissèrent parmi les utilisateurs, adoptant des pseudonymes soigneusement choisis et simulant des transactions pour collecter des informations précieuses. Parmi eux, Carl Force, agent de la DEA opérant sous l'identité de Nob, parvint à établir un dialogue direct avec Ulbricht lui-même. Derrière cette façade d'infiltration professionnelle se cachaient aussi des actes de corruption : certains agents détournèrent des Bitcoins saisis pour leur usage personnel, ajoutant une couche de complexité à cette enquête déjà labyrinthique.

En parallèle, un agent de l'IRS nommé Gary Alford fit une découverte capitale. En fouillant les archives numériques, il établit un lien entre le pseudonyme "altoid", utilisé pour promouvoir *Silk Road* lors de ses débuts, et une adresse e-mail contenant le nom complet de Ross Ulbricht. Cette erreur fatale permit aux enquêteurs d'identifier leur suspect principal et d'affiner leur traque.

La chasse s'intensifia lorsque les autorités localisèrent un serveur clé en Islande, hébergeant une partie des données de *Silk Road*. Ce serveur fut saisi, révélant des volumes massifs d'informations cryptées sur les opérations du site. Mais le coup décisif fut porté en octobre 2013 dans une bibliothèque publique de San Francisco. Là, Ross Ulbricht fut arrêté après une diversion orchestrée par des agents fédéraux, qui récupérèrent son ordinateur avant qu'il ne puisse effacer les preuves incriminantes. Sur cet appareil reposaient les journaux détaillant ses activités ainsi que plus de 144 000 bitcoins, une fortune colossale à l'époque.

Ainsi s'acheva le règne de Dread Pirate Roberts, non sans laisser derrière lui un héritage complexe et controversé. L'arrestation d'Ulbricht marqua le début d'un procès retentissant qui révélerait non seulement les rouages du commerce illicite sur le dark web mais aussi les failles humaines au sein même des forces fédérales. Dans ce jeu d'ombres et de lumières, où idéaux libertariens et réalités criminelles s'entrechoquaient, le rêve numérique d'Ulbricht s'effondra sous le poids des lois qu'il avait défiées.

L'histoire s'apprête à plonger dans les méandres du procès et des conséquences qui suivirent : un théâtre où se joueront la condamnation du créateur de *Silk Road* et la corruption insoupçonnée de ses poursuivants. Car si l'étoile noire du dark web s'est éteinte en 2013, son éclat continue d'éclairer les débats sur la liberté numérique et les dangers du commerce décentralisé.

Sources :

https://www.fbi.gov/history/artifacts/ross-william-ulbrichts-laptop

https://www.ice.gov/news/releases/ross-ulbricht-aka-dread-pirate-roberts-sentenced-life-federal-prison-creating

https://www.lesinrocks.com/actu/lincroyable-histoire-de-ross-ulbricht-le-fondateur-de-silk-road-condamne-la-prison-la-vie-49609-08-06-2017/

https://fr.beincrypto.com/marches/288526/satoshi-nakamoto-dealer-dark-web/

https://www.la-croix.com/international/pourquoi-trump-a-gracie-ross-ulbricht-le-fondateur-de-l-ebay-de-la-drogue-20250122

https://journalducoin.com/analyses/silk-road-marche-noir-dark-web-creation-ross-ulbricht/

https://academy.bit2me.com/fr/quien-es-ross-ulbricht/

https://fr.wikipedia.org/wiki/Ross_Ulbricht

https://www.cointribune.com/qui-est-ross-ulbricht/

https://www.france24.com/fr/20150530-silk-road-prison-vie-perpetuite-ross-ulbricht-trafic-drogue-us-bitcoin

LE CONSEIL DE L'EUROPE FACE À LA CORRUPTION : NORMES, EFFECTIVITÉ ET LEVIERS DE RENFORCEMENT

COURS PRONONCÉ À L'OCCASION DE L'UNIVERSITÉ D'ÉTÉ OCEAN 2025

CHANTAL CUTAJAR
DIRECTRICE DU GRASCO
UMR DRES 7354 UNIVERSITÉ DE STRASBOURG

Fondé en 1949, le Conseil de l'Europe est la plus ancienne organisation paneuropéenne. Réunissant aujourd'hui 46 États membres, il se distingue par une triple vocation : la défense des droits de l'homme, le renforcement de la démocratie et la promotion de l'État de droit. C'est dans le cadre de cette mission fondatrice qu'il s'est saisi, dès les années 1990, de la lutte contre la corruption.

Car la corruption ne constitue pas seulement une infraction pénale : elle sape dangereusement les institutions démocratiques, mine la confiance des citoyens et compromet l'égalité devant la loi. Le rapport SOCTA 2025 – European Union Serious and Organised Crime Threat Assessment, publié par Europol, met en garde contre une criminalité organisée « plus enracinée et déstabilisatrice que jamais », soulignant une corrélation croissante entre les réseaux criminels et certains agents des institutions publiques. La corruption y est décrite non comme un simple effet collatéral, mais comme un outil stratégique utilisé pour infiltrer les administrations, manipuler les marchés publics et neutraliser les mécanismes de contrôle dans des secteurs clés comme les ports, la logistique ou les douanes.

Le rapport attire également l'attention sur la dynamique de « captation de l'État » (state capture), dans laquelle les acteurs corrompus ne se contentent pas de contourner la règle de droit, mais structurent l'action publique à leur profit. Ces processus dégradent l'exercice éthique du pouvoir, affaiblissent la régulation démocratique et nourrissent le sentiment d'impunité, avec pour conséquence une défiance croissante à l'égard des institutions publiques. À cela s'ajoute l'utilisation croissante des technologies : paiements en cryptomonnaies, plateformes opaques de passation des marchés, faux profils institutionnels... Les outils numériques offrent aux réseaux criminels de nouvelles opportunités pour organiser, dissimuler et automatiser la corruption.

Dans ce contexte, la lutte contre la corruption ne peut être dissociée des principes fondamentaux du Conseil de l'Europe. Elle doit être pensée comme un impératif transversal : un enjeu à la fois juridique, institutionnel, éthique et technologique. Le Conseil de l'Europe s'y attelle par une triple action : l'adoption d'instruments normatifs ambitieux, un mécanisme de suivi (le GRECO) permettant d'évaluer la mise en oeuvre concrète de ces normes, et un ensemble de dispositifs d'assistance technique pour renforcer les capacités nationales.

L'intervention d'aujourd'hui n'a pas pour objet de présenter dans le détail le fonctionnement du GRECO, qui fera l'objet d'un

atelier spécifique. Elle propose en revanche d'examiner les normes adoptées par le Conseil de l'Europe, d'évaluer leur effectivité sur le terrain, et de s'interroger collectivement sur les leviers susceptibles d'en renforcer l'impact. De puissants instruments existent ; encore faut-il qu'ils transforment les pratiques, qu'ils influencent les décisions, et qu'ils soient compris comme des outils vivants de protection de l'intérêt général.

I. L'ambition normative du Conseil de l'Europe : construire un cadre de référence européen

Afin de saisir toute la portée de cette ambition normative, nous examinerons d'abord les instruments juridiques contraignants qui constituent le socle du droit anticorruption européen (A). Puis, dans un second temps, nous nous intéresserons aux normes dites « souples », qui bien qu'elles ne soient pas juridiquement obligatoires, exercent une influence structurante sur les systèmes juridiques nationaux et les politiques publiques (B).

Avant toute chose, arrêtons-nous sur le fondement juridique dur du Conseil de l'Europe en matière de lutte contre la corruption : les conventions internationales multilatérales, véritables piliers de l'action normative européenne.

A. Des instruments juridiques multilatéraux structurants

Le Conseil de l'Europe a joué un rôle pionnier dans la construction d'un cadre juridique commun de lutte contre la corruption en Europe. Il s'est doté, dès la fin des années 1990, de conventions internationales contraignantes qui constituent aujourd'hui encore le socle normatif de son action. Ces textes, qui lient juridiquement les États signataires, visent à harmoniser les droits nationaux, à renforcer l'efficacité des dispositifs nationaux de prévention et de répression, et à favoriser la coopération entre les pays

- **Convention pénale sur la corruption (CETS 173)** : incrimination, responsabilité des personnes morales, coopération judiciaire.

Le premier de ces instruments, la Convention pénale sur la corruption (CETS n°173), a été adoptée à Strasbourg le 27 janvier 1999. Elle oblige les États parties à ériger en infractions pénales un ensemble de comportements liés à la corruption. Elle couvre aussi bien la corruption active, c'est-à-dire le fait d'offrir, de promettre ou d'accorder un avantage indu, que la corruption passive, consistant à solliciter ou à accepter un tel avantage. Ces infractions doivent être réprimées tant dans le secteur public que dans le secteur privé, et s'appliquent à une large gamme d'acteurs : agents publics nationaux, membres d'assemblées publiques, juges, fonctionnaires étrangers ou internationaux, et acteurs économiques. La Convention impose également l'incrimination du trafic d'influence, du blanchiment des produits de la corruption, ainsi que de la complicité, de l'incitation et de la tentative de ces infractions. Les États doivent veiller à ce que ces comportements soient punis de sanctions effectives, proportionnées et dissuasives. Par ailleurs, la Convention prévoit l'obligation d'instaurer une responsabilité des personnes morales, de manière pénale, civile ou administrative, pour les actes de corruption commis pour leur compte. Elle ouvre également la voie à la coopération internationale en matière d'enquêtes, de poursuites, d'extradition ou de saisie des biens issus de la corruption. Elle est accessible non seulement aux États membres du Conseil de l'Europe, mais aussi aux États tiers, dans une logique d'universalisation des standards européens.

À côté de cette approche répressive, le Conseil de l'Europe innove également en introduisant une logique réparatrice, incarnée par la Convention civile sur la corruption. Celle-ci rééquilibre le dispositif en plaçant les victimes au coeur de la réponse juridique.

- **Convention civile (CETS 174) :** droit à réparation, prévention contractuelle.

La Convention civile sur la corruption (CETS n°174), signée à Strasbourg le 4 novembre 1999 et entrée en vigueur en 2003, constitue une innovation majeure dans le paysage juridique international en ce qu'elle introduit une perspective réparatrice dans la lutte contre la corruption, jusque-là dominée par l'approche pénale. Elle affirme le droit des personnes physiques ou morales lésées par un acte de corruption à obtenir réparation intégrale du préjudice subi — qu'il soit matériel ou moral. En posant ce principe, elle engage les États parties à doter leur droit interne de procédures permettant

de faire valoir efficacement ce droit à réparation, notamment en facilitant l'accès au juge civil, en aménageant les règles de preuve ou encore en clarifiant la responsabilité des auteurs directs ou indirects de l'acte illicite.

Au-delà du contentieux, cette convention promeut une approche préventive de la corruption fondée sur la transparence contractuelle et la sécurité juridique. Elle encourage les États à insérer dans leurs législations des clauses types ou des obligations d'information visant à prévenir les pratiques corruptives dans les relations commerciales, les marchés publics ou les activités professionnelles exposées. Elle invite à renforcer les obligations de diligence et de conformité dans les relations contractuelles, anticipant par-là l'essor ultérieur des dispositifs de compliance dans le secteur privé.

Par son objet, la Convention civile comble un angle mort de la lutte anticorruption en plaçant les victimes au coeur du dispositif normatif. Elle souligne que la corruption n'est pas seulement une atteinte à l'ordre public ou aux intérêts de l'État, mais aussi un facteur de déséquilibre économique, de rupture de l'égalité des chances et d'atteinte aux droits des acteurs lésés. Elle ouvre ainsi une voie pour responsabiliser les acteurs économiques et faire de la lutte contre la corruption un enjeu partagé entre secteur public et secteur privé. Elle anticipe, en ce sens, les développements récents relatifs au devoir de vigilance des entreprises et à l'accès effectif à la justice pour les victimes d'atteintes à la probité.

Enfin, cette convention participe à l'harmonisation du droit civil européen en matière de corruption, en instaurant un cadre commun qui favorise la coopération judiciaire en matière civile et commerciale, notamment en cas de contentieux transfrontalier. Bien que moins ratifiée que son pendant pénal, elle s'inscrit dans la stratégie globale du Conseil de l'Europe visant à traiter la corruption sous toutes ses dimensions — répressive, préventive et réparatrice — et à rééquilibrer la relation entre auteurs et victimes.

Mais l'ambition ne s'arrête pas là. Le Conseil de l'Europe veille aussi à l'élargissement du champ personnel de sa norme pénale, comme en témoigne l'adoption du Protocole additionnel de 2003, destiné à protéger l'intégrité de fonctions juridictionnelles trop longtemps restées en marge.

- **Protocole additionnel (CETS 191) :** extension à d'autres professions juridictionnelles.

Enfin, le Protocole additionnel à la Convention pénale sur la corruption (CETS n°191), signé à Strasbourg le 15 mai 2003, constitue un pas supplémentaire dans la consolidation du socle juridique européen de lutte contre la corruption. Il vise à étendre le champ d'application personnel de la Convention de 1999, en y incluant des catégories d'acteurs jusqu'alors laissées en marge, malgré leur rôle central dans le fonctionnement de la justice et de l'arbitrage. Plus précisément, ce protocole impose aux États parties d'ériger en infractions pénales les actes de corruption active et passive commis à l'égard — ou par — des arbitres (qu'ils exercent dans un cadre judiciaire ou extrajudiciaire) ainsi que des jurés, dans les systèmes où ces derniers interviennent.

Ce choix n'est pas anodin : il reflète une prise de conscience des vulnérabilités spécifiques des modes alternatifs de règlement des différends (ADR) et de la justice participative face aux tentatives de manipulation ou d'influence indue. Dans un contexte d'internationalisation croissante de l'arbitrage commercial et d'européanisation des procédures judiciaires, la protection de l'intégrité de ces acteurs est cruciale pour garantir la légitimité et l'impartialité des décisions rendues. En sanctionnant la corruption dans ces sphères, le Conseil de l'Europe affirme que l'ensemble des fonctions juridictionnelles — formelles comme informelles — doivent être à l'abri de toute tentative de captation d'intérêts privés.

Le Protocole répond également à des préoccupations concrètes liées à des scandales qui ont révélé la porosité de certains mécanismes arbitraux à des pressions économiques ou politiques. Dans les contentieux à forts enjeux financiers, l'arbitrage international a parfois été perçu comme un lieu d'opacité et de pouvoir concentré, peu contrôlé par les États. En imposant des obligations claires d'incrimination, le Protocole contribue à rétablir la confiance dans ces mécanismes et à renforcer leur transparence.

Enfin, ce texte complète utilement le dispositif initial de la Convention de 1999 en assurant une couverture plus complète de l'ensemble des fonctions juridictionnelles. Il renforce la cohérence de

l'architecture normative du Conseil de l'Europe en matière d'intégrité, en affirmant que l'exemplarité attendue des juges s'étend à toute personne investie d'un pouvoir de décision ayant des effets juridiques. Il s'inscrit pleinement dans la logique du Conseil de l'Europe : celle d'un État de droit exigeant, fondé sur des institutions impartiales, transparentes et responsables.

Ces trois textes forment un ensemble cohérent et structurant qui permet d'appréhender la corruption de manière transversale, en articulant les responsabilités pénales, civiles et institutionnelles. En érigeant des standards juridiquement contraignants, le Conseil de l'Europe engage les États parties à bâtir des dispositifs complets de prévention, de sanction et de réparation, et contribue ainsi à consolider l'État de droit, à garantir une protection effective des droits fondamentaux, et à forger une culture paneuropéenne d'intégrité.

Cependant, la normativité du Conseil de l'Europe ne se limite pas à la contrainte juridique. Elle s'exprime également à travers un ensemble de recommandations, principes directeurs et résolutions non contraignants qui, tout en étant dépourvus de force obligatoire, exercent une influence déterminante sur les réformes nationales. Ces instruments souples, par leur dimension éthique, pédagogique et prospective, jouent un rôle essentiel dans la diffusion des standards européens et dans l'orientation des politiques publiques. C'est à cette normativité incitative que nous allons à présent nous intéresser.

B. Des normes éthiques et politiques souples mais influentes

Cet ensemble de textes non contraignants jouent un rôle fondamental dans la structuration des politiques publiques de prévention de la corruption au sein des États membres. Ces instruments prennent la forme de résolutions ou de recommandations du Comité des Ministres. Bien qu'ils ne produisent pas d'effets juridiques obligatoires, leur portée normative est réelle : ils orientent les réformes nationales, inspirent les législateurs et servent de cadre d'évaluation pour les mécanismes de suivi, en particulier ceux du GRECO.

• Résolution (97)24 – les 20 principes directeur

Adoptée le 6 novembre 1997, la Résolution (97)24 du Comité des Ministres du Conseil de l'Europe constitue un texte fondateur de la politique anticorruption paneuropéenne. Elle énonce vingt principes directeurs, qui bien qu'ils soient non contraignants, tracent une feuille de route complète pour les États membres souhaitant mettre en place une stratégie globale, cohérente et efficace de lutte contre la corruption. Ces principes couvrent l'ensemble du spectre institutionnel et normatif, en combinant prévention, répression, éthique publique et coopération internationale.

La Résolution commence par rappeler que la lutte contre la corruption ne peut être efficace sans une stratégie globale (principe n° 1), fondée sur un engagement politique fort, la coordination des actions, et la continuité dans le temps. Elle insiste ensuite sur la nécessité d'institutions stables, indépendantes et correctement dotées pour mettre en oeuvre cette stratégie (principe n°2). Elle exige l'adoption de législations claires et répressives (principe n° 3), mais ne se limite pas à l'incrimination des faits : elle impose également l'établissement de règles de procédure efficaces, transparentes et respectueuses des droits fondamentaux pour la poursuite et le jugement des infractions de corruption (principe n°4). Ce volet procédural est essentiel pour garantir l'effectivité de la répression et éviter les blocages judiciaires ou les interférences politiques.

La Résolution encourage en outre une approche intégrée de la criminalisation (principe n°5), en englobant la corruption active et passive, le trafic d'influence, et les infractions connexes comme le blanchiment ou la dissimulation de preuves. Elle appelle les États à étendre les exigences d'intégrité au secteur privé (principe n°6), à prévoir des sanctions pénales ou administratives effectives (principe n°7), et à instaurer une responsabilité des personnes morales pour les actes de corruption commis pour leur compte (principe n°8). Elle recommande également l'interdiction, dans les relations entre secteur public et secteur privé, de tout avantage indu qui pourrait fausser les décisions publiques (principe n°9).

Dans une perspective préventive, elle promeut une culture d'éthique publique fondée sur la clarté des obligations déontologiques (principe n°10), la prévention des conflits d'intérêts (principe n°11), la déclaration

de patrimoine (principe n°12), la transparence des décisions (principe n°13) et la responsabilisation des agents publics (principe n°14). Cette dynamique s'étend au champ politique avec l'encadrement strict du financement des partis et campagnes électorales (principe n°15), perçu comme une condition indispensable d'égalité démocratique.

Le texte prescrit également le renforcement des institutions de contrôle indépendantes, dotées de pouvoirs effectifs d'investigation et de sanction (principe n° 16), ainsi qu'un système de protection fiable et dissuasif pour les lanceurs d'alerte (principe n° 17). Ces éléments visent à créer un environnement où les pratiques d'intégrité peuvent s'enraciner durablement.

Enfin, la Résolution reconnaît que la corruption dépasse les frontières et appelle à intensifier la coopération internationale (principe n°18), à développer l'assistance technique entre États (principe n°19), et à promouvoir une éducation civique à la probité dès le plus jeune âge (principe n°20), pour faire émerger une conscience collective de l'intérêt général.

Par cette architecture cohérente, la Résolution (97)24 fournit un cadre souple mais robuste pour les réformes internes. Elle irrigue les recommandations du GRECO, inspire des révisions constitutionnelles ou législatives, et alimente les politiques publiques dans les États membres. En articulant exigences pénales, garanties procédurales, prévention éthique et coordination institutionnelle, elle demeure aujourd'hui encore une référence incontournable pour tous les acteurs engagés dans la consolidation de l'État de droit face à la corruption.

• Recommandation (2000)10 sur les codes de conduite des agents publics.

Adoptée par le Comité des Ministres du Conseil de l'Europe le 11 mai 2000, la Recommandation n° R (2000)10 sur les codes de conduite pour les agents publics marque une étape déterminante dans la construction d'une éthique de la fonction publique à l'échelle européenne. Elle ne se contente pas de rappeler des principes généraux, mais propose un véritable modèle normatif détaillé que les États membres sont invités à adapter dans leurs systèmes juridiques et administratifs respectifs. Ce texte s'adresse à l'ensemble des agents exerçant une fonction publique, qu'ils soient fonctionnaires, contractuels, ou élus locaux, en soulignant que l'exemplarité de leur comportement est une condition essentielle de la légitimité de l'action publique.

La recommandation articule autour de quelques grands piliers les valeurs cardinales de la probité, de l'impartialité, de l'indépendance, de la transparence et de la responsabilité. Elle affirme que les agents publics doivent exercer leurs fonctions dans l'intérêt exclusif du public, sans chercher à tirer un avantage personnel ni favoriser un tiers. À ce titre, elle fournit un cadre précis pour encadrer les situations à risque, notamment l'acceptation de cadeaux ou d'avantages (notion de "gratuities"), les conflits d'intérêts, le cumul de fonctions, l'usage privé des biens publics, et les comportements susceptibles d'altérer la confiance dans l'administration. Le texte insiste sur la nécessité de prévoir des mécanismes clairs de prévention, de déclaration, de contrôle et de sanction.

Par ailleurs, la Recommandation met en exergue l'importance des mécanismes de transparence et de redevabilité : elle encourage notamment l'adoption de dispositifs de déclaration de patrimoine et d'intérêts, la mise en place de procédures d'alerte éthique (whistleblowing), ainsi que l'existence d'autorités ou d'officiers de déontologie dotés de moyens d'action. Elle souligne également le rôle de la formation initiale et continue à l'éthique publique, considérée comme un levier essentiel pour instaurer une culture de l'intégrité durable.

Ce texte, qui conjugue exigence morale et ingénierie administrative, a inspiré de nombreux pays dans l'élaboration ou la révision de leurs chartes de déontologie, qu'il s'agisse de codifier les obligations des agents, d'instaurer des référents déontologiques ou de créer des systèmes de supervision indépendants. Il a aussi favorisé l'émergence d'une vision professionnelle de la fonction publique, tournée vers la qualité du service rendu, la gestion des risques d'intégrité et la régulation des comportements par la norme éthique.

En somme, la Recommandation n° R (2000)10 constitue un vecteur essentiel de diffusion d'une culture européenne de la déontologie publique. Elle renforce la prévention institutionnelle de la corruption en agissant sur les comportements individuels, tout en contribuant à restaurer la confiance des citoyens dans la neutralité, l'exemplarité et l'équité de l'administration.

• **Recommandation (2003)4 sur le financement politique.**

Enfin, en 2003, la Recommandation Rec(2003)4 a traité spécifiquement de la corruption dans le financement des partis politiques et des campagnes électorales. Elle invite les États à adopter des règles communes pour garantir la transparence, l'équité et la traçabilité des flux financiers dans le champ politique. Sont notamment visées les obligations de déclaration des dons, la limitation des dépenses électorales, le contrôle des sources de financement, ainsi que l'existence d'organes de contrôle indépendants dotés de pouvoirs d'investigation et de sanction. Cette recommandation s'inscrit dans une perspective de consolidation démocratique, en ce qu'elle vise à prévenir les captations d'intérêts, à limiter l'influence des puissances économiques sur le débat politique, et à restaurer la confiance des citoyens dans les institutions représentatives.

Ainsi, même si elles ne revêtent pas un caractère juridiquement contraignant, les recommandations et principes éthiques du Conseil de l'Europe ont progressivement acquis une autorité normative qui dépasse leur statut formel. En structurant les attentes, en influençant les législateurs, et en orientant les réformes nationales, ils forment une véritable grammaire commune de la probité publique en Europe. Leur intégration croissante dans les systèmes juridiques internes, appuyée par les cycles d'évaluation du GRECO, atteste de leur capacité à irriguer en profondeur les pratiques institutionnelles, à stimuler la prévention et à diffuser une culture durable de l'intégrité.

De manière plus générale, le corpus normatif élaboré par le Conseil de l'Europe exerce un rôle structurant dans l'harmonisation des cadres juridiques nationaux. En définissant avec précision les comportements à incriminer — corruption active et passive, trafic d'influence, blanchiment des produits de la corruption — la Convention pénale (CETS n°173) et son protocole additionnel (CETS n°191) constituent le socle commun de l'espace juridique anticorruption. À cette base pénale s'ajoute la Convention civile (CETS n°174), qui reconnaît aux victimes un droit à réparation, ouvrant ainsi une voie de responsabilisation complémentaire. Le tout est renforcé par des instruments souples mais prescriptifs, qui encadrent des champs essentiels de la vie publique, tels que la conduite des agents, la prévention des conflits d'intérêts, ou encore le financement des partis.

L'ensemble de ces textes participe à la construction d'un espace européen de l'intégrité fondé sur les valeurs de transparence, de responsabilité et de respect de l'État de droit. Ils facilitent également la coopération judiciaire et administrative, en créant un langage commun entre États, condition indispensable à toute action coordonnée contre une corruption de plus en plus transnationale.

Mais produire des normes, aussi cohérentes soient-elles, ne suffit pas. Encore faut-il en garantir la mise en oeuvre effective. Or, c'est sur ce terrain que se joue la crédibilité de l'engagement anticorruption du Conseil de l'Europe. C'est pourquoi son action ne se limite pas à l'édiction de standards : elle s'accompagne d'une approche plus souple, fondée sur l'éthique, la pédagogie et la coopération. Cette seconde dimension, complémentaire et pragmatique, vise à accompagner les États dans l'appropriation des instruments, à outiller les acteurs publics, et à mobiliser l'ensemble des forces vives – administrations, société civile, chercheurs – autour d'un projet commun d'intégrité. C'est cette facette, essentielle et parfois sous-estimée, que nous allons à présent explorer.

II. L'action éthique, pédagogique et coopérative : accompagner la mise en oeuvre

Au-delà de son rôle de production normative, le Conseil de l'Europe s'illustre par un engagement concret auprès des États membres pour les accompagner dans la mise en oeuvre effective des standards anticorruption. Ce rôle d'appui s'inscrit dans une logique d'action éthique, pédagogique et coopérative, centrée sur les besoins des administrations nationales, la professionnalisation des acteurs publics et la création de dynamiques d'intégrité durables. Trois dimensions structurent cette stratégie d'accompagnement : le soutien technique adapté aux contextes locaux, le renforcement des capacités institutionnelles, et l'intégration d'approches pluridisciplinaires dans un cadre de

coopération internationale.

A. Une assistance technique contextualisée pour adapter les normes aux réalités nationales

La première modalité de cet accompagnement réside dans l'assistance technique ciblée que le Conseil de l'Europe propose aux États. Cette assistance ne se limite pas à une simple transposition juridique des normes internationales : elle vise à traduire les standards en solutions concrètes, tenant compte des contraintes administratives, politiques ou culturelles propres à chaque pays.

Cette ambition se traduit notamment par la mise en oeuvre de programmes conjoints avec l'Union européenne, à l'image du Partenariat pour la bonne gouvernance (EU-CoE PGG) ou du programme PAII-T en Tunisie, qui offrent un cadre opérationnel pour conduire des audits législatifs, formuler des recommandations de réforme, élaborer des stratégies nationales d'intégrité ou soutenir les mécanismes de contrôle existants. Ces programmes sont définis en concertation avec les autorités nationales, dans une logique d'appropriation locale et d'impact mesurable, grâce à des calendriers précis, des indicateurs d'évaluation et des boucles de rétroaction.

En ce sens, le Conseil de l'Europe n'impose pas un modèle uniforme, mais propose une ingénierie de gouvernance fondée sur le dialogue et la co-construction, à même de susciter des réformes ancrées dans les réalités nationales.

B. Le renforcement des capacités : former, accompagner, créer des communautés de pratiques

Cet accompagnement normatif et technique serait inopérant sans une attention particulière portée à la montée en compétence des acteurs institutionnels. C'est pourquoi le Conseil de l'Europe développe un large éventail d'actions de formation et de professionnalisation à destination de publics variés : magistrats, fonctionnaires, membres des corps de contrôle, élus, journalistes, mais aussi représentants de la société civile.

Ces actions prennent des formes diversifiées – séminaires, ateliers, conférences, missions d'immersion – et reposent sur une pédagogie active fondée sur l'analyse de cas pratiques, l'échange d'expériences et la résolution de problèmes. L'objectif est double : d'une part, renforcer la maîtrise des normes européennes et, d'autre part, stimuler la circulation des bonnes pratiques entre institutions et entre pays.

Par cette démarche, le Conseil de l'Europe contribue à faire émerger de véritables communautés professionnelles de l'intégrité, porteuses d'un changement culturel durable. Loin d'une approche descendante, ce modèle valorise la co-production du savoir et l'autonomisation des agents publics, acteurs clés de la mise en oeuvre effective des principes d'intégrité.

C. Une approche interdisciplinaire et partenariale au service d'une gouvernance éthique

Enfin, cette action éthique et pédagogique s'inscrit dans une approche résolument interdisciplinaire, qui constitue l'une des signatures du Conseil de l'Europe. La lutte contre la corruption n'y est pas envisagée comme un enjeu strictement juridique ou répressif, mais comme un défi global de gouvernance démocratique, mobilisant à la fois les savoirs juridiques, éthiques, politiques, économiques et technologiques.

Cela se traduit par le recours croissant à des outils innovants – open data, blockchain, intelligence artificielle, plateformes numériques – mais aussi par l'intégration dans les programmes de politiques de compliance, d'éducation à la citoyenneté, et de stratégies de communication publique. Cette vision holistique permet d'adapter les réponses à la complexité des enjeux, tout en renforçant la résilience institutionnelle face aux risques systémiques.

Par ailleurs, cette démarche s'inscrit dans une logique de partenariat international : le Conseil de l'Europe travaille en articulation avec d'autres acteurs majeurs tels que l'Union européenne, l'OCDE, l'Organisation des Nations Unies, ou encore la Banque mondiale. Cette coordination permet d'éviter la fragmentation des initiatives, de mutualiser les expertises, et de garantir la cohérence des efforts à l'échelle continentale et mondiale. Elle confirme également la reconnaissance du Conseil de l'Europe comme un référent incontournable en matière

de prévention de la corruption et de promotion de l'intégrité démocratique.

Ainsi, loin de se limiter à la production de normes, le Conseil de l'Europe s'affirme comme un acteur engagé dans l'opérationnalisation des principes d'intégrité publique. Son approche repose sur une triangulation vertueuse entre l'assistance technique adaptée, le renforcement des capacités humaines et institutionnelles, et l'innovation interdisciplinaire. En combinant expertise normative, pédagogie active et coopération stratégique, il contribue à réduire le fossé entre le droit et les pratiques, entre les ambitions politiques et les réalités administratives.

Cette stratégie d'accompagnement favorise une appropriation progressive et contextualisée des standards anticorruption, au sein même des structures étatiques et des corps intermédiaires. Elle participe à l'ancrage durable d'une culture de l'éthique publique, condition indispensable à l'effectivité des réformes dans des environnements parfois instables ou résistants.

Cependant, malgré la richesse de cet arsenal normatif et l'intensité des efforts d'accompagnement, des écarts persistants subsistent entre les engagements formels des États et leur mise en oeuvre concrète. Ces écarts soulèvent des interrogations sur les limites de l'influence du Conseil de l'Europe, mais aussi sur les obstacles structurels, politiques ou institutionnels qui freinent l'adhésion pleine et entière à ses principes.

C'est pourquoi il est désormais nécessaire d'interroger l'effectivité réelle de cette action, d'identifier les freins qui persistent, et de réfléchir aux leviers d'amélioration. Tel est l'objet de la troisième partie :

III. L'évaluation de l'effectivité : entre ambitions normative et réalités fragmentées

Si l'ambition normative du Conseil de l'Europe et ses actions d'accompagnement constituent des avancées majeures, leur portée réelle dépend de la capacité des États à transposer et mettre en oeuvre ces standards dans leurs systèmes juridiques et administratifs. C'est à l'épreuve de cette effectivité que se joue la crédibilité de l'ensemble du dispositif européen de lutte contre la corruption.

A. Un écart persistant entre normes adoptées et réalités nationales

L'un des défis majeurs que rencontre le Conseil de l'Europe dans sa lutte contre la corruption réside dans la difficile articulation entre l'arsenal normatif adopté — conventions, protocoles, résolutions, recommandations — et sa transposition effective dans les ordres juridiques nationaux. Si l'adhésion formelle aux textes du Conseil est souvent rapide, elle ne garantit ni une transposition sincère, ni une application pérenne. Cette disjonction entre l'intention normative et la mise en oeuvre concrète constitue aujourd'hui un angle mort préoccupant de la stratégie anticorruption européenne.

Ainsi, sous l'impulsion des conventions pénale (CETS n°173) et civile (CETS n°174), ou à la suite des évaluations du GRECO, de nombreux États membres ont adopté des lois en apparence conformes aux standards européens. Mais dans la pratique, la transposition reste incomplète, les interprétations nationales tendent parfois à neutraliser les effets des normes, et la volonté politique fléchit dès que les réformes heurtent des intérêts établis. L'appropriation des instruments du Conseil reste hétérogène : tandis que des États comme la Géorgie ou la Lituanie ont engagé des réformes structurelles ambitieuses, d'autres comme la Hongrie ou la Turquie font l'objet de critiques récurrentes pour leur manque de coopération et leur refus de se conformer aux recommandations du GRECO, notamment en matière de transparence politique ou d'indépendance de la justice.

B. Des freins institutionnels et opérationnels multiformes

Au-delà du manque de volonté politique, l'effectivité souffre également de résistances structurelles. Dans plusieurs États, les réformes se heurtent à des oppositions internes : inerties administratives, blocages parlementaires, réticences au sein des corps de contrôle. En Bulgarie, par exemple, le dispositif de prévention des conflits d'intérêts reste largement inefficace, faute de moyens humains et financiers suffisants, et en l'absence d'un véritable pilotage

politique.

Les inégalités de capacité sont également flagrantes. Dans de nombreux pays des Balkans occidentaux, les agences anticorruption fonctionnent avec des effectifs très limités, des compétences restrictives, et une exposition directe aux pressions politiques, qui nuit à leur indépendance et affaiblit leur légitimité. Dans ces contextes, les réformes juridiques restent souvent formelles, sans capacité réelle de mise en oeuvre.

C. Une culture éthique encore fragile dans de nombreux États

Mais la technicité institutionnelle ne saurait masquer un autre facteur, plus diffus mais tout aussi décisif : la faiblesse, voire l'absence, d'une culture solide de l'éthique publique. L'édiction de codes de conduite ou la création d'instances de contrôle ne suffisent pas à transformer les pratiques si ces dispositifs ne s'accompagnent pas d'un travail sur les représentations, les incitations et les comportements. Dans les régimes où les institutions sont affaiblies, la société civile marginalisée, et les contre-pouvoirs réduits, les mécanismes éthiques restent symboliques ou purement cosmétiques.

Le cas de la Serbie en est une illustration marquante : malgré l'existence d'une stratégie anticorruption et d'un cadre législatif relativement complet, le GRECO pointe l'ineffectivité des instances mises en place, l'absence de contrôle parlementaire, et la persistance de l'impunité des élites. Sans culture d'intégrité, sans responsabilisation collective, les normes restent lettre morte.

Ainsi, l'un des enseignements majeurs de cette analyse réside dans la nécessité, pour le Conseil de l'Europe, de dépasser l'approche strictement formelle de l'évaluation normative. Ce dépassement est désormais engagé. Depuis 2021, un tournant stratégique s'est amorcé, notamment dans le cadre des 4e et 5e cycles du GRECO, avec une attention accrue portée à l'effectivité des normes dans les pratiques, les institutions, et les représentations. L'approche évolue ainsi vers une logique fondée sur les résultats concrets : réduction des opportunités de corruption, efficacité des organes de contrôle, transformation des comportements, perception citoyenne de l'intégrité publique.

Ce nouveau paradigme suppose une montée en puissance des instruments qualitatifs et quantitatifs : évaluations ex post, indicateurs d'impact, analyses contextuelles, enquêtes de terrain. Il appelle également une plus grande implication des acteurs non institutionnels — société civile, chercheurs, journalistes — dans la production de données et l'analyse critique des politiques. Il s'agit d'instaurer une culture de la redevabilité réelle, non pas fondée sur les engagements proclamés, mais sur leur mise en oeuvre effective. Cette dynamique, encore inégale, constitue un levier stratégique pour donner vie aux normes anticorruption et renforcer la confiance dans les institutions démocratiques.

IV. Vers une meilleure effectivité : quels leviers de renforcement ?

Si le Conseil de l'Europe a joué un rôle pionnier dans la structuration d'un droit européen de la lutte contre la corruption, l'un des défis les plus pressants aujourd'hui est celui de l'effectivité réelle des instruments adoptés. Cette effectivité ne dépend pas uniquement de la qualité intrinsèque des normes, mais aussi de leur appropriation institutionnelle, de leur déploiement pratique, et de leur réception sociale. Pour combler l'écart persistant entre ambitions normatives et réalités d'application, plusieurs leviers de renforcement peuvent être envisagés, à la fois juridiques, institutionnels et démocratiques.

A. Renforcer la contrainte sans briser l'adhésion

Le Conseil de l'Europe repose sur un modèle de soft law, fondé sur l'incitation, la coopération et la pression des pairs. Ce modèle a permis d'établir un socle commun de principes éthiques et juridiques, tout en respectant les souverainetés nationales. Mais cette souplesse atteint ses limites lorsque certains États adoptent une stratégie d'apparence : ratification rapide, transposition partielle, application dévoyée ou neutralisation administrative. La montée des régimes illibéraux dans certains États membres a révélé la vulnérabilité de ce système fondé sur la loyauté coopérative.

Dans ce contexte, un premier axe de renforcement consiste à mieux

articuler incitation et contrainte. Les recommandations du GRECO n'ont pas de force obligatoire juridique mais leur suivi repose sur des rapports de conformité rendus publics. Depuis le quatrième cycle d'évaluation, ce mécanisme a été renforcé, avec des procédures plus rigoureuses et une pression accrue fondée sur la réputation. Il serait désormais opportun d'envisager un statut renforcé pour certaines recommandations-clés – par exemple, celles touchant à l'indépendance du pouvoir judiciaire, à la prévention des conflits d'intérêts ou à la transparence du financement politique – en les liant à des incitations positives : accès conditionné à des programmes d'assistance technique, à des plateformes de coopération, voire à certains financements européens.

La question de la cohérence normative avec l'Union européenne se pose également. Pour les États membres des deux organisations, les exigences issues du Conseil de l'Europe et de l'UE peuvent parfois paraître redondantes, voire contradictoires. Pourtant, une meilleure coordination entre les instruments du Conseil (conventions anticorruption, recommandations du GRECO) et ceux de l'Union (Parquet européen, directive sur les lanceurs d'alerte 2019/1937, directive 2024/1260 sur la confiscation et le recouvrement des avoirs) permettrait d'éviter les chevauchements et d'accroître l'efficacité globale des dispositifs. L'expérience des conditionnalités liées à l'état de droit dans l'Union européenne pourrait inspirer des mécanismes similaires de coopération différenciée au sein du Conseil de l'Europe.

B. Mieux outiller les institutions nationales

Une législation conforme aux standards européens ne suffit pas à garantir l'intégrité publique : encore faut-il que les institutions nationales chargées de sa mise en oeuvre disposent des ressources, des compétences, et de l'indépendance nécessaires pour en assurer l'opérationnalité.

Le Conseil de l'Europe joue ici un rôle fondamental à travers ses programmes de coopération technique. Des initiatives conjointes, comme le Partenariat pour la bonne gouvernance (EU–CoE PGG) dans les pays du Partenariat oriental, ou le programme régional Sud V en Méditerranée, permettent de proposer des missions d'assistance sur mesure, allant de l'audit législatif à l'élaboration de politiques publiques, en passant par l'appui à la réforme institutionnelle. Ces interventions sont co-construites avec les autorités nationales et incluent des mécanismes de suivi pour garantir leur ancrage et leur efficacité.

La formation des acteurs publics constitue un autre pilier central. Le Conseil propose des modules de sensibilisation destinés aux magistrats, parlementaires, agents publics, responsables de l'éthique ou des corps de contrôle, adaptés aux enjeux contemporains : cybercorruption, opacité du lobbying, corruption environnementale. L'approche pédagogique privilégie la résolution de cas concrets, le partage d'expériences entre pairs, et la création de communautés de pratiques.

Les agences anticorruption indépendantes, lorsqu'elles existent, doivent aussi faire l'objet d'un soutien prioritaire. Cela implique des garanties juridiques solides d'indépendance, des dotations budgétaires adéquates, des pouvoirs d'enquête autonomes, et une reconnaissance institutionnelle claire. L'exemple de la DNA en Roumanie ou de la Commission nationale anticorruption en Géorgie montre que, lorsqu'elles sont appuyées de manière durable et respectueuse du contexte local, ces structures peuvent devenir des piliers crédibles de la lutte contre la corruption.

C. Impliquer la société civile et les chercheurs

L'intégrité publique ne saurait être imposée par le seul haut de la pyramide. Elle repose aussi sur la mobilisation des citoyens, des journalistes, des chercheurs, des ONG, et des lanceurs d'alerte. Le Conseil de l'Europe promeut de plus en plus une gouvernance anticorruption participative, dans laquelle la transparence et le contrôle citoyen jouent un rôle central.

L'ouverture des données publiques, l'accès aux registres d'intérêts, la transparence budgétaire doivent devenir des standards partagés. Mais cette ouverture doit être effective et utilisable : les données doivent être accessibles, lisibles, interopérables, exploitables par les acteurs de la société civile. Le développement de technologies citoyennes — plateformes d'alerte, algorithmes de détection des anomalies, intelligence artificielle

pour analyser les marchés publics — ouvre des perspectives prometteuses. Le Conseil pourrait renforcer son soutien à ces initiatives dans le cadre du programme Octopus ou à travers ses réseaux sur l'éthique numérique.

Le monde académique a, lui aussi, un rôle essentiel à jouer. Il peut contribuer à la production d'analyses critiques, à la mesure indépendante des politiques publiques, à l'élaboration d'indicateurs d'impact. Le Conseil devrait amplifier ses partenariats avec les universités, soutenir les jeunes chercheurs spécialisés en gouvernance publique, et favoriser la recherche interdisciplinaire.

Enfin, les lanceurs d'alerte doivent bénéficier d'un cadre de protection effectif. La directive (UE) 2019/1937 en fournit une base robuste pour les États membres de l'UE, mais de nombreux États du Conseil de l'Europe restent en retrait. Le Conseil pourrait engager un dialogue intergouvernemental sur la convergence des normes de protection, appuyer les mécanismes internes de signalement, et soutenir les plateformes d'accompagnement psychologique et juridique.

Garantir l'effectivité des instruments anticorruption suppose d'agir simultanément sur trois fronts stratégiques. Il faut d'abord consolider l'autorité des normes, en renforçant la portée politique des recommandations-clés. Ensuite, outiller durablement les institutions nationales, en leur donnant les moyens de mettre en oeuvre les standards adoptés. Enfin, il est indispensable d'associer les sociétés civiles, les chercheurs et les citoyens à la construction d'un écosystème d'intégrité. Cette approche intégrée, qui combine incitation, capacitation et participation, est la seule à même de garantir des transformations profondes, légitimes et pérennes. Elle incarne l'ambition d'un Conseil de l'Europe qui ne se contente pas de fixer des normes, mais s'attache à les rendre vivantes et appropriées, au coeur des institutions comme au sein des sociétés européennes.

Conclusion générale

Le parcours que nous avons tracé à travers les quatre premières parties de ce cours met en lumière l'ampleur de l'ambition du Conseil de l'Europe dans la lutte contre la corruption, mais aussi les tensions qui en limitent encore l'effectivité.

À l'origine, une ambition normative forte : conventions pénale et civile, protocoles additionnels, recommandations éthiques — autant d'instruments qui posent un socle européen cohérent articulant prévention, sanction, réparation et responsabilité. À cette base s'ajoute un accompagnement éthique, pédagogique et coopératif, fondé sur la co-construction avec les États, la formation des acteurs publics, l'appui à l'expertise locale et l'innovation interdisciplinaire. Toutefois, comme l'a montré l'évaluation de l'effectivité, ce socle normatif ne produit ses effets que s'il rencontre une volonté politique sincère, des institutions crédibles et une culture de l'intégrité partagée.

Des résistances persistent, tantôt institutionnelles, tantôt politiques ou culturelles. La fragmentation de la mise en oeuvre, l'ineffectivité de certaines agences anticorruption, la faiblesse de la culture déontologique dans plusieurs États membres nuisent à la crédibilité des engagements pris. C'est pourquoi l'enjeu actuel est moins de produire de nouvelles normes que de renforcer leur appropriation, leur contrôle, leur incarnation. Ce renforcement suppose de mieux articuler incitation et contrainte, d'outiller les institutions publiques et d'impliquer pleinement la société civile et les milieux académiques.

L'UNIVERSITÉ D'ÉTÉ OCEAN 2025 : SCIENCE, DROIT ET ENGAGEMENT CONTRE LA CORRUPTION

Du 30 juin au 4 juillet 2025, l'Université de Strasbourg, en partenariat avec le Conseil de l'Europe, a accueilli une université d'été consacrée aux instruments juridiques du Conseil de l'Europe de lutte contre la corruption. Cette session, organisée dans le cadre du réseau OCEAN (Open Council of Europe Academic Networks), s'est tenue à la Faculté de droit et au siège du Conseil de l'Europe. Elle a réuni une vingtaine de doctorants, des magistrats, universitaires, experts internationaux, membres d'ONG et représentants d'entreprises privées, dans un format pluridisciplinaire résolument interactif.

Cette université d'été s'inscrit dans le prolongement d'un travail collectif initié en février 2022 sous l'impulsion d'Olaf Kondgen. Elle fait suite au colloque international du 13 octobre 2023 à Strasbourg, intitulé « L'apport des conventions du Conseil de l'Europe à la lutte contre la corruption ». Elle marque un tournant : celui de l'entrée de ces instruments dans le champ académique comme leviers normatifs d'actions concrètes.

Le réseau OCÉAN : renforcer l'impact des conventions par la recherche

Fondé en 2018 à l'initiative du professeur Michele Nicoletti, alors président de l'Assemblée parlementaire du Conseil de l'Europe, le réseau OCEAN vise à

ancrer durablement les conventions du Conseil dans l'enseignement supérieur et la recherche. L'Université de Strasbourg, membre institutionnel actif du réseau, s'engage dans cette dynamique à travers des formations, des publications et l'organisation d'événements scientifiques. Cette université d'été en est une illustration exemplaire.

Des échanges féconds entre savoirs académiques et pratiques de terrain

La session dédiée à la lutte contre la corruption, codirigée avec ma collègue Florence Thépot, s'est articulée autour d'un principe fondateur : le croisement des savoirs. Nous avons donné la parole à des intervenants aux parcours et compétences complémentaires :

Juliette Lelieur, Vincent Filhol, Anne Weber, Lise Chipault, Yves-Marie Doublet, Anna Myers, Sébastien Dupent, Thomas Schaller, Grégoire Moreels, Maximilien Roche

Leur contribution a permis d'explorer des thématiques telles que la protection des lanceurs d'alerte, le rôle du GRECO, les normes anti-blanchiment, ou encore les liens entre compliance et probité institutionnelle.

Remerciements

Je tiens à exprimer ma profonde gratitude au Conseil de l'Europe, et particulièrement à Olaf Kondgen, moteur de cette dynamique, ainsi qu'à Gianluca Esposito, aujourd'hui directeur général des droits humains et de l'État de droit, dont le parcours au sein du GRECO, puis comme directeur de cabinet de la Secrétaire générale, incarne une vision rigoureuse et engagée du service public européen.

Merci également à tous les intervenants, aux doctorants, aux services de la Faculté de droit, de l'École doctorale et de la Fédération de recherche « L'Europe en mutation » pour leur appui précieux.

Ensemble, nous faisons vivre cette exigence collective de probité et de justice.

CONFÉRENCE

COMPTE RENDU DU SÉMINAIRE « L'INTELLIGENCE ARTIFICIELLE AU SERVICE DE LA COMPLIANCE : INNOVATIONS ET PERSPECTIVES »

16 mai 2025 – Faculté de droit de l'Université de Strasbourg

Organisé par les étudiants du Master 2 Juriste Conseil des Collectivités et des Organisations (JCCO), sous la direction de Mme Chantal Cutajar.

Le présent compte rendu restitue les échanges du séminaire organisé le 3 juillet 2025 par les étudiants du Master 2 « Juriste conformité et conformité opérationnelle » (JCCO) de l'Université de Strasbourg, sous la direction de Mme Chantal Cutajar, Maître de conférences HDR, directrice du Master.

Ce séminaire, inscrit dans le cadre d'un module de projet collectif, avait pour ambition de croiser les regards sur un thème émergent et structurant : **« L'intelligence artificielle au service de la compliance : innovations et perspectives »**.

Le choix de cette thématique a émergé d'un travail de réflexion collective mené avec les étudiants, qui ont identifié les enjeux multiples soulevés par l'IA dans les pratiques de conformité : détection des schémas de blanchiment complexes, réduction des faux positifs, explicabilité des algorithmes, responsabilité juridique, protection des données personnelles, etc.

Organisé autour de **trois tables rondes**, ce séminaire a réuni des intervenants issus du monde académique, du secteur bancaire, des legaltechs, ainsi que des professions juridiques, permettant d'ouvrir un **dialogue interdisciplinaire** sur les défis et opportunités de l'IA en matière de LCB-FT, de protection des données et de lutte contre la corruption.

Ce document est le **fruit d'un travail collectif**, entièrement conçu, structuré et rédigé par les étudiants. Il a fait l'objet d'une relecture approfondie, dans le respect des exigences éditoriales, afin d'en faire une contribution publiable et utile aux professionnels de la compliance, aux chercheurs, ainsi qu'aux régulateurs.

Il témoigne de l'engagement pédagogique du Master JCCO à former des juristes capables de penser et de piloter l'innovation juridique dans un monde en transformation.

Introduction

Ce séminaire a été organisé dans le cadre du module « Projet collectif » du Master 2 JCCO, qui vise à développer des compétences transversales essentielles à l'exercice des professions juridiques : la gestion de projet, le travail en équipe, la communication institutionnelle, et la capacité à problématiser une question contemporaine dans une perspective juridique et opérationnelle.

Le thème retenu – L'intelligence artificielle au service de la compliance – a émergé à la suite d'un brainstorming collectif conduit par les étudiants. Ce choix s'inscrit dans une actualité juridique et technologique dense, marquée notamment par l'adoption du règlement européen sur l'intelligence artificielle (IA Act). L'intelligence artificielle, en pleine expansion, transforme les pratiques de conformité, soulève de nouveaux défis éthiques et juridiques, et interroge la place du facteur humain dans la prise de décision automatisée.

Le séminaire s'est structuré en quatre temps :

- une conférence introductive sur le cadre juridique de l'intelligence artificielle, centrée sur

l'IA Act ;

- suivie de trois tables rondes thématiques :
  - la première consacrée à l'IA et à la protection des données à caractère personnel ;
  - la deuxième à l'IA appliquée à la lutte contre le blanchiment de capitaux et le financement du terrorisme (LCB-FT) ;
  - la troisième aux usages de l'IA dans la prévention de la corruption.

Les échanges ont été nourris, riches en perspectives croisées entre le monde académique, les praticiens du droit, les experts en conformité et les professionnels de la cybersécurité.

Conférence introductive : Présentation du règlement européen IA Act

Intervenant : M. Emmanuel Netter, professeur de droit privé à l'Université de Strasbourg, spécialiste du droit du numérique, des données personnelles et de l'intelligence artificielle.

La conférence introductive a permis de poser les fondations juridiques du séminaire, à travers une présentation claire et synthétique du règlement européen sur l'intelligence artificielle, connu sous le nom d'IA Act. Ce texte, récemment adopté, constitue la première tentative au niveau mondial de réguler l'IA selon une approche fondée sur les risques que ces systèmes peuvent faire peser sur les droits fondamentaux.

Objectifs du règlement

Le professeur Netter a rappelé que le texte poursuit plusieurs objectifs majeurs :

- Encadrer le développement, le déploiement et l'usage des systèmes d'IA dans l'Union européenne ;
- Prévenir les usages abusifs de l'IA, notamment en matière de surveillance de masse ou de discrimination ;
- Renforcer la transparence, la sécurité et la robustesse des systèmes d'IA, en imposant des obligations spécifiques aux développeurs, importateurs et utilisateurs.

Classification des systèmes d'IA

Le coeur du dispositif repose sur une classification des systèmes d'IA selon leur niveau de risque, permettant d'ajuster les obligations à la dangerosité potentielle des usages :

- Les IA interdites : ce sont les systèmes jugés contraires aux droits fondamentaux, comme les techniques de manipulation subliminale, le scoring social de type chinois, ou encore l'usage en temps réel de la reconnaissance faciale dans l'espace public (sauf exceptions très limitées, notamment pour la lutte contre le terrorisme).
- Les IA à haut risque : ces systèmes, souvent intégrés dans des domaines sensibles (emploi, éducation, santé, police, justice, infrastructures critiques), doivent respecter des exigences strictes en matière de qualité des données, de documentation, de traçabilité, de cybersécurité et d'auditabilité.
- Les systèmes à usage général (comme ChatGPT) : bien qu'ils ne soient pas intrinsèquement à haut risque, ils peuvent générer des usages problématiques. Une nouvelle catégorie leur est dédiée, afin d'assurer transparence, contrôle des données d'apprentissage et devoirs de vigilance.
- Les systèmes d'IA interactifs : ceux qui interagissent avec des humains doivent signaler leur nature non humaine pour éviter toute confusion.

Incidences pour les acteurs de la compliance

Le professeur Netter a insisté sur les implications concrètes du règlement pour les professionnels de la conformité :

- L'obligation de transparence algorithmique, de traçabilité des décisions et de documentation des processus;
- L'intégration de l'IA dans des dispositifs de conformité sectorielle (LCB-FT, anticorruption, RGPD, etc.) ;
- La nécessité pour les organisations concernées de mettre en place des procédures d'évaluation de conformité, y compris le marquage CE, et de s'appuyer sur des normes ISO, comme la future ISO 42001 (système de management de l'IA).

Défis juridiques identifiés

Plusieurs défis ont été soulevés :

- La définition large et floue de l'intelligence artificielle, calquée sur celle de l'OCDE, soulève des incertitudes quant au champ d'application exact du règlement ;
- L'encadrement encore partiel des modèles d'IA générative et des deepfakes, ainsi que les difficultés liées à l'articulation avec d'autres cadres juridiques (RGPD, propriété intellectuelle,

secret des affaires) ;

- Le risque d'une surveillance accrue, notamment à travers les usages de la reconnaissance faciale ou du profilage prédictif.

Cette intervention a permis de montrer que le règlement IA Act est à la fois une avancée normative importante et un défi de mise en oeuvre, qui exigera des entreprises une vigilance juridique renforcée et une adaptation de leurs pratiques internes de conformité.

Table ronde n°1 : L'intelligence artificielle et la protection des données à caractère personnel

Intervenants :

- Maître Anaïs Merires, avocate au barreau de Paris, spécialisée en droit du numérique
- Maître Flora Brac de la Perrière, ancienne juriste à la CNIL, avocate au cabinet Vigo, spécialisée en droit du numérique, IA et données à caractère personnel
- M. Sébastien Dupent, professeur agrégé d'économie-gestion option système d'information, spécialiste en cybersécurité et cybercriminalité

Modératrices :

- Oriana Saunier et Mathilde Denny

Cette première table ronde a porté sur les tensions et articulations entre le développement de l'intelligence artificielle et les exigences de protection des données personnelles dans un cadre dominé par le Règlement général sur la protection des données (RGPD). Si l'IA ouvre de nombreuses possibilités pour améliorer la gestion de l'information et automatiser certains processus de conformité, elle fait aussi naître des risques accrus en matière de surveillance, de discrimination, et de perte de contrôle sur les données.

Compatibilité de l'IA avec le RGPD

Les intervenants ont rappelé que, malgré les bouleversements technologiques, le RGPD reste pleinement applicable aux systèmes d'IA qui traitent des données personnelles. L'article 22 du RGPD, relatif aux décisions automatisées, constitue un point central du débat. La suspension de ChatGPT en Italie a illustré les tensions possibles entre innovation technologique et respect des obligations de transparence et de licéité.

Toutefois, plusieurs limites d'ordre technique et juridique ont été soulignées : la mise en oeuvre du droit à l'effacement dans un système d'apprentissage automatique, par exemple, pose des difficultés pratiques majeures. Cela implique de repenser la notion de finalité et d'adapter les outils juridiques existants.

Encadrement juridique de l'apprentissage automatique

L'apprentissage d'un système d'IA repose généralement sur des bases de données massives, parfois constituées à partir de données personnelles. La CNIL a publié des fiches techniques pour guider les professionnels sur des points comme l'anonymisation, la minimisation des données, ou le principe de finalité. Elle insiste sur la nécessité de maintenir une approche de « Privacy by Design », c'est-à-dire d'intégrer la protection des données dès la conception des systèmes.

Gouvernance des données et nouveaux risques

Un autre axe de discussion a porté sur les modalités concrètes de gouvernance des données en contexte d'IA. Les intervenants ont évoqué la nécessité de mettre en place une cartographie des traitements, un référent IA, et une documentation des processus, afin d'assurer un pilotage maîtrisé des risques.

Les nouveaux risques identifiés incluent :

- les deepfakes, menaçant l'intégrité des identités numériques ;
- les phénomènes de biais discriminants, issus de corpus d'entraînement non représentatifs (ex. : cas d'Amazon) ;
- les effets de boîte noire, qui rendent les décisions difficilement explicables et auditables ;
- la surveillance prédictive, facilitée par le croisement d'ensembles de données massives.

Anonymisation et performance de l'IA

La question de l'impact de l'anonymisation sur la performance des IA a également été abordée. Les intervenants ont souligné que des techniques comme la pseudonymisation, la differential privacy ou encore l'usage de données synthétiques permettent de limiter les atteintes à la vie privée sans compromettre la qualité de l'apprentissage algorithmique. Plusieurs normes ISO sont en cours d'élaboration ou déjà disponibles sur ces points.

IA et cybersécurité

L'impact de l'IA sur la cybersécurité a été envisagé dans une double perspective :

- Négative, car l'IA peut être détournée à des fins malveillantes : attaques de phishing renforcées, cassage automatisé de

mots de passe, usurpations d'identité via des contenus générés artificiellement ;

- Positive, en tant qu'outil de défense : détection automatisée des menaces, surveillance en temps réel, analyse prédictive des comportements à risque.

Auditabilité des algorithmes

Enfin, les participants ont discuté de la possibilité d'auditer un algorithme comme on audite un processus. Cela suppose de pouvoir en évaluer la transparence, la loyauté et les éventuels biais. Cette audibilité conditionne la conformité aux principes du RGPD et le respect du droit à l'explication.

Points saillants

Plusieurs enseignements et controverses ont émergé de cette table ronde :

- La tension entre l'efficacité technologique et la protection des libertés fondamentales ;
- La difficulté de mettre en oeuvre certains droits (comme l'effacement) dans un contexte d'IA ;
- Le risque de voir les systèmes algorithmiques renforcer des biais systémiques existants ;
- La nécessité absolue de maintenir une supervision humaine dans toutes les situations à fort enjeu éthique ou juridique.

Table ronde n°2 : L'intelligence artificielle au service de la lutte contre le blanchiment de capitaux et le financement du terrorisme (LCB-FT)

Intervenantes :

- Maître Flora Brac de la Perrière, ancienne juriste à la CNIL, avocate au cabinet Vigo, spécialisée en droit du numérique, IA et données à caractère personnel
- Mme Chantal Cutajar, maître de conférences HDR à l'Université de Strasbourg, directrice du Master JCCO et experte en LCB-FT

Modérateurs :

- Ilyas Aynan et Bartu Deger

Cette deuxième table ronde a permis d'aborder les apports opérationnels de l'intelligence artificielle dans les dispositifs de LCB-FT, tout en examinant les risques éthiques, juridiques et techniques associés à son utilisation croissante. L'objectif était de mettre en lumière la manière dont l'IA modifie en profondeur la prévention des risques financiers, tout en interrogeant sa compatibilité avec les principes fondamentaux de l'État de droit.

Un nouveau levier face à des fraudes toujours plus complexes

Les intervenantes ont d'abord rappelé le contexte : les schémas de blanchiment sont de plus en plus sophistiqués, les volumes de transactions explosent, et les dispositifs traditionnels de surveillance (fondés sur des règles fixes ou des seuils) montrent leurs limites.

Dans ce cadre, l'intelligence artificielle constitue un outil d'aide à la détection et à la priorisation : elle permet de traiter des volumes massifs de données, de repérer des signaux faibles, d'analyser le comportement des clients, et de cartographier des relations cachées entre entités. Elle facilite également l'identification des bénéficiaires effectifs, la détection de structures opaques ou circulaires, et l'analyse de rétrotransferts.

Mais l'IA ne se substitue pas à l'expertise humaine : elle fournit des indicateurs, des probabilités, des hypothèses. Seul l'humain peut en tirer des conclusions juridiques et décider d'un éventuel signalement à TRACFIN.

Détection de schémas complexes

Mme Cutajar a précisé que l'intelligence artificielle permet de dépasser les approches traditionnelles fondées sur des typologies figées. Grâce au machine learning, il est désormais possible de détecter des circuits de blanchiment non répertoriés, en constante évolution, qui seraient passés inaperçus avec les seuls outils classiques.

Un exemple concret a été cité : en 2021, l'IA a permis à une banque européenne de détecter un réseau de sociétés-écrans impliquées dans du blanchiment circulaire en Europe de l'Est, grâce à la reconstitution de flux faibles, fragmentés, mais récurrents — là où chaque transaction, prise isolément, paraissait anodine.

Réduction des faux positifs

Un enjeu essentiel est la réduction du nombre de faux positifs, qui peut atteindre plus de 90 % dans certaines institutions. Ces alertes non pertinentes créent une surcharge pour les équipes de conformité et un affaiblissement du dispositif global.

L'IA permet d'améliorer significativement la qualité des alertes grâce à plusieurs leviers :

- le remplacement des règles figées par des modèles auto-apprenants (machine learning) ;

- l'analyse comportementale dynamique, qui tient compte du profil, des habitudes, et du contexte des opérations ;

- l'intégration du retour d'expérience des analystes humains (feedback loop), qui affine progressivement les algorithmes ;

- la segmentation des clients, afin d'adapter les seuils et les scénarios selon le type d'activité, la taille ou le profil de risque.

Des exemples ont été évoqués : la banque ING a réduit de 40 % ses faux positifs grâce à ces outils ; Revolut, de son côté, applique une segmentation comportementale fine qui ajuste les règles de détection en temps réel.

Proportionnalité et loyauté des traitements

Me Brac de la Perrière a ensuite abordé la question de la compatibilité de l'usage de l'IA avec les principes de proportionnalité et de loyauté. Elle a souligné que les outils d'IA, par leur nature intrusive, doivent faire l'objet d'une analyse d'impact juridique et éthique. La CNIL a d'ailleurs appelé à une vigilance particulière dans le cadre des textes européens relatifs à la LCB-FT, notamment s'agissant des données sensibles (infractions pénales, convictions religieuses, etc.).

Elle a rappelé que l'inefficacité actuelle de la LCB-FT ne résulte pas d'un manque d'IA, mais d'une inflation de déclarations de soupçons peu qualifiées, souvent motivées par une logique de protection juridique des assujettis. L'enjeu est donc de restaurer la qualité de l'analyse, et non simplement d'en automatiser le volume.

Risque de surveillance généralisée

La discussion s'est poursuivie autour du risque de surveillance généralisée, notamment en cas de mutualisation excessive des données entre acteurs. Une disposition du projet de règlement LCB-FT prévoyait le partage d'informations entre assujettis ; la CEPD s'y est opposée, soulignant le risque de disproportion et d'atteinte aux libertés individuelles.

La question de la responsabilité a été posée : selon Me Brac de la Perrière, celle-ci incombe au responsable du traitement, c'est-à-dire à l'entité qui détermine les finalités et les moyens du traitement algorithmique.

Auditabilité des outils par les régulateurs

Enfin, il a été précisé que les régulateurs doivent pouvoir auditer les outils d'IA utilisés dans un contexte LCB-FT, y compris s'ils reposent sur des logiques propriétaires ou complexes. La sensibilité de la finalité (lutte contre la criminalité financière) ne dispense pas d'un contrôle indépendant.

L'humain au coeur du processus décisionnel

Mme Cutajar a conclu en soulignant que l'IA ne saurait remplacer le rôle du juriste, du compliance officer ou du DPO dans l'analyse éthique et juridique des alertes. L'humain reste le garant de la loyauté des traitements, de la contextualisation des soupçons, et de la prise en compte des droits fondamentaux.

Plutôt que de marginaliser l'expertise humaine, l'IA doit la renforcer en libérant du temps, en améliorant la précision des alertes, et en fournissant des outils d'aide à la décision plus performants.

Table ronde n°3 : L'intelligence artificielle et la prévention de la corruption

Intervenants :

- M. Philippe Lesoing, cofondateur et directeur général d'EuroCompliance

- Mme Florence Thépot, maître de conférences

- M. Cyrille Cardonne, fondateur du cabinet Arkane Risk

Modérateurs :

- Aysegul Can et Sufyan Demir

Cette dernière table ronde a exploré les applications de l'intelligence artificielle dans la prévention et la détection des situations de corruption, avec un accent mis sur les signaux faibles, les conflits d'intérêts, les cartographies de risques et les dérives potentielles de l'automatisation. L'enjeu était double : comprendre ce que l'IA peut apporter de manière concrète aux dispositifs anticorruption, tout en identifiant les limites, biais et risques liés à son usage.

Détection des signaux faibles et conflits d'intérêts

M. Philippe Lesoing a expliqué que l'IA permet aujourd'hui de détecter des signaux faibles souvent indécelables par l'analyse humaine. Elle est capable de :

- traiter de volumes massifs de données financières et contractuelles ;

- identifier des anomalies statistiques dans les flux ou les comportements ;

- cartographier les réseaux relationnels entre personnes morales et physiques, pour révéler des conflits d'intérêts cachés ;

- analyser les langages et les échanges (emails, appels d'offres) pour identifier des indices de favoritisme.

Il a distingué deux types d'apprentissage :

- supervisé, qui s'appuie sur des cas connus pour identifier des schémas similaires ;

- non supervisé, qui détecte des regroupements inhabituels de comportements (clusters), sans connaissance préalable.

Toutefois, il a rappelé que les signaux faibles ne sont jamais des preuves : ils doivent toujours être vérifiés, contextualisés et interprétés par un analyste humain, notamment pour éviter les faux positifs.

Apports concrets en entreprise

M. Cyrille Cardonne a illustré ces propos par des exemples concrets issus de la pratique. Les entreprises, lorsqu'elles souhaitent évaluer l'exposition à la corruption d'un partenaire ou d'un client, sollicitent des cabinets spécialisés qui mobilisent des bases de données externes (souvent non soumises au RGPD). Ces analyses permettent une évaluation initiale des risques, complétée ensuite par une cartographie plus qualitative, fondée sur des audits et des entretiens.

Il a évoqué l'utilisation de l'IA dans la constitution de profils psychologiques, pour anticiper certaines vulnérabilités comportementales. Il a également insisté sur la capacité de l'IA à produire une cartographie dynamique et évolutive des risques, qui se réajuste au fil des données nouvelles.

Gains d'efficience pour les autorités

Mme Florence Thépot a apporté un éclairage universitaire sur les usages institutionnels de l'IA. Elle a rappelé que les autorités fiscales et anticorruption utilisent déjà des outils d'intelligence artificielle, notamment :

- l'OLAF (Office européen de lutte antifraude), qui analyse les correspondances électroniques pour détecter des réseaux frauduleux ;

- le Serious Fraud Office (Royaume-Uni), qui recourt à l'IA pour trier des volumes importants de documents ;

- la Banque mondiale, qui met à disposition des États des outils comme GRAS (Governance Risk Assessment System), utilisés pour identifier des anomalies dans les procédures de marchés publics.

L'IA permet donc un ciblage plus précis des enquêtes et un gain de temps considérable, sans pour autant évacuer la nécessaire interprétation humaine.

Apports de l'IA à la cartographie des risques

Les échanges ont ensuite porté sur la cartographie des risques anticorruption, qui constitue un pilier des dispositifs de conformité. Les intervenants ont souligné que l'IA :

- permet une actualisation en temps réel des cartographies en fonction des données internes et des évolutions réglementaires ;

- offre des capacités de personnalisation selon les secteurs, la taille de l'entreprise, les zones géographiques ;

- facilite une hiérarchisation dynamique des risques, grâce à un scoring évolutif en fonction des probabilités et des impacts.

Toutefois, cette puissance dépend de la qualité des données utilisées, et de la transparence des algorithmes. La supervision humaine reste indispensable pour interpréter les résultats, justifier les arbitrages et éviter les dérives.

Risques de dérives et de stigmatisation

La question des risques liés à l'automatisation de l'analyse éthique des comportements a ensuite été débattue. Mme Thépot a alerté sur plusieurs dangers :

- la fiabilité incertaine des données d'entrée, qui peuvent induire des biais ou des erreurs ;

- le risque de surveillance excessive, en particulier dans les outils prédictifs utilisés par les administrations publiques ;

- le danger de stigmatisation, lorsqu'un comportement est mal interprété ou sorti de son contexte.

Elle a cité un exemple marquant : aux Pays-Bas, un système algorithmique utilisé pour détecter les fraudes aux aides sociales a été jugé discriminatoire et non transparent, entraînant sa suspension. Ce cas illustre les conséquences graves d'un usage mal encadré de l'IA.

L'IA et l'éthique : vers un cadre de référence

La table ronde s'est achevée par une discussion sur les principes éthiques devant encadrer l'usage de l'IA en conformité.

Les intervenants ont rappelé l'importance :

- du respect des droits fondamentaux (non-discrimination, vie privée) ;
- de la transparence des systèmes et de leur auditabilité ;
- de la clarté dans l'imputation des responsabilités ;
- et de la nécessité de maintenir l'humain dans la boucle décisionnelle.

M. Lesoing a souligné qu'un compliance officer ne suffit plus : les organisations devront intégrer des profils spécialisés, comme des DPO formés aux problématiques de l'IA. Mme Thépot a insisté sur le fait qu'une IA « éthique » n'est pas seulement une IA conforme au droit, mais une IA respectueuse des finalités démocratiques et du principe de loyauté.

Pour une meilleure lisibilité, les quatre défis majeurs évoqués dans cette conclusion pourraient être présentés sous forme de liste structurée ou de paragraphes séparés.

Conclusion

Ce séminaire a permis de dresser un panorama approfondi et pluriel des interactions entre intelligence artificielle et dispositifs de compliance, à la lumière des enjeux soulevés par le règlement européen IA Act et des exigences pratiques des secteurs concernés.

L'intelligence artificielle, en tant qu'outil technologique, offre des perspectives prometteuses pour renforcer la détection des anomalies, améliorer la qualité des alertes, optimiser la gestion des risques, et soutenir les professionnels de la conformité dans leurs missions de prévention et de contrôle. Qu'il s'agisse de protection des données, de lutte contre le blanchiment et le financement du terrorisme, ou de prévention de la corruption, l'IA est d'ores et déjà intégrée dans de nombreux dispositifs, publics comme privés.

Toutefois, ces avancées ne doivent pas occulter les défis majeurs qui les accompagnent :

- la nécessité d'un encadrement juridique clair, articulé avec les cadres existants (RGPD, droit pénal, normes ISO) ;
- la garantie de l'explicabilité et de l'auditabilité des systèmes automatisés ;
- la qualité des données d'entrée, sans laquelle aucun modèle ne peut produire des résultats fiables ;
- la vigilance éthique face aux risques de biais, de discrimination, de surveillance excessive, ou de déresponsabilisation humaine.

Ce séminaire a mis en évidence un principe transversal : l'IA ne peut ni remplacer le discernement humain, ni se substituer à l'analyse juridique et éthique. Elle doit être conçue et utilisée comme un levier de performance responsable, au service d'une conformité plus efficace, plus dynamique, mais aussi plus respectueuse des droits fondamentaux.

Le compliance officer, le juriste, le DPO ou encore l'expert en cybersécurité restent les garants de cette exigence d'équilibre. La formation continue, la pluridisciplinarité et le dialogue constant entre droit et technologie apparaissent plus que jamais essentiels.

En conclusion, Mme Chantal Cutajar a salué l'engagement des étudiants du Master JCCO dans l'organisation de ce séminaire, ainsi que la qualité des interventions proposées par les professionnels invités, qui ont su croiser les approches juridiques, techniques et opérationnelles. La richesse des échanges témoigne de la nécessité d'une réflexion collective et anticipatrice sur l'usage de l'IA en matière de compliance.

MOT MÊLÉ

LES MOTS SONT PLACÉS

HORIZONTALEMENT, VERTICALEMENT, DIAGONALES ET INVERSÉS

E T I M R O F N O C N B S E E N N O D U
C O R R U P T I O N W T E Y Z U S T F J
G T D E J Z Z X V C P N V F F M J C B E
G V G T C R H R H A R H A R R T S U C R
Z P W I H O R F M M A B Q A S E Q X P U
L O J L C I N B R C O A Q U N X Y F E D
E U Q I P T N T S R I N U D O N G U G E
Q E I B Y A R T R N K G Z E I D M K I C
Q L O A Y K D I E A L R V U T Q R Q T O
A Y C S R E G Q S G T U L H C C H S I R
L D G N I F E B B Q R J C J N A C A L P
E E D O C O H P G G U I G F A D N F O F
R N R P W E F C Y R H E T S S S P O L O
T R N S D S Z G N I K T N E M E L G E R
E Z M E R D V Y G G U X I B T C X H R F
Z M P R O A U D I T W J C R I R M P W O
S G Q B I X E T H I Q U E Y W O G A M O
S W F I T D E O N T O L O G I E F V C K
V I Y Y M D A T R A N S P A R E N C E A
F R A B O K Z I L S H V S Q A N E W D J

Mots à trouver :

- CONFORMITE
- ETHIQUE
- RGPD
- FRAUDE
- CORRUPTION
- SANCTIONS
- AUDIT
- ALERTE
- RESPONSABILITE
- PROCEDURE
- INTEGRITE
- DEONTOLOGIE
- TRANSPARENCE
- CODE
- CONTRAT
- DROIT
- LITIGE
- REGLEMENT
- RISQUE
- DONNEES

DROIT ET FINANCE : UN NOUVEAU CAP POUR LES PROFESSIONNELS DE L'INVESTIGATION ÉCONOMIQUE

Découvrez le Master 2 Investigations financières à l'échelle européenne sur le site internet du Service formation continue de l'Université de Strasbourg :https://sfc.unistra.fr

Face à l'essor de la criminalité économique et financière à l'échelle européenne, les besoins en compétences juridiques et financières spécialisées n'ont jamais été aussi marqués. C'est dans ce contexte qu'a été conçu le Master 2 *Investigations financières à l'échelle européenne*, proposé à distance par l'Université de Strasbourg, dans le cadre du parcours Droit des affaires.

Cette formation diplômante, unique en son genre, se donne pour ambition de former des professionnels capables d'évoluer dans un environnement où se croisent enquêtes financières, droit pénal des affaires et coopération judiciaire européenne. À travers une approche résolument ancrée dans la pratique, les étudiants apprennent à mobiliser les outils d'investigation, de gel, de saisie et de restitution des avoirs, tout en s'appropriant les mécanismes de coopération transfrontalière.

Pensé pour les actifs, ce parcours mise sur la flexibilité sans faire l'impasse sur l'exigence : modules mensuels, évaluation continue à distance, cas pratiques, classes virtuelles hebdomadaires et ressources pédagogiques variées (capsules vidéo, documentation spécialisée…).

Ouverte aussi bien aux juristes qu'aux profils issus de l'audit, de la finance, de la gestion ou du secteur public, la formation couvre un large champ de compétences : comptabilité financière, cybercriminalité, renseignement financier, droit pénal, coopération judiciaire, etc. L'enseignement est assuré par une équipe mixte d'universitaires et de professionnels de terrain, issus aussi bien du secteur privé que d'administrations spécialisées.

« Un encadrement rigoureux, à la fois théorique et opérationnel, où la notion de probité est centrale », souligne Cécile GRENARD, spécialiste de la compliance et des achats, qui a renforcé sa pratique de la conformité internationale à travers cette formation, après un premier MBA.

Pourquoi cette formation ?

- **Une formation inédite** : aucun autre master d'État ne propose aujourd'hui un programme aussi complet consacré à l'investigation financière à l'échelle européenne.
- **Une formule pensée pour les professionnels** : le rythme, le format et les outils s'adaptent aux contraintes des actifs en poste.
- **Une communauté d'experts** : la formation s'appuie sur un réseau d'intervenants expérimentés, engagés dans la lutte contre les fraudes économiques.

Informations pratiques

- **Informations à propos de ce Master** : https://sfc.unistra.fr
- **Candidatures** : ouvertes sur la plateforme eCandidat de l'Université de Strasbourg, du 2 juin au 31 octobre 2025.
- **Sélection** : sur dossier, suivi d'un entretien individuel.
- **Organisation** : un module par mois, soutenance du mémoire prévue en février 2027.