Sentinelles et outils à l'œuvre dans la lutte antiblanchiment

Gilles Favarel-Garrigues, Thierry Godefroy, Pierre Lascoumes

Actualité de la recherche

XXII.4
Septembre 2009

Questions Pénales

CESDIP
Centre de Recherches Sociologiques sur le Droit et les Institutions Pénales
UMR 8183

www.cesdip.fr

Sentinelles et outils à l'œuvre dans la lutte antiblanchiment

Gilles FAVAREL-GARRIGUES *(CERI-Sciences Po),* ***Thierry GODEFROY*** *(CESDIP) et* ***Pierre LASCOUMES*** *(CEVIPOF-Sciences Po)* *rendent compte d'une enquête menée auprès des acteurs professionnels de l'antiblanchiment. Ce numéro de* Questions Pénales *porte plus particulièrement sur la mise en œuvre des dispositifs de vigilance et de signalement dévolus aux acteurs bancaires.*

Il y a vingt ans se tenait à Paris, en juillet 1989, la réunion du G7 qui lançait la lutte internationale contre le blanchiment des capitaux issus du trafic de drogue et propulsait les banques à l'avant-poste de ce combat en leur confiant des missions de surveillance des flux financiers. Cette innovation surprenante, en contradiction avec les principes les plus ancrés de la profession (la non-intrusion dans les décisions économiques des clients et le respect d'une stricte confidentialité à l'égard de tout acteur extérieur, sauf exceptions administratives et judiciaires strictement limitées) a connu un profond succès international. Le message a été largement diffusé et la lutte institutionnalisée. Tous les pays ont progressivement adopté les normes internationales de l'antiblanchiment et un nouvel organisme international, le Groupe d'Action Financière Internationale, créé à l'issue de ce sommet de l'Arche, a vu ses missions étendues à de nouvelles cibles (le financement du terrorisme, la lutte contre la prolifération nucléaire).

La lutte antiblanchiment combine un double registre d'action : d'une part une législation pénale instituant une nouvelle incrimination (introduite en France dès 1987 dans le Code de la santé publique au titre de la législation contre les drogues) ; et d'autre part un ensemble d'obligations de vigilance dévolues aux acteurs professionnels (créé en juillet 1990 et intégré ensuite au Code monétaire et financier). La législation, assez sévère, reste en pratique totalement subordonnée au système de vigilance, qui est bien plus souple car il reste entre les mains d'acteurs professionnels privés au premier rang desquels se trouvent les banques. Celles-ci ont été contraintes d'adapter une logique jusque-là exclusivement commerciale à une mission de police : elles doivent détecter, et au besoin signaler, les transactions jugées douteuses. Si, à l'origine, seul l'argent du trafic de stupéfiant était concerné, le champ qu'elles ont à scruter a été progressivement élargi aux produits financiers générés par la quasi-totalité des infractions (toutes celles punies d'au moins un an d'emprisonnement) et les acteurs professionnels visés multipliés : cela concerne non seulement tous les intermédiaires financiers mais également les avocats, comptables, agents immobiliers, directeurs de casinos, les marchands d'art, les acteurs des jeux et loteries tous les commerçants pour des paiements supérieurs à 15 000 euros en espèces.

Le dispositif de vigilance et de signalement ainsi créé oblige les banques à surveiller leurs clients et leurs opérations et à déclarer leurs soupçons à Tracfin (organisme créé à cet effet au ministère des Finances). Cette unité de renseignement financier reçoit ainsi annuellement de l'ordre de 12 000 signalements d'opérations financières atypiques (les déclarations de soupçon). Après analyses, ces déclarations peuvent conduire Tracfin à informer le Procureur de la République (environ 400 dossiers par an) qui décide des suites pénales. En 2008, les déclarations reçues par Tracfin ont augmenté pour dépasser les 14 000 alors que les transmissions à la justice en vue de

Méthodologie

Cette recherche s'appuie sur plus de soixante-dix entretiens réalisés en deux vagues entre 2005 et 2008. Certains interlocuteurs ont pu être interrogés au début et au terme de la recherche. En outre une dizaine d'entretiens ont été menés avec des responsables suisses de l'antiblanchiment. Ils ont permis de valider nos hypothèses dans un contexte national différent. Les trois quarts des personnes rencontrées sont des responsables de la lutte antiblanchiment dans les établissements bancaires. Ces professionnels agissent en tant que responsables de la conformité ou *chief compliance officers*, coordonnant à un titre ou à un autre la lutte antiblanchiment dans l'établissement bancaire.

Nous avons veillé à varier les profils d'établissement bancaire, en fonction de leur domaine d'activité (banques de détail, banques d'affaires et d'investissement), de leur périmètre d'action (du global au national) et de leur clientèle (vocation populaire de la « banque de masse » ou au contraire élitiste dans le cas de la gestion des fortunes).

Cette enquête a été complétée par des entretiens avec les autres acteurs de la lutte anti-blanchiment, qu'ils participent à l'édiction des normes au niveau national (ministères de la Justice et de l'Économie) ou international (GAFI et FMI) ; ou qu'ils constituent l'environnement professionnel des *compliance officers*, des régulateurs publics (Tracfin, Commission bancaire) aux consultants privés et aux producteurs d'outils informatiques spécialisés.

Nous avons conduit des entretiens semi-directifs, à partir d'une grille combinant des questions personnelles sur la carrière de l'interlocuteur, l'attrait exercé par la lutte anti-blanchiment, les difficultés rencontrées, les projets poursuivis et des interrogations plus générales valorisant son expertise (sur l'actualité, les pratiques, la politique gouvernementale, le milieu même des experts…).

UNIVERSITÉ DE VERSAILLES SAINT-QUENTIN-EN-YVELINES

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE LA JUSTICE

poursuites éventuelles ont sensiblement diminué (*cf.* graphique *infra*).

Les établissements se sont ainsi progressivement dotés d'une organisation interne de contrôle du risque de non-conformité et de procédures propres à assurer ces obligations dont le contrôle est assuré par la Commission bancaire. Si, aujourd'hui, le dispositif bancaire de vigilance, équipé d'outils de filtrage, de profilage et de gestion des risques, concerne tous les clients et toutes les opérations, le ralliement de la profession fut cependant laborieux.

Un ralliement laborieux des banques

Durant les années 1990, la sensibilisation du milieu bancaire à ces nouvelles obligations s'opère lentement. À la fin de la décennie, la traduction opérationnelle demeure inégale et globalement faible, ainsi que le constate une enquête de la Commission Bancaire, dont les commentaires jugés « décevants, dévalorisants pour le secteur bancaire » par le responsable de la Commission de l'époque ne furent jamais publiés. De même, le procès dit du « Sentier II » mettant en cause la Société Générale pour des faits de blanchiment entre 1998 et 2001 révèle qu'en son sein, la cellule de lutte antiblanchiment de la banque ne dispose pas des moyens nécessaires pour se conformer à ces obligations : elle ne comprend que deux personnes...

À partir de 2000-2001, les choses évoluent : la totalité des établissements se dotent de dispositifs internes, de cellules spécialisées, de procédures écrites, d'une politique de formation des personnels, tandis qu'une nouvelle spécialité professionnelle, celle de responsable de la conformité ou *compliance officer* selon le terme employé dans la profession, est inventée sur le tas. Dans les plus grands réseaux financiers, 500 à 1 000 personnes peuvent maintenant exercer des missions de lutte antiblanchiment. Elles sont même souvent plus de 2 000, si l'on compte celles occupées à des tâches connexes d'audit interne et de gestion des risques. Les banques s'équipent enfin d'instruments informatiques onéreux et le recours à des outils de filtrage des opérations et d'analyse comportementale des clients est devenu aujourd'hui une pratique ordinaire.

En contrepartie de leur rôle pivot dans la lutte antiblanchiment, les banques obtiennent de bénéficier d'une grande latitude pour apprécier la gravité des situations atypiques. Elles peuvent maintenant graduer leur vigilance, allégée ou renforcée, selon le risque, sans toutefois se soustraire à l'obligation de signalement dès lors qu'elles soupçonnent une opération de blanchiment.

Ce changement complet est un cas de rupture brutale sous l'effet conjugué d'un événement critique (les attentats du 11 septembre et l'orientation prise vers la lutte contre le financement du terrorisme), de la mise en examen de certains dirigeants de grands établissements bancaires (Société Générale) et d'assurance (AXA), et d'un changement de modalités d'action (désormais fondées sur l'évaluation des risques).

Le développement des instruments

Le développement des outils qui prend forme au milieu des années 1990 à un niveau expérimental, se généralise à partir de 2001. Conçus sur la base de techniques différentes (aide aux diagnostics médicaux par la combinaison d'antécédents ; analyse de liens issue des développements de l'analyse criminelle et appliqués aux meurtres en série, analyse textuelle), ces outils ont convergé et proposé des solutions pour mettre en œuvre la lutte antiblanchiment.

La possibilité d'utiliser des systèmes automatisés de détection en matière financière est d'abord considérée pour l'aide qu'elle peut apporter à la régulation publique. Le FinCEN, l'unité chargée de recevoir aux États-Unis les déclarations obligatoires des banques, doit gérer dès le milieu des années 1990 plus de 10 millions de ces déclarations. En 1994, l'*Office of Technology Assessment* rédige un rapport qui amorce le recours à l'extraction de données (*data mining*). L'attention commence également à se porter à ce moment-là sur le développement des systèmes de transfert de fonds électroniques en liaison avec les mesures prises dans le cadre de la lutte contre le trafic de stupéfiants et le terrorisme. De nouveaux instruments proposent de repérer, au sein d'un flux, les transactions suspectes par rapport à des normes externes prédéfinies : listes de personnes ou critères (chèques supérieurs à 30 000 euros par exemple). Ce sont des outils prescriptifs qui imposent une décision.

À partir des années 2000-2001 le nouvel impératif mondial de lutte contre le financement du terrorisme et la nouvelle orientation de la lutte antiblanchiment modulant les obligations de vigilance selon le risque accélèrent la diffusion des instruments informatisés. Les listes produites par des organismes internationaux sont complétées par des listes de personnes à haut risque dites « politiquement exposées », produites par des prestataires privés. L'un des leaders de ce type de prestations d'information sur le client (Factiva) intégré au groupe Dow Jones génère, à partir de l'analyse de plus de 10 000 sources (journaux, dépêches d'agences, informations en ligne, rapports de sociétés…) venant d'une centaine de pays, les profils détaillés de plus de 500 000 personnes dont 30 000 pour la France. L'outil, mis à jour quotidiennement, peut être paramétré en fonctions des risques spécifiques que l'organisation veut cibler. Il s'agit d'un outil semi-prescriptif.

La seconde grande catégorie d'outils est plus complexe et concerne l'analyse des comportements des clients et des comptes par modélisation des risques. Elle doit permettre de fonder un choix, en différenciant les pratiques « normales » et « anormales » pour chaque client et en établissant notamment des relations non apparentes entre des transactions. Ce type d'instrument s'efforce de tenir compte des caractéristiques propres à chacun des clients ; de détecter les schémas habituels de blanchiment mais aussi leurs formes plus rares ou encore inconnues ; d'aider à l'analyse du contexte (historique d'un client et d'un compte, comparaison avec le profil de pairs) ; enfin, de centraliser toutes les alertes au sein d'une même organisation indépendamment du lieu de l'opération. Très clairement, il s'agit de fournir à ces sentinelles que sont les *compliance officers*, une aide à la décision et une trace des diligences accomplies. Les outils les plus récents proposent ainsi une intervention en quatre étapes : l'alerte, l'investigation-analyse, le suivi de la gestion du dossier d'alerte et le signalement (déclaration de soupçon) automatisé.

Les instruments actuels tendent à intégrer dans une seule offre les différentes approches en proposant un système expert qui travaille à partir de faits et de règles connus (une liste, un seuil quantitatif…) ; un système d'identification de profils, qui raisonne à partir d'une mémoire de situations déjà identifiées et les met en relation pour distinguer des indices ; enfin, un système d'évaluation en continu des clients, qui analyse toutes les transactions et les note selon trois coefficients de risque (faible, normal, élevé). En produisant un journal des alertes, l'outil offre la trace de l'action entreprise, une preuve « auditable » des diligences effectuées.

Les instruments et les sentinelles en action

La définition des paramètres à la base de leur fonctionnement tout comme l'interprétation des résultats fournis reposent en très grande partie sur les acteurs bancaires. Tous insistent sur l'importance capitale des opérations de paramétrage, comme ce responsable antiblanchiment d'une banque internationale : « C'est nous qui définissons le profil, ce n'est pas un profil *a priori* ». Les choix qui en découlent constituent donc un enjeu central, auquel tous les acteurs répondent sur la base de leur expérience interne. Il s'agit pour eux de trouver empiriquement un équilibre entre deux risques : d'un côté, celui de l'acceptation d'un client ou d'une opération problématique susceptible de rejaillir sur la réputation de l'établissement, d'un autre côté, celui d'être submergé par des alertes ingérables. Il n'existe pas de règles professionnelles générales en ce domaine. La pratique est le principal facteur de stabilisation de ces choix.

Toutes les présentations publicitaires des instruments insistent sur leur capacité à faciliter la conformité avec les régulations nationales et internationales en éliminant la réalisation de transactions irrégulières et en détectant les clients à haut risque financier. Mais, contrairement à ces annonces, ces instruments sont loin de résoudre la totalité des difficultés auxquelles sont confrontés les chargés de clientèles et les *compliance officers*. En effet, leur niveau élevé de sophistication technologique pose, à l'usage, de nombreux problèmes pratiques.

Il n'échappe pas aux utilisateurs qu'il existe un écart important entre les alertes produites par l'instrument et la réalité des situations qu'ils ont concrètement à gérer. Ainsi pour l'établissement Île-de-France d'un grand réseau bancaire national, ce sont 45 000 alertes/an que produisent les

outils. Parmi ces « remontées de doutes », un millier environ sera pris au sérieux et conduira *in fine* à la transmission d'une centaine de déclarations de soupçon à Tracfin. Ces chiffres soulignent combien l'intervention des sentinelles reste, malgré l'automaticité vendue, déterminante dans les signalements.

En ce qui concerne les listes, leur contenu est devenu tellement pléthorique qu'il arrive régulièrement d'avoir affaire à des homonymes (source de « faux positifs »). La gestion des listes de PPE (personnes politiquement exposées) a démultiplié les problèmes pour les utilisateurs : « On s'y perd. Il y a des listes officielles : OFAC (5 000 à 6 000 noms), UE (1 500 noms[1]), France (200), et des listes commerciales : les listes PPE font 275 000 noms ou même, pour un outil comme Factiva, 470 000 ! Pour les PPE, il n'y a pas de listes officielles. Les fournisseurs y mettent ce qu'ils veulent » déplore un consultant chargé d'implanter ces instruments.

Quant aux analyses comportementales, leur sensibilité aux situations atypiques est parfois telle qu'une opération sortant légèrement de l'ordinaire de la part d'un client régulier (montant ou destinataire inhabituel, par exemple) peut être repérée. Dans ces différents cas, souvent après un premier tri opéré par le service central antiblanchiment de l'établissement, les chargés de clientèle reçoivent un message de demande d'information sur le dossier. Et il leur appartient d'opérer les vérifications. En pratique, celles-ci se limitent souvent à un échange téléphonique avec le client, malgré toutes les difficultés (et le risque commercial) qu'impliquent ce type d'échanges lors desquels un prestataire de service manifeste sa suspicion. Les possibilités concrètes de contrôle de ce dernier demeurent limitées. Comment valider une identité ? Comment s'assurer de la légalité d'un versement lorsque le client déclare rémunérer un fournisseur ou effectuer un placement ? Il faudrait une situation particulièrement alarmante pour que la banque demande (en dehors de l'ouverture d'un compte) à consulter des documents d'identité ou l'original d'un contrat ou d'une facture qui justifierait un paiement

Inversement, si les « faux positifs » sont un problème, les professionnels en pointent volontiers un autre tout aussi aigu : les difficultés de repérage des opérations litigieuses, bien dissimulées sous l'apparence d'opérations commerciales. Le propre des opérations financières illicites en général et de celles de blanchiment en particulier est de reposer sur une volonté de dissimulation ; l'organisation de l'opacité est une dimension centrale, qui atteint souvent un niveau élevé de sophistication. Les ressources en ce domaine ont été multipliées par l'internationalisation des échanges, par l'offre émanant des places *offshore*, mais aussi par celle des établissements qui, en pratique, n'adhèrent pas à la lutte antiblanchiment. Enfin, les blanchisseurs sont les meilleurs connaisseurs des techniques de surveillance et ils ne cessent d'adapter leurs méthodes aux systèmes de contrôle des établissements financiers. C'est pourquoi les opérateurs sont particulièrement dubitatifs quant à la capacité des instruments à détecter les fraudes sophistiquées. Comme l'observe le responsable de la lutte antiblanchiment d'une banque internationale : « les systèmes informatiques sont rassurants mais ils n'apportent pas beaucoup d'informations sur le lieu où sont abrités les fonds. Si nous avons du hors-bilan et que ça passe par une structure à Jersey (…), je n'ai pas vu beaucoup d'outils informatiques qui soient capables de détecter ça. Il n'y a souvent rien qui retienne l'attention ».

Si le repérage des opérations primaires de blanchiment (remise ou retrait d'une grande quantité d'espèces, ouverture d'un compte par une PPE d'un pays en développement, approvisionnement soudain d'un compte dormant par un virement massif émanant d'un établissement inconnu ou établi dans une place listée, etc.) a très peu de chance d'échapper à la vigilance des professionnels (soutenus par les instruments), il est loin d'en être de même pour les opérations sophistiquées, en particulier celles qui utilisent le canal d'intermédiaires « honorablement connus ».

Cette gestion différentielle des soupçons de blanchiment en fonction de la nature supposée des infractions sous-jacentes conduit-elle par contrecoup à privilégier certaines formes supposées de délinquance ? C'est ce que suggèrent plusieurs interlocuteurs, qui considèrent que la lutte antiblanchiment ne parvient à saisir que la « petite délinquance » incapable de déjouer les dispositifs de détection mis en place. Les *compliance officers*, soucieux de présenter des résultats, sont tentés de privilégier les cibles les plus exposées : « On a une obligation de moyens : il faut qu'on soit blanc vis-à-vis de la Commission bancaire. Le contenu, tout le monde s'en fout. Concrètement, on trouve de petits dealers que de toute façon on n'a pas intérêt à avoir comme clients. Ça sert à les repérer et les éliminer de notre clientèle ».

Profilage incertain et atteintes aux libertés

Les techniques de *profiling* sur lesquelles reposent en grande partie ces instruments suscitent également des réserves. Les points de discussion que nous avons relevés dans notre enquête, menée en France et en Suisse, rejoignent ceux présentés dans les travaux anglo-saxons[2]. Les débats s'organisent autour de trois axes : des questions de principe sur le *profiling*, des problèmes pratiques de mise en œuvre et d'efficacité, enfin, des questions liées à l'impact de ces instruments sur l'identité professionnelle des banquiers.

Tout d'abord, le principe même du recours au *profiling* est discuté dans la mesure où il ne peut être qu'une abstraction inférée à partir de comportements observés ou considérés comme possibles. Le profil repose sur la corrélation de données censées caractériser un modèle identifiant une personne, une organisation ou une pratique. Tout dépend donc de la qualité ou de la pertinence des informations sur lesquelles il repose. Certes le renseignement financier a été considérablement développé depuis une vingtaine d'années et le *profiling* permet d'optimiser l'utilisation de ressources rares. Mais, dans l'esprit d'un nombre important d'utilisateurs, la compilation maximale de cas pas davantage que la forte capacité des logiciels à établir des corrélations entre des faits épars ne sont une garantie absolue de la validité des profils. Les spécialistes des instruments observent aussi une tendance inflationniste dans la collecte de données. Initialement, le *profiling* ne repose que sur des données nécessaires à la compréhension des seules transactions, mais peu à peu le champ a été considérablement élargi. La tendance a été de maximiser le recueil des informations, y compris en incluant des données personnelles, pour les utiliser à des fins de marketing, de renforcement de la sécurité et/ou de compréhension du comportement des clients : « C'est un peu *Big Brother*, on sait tout d'un client, mais que fait-on de tout ça ? » déclare un *compliance officer*.

Cette dynamique cumulative est renforcée par un mouvement qui fait passer le *profiling* d'une simple description synthétique du passé à des tentatives de prédiction, dont les pratiques de *scoring* des clients sont symptomatiques. Ce renforcement de la centralisation des informations conduit certains professionnels à s'interroger sur les conséquences de ces pratiques par rapport aux valeurs professionnelles de garantie du secret bancaire, et parfois, plus largement, par rapport au respect des droits individuels. Dans les pays anglo-saxons, le débat est beaucoup plus nourri, dans la mesure où le *profiling* est mis en relation avec les risques de discrimination au sein de la clientèle[3] et pose de façon plus large la question de la protection de la vie privée, mise en cause par les possibilités contemporaines de surveillance par les données (*dataveillance*[4]).

L'étendue des possibilités offertes par ces outils pose potentiellement des problèmes d'atteintes aux libertés fondamentales, comme l'a relevé, la CNIL, pour la France dans un rapport de 2003. Celui-ci souligne que ces dispositifs négligent la protection des données nominatives et que les textes ne se réfèrent pas clairement à la réglementation Informatique et libertés. Pour la CNIL, si l'inobservation de la réglementation antiblanchiment « est pénalement

[1] La liste UE ne comporte en fait que trente organisations et vingt-six personnes.

[2] CANHOTO A.I., 2007, Profiling Behaviour : the Social Construction of Categories in the Detection of Financial Crime, *Department of Management*, London, London School of Economics and Political Science. WEBB L., 2004, A Survey of Money Laundering Reporting Officers and their Attitudes Towards Money Laundering Regulations, *Journal of Money Laundering Control*, 7, 4, 367-375.

[3] SCHAUER F., 2003, *Profiles, Probabilities and Stereotypes*, Cambridge, Harvard University Press. HILDEBRANDT M., GUTWIRTH S., 2008, *Profiling the European Citizen. Cross-Disciplinary Perspectives*, Dordrecht, Springer.

[4] LEVI M., WALL D.S., 2004, Technologies, Security and Privacy in Post 9/11 European Information Society, *Journal of Law and Society*, 31, 2, 194-220.

sanctionnée, le non-respect de règles relatives à l'Informatique et aux libertés est susceptible d'entraîner des condamnations pénales d'une égale importance »[5].

Cette intervention de la CNIL dans le paysage semble constituer, au premier abord, une source de tensions entre les impératifs nés du cadre normatif de la lutte antiblanchiment et contre le financement du terrorisme et ceux de la protection des libertés individuelles, continuellement renforcée tant au niveau hexagonal qu'européen. Ces principes, ont cependant progressivement perdu de leur vigueur : les contraintes de déclaration des banques ont été simplifiées dès 2005, puis, en 2006-2007, de nouvelles décisions ont élargi les modalités de partage de l'information – jusque-là proscrit – au sein des groupes bancaires et facilité la mise en œuvre des fermetures de comptes. Les nécessités de la lutte anticlanchiment, et surtout de la lutte contre le terrorisme, sont des impératifs avec lesquels la CNIL a dû composer.

Les *compliance officers* qui s'inquiètent du climat d'insécurité juridique dans lequel ils évoluent déclarent « craindre » la CNIL et éprouvent des difficultés à anticiper et à répondre à ses attentes : l'un d'entre eux la compare même à un « angle mort ».

[5] CNIL, 2003, *La lutte contre le blanchiment d'argent et le financement du terrorisme au sein des organismes financiers : quels enjeux pour la vie privée de la clientèle bancaire ?*, séance du 7 octobre 2003, 10.

Une conformité défendable

Pas davantage la sophistication des instruments que leur empilement n'ont donc résolu toutes les difficultés et incertitudes auxquelles sont confrontés les acteurs bancaires depuis qu'ils sont en charge de la lutte antiblanchiment. Notre recherche montre que le développement de ces outils ne repose pas sur un large accord quant à leur efficacité et à leur but.

Leur diffusion dans la pratique bancaire paraît, au bout du compte, paradoxale.

Notre interprétation est que la contradiction apparente entre la réussite et le doute se résout lorsqu'on déplace le questionnement en montrant que les attentes principales à l'égard des outils ne portent pas principalement sur ce qu'ils affichent officiellement, à savoir une performance sélective. Leur efficacité pour l'organisation et ses acteurs se situe ailleurs. L'appui sur les instruments est avant tout un signal de conformité. Leur usage et les empreintes qu'ils produisent sont là pour témoigner concrètement de la soumission aux normes publiques et aux bonnes pratiques professionnelles de l'organisation en matière de lutte antiblanchiment.

En définitive, la brillante carrière de ces instruments s'explique sans doute moins par la sécurité qu'ils offrent en matière de risque-clientèle, que par celle qu'ils procurent par rapport au risque de régulation publique. L'instrument produit ici moins une sécurité opérationnelle qu'une sécurité « d'auditabilité[6] », une conformité crédible (« *défendable compliance*[7] »), au sens d'un dispositif qui vise à protéger l'établissement contre des mises en cause et qui peut aussi être assumé publiquement.

Gilles FAVAREL-GARRIGUES
(*favarel@ceri-sciences-po.org*),
Thierry GODEFROY
(*godefroy@cesdip.fr*)
et
Pierre LASCOUMES
(*pierre.lascoumes@sciences-po.fr*)

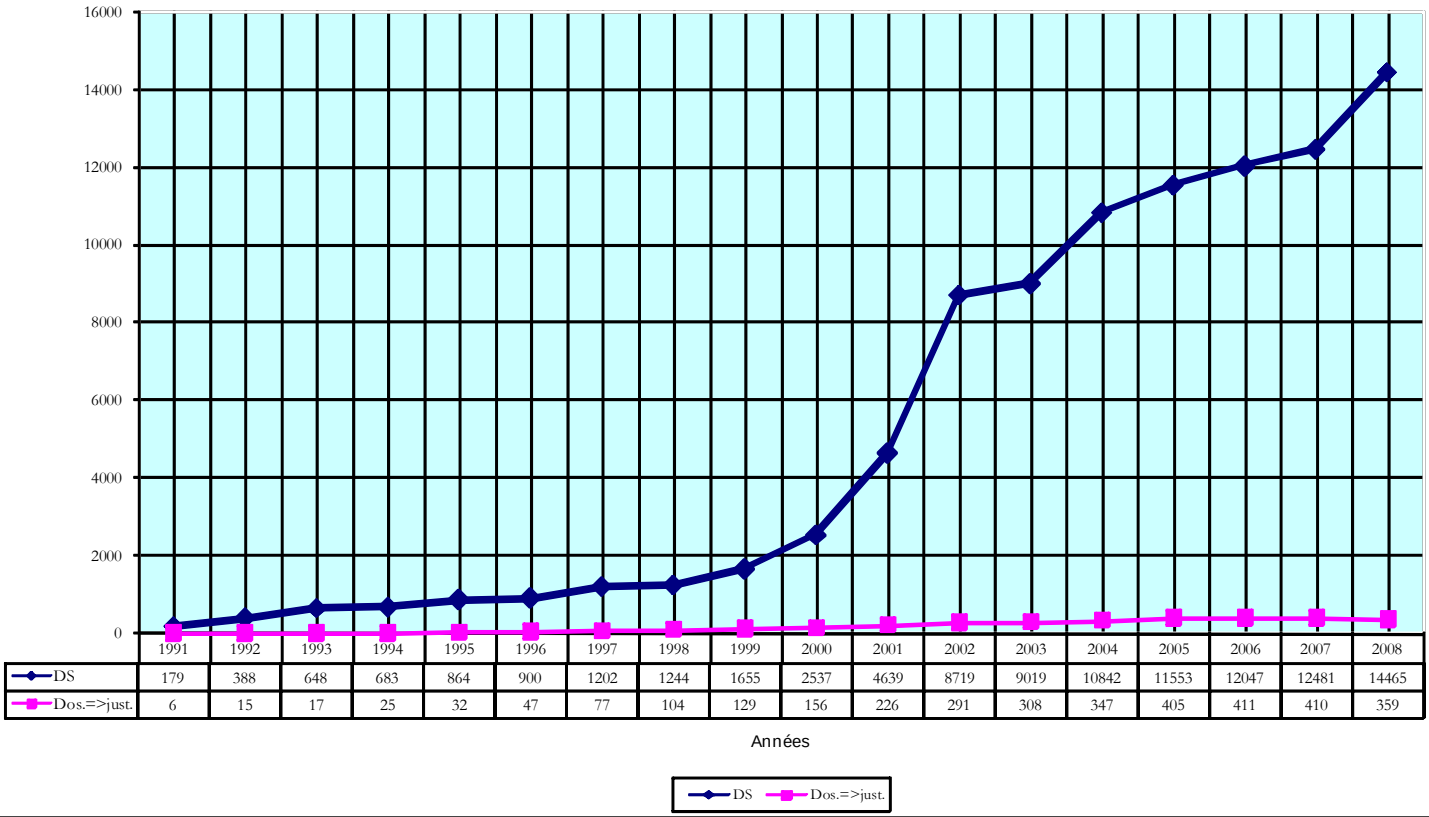
Pour en savoir plus :

FAVAREL-GARRIGUES G., GODEFROY Th., LASCOUMES P., 2009, *Les sentinelles de l'argent sale. Les banques aux prises avec l'antiblanchiment*, Paris, La Découverte.

[6] POWER M., 2005 (1997), *La société de l'audit. L'obsession du contrôle*, Paris, La Découverte.

[7] Selon le terme de ERICSON R., 2006, Ten Uncertainties of Risk-Management Approaches to Security, *Revue Canadienne de Criminologie et de Justice Pénale*, 48, 3, 345-359.

Graphique : Déclarations de soupçon et dossiers transmis à la justice (source : Tracfin)



	1991	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008
DS	179	388	648	683	864	900	1202	1244	1655	2537	4639	8719	9019	10842	11553	12047	12481	14465
Dos.=>just.	6	15	17	25	32	47	77	104	129	156	226	291	308	347	405	411	410	359

Diffusion : CESDIP : Isabelle Pénin
Imprimerie : *Techniplan* - 21 rue Albert Calmette - 78350 Jouy-en-Josas
Dépôt légal : 3e trimestre 2009 **ISSN** : 0994-3870

CESDIP - UMR 8183
Immeuble Edison - 43, boulevard Vauban - F-78280 Guyancourt
Tél. : +33 (0)1 34 52 17 00 - Fax : +33 (0)1 34 52 17 17