Le Whistleblowing
Perspectives croisées

UN EVENEMENT ORGANISE PAR LA CHAIRE KPMG-ESCP EUROPE, ANNE SOPHIE BARTHEZ, UNIVERSITE DE CERGY PONTOISE, DAVID CHEKROUN, ESCP EUROPE, SARAH ALBERTIN, IHEJ

Conférence-débat

Mardi 4 décembre 2012 à 16h00 - Paris

CHAIRE DROIT & ÉTHIQUE DES AFFAIRES

ESCP EUROPE

KPMG

ESCP Europe Master in Management - Ranked n°2 Worldwide

FT FINANCIAL TIMES Masters in Management Ranking 2012

UNIVERSITÉ de Cergy-Pontoise

INSTITUT DES HAUTES ÉTUDES SUR LA JUSTICE

une école de la Chambre de commerce et d'industrie de Paris

The New York Times

September 21, 2012

The Price Whistle-Blowers Pay for Secrets

By PAUL SULLIVAN

A $104 million award for a whistle-blower is probably enough of an incentive to make most people divulge secrets about their employer, or even their friends, for that matter. The award, the largest ever paid by the Internal Revenue Service, went to Bradley C. Birkenfeld last week for revealing secrets about the Swiss banking system.

But lawyers and government officials had this warning for anyone thinking about following in Mr. Birkenfeld's footsteps: Make sure you understand what you are getting into.

"It's a life-changing experience," said John R. Phillips, founder of the law firm Phillips & Cohen and the man credited with devising the amendments that strengthened the government antifraud law, the False Claims Act, in 1986. "If you look at the field of whistle-blowers, you see a high degree of bankruptcies. You may find yourself unemployable. Home foreclosures, divorce, suicide and depression all go with this territory."

As if that were not sobering enough, he added, "You can't believe how long these things take."

And the payoff for putting your career and family at risk is usually a fraction of what Mr. Birkenfeld received. Last year, the I.R.S. paid $8 million to 97 people. This year, it said it was on track to pay $24 million to about 100 people, excluding the amount awarded to Mr. Birkenfeld.

But even the Justice Department, which administers awards through the False Claims Act, generally pays out 16.8 percent of what it takes in, and the average penalty is $2 million to $3 million. That works out to about $330,000 to $500,000, before taxes and lawyer fees are deducted.

That is a not a lot of money considering the risks. (Mr. Birkenfeld will probably pocket around $40 million, if the usual third of his award goes to his lawyers and 40 percent of what is left goes to taxes.)

Still, the interest in inducing whistle-blowers to come forward is on the rise.

Under the Dodd-Frank Act, the Securities and Exchange Commission created the Office of the Whistleblower. It began operating in August 2011, and received 2,700 tips in the first year, said Sean McKessy, chief of the office.

“Not every tip was a home run, but I’ve been surprised by the quality,” he said. “We require that people sign a declaration under penalty of perjury that the information they are submitting is true. It’s a control. We didn’t want to be inundated with nonsense.”

Last month, the office made its first award of $50,000, which was a third of the fine collected. Mr. McKessy defended what was a meager sum by whistle-blower standards, saying he would be happy if his office consistently paid out small sums over many years. “That will show that we’re getting to things before they get to a catastrophic level,” he said.

So if you still want to be a whistle-blower, what should you do?

The short answer is to think long and hard about it. All the lawyers I talked to — and they’ve all made millions of dollars from cases like these — said they discouraged anyone who walked into their offices from becoming a whistle-blower. Doing the right thing, they said they tell their visitors, will be emotionally costly, even if there’s eventually a monetary award.

“There is a 100 percent chance that you will be unemployed — the question is, Will you be forever unemployable?” said Patrick Burns, a spokesman for Taxpayers Against Fraud. “The other 100 percent factor is the person who fired you, the person who designed and implemented the fraud, won’t be fired. He’ll probably be promoted again.”

Stephen M. Kohn, one of Mr. Birkenfeld’s lawyers and the author of “The Whistleblower’s Handbook,” said that despite laws to protect whistle-blowers against retaliation, companies still marginalized and harassed employees who came forward.

Then, there is the length of these trials to consider. Mr. Phillips said he spent 10 years representing two of the whistle-blowers in a case against GlaxoSmithKline that centered on accusations that it promoted its antipsychotic drugs for unapproved uses. The case was settled in July for $3 billion.

There was a divide on how much the award mattered to whistle-blowers. Mr. Kohn said the rewards were often the deciding factor in whether to go ahead with a case.

Other people said whistle-blowers were motivated more by the desire to right a wrong, particularly in instances where people’s lives were at risk. “When people

talk about the big whistle-blower payouts, I say, you don't get it," Mr. Burns said. "You don't see the train of pain I see every day. They can't tell you their story without quivering and crying, even though they're millionaires."

But since the failure rate of these cases is so high — 80 percent are not pursued by the Justice Department program — whistle-blowers want confidentiality. That is not always possible.

When people come forward under the False Claims Act, their identity may be protected at first, but since they are essentially filing a case on behalf of the United States, it will eventually come out.

When people send claims to the I.R.S. and S.E.C. programs, these are considered administrative actions, not cases, which gives whistle-blowers a better chance of anonymity.

"We can't guarantee their name won't come out since they may be called as a witness," said Stephen A. Whitlock, director of the I.R.S. Whistleblower Office. "Generally when it does get out, it's because of something the whistle-blower did, not something we did."

So who makes a good whistle-blower? Someone who has a lot of detailed information that the government could not learn about otherwise. But since the people who have that kind of information are usually high-ranking and have a lot to lose, they are not easy to find.

This is where Mr. Kohn said the headline-making awards were so important. "It's pie in the sky," he said. "But it is what it takes to have an employee risk everything."

Mr. Birkenfeld's award, though, is complicated. Depending on your point of view, he is either a felon who was complicit in the crime he reported and does not deserve his reward or he is a new type of whistle-blower — one with knowledge of a complicated crime that came from being part of it.

His lawyer said paying a reward to someone like Mr. Birkenfeld sent a positive message. "These laws are designed to induce those who may have been participants and done lots of bad things for years to come forward," he said. "They're designed to instill distrust among the conspirators, especially in a complex white-collar fraud."

Mr. Birkenfeld is being credited with unlocking billions of dollars of tax revenue that had been hidden in offshore banking accounts.

By law, the I.R.S. cannot comment on individual cases. But in general, it said that

to get good information, it may need to rely on people who do bad things. “The people who will know what is going on often times don’t have clean hands,” Mr. Whitlock said. “The law recognizes that, and that’s O.K.”

(The statute draws a distinction between a participant, who is eligible for an award, and the mastermind, who is not.)

Mr. Kohn, who started defending whistle-blowers in the 1980s, said there were still a few whistle-blowers who would risk everything without any chance of a reward. He cited another client, Richard Convertino, a former assistant United States attorney in Detroit, as an example of just how messy these suits can become.

Mr. Convertino prosecuted the first post-Sept. 11 terrorism case against a sleeper cell in Detroit. He won a conviction of three of the four men involved, but in 2003 he was removed from the case. The convictions were later overturned after he was charged with withholding evidence. Mr. Convertino said that he did not withhold information and that the Justice Department tried to discredit him because he was talking to Senator Charles E. Grassley, Republican of Iowa who is a champion of whistle-blowers, about failings in the Justice Department’s war on terror.

Even though the criminal case brought by the government against him was thrown out, Mr. Convertino said he had spent his life’s savings on nearly a decade of litigation to clear his name. And while he is working as a lawyer, he is not earning close to the $130,000 he made as an assistant United States attorney.

Still, he won a small victory in June when the United States Court of Appeals for the District of Columbia reinstated his case to determine the identity of the person who leaked information about an internal government investigation about him.

“I think we’re going to prevail,” he said. “I’m not going to get $104 million. But I’ll get a different pot of gold that is more important to me. I’ve lost everything, but I haven’t lost me.”

Aux Etats-Unis, le combat solitaire des “whistleblowers”, patriotes de la transparence

SPÉCIAL SECRET | Aussi appelés lanceurs d’alerte, ils percent des scandales tels qu'Enron ou Abou Ghraib. Mais en divulguant des infos top secret, ils défient l’Etat et les industriels. Et se mettent en danger.

Le 11/08/2012

Olivier Tesquet - Télérama n° 3265

« J'ai prêté quatre fois serment pour ce pays. Deux fois dans l'armée, une fois à la CIA, et une fois à la NSA (1) *. »* A 55 ans, dont trente à servir l'Administration jusque dans ses recoins les plus secrets, Thomas Drake est devenu un ennemi d'Etat. Son crime ? Avoir parlé au Congrès – puis à la presse – du nébuleux projet Trailblazer, un système de surveillance généralisée des télécommunications développé par la National Security Agency.
En dénonçant une suite de dysfonctionnements, il pense légitimement être couvert par la loi qui, aux Etats-Unis, protège constitutionnellement les *whistleblowers*, les lanceurs d'alerte (lire encadré page 21). Seulement, un beau matin de 2007, une douzaine d'agents du FBI débarquent sur la pelouse de sa propriété du Maryland. Ils perquisitionnent tout. Ils désossent sa bibliothèque. Ils veulent même embarquer les ordinateurs 8-bits de collection de cet expert informatique décoré dans l'armée et fan de *Star Trek*.

Drake est poursuivi au nom de l'Espionage Act, un texte centenaire et en partie anticonstitutionnel qui punit les activités anti-américaines (pour mémoire, c'est celui qui a mené les époux Rosenberg à la chaise électrique). En tout, il va passer un an de sa vie à essayer de ne pas en passer trente-cinq derrière les barreaux.

Nous le rencontrons à Washington, dans les bureaux du Government Accountability Project (GAP), une organisation qui représente et défend environ soixante *whistleblowers* par an. Sur K Street, bien évidemment, l'avenue historique des cabinets de lobbying et des think tanks. Les traits émaciés par un combat de plus de six ans qui l'a épuisé mais le regard d'un bleu toujours patriote, Thomas Drake a longtemps fait partie du système.

Cet échalas de 1,90 m, aux cheveux grisonnants, a grandi avec les auditions télévisées du Watergate ; pour le compte de la CIA, il a travaillé comme expert en renseignement électronique en Allemagne de l'Est aux grandes heures de la Stasi ; il connaît le visage de l'espionnage. Mais rien ne pouvait le préparer à ce qu'il a enduré.

« On m'a traité comme un espion du KGB pendant la guerre froide. Je suis radioactif. A la NSA, une seule personne m'adresse encore la parole. » Thomas Drake, lanceur d'alerte

« J'ai vécu l'Etat policier, lâche-t-il en se repeignant et en citant *Les Trois Jours du Condor*. *On m'a traité comme un espion du KGB pendant la guerre froide. Je suis radioactif. A la NSA, une seule personne m'adresse encore la parole*. » Malgré les pressions, il n'a jamais voulu plaider coupable dans son affaire, un dossier de plusieurs milliers de pages : *« Devant la cour, la vérité ne suffisait pas*. *»*

Aux Etats-Unis, les *whistleblowers* bénéficient pourtant d'un statut sanctuarisé depuis un siècle et demi, grâce au Whistleblower Protection Act (en 1863, il s'appelait encore le False Claims Act). Leur rôle vertueux n'est plus à prouver. Sans eux, la presse aurait bien du mal à révéler certains scandales. Sans eux, le public n'aurait peut-être jamais eu connaissance de Guantanamo ou des tortures d'Abou Ghraib, mises au jour par le soldat Joseph Darby.

« On leur doit les plus gros-ses révélations des dix dernières années », renchérit Jesselyn Radack, l'avocate de Drake, une ancienne du Département de la Justice. Elle défend plusieurs autres clients. Il faut dire que les candidats ne manquent pas. *« Toutes les relations entre les hommes reposent, cela va de soi, sur le fait qu'ils savent des choses les uns sur les autres »*, écrivait le philosophe allemand Georg Simmel en incipit de *Secret et sociétés secrètes*.

Aux Etats-Unis, les relations entre les hommes reposent sur le fait que 4,8 millions de personnes savent des choses sur l'Administration. C'est le nombre faramineux d'accréditations secret-défense disséminées à travers le territoire. En 2011, les agences américaines ont dépensé plus de 11 milliards de dollars pour garder secrets leurs secrets, investis dans du matériel informatique sécurisé ou des formations à la confidentialité. C'est 30 % de plus qu'en 2009. Pour un peu, on y verrait presque une bulle spéculative de la cachotterie. Certains racontent même qu'au Département d'Etat, des employés n'hésitent pas à classifier cartes de voeux et avis de naissance.

Contre toute attente, de soupapes de sécurité démocratiques les *whistleblowers* sont devenus les ennemis numéro 1 de l'Administration. Le cas de Thomas Drake a été très médiatisé, jusqu'à un long portrait dans *The New Yorker*. Mais ce n'est pas le seul, loin de là. En tout, l'administration Obama a déjà poursuivi six fonctionnaires (dont la moitié au FBI et à la CIA), contre trois avant l'arrivée du si gentil Barack à la Maison-Blanche.

« La sécurité nationale est devenue une religion d'Etat. Et ce n'est plus personnalisé, {…} c'est incarné par toute l'Administration. » Thomas Drake

Le prochain à visiter les prétoires, au mois de septembre ? Le soldat Bradley Manning, 24 ans, qui aurait transmis des centaines de milliers de télégrammes diplomatiques à WikiLeaks. Après avoir échappé de justesse à la peine de mort, il risque fort de finir sa vie en prison.

Aujour-d'hui, parler est devenu un crime. Comme les Romains, qui plantaient les têtes de leurs ennemis au bout d'une pique en guise d'avertissement, le gouvernement veut faire des exem-ples pour tuer les vocations dans l'œuf. *« Le livre le plus facile à censurer est celui qui n'a pas été écrit »*, avance Peter Van Buren sur un ton sibyllin.

Il sait de quoi il parle. Après vingt-quatre ans de bons et loyaux services au Département d'Etat, ce diplomate polyglotte du Foreign Service, grand chauve à l'air affa-ble, a été mis à pied sans ménagement il y a quelques mois : son ouvrage sur la reconstruction en Irak (*We meant well*) n'a pas beaucoup plu à Hillary Clinton. Même les journalistes sont contaminés par la paranoïa.

Tous ont en mémoire l'exemple de James Risen, un reporter du *New York Times*, colauréat du prix Pulitzer, à deux doigts d'être poursuivi en 2008 pour avoir – devinez quoi – menacé la sécurité nationale en dévoilant les détails de l'Opération Merlin (une manœuvre de l'administration Clinton pour retarder le programme nucléaire iranien).

Quand on leur demande quel est le point de basculement, nos interlocuteurs familiers du monde du renseignement sont formels : le 11 Septembre. *« J'ai su que quelque chose ne tournait pas rond dans les semaines qui ont suivi les attentats »*, raconte Thomas Drake.

A l'époque, il était aux premières loges, à Fort Meade, la base de la NSA, sortie 32 sur l'autoroute, à une vingtaine de miles du centre de Washington. C'est dans ce bâtiment aveugle ultra classifié, dont l'existence ne fut reconnue qu'en 1957, que se transmettent les informations les plus sensibles, que s'élaborent les opérations les plus confidentielles. *« La sécurité nationale est devenue une religion d'Etat*, s'inquiète encore Drake. *Et ce n'est plus personnalisé, comme au temps de McCarthy, c'est incarné par toute l'Administration. »*

Le régime d'exception en vigueur depuis 2001, matérialisé par le Patriot Act ou les National Security Letters (2), est en train d'être inscrit dans la Constitution. Officials Secret Act, Shield Act, les projets pullulent, poussant chaque fois le curseur un peu plus loin. Tous fondaient beaucoup d'espoirs en Barack Obama, le professeur de droit constitutionnel, qui avait promis de légiférer en leur faveur. Le retour de manivelle a été violent.

A quelques blocs des locaux climatisés du GAP, Steven Aftergood est chercheur à la Federation of American Scientists. Depuis 1989, cet expert reconnu dans tout le pays étudie méthodiquement les secrets de l'Administration. Dans son bureau du sixième étage d'un bâtiment anonyme, noyé sous les piles de livres, il tente de prendre un peu de hauteur sur la situation.

« Dans le meilleur des cas, ils finissent
ruinés, au chômage et marginalisés.
Dans le pire, ils mettent fin à leurs jours. »
Jesselyn Radack, avocate de Drake

« Obama n'est pas si différent de ses prédécesseurs, plaide-t-il. *Déjà, en 2000, nous avons failli adopter une législation draconienne vis-à-vis des* whistleblowers*, et il a fallu le veto in extremis de Clinton pour que le texte ne*

passe pas. Cependant, il y a trois facteurs à prendre en compte. Primo, les moyens technologiques permettent de faire fuiter des informations plus facilement, mais aussi d'identifier les whistleblowers *de façon beaucoup plus rapi-de. Deusio, il y a eu un trauma WikiLeaks, et l'Administration veut faire un exemple. Tertio, nous sommes dans une année électorale, et tous les politiques rivalisent d'ingéniosité pour serrer la vis. »*

Bingo : quelques jours avant ma visite, trois sénateurs républicains se fendaient d'une tribune dans le *Washington Post* titrée *« Leaks must be plugged »,* « Les fuites doivent être colmatées ». Et tant pis si la Constitution prévoit que le Congrès ne puisse pas voter une loi contraire au premier amendement, relatif à la liberté d'expression.

Dans ce dédale législatif, les *whistleblowers* pourraient être livrés à eux-mêmes, chair à canon d'une bureaucratie revancharde. Heureusement, dans la région de Washington DC, une demi-douzaine de structures sont là pour leur tracer des itinéraires sécurisés. Pour les épauler au quotidien, aussi. Une poignée d'avocats se sont d'ailleurs spécialisés dans ces parties d'échecs interminables. Stephen M. Kohn en fait partie. On pourrait même dire qu'il a inventé le gambit procédural.

Ami de feu l'historien Howard Zinn, il défend des lanceurs d'alerte depuis 1984, de son confortable cabinet situé dans une maison en *brownstone* du quartier de Georgetown. Il a fondé le National Whistleblowers Center, une structure pour les protéger, et a même rédigé un guide pratique à leur intention (3) . En ce moment, inutile de dire qu'il ne chôme pas. Son meilleur conseil ? Venir le voir immédiatement, avant même de sortir la moindre information. *« Sinon, vous êtes broyés par le système*. *»*

Même s'il s'inscrit dans de grands principes de démocratie et de transparence, le petit monde de la fuite est fait de cas particuliers et d'interrogations personnelles. Surtout, c'est un immense sacrifice humain. *« Nous ne voulons pas détruire le gouvernement, nous voulons le rendre meilleur »,* soupire Peter Van Buren.

« Le premier amendement, qui fonde la liberté d'expression, est un droit mais c'est surtout une responsabilité. » Thomas Drake

Pour l'heure, c'est surtout le gouvernement qui semble vouloir anéantir les *whistleblowers*. La femme de l'ex-diplomate craint pour l'avenir de ses enfants, qu'ils soient blacklistés à l'université. Lui sait qu'il doit déménager, changer de vie. Dans une région (la Beltway, qui court entre la Virginie et le Maryland) où tout le monde travaille de près ou de loin pour l'Administration, sortir du bois peut vite vous emmener dans un no man's land.

Le placardisé du Département d'Etat raconte même qu'un ancien collègue, effrayé à l'idée de perdre son job, a dépêché sa femme dans un café pour qu'il lui remette un exemplaire dédicacé de son livre. Dans leur bouche, un mot revient inlassablement, « isolement ». *« Dans le meilleur des cas, ils finissent ruinés, au chômage et marginalisés,* lâche Jesselyn Radack. *Dans le pire, ils mettent fin à leurs jours. »*

Au moment de l'abandon des charges qui pesaient contre lui, Drake a ressenti des symptômes de stress post-traumatique, comme un soldat de retour du front. Il lui a fallu plus d'un an pour se remettre d'aplomb, apprivoiser les flash-back. Son propre père a fini par se poser des questions sur sa culpabilité, et son fils, étudiant en droit, s'est demandé *« à quoi rimait ce bordel ». « Plus ça dure, plus la pression est forte,* reconnaît-il, précisant : *Je ne peux pas abandonner mais le prix est élevé*. *»*

Entre hypothèques immobilières et familiales, son combat lui a coûté, dit-il, un million de dollars. Depuis, l'ancien cadre du renseignement s'est inscrit en doctorat, et il a même trouvé un petit boulot dans une grande entreprise d'informatique. Malgré les coups qu'on lui a assénés, il tient toujours debout : *« Les Pères fondateurs de ce pays l'ont énoncé très clairement. Le premier amendement, qui fonde la liberté d'expression, est un droit mais c'est surtout une responsabilité. »*

Et en France ?

Sans statut légal protégé, les *whistleblowers* français doivent même composer avec une carence : il n'existe pas de véritable traduction du mot. Par commodité, on les appelle « lanceurs d'alerte ». Et ils œuvrent dans le flou. Hormis l'article 40 du Code de procédure pénale, qui oblige tous les fonctionnaires à dénoncer les infractions dont ils ont connaissance dans le cadre de leur activité, c'est le vide.

Dotée d'un système rudimentaire d'alertes légales, la Cnil n'a jamais voulu se pencher sérieusement sur la question, craignant de mettre sur pied *« un système organisé de délation professionnelle »*. Résultat : peu de Français soufflent dans le sifflet. On pourrait évoquer Sihem Souid, la fliquette auteur du brûlant *Omerta dans la police.* Ou Jean-Luc Touly, terreur des marchés de l'eau, licencié de Veolia puis réintégré sur décision de justice.

Conseiller régional Europe Ecologie depuis 2010, ce dernier est également membre historique d'Anticor, une association qui combat la corruption et les conflits d'intérêts. C'est d'ailleurs accompagné de son avocat William Bourdon qu'il était allé réclamer, en 2008, un encadrement du *whistleblowing* à Gérard Larcher, alors président du Sénat. En vain. A la faveur du changement de majorité, les militants de la transparence espèrent inscrire leurs doléances dans l'agenda. Ce n'est pas gagné.

(1) Créée en 1952, la National Security Agency (NSA) est la plus secrète des agences de renseignements américaines. L'un de ses sobriquets l'énonce clairement : « Never Say Anything », « Ne dites jamais rien ».

(2) Renforcées après le 11 Septembre, ces requêtes autorisent les agences de renseignements à réclamer les données personnelles d'un individu à n'importe quelle entreprise privée (un fournisseur d'accès à Internet, par exemple).

(3) *The Whistleblower's Handbook, A step-by-step guide to doing what's right and protecting yourself* aux éditions Lyons Press, 2011.

The Banking Law Journal

VOLUME 129 NUMBER 10 NOVEMBER/DECEMBER 2012

THE BANKING LAW JOURNAL (ISSN 0005 5506) (USPS 003-160) is published ten times a year by A.S. Pratt & Sons, 805 Fifteenth Street, NW., Third Floor, Washington, DC 20005-2207. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices.
POSTMASTER: Send address changes to THE BANKING LAW JOURNAL, A.S. Pratt & Sons, 805 Fifteenth Street, NW., Third Floor, Washington, DC 20005-2207.

The Evolution of the SEC Whistleblower: From Sarbanes-Oxley to Dodd-Frank

SARAH L. REID AND SERENA B. DAVID

The authors analyze the whistleblower regimes that have been enacted by Congress over the past decade, which now are central to the regulation of the financial services industry and which will be increasingly utilized given the new whistleblower provisions under Dodd-Frank.

This article analyzes the whistleblower regimes that have been enacted by Congress since 2002 in connection with efforts to combat fraud in areas subject to the regulation of the Securities Exchange Commission (the "SEC"). These whistleblower regimes are now central to the regulation of the financial services industry, and will be increasingly utilized, given that the new whistleblower provisions under the Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank") offer strong incentives to a potential whistleblower who sees the large settlements the SEC has been able to obtain, such as the 2010 $550 million settlement with Goldman Sachs over a subprime mortgage product.[1]

Sarah L. Reid, a member of the board of editors of *The Banking Law Journal*, is a partner in the litigation department in the New York office of Kelley Drye & Warren LLP. Ms. Reid has extensive experience representing major international and U.S. companies in trials, arbitrations, mediations and bankruptcy-related litigation. She has argued appeals before numerous appellate courts, including the U.S. Supreme Court. She can be reached at sreid@kelleydrye.com. Serena B. David is an associate in the firm's New York office, where she focuses on litigation. She can be reached at sdavid@kelleydrye.com.

Published by A.S. Pratt in the November/December 2012 issue of *The Banking Law Journal*.

SARBANES-OXLEY

A decade ago, in the wake of the Enron and WorldCom scandals, Congress enacted the Sarbanes-Oxley Act of 2002 ("Sarbanes-Oxley"), which was signed into law by President Bush on July 30, 2002.[2] Sarbanes-Oxley includes a whistleblower provision in an attempt to prevent securities fraud, and to protect investors and corporate shareholders from fraudulent accounting practices and other conduct that defrauds shareholders. The goal is to safeguard investors and shareholders by "improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws."[3] Sarbanes-Oxley contains provisions requiring publicly held companies to have independent directors and audit committees and provides for various other changes to overall corporate governance.[4] Section 301(4) requires the audit committees of all of the covered companies to establish procedures for the "receipt, retention, and treatment of complaints received by the issuer regarding accounting, internal accounting controls, or auditing matters" and also provides for the employees to submit these complaints confidentially and anonymously.[5]

The Sarbanes-Oxley whistleblower statute is also notable for the protection that it affords potential whistleblowers against retaliation from employers. Section 806 protects employees of publicly traded companies from employment retaliation for disclosing alleged corporate malfeasance.[6] Specifically, Section 806 prohibits covered employers from firing or discriminating against an employee who files, causes to be filed, testifies, participates in, provides information, or assists in an investigation regarding employer conduct that the employee reasonably believes constitutes a violation of (1) mail, bank, wire, or securities law; (2) any rule or regulation of the SEC; or (3) any provision of federal law relating to fraud against shareholders.[7] This protected activity includes reports made to federal regulatory and law enforcement agencies, Congress, an employee's supervisor, and internal corporate investigators.[8] The law also protects employees who participate or testify in SEC regulatory proceedings or other federal proceedings related to fraud against shareholders.[9]

However, Sarbanes-Oxley does not provide any financial incentive for the whistleblower, only protection from retaliation. When it was passed, investment banks, their clients and others in the financial services industry were concerned that a floodgate of complaints would open, though this did

not prove to be the case. In fact, Sarbanes-Oxley did not prove to be as useful a remedy to uncover fraud and corporate malfeasance because the anti-retaliation provisions were not as effective in practice at protecting the whistleblowers.[10] Department of Labor (the agency tasked with investigating Sarbanes-Oxley retaliation complaints) and federal court decisions effectively narrowed who was protected by Sarbanes-Oxley and what protections those covered employees could invoke.[11] Thus, there was less of an incentive for an employee to come forward with any information.

DODD-FRANK

The more recent financial crisis, including the collapse of Lehman Brothers and the Madoff Ponzi scheme, led to Dodd-Frank being signed into law by President Obama on July 21, 2010. Dodd-Frank is an attempt to address the deficiencies in prior regulatory programs, including those contained in Sarbanes-Oxley, and to broaden the oversight power of regulatory agencies such as the SEC and the Commodity Futures Trading Commission ("CFTC"). The new regulatory scheme gives the SEC and the CFTC greater oversight in areas such as consumer protection, trading restrictions, credit ratings, regulation of financial products, corporate governance and disclosure, and transparency. Dodd-Frank took the whistleblower concept further by providing significant economic incentives for whistleblowers to report violations of securities laws to regulators.

In providing these financial incentives, the legislation adopted an approach similar to that of the False Claims Act ("FCA"), which has its own whistleblower provision.[12] The whistleblower provisions under the FCA is a mechanism allowing individuals who have evidence of false claims being paid by the government to sue on the government's behalf.[13] Those who knowingly submit, or cause others to submit, false claims for payment of government funds are liable for treble damages plus civil penalties of between $5,000 and $10,000 for each false claim.[14] The individual who acts as a "relator," and files the suit on the government's behalf, may be awarded up to 30% of the funds recovered.[15]

Similar to the whistleblower program under the FCA, the Dodd-Frank whistleblower provisions state that individuals who provide the SEC or the

CFTC with "original information" about a violation of federal securities laws which leads to a successful enforcement action that recovers upwards of $1 million, are entitled to between 10% and 30% of the recovered amount.[16] Moreover, unlike under FCA, the whistleblower provisions under Dodd-Frank do not require that the fraud be perpetrated against the government, they merely require fraud against private investors or the financial markets. [17]

THE SEC

Prior to the implementation of Dodd-Frank, the SEC's "bounty program" was only for use in insider trading cases and the award that a whistleblower could receive was capped at ten percent of the amount that the SEC was able to recover.[18] During the two decades during which the prior bounty program existed, the SEC only paid six whistleblowers, and the payment of all six claims totaled just over $1.15 million.[19] These statistics are likely to dramatically increase under Dodd-Frank, given the enhanced financial incentives provided to potential whistleblowers.

Soon after Dodd-Frank was enacted, a cross-disciplinary working group was formed and tasked with drafting proposed rules to implement Dodd-Frank's whistleblower provisions. As part of this process, the SEC provided an email link on its website to allow for public input into the whistleblower award program.[20] In response, the SEC received more than 240 comments letters and 1,300 form letters on the proposed rules.[21] Many of these comments were regarding what is arguably the most controversial aspect of the Dodd-Frank whistleblower provisions: the lack of an internal reporting requirement for most whistleblowers. On May 25, 2011, after revising the rules pursuant to the comments received, the SEC adopted final Regulation 21F, the final rules implementing the whistleblower provision, which became effective on August 12, 2011.[22] Pursuant to the final rules, and contrary to the urging of many parties that weighed in on this aspect of Dodd-Frank, potential whistleblowers need not report the alleged misconduct internally before reporting it directly to the SEC. If, however, the whistleblower chooses to first report the violations internally, the whistleblower must then report this violation to the SEC within 120 days of the internal report in order to qualify for the whistleblower bounty under Dodd-Frank.[23]

Aside from the lack of an internal reporting requirement, corporations are likely to be most concerned that Dodd-Frank provides few limitations as to who can actually qualify as a whistleblower. Even individuals who have a fiduciary duty to report securities law violations to the company — such as compliance and internal audit personnel, certain legal counsel and certain public accountants — can become eligible for whistleblower awards. Once 120 days have elapsed after an officer, trustee or partner has informed the corporation's audit committee or other legal or compliance officer of the perceived violations, that individual with the fiduciary duty may then become eligible for the whistleblower bounty.[24] Thus, under certain circumstances, an individual that is engaged in compliance, internal audit, human resources or public accounting activities for a corporation could actually qualify as a whistleblower.

Not only are the requirements in terms of who may be a whistleblower broadly defined, but Dodd-Frank also incorporates enhanced anti-retaliation employment protection for those whistleblowers, above and beyond what was available under Sarbanes-Oxley, and also includes provisions to protect the whistleblower's identity.[25] The SEC and the CFTC are prohibited from disclosing the information that is provided by a whistleblower or any other information which could be expected to directly or indirectly reveal a whistleblower's identity.[26] Moreover, the anti-retaliation provisions even protect a whistleblower whose tip does not lead to a successful enforcement action or if a whistleblower does not receive the bounty.

Under the rules, the "original information" provided to the SEC must be based on "independent knowledge." "Original information" is defined by the SEC as information that is (1) not already known to the SEC; (2) derived from independent knowledge or analysis; and (3) not exclusively derived from an allegation in a judicial or administrative hearing, or similar action.[27] The SEC defines "independent knowledge" as information that is not obtained from public sources, though this does not mean that the whistleblower needs to have first-hand knowledge of the alleged violations. To be eligible for an award, the potential whistleblower must be voluntarily providing the information to the SEC, meaning that the information is not being provided in response to any SEC demand for information or inquiry. Lastly, in order to collect the reward, the whistleblower's information must actually lead to a

successful SEC enforcement action.[28]

In order to handle the inevitable influx of whistleblower tips resulting from Dodd-Frank, Section 924(d) of the act directs the SEC to establish a separate office under its auspices to administer and to enforce the Dodd-Frank whistleblower provisions. On February 18, 2011, the SEC announced that Sean McKessy was appointed chief of the newly created Office of the Whistleblower, and the office officially opened on August 12, 2011.[29] The Office of the Whistleblower has focused primarily on establishing the office and generally implementing the whistleblower program.[30] Additionally, the SEC has funded the Investor Protection Fund, which was created to pay whistleblower rewards.[31]

It has been widely reported that corporate whistleblowers have been calling in so many tips since Dodd-Frank became effective that the SEC staff is struggling to keep pace.[32] It is believed that the SEC has received thousands of whistleblower complaints since the Office of the Whistleblower opened.[33] In just its first seven weeks of operation, the Office of the Whistleblower reported that it had already received 334 tips, most of which were related to market manipulation, corporate disclosures and financial statements or offering fraud.[34] Out of the approximately seven complaints received by the SEC per day, between two and three of these tips are usually worth investigating, leaving the SEC enforcement division facing a monumental task with its current staffing.[35]

JUSTICE'S OMBUDSMAN

There are plenty of indications that, going forward, whistleblowers will likely play a greater role in uncovering and preventing fraud, waste and other malfeasance in the financial industry. In the early part of August 2012, the Department of Justice appointed a federal prosecutor as its whistleblower ombudsman.[36] This is a new position and could be indicative of the government's increased reliance on whistleblowers to jumpstart these financial investigations. The purpose of this position is to "train and educate employees on the role of whistleblowers in improving government operations, monitor whistleblower investigations and advise employees on legal rights and protections against retaliation."[37] In essence, the government believes that whistleblowers provide a useful and potentially untapped source of infor-

mation and, therefore, it is important to have someone to properly liaise with these whistleblowers to ensure that the reporting is as fruitful and as helpful as possible.

LARGE PAYMENTS

The potential for large whistleblower payouts under Dodd-Frank has now become a reality. On August 21, 2012, almost exactly one year after the Office of the Whistleblower opened, the SEC announced that it had paid out its first whistleblower bounty under Dodd-Frank.[38] The whistleblower received nearly $50,000, which was 30 percent of the amount collected, the maximum payout allowed under the regime.[39] The whistleblower provided both information and documents to the SEC, which allowed the enforcement group to investigate the allegations in an expedited fashion and prevented additional individuals from becoming victims of the fraudulent scheme.[40] The court involved in the enforcement action ordered more than $1 million in sanctions, $150,000 of which has already been collected thus far. It is possible that the court will issue a final judgment against other defendants in this matter and, were this to happen, any increase in the amount collected would also increase the payment to the whistleblower.[41] The SEC's press release also notes that there was an additional individual who sought an award in connection with this matter, but the SEC did not approve it because the information provided by that individual did not significantly contribute to the SEC's enforcement action.[42] This indicates the SEC is adopting a nuanced approach to whistleblower payments, which is encouraging.

CONCLUSION

Ultimately, it is clear that whistleblowing in the financial services industry is going to increase given the whistleblowing regime put in place by Dodd-Frank. The financial incentives and other protections afforded to whistleblowers under Dodd-Frank will encourage those who might not have been willing to come forward before to now do so. Since the first whistleblower has actually been paid pursuant to Dodd-Frank, many others will likely be waiting in line to claim similar rewards.

NOTES

[1] "Goldman Sachs to Pay Record $550 Million to Settle SEC Charges Related to Subprime Mortgage CDO," SEC Press Release, July 15, 2010.
[2] Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745 (2002) (hereinafter "Sarbanes-Oxley").
[3] *Id.*
[4] Sarbanes-Oxley § 301.
[5] *Id.* at § 301(4).
[6] *Id.* at § 806.
[7] *Id.*
[8] National Whistleblowers Center, Sarbanes-Oxley FAQ, *available at* http://www.whistleblowers.org/index.php?option=com_content&task=view&id=36&Itemid=65.
[9] *Id.*
[10] Jonathan Ben-Asher, *New and Improved Whistleblower Protections for Employees*, New York University School of Law, Center for Labor and Employment Law, 64th Annual Conference on Labor, The Impact of the Global Economic Crisis on the Workplace, June 9, 2011, at 6.
[11] *Id.*
[12] Gordon Schnell and Jason Enzler, *The Age of the Whistleblower: Incentives and Protections*, Law 360, September 6, 2012.
[13] False Claims Act, 31 U.S.C. § 3730 *et seq.* (2009).
[14] *Id.* at § 3729(a)(1).
[15] *Id.* at § 3730(d).
[16] Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub.L. 111-203, H.R. 4173 §§ 748 and 922(a) (2010) (hereinafter "Dodd-Frank").
[17] Schnell, *supra* note 12.
[18] "SEC Adopts Rules to Establish Whistleblower Program," SEC Press Release, May 25, 2011.
[19] Marc S. Raspanti and Bryan S. Neft, *What's Next for the Year-Old SEC Whistleblower Program?*, The Legal Intelligencer, November 11, 2011.
[20] http://www.sec.gov/spotlight/regreformcomments.shtml.
[21] "Annual Report on the Dodd-Frank Whistleblower Program, Fiscal Year 2011," Securities and Exchange Commission, at 3 (November 2011).
[22] *Id.*
[23] "Implementation of the Whistleblower Provisions of Section 21F of the Securities Exchange Act of 1934," Securities and Exchange Commission, Release No. 34-64545, effective August 12, 2011.

[24] *Id.*
[25] Dodd-Frank § 922(h)(1)-(2).
[26] Dodd-Frank §§ 922(h)(2) and 748(h)(2).
[27] Dodd-Frank § 922(a); *see also* "SEC Adopts Rules to Establish Whistleblower Program," *supra* note 18.
[28] Dodd-Frank § 922(b)(1).
[29] "Annual Report on the Dodd-Frank Whistleblower Program, Fiscal Year 2011," *supra* note 21, at 3.
[30] *Id.* at 4.
[31] Raspanti, *supra* note 19.
[32] Ian Thoms, *SEC Enforcement Division Buried in Whistleblower Tips*, Law 360, June 5, 2012.
[33] *Id.*
[34] "Annual Report on the Dodd-Frank Whistleblower Program, Fiscal Year 2011," *supra* note 21, at 5.
[35] Thoms, *supra* note 32.
[36] Brian Mahoney, *DOJ Taps Prosecutor as First Whistleblower Ombudsman*, Law 360, August 8, 2012.
[37] *Id.*
[38] "SEC Issues First Whistleblower Program Award," SEC Press Release, August 21, 2012.
[39] *Id.*
[40] *Id.*
[41] *Id.*
[42] *Id.*

DU WHISTLEBLOWING À L'AMÉRICAINE À L'ALERTE ÉTHIQUE À LA FRANÇAISE : ENJEUX ET PERSPECTIVES POUR LE GOUVERNEMENT D'ENTREPRISE

Sandra Charreire Petit et Joëlle Surply

AIMS | *M@n@gement*

2008/2 - Vol. 11
pages 113 à 135

ISSN 1286-4692

M@n@gement, Vol. 11, No. 2, 2008, 113-135
Special Issue: Corporate Governance and Ethics

Du *whistleblowing* à l'américaine à l'alerte éthique à la française : enjeux et perspectives pour le gouvernement d'entreprise

Sandra Charreire Petit . Joëlle Surply

Université Paris Sud 11
PESOR
eMail: sandra.charreire-petit@u-psud.fr
Université Paris Sud 11
PESOR
eMail: joelle.surply@u-psud.fr

Le *whistleblowing* peut être défini « comme le fait, pour un membre d'une organisation (ancien ou actuel), de révéler l'existence de pratiques illégales, immorales ou illégitimes dont l'employeur a la maîtrise, à une personne ou à un organisme susceptible de remédier à la situation » (Near et Miceli, 1985: 4). La mise en place du *whistleblowing,* dont nous verrons qu'il devient « alerte éthique » en France, vise à restaurer la confiance des investisseurs, en renforçant la fiabilité de l'information financière et en améliorant la responsabilité des gestionnaires. Que se passe-t-il lorsqu'une pratique de contrôle interne américaine *(whistleblowing)* est déployée au sein d'entreprises françaises cotées aux Etats-Unis ou au sein de filiales d'entreprises américaines établies en France ? Cet article tente de répondre à cette question en analysant le déploiement de cette pratique qui nous vient d'outre-Atlantique (volet de la loi Sarbanes-Oxley, 2002). Cette recherche est qualitative et exploratoire. Elle propose l'identification de trois enjeux managériaux et interroge deux vecteurs susceptibles d'infléchir les pratiques de gouvernement d'entreprise dans les pratiques de contrôle interne.

Cet article s'interroge sur les possibles transformations du système de gouvernement pour les entreprises françaises, par le biais de la mise en œuvre du volet *whistleblowing* de la loi Sarbanes-Oxley (SOX) qui nous vient d'outre-Atlantique.

Le thème est nouveau et les recherches sur les effets de la récente loi SOX, votée en 2002, sont encore très peu nombreuses. En France, la Commission Nationale Informatique et Libertés (CNIL) a attendu décembre 2005 pour mettre en place un mécanisme d'autorisation unique du dispositif *whistleblowing.* Par ailleurs, l'obligation de se conformer à la loi américaine ne concerne, dans notre pays, qu'une centaine de sociétés (DIPAC, 2006). Une première série de travaux réalisés sur le *whistleblowing,* aux Etats-Unis (Miceli et Near, 1985, 1996 ; Moberly, 2006) ou en France (Pesqueux, 2007) ont essentiellement porté sur la définition du dispositif (de Bry, 2006), ses caractéristiques, les conditions de recours à l'usage du droit ou encore les motivations du *whistleblower.* Après quelques années d'application, aux Etats-Unis, nombre de préoccupations sont orientées vers les coûts et l'efficacité des modalités de contrôle interne. En Europe, le *whistleblowing* est appréhendé comme un dispositif qui doit prendre sens dans une vision de la responsabilité (Fayol, 2005), alors que son caractère « litigieux et tendancieux » interroge sur « la réelle plus

value apportée dans les environnements professionnels » (de Pover, 2006: 14).

Notre article adopte une approche particulière ; il appréhende le déploiement en France de la pratique du *whistleblowing* et ses incidences potentielles sur le management et le gouvernement d'entreprise. Le contexte est celui de la loi Sarbanes-Oxley (SOX), adoptée par le Congrès américain, en 2002, après les scandales comptables et financiers, tels ceux d'Enron et de Worldcom. La loi SOX vise à restaurer la confiance des investisseurs en renforçant la fiabilité de l'information financière et en améliorant la responsabilité des gestionnaires. Cet objectif s'accompagne de l'obligation de mettre en œuvre un contrôle interne, exercé au bénéfice des investisseurs. Le socle juridique sur lequel repose cette loi est anglo-saxon. L'une des dispositions de la loi Sarbanes-Oxley impose aux sociétés américaines ou étrangères cotées aux Etats-Unis, ainsi qu'à leurs filiales localisées à l'étranger, de mettre en place des procédures de *whistleblowing.* Ceci n'est pas sans incidence lorsque les pratiques managériales des grandes firmes multinationales d'origine américaine tendent à faire respecter, ailleurs que sur leur sol, des lois américaines.

Cependant, si les liens entre des pratiques issues de la loi et le gouvernement d'entreprise sont déjà bien étudiés de part et d'autre de l'Atlantique (La Porta, Lopez-de-Silanes, Schleifer et Vishny, 1999 ; Boughanmi et Deffains, 2006), il nous semble que les conséquences de l'extra-territorialité de fait de la loi SOX constituent un objet pertinent d'étude pour revisiter ces questions sous un angle managérial. En effet, que se passe-t-il lorsque la protection des investisseurs rencontre les pratiques des salariés en matière de contrôle interne, dans des contextes économiques (américain et européen) aux fonctionnements hétérogènes ? Plus précisément, que se passe-t-il lorsqu'une pratique de contrôle interne américaine est déployée au sein d'entreprises françaises cotées aux Etats-Unis ou au sein de filiales d'entreprises américaines établies en France ?

Certes, la problématique est susceptible de s'inscrire dans des débats plus larges qui questionnent la dualité *soft law/hard law* ou abordent la mise en place du dispositif *whistleblowing* dans une perspective culturelle. Cependant, à des fins de clarté, nous focalisons essentiellement notre analyse sur les enjeux et les perspectives du déploiement de la pratique d'alerte pour le gouvernement d'entreprise, en France.

Les entreprises concernées sont aux prises avec les réalités internationales et les normes qui s'imposent aux acteurs mondiaux, mais aux prises aussi avec un socle juridique français et notamment un droit du travail qui encadre, pour partie déjà, ces questions avec le souci de protéger le salarié. C'est dans un tel cadre que notre analyse se situe.

Notre questionnement trouve son origine dans des pratiques de gouvernement d'entreprise reposant sur des socles distincts. Le gouvernement d'entreprise désigne classiquement « l'ensemble des pratiques, des structures et des procédures qui définissent le partage du pouvoir, la répartition des responsabilités et les modes de contrôle entre les différentes parties prenantes d'une organisation » (Johnson, Scholes, Whittington et Frery, 2005 : 197). En définissant le gouverne-

M@n@gement, Vol. 11, No. 2, 2008, 113-135
Special Issue: Corporate Governance and Ethics

ment d'entreprise comme « l'ensemble des mécanismes organisationnels qui ont pour effet de délimiter les pouvoirs et d'influencer les décisions des dirigeants », Charreaux (1997 : 1 ; 2002: 7) insiste davantage sur les mécanismes qui « gouvernent la conduite des dirigeants et définissent leur espace discrétionnaire ». Aux Etats-Unis, et par le biais de fonds de pension, nombre de salariés sont également actionnaires. Le gouvernement d'entreprise est essentiellement orienté vers la satisfaction des intérêts des actionnaires. Alors, « le salarié-actionnaire, indigné par les scandales successifs », peut-il trouver son compte au *whistleblowing* dès lors que ses intérêts sont alignés, même partiellement, sur ceux des actionnaires majoritaires (propos de M. Oxley, conférence Institut français des administrateurs, Paris, 1er février 2007). Il en est différemment en France pour deux raisons principales. La première tient au mode de financement des retraites[1]. La seconde à la faible participation d'administrateurs salariés au sein des conseils d'administration[2].

Le terme *whistleblowing* mérite d'être précisé dès nos propos introductifs. Ce terme n'est pas nouveau et fait son apparition aux Etats-Unis en 1963, à l'occasion de l'affaire Otto Otopeka[3]. Le *whistleblowing* est défini « comme le fait, pour un membre d'une organisation (ancien ou actuel), de révéler l'existence de pratiques illégales, immorales ou illégitimes dont l'employeur a la maîtrise, à une personne ou à un organisme susceptible de remédier à la situation » (Near et Miceli, 1985: 4). Il représente aussi la voix de la conscience (Berry, 2004).

Le *whistleblowing,* consiste, littéralement, à « souffler dans le sifflet » pour donner l'alerte. Le droit d'alerte existe déjà en droit du travail français sans connotation négative. L'alerte, exercée par les salariés, permet de signaler à l'employeur toute situation dangereuse pour la vie ou la santé[4] ; le droit d'alerte est encore conféré au comité d'entreprise qui peut intervenir auprès des organes chargés de l'administration ou de la surveillance de l'entreprise, ou auprès des associés, « lorsque la situation économique de l'entreprise se révèle préoccupante » (art. L. 432-5 du Code du travail).

Le *whistleblowing* est une pratique de contrôle au statut particulier qui ne se substitue pas mais s'ajoute bien aux autres possibilités existantes de contrôle interne *(reporting,* audit interne, outils de gestion type tableaux de bord...), déjà institutionnalisées dans les organisations. Précisons ce que nous entendons ici par la notion de contrôle : elle se réfère à l'atteinte d'un objectif et à la dichotomie, plus ou moins marquée, entre décision et action. Le contrôle est, traditionnellement, envisagé dans une relation hiérarchique, verticale, *top down.* Il concerne alors « l'ensemble des procédures que doit mettre en œuvre un supérieur hiérarchique par rapport à ses subordonnés, pour assurer sa maîtrise des décisions et leur exécution » (Ménard, 1997: 33).

Le contrôle, tel qu'il est introduit par le *whistleblowing,* peut être compris et interprété comme une contrainte imposée, au moins partiellement de l'extérieur —la loi Sarbanes-Oxley. Il s'étend à des relations verticales *down top* et latérales. Il se conçoit, de manière dynamique, comme mode de relation entre acteurs permettant d'atteindre la per-

1. Le financement des retraites, en France, relève, très majoritairement, de la protection sociale. La gestion des fonds, issus des prélèvements obligatoires des salariés et des employeurs, par la Sécurité sociale, n'est pas orientée vers le financement des entreprises. Aux Etats-Unis, au système de base, peuvent s'ajouter des contributions versées par les salariés et/ou les entreprises. Les sommes collectées par les organismes de retraite appelés "fonds de pension" sont susceptibles d'être affectées au financement des entreprises cotées ou non, aux Etats-Unis et dans le monde. Les salariés, futurs retraités américains, se transforment alors en actionnaires.

2. La loi française (n° 2001-152 ; n° 2001-420) prévoit la présence d'administrateurs salariés actionnaires ou administrateurs représentant les salariés (ADSA) dans les conseils d'administration des sociétés privées. Pour ce qui est des entreprises du CAC 40, 52 % ont un ADSA et 30 % (soit 11/40) des entreprises du CAC 40 ont des administrateurs représentant les salariés actionnaires (Institut français de gouvernement des entreprises, 2005).

3. Après avoir révélé au comité du Sénat américain, en charge de la sécurité intérieure, des informations confidentielles, Otto Otopeka, fonctionnaire *whistleblower* fut démis de ses fonctions, pour conduite déplacée.

4. L'article L. 231-8 du Code du travail dispose que le salarié « signale immédiatement à l'employeur ou à son représentant toute situation de travail dont il a un motif raisonnable de penser qu'elle présente un danger grave et imminent pour sa vie ou sa santé ainsi que toute défectuosité qu'il constate dans les systèmes de protection ».

formance, définie à partir d'objectifs qui satisfont d'abord l'intérêt de l'actionnaire.

Notre réflexion, nourrie par des entretiens semi-directifs et par l'étude de nombreux documents et rapports (voir méthodologie ci-après) vise à identifier quels sont les principaux enjeux managériaux du déploiement en France d'une pratique américaine de contrôle interne. Nous verrons que trois enjeux types méritent d'être analysés. Ils ont trait : 1/à la redistribution des pouvoirs ; 2/aux légitimités distinctes de l'alerte et du contrôle et ; 3/au glissement sémantique qui accompagne la migration d'une pratique de contrôle interne pour devenir une pratique "d'alerte éthique". Ces différents enjeux font écho aux représentations contrastées du salarié, en tant qu'agent du contrôle interne. En effet, introduire le *whistleblowing* revient à étendre le champ du contrôle interne jusqu'à présent en vigueur dans les organisations, faisant apparaître une nouvelle relation d'agence entre salariés et actionnaires. Les développements ci-dessus font l'objet de la première partie de l'article. La seconde partie est consacrée à une analyse des pratiques de *whistleblowing,* telles qu'elles sont repérables en France aujourd'hui.

L'appui plus marqué sur quelques exemples (Kodak en France notamment) a pour premier projet de mettre en évidence les tensions sur les pratiques du contrôle interne, sous tendues par le déploiement du whistleblowing dans un contexte français. Le second objectif est de montrer que, si le système tel qu'il est déployé aujourd'hui est à une phase embryonnaire de son utilisation, les ingrédients d'une transformation plus en profondeur des pratiques de contrôle interne nous semblent réunis.

ÉLÉMENTS DE MÉTHODE

La recherche est exploratoire et qualitative et prend appui sur des données construites et secondaires. Le domaine est encore mal connu et notre projet consiste à étudier les impacts possibles du déploiement d'une pratique sur le gouvernement d'entreprise. Il était donc nécessaire, selon la perspective campbellienne revisitée par Kœnig (2005: 9), d'être capable de mettre à profit une connaissance approfondie des situations étudiées afin d'être en mesure « d'estimer de façon compétente l'impact » probable du déploiement du *whistleblowing.* Afin d'atteindre ce niveau de connaissance approfondie, nous avons fait le choix de nous appuyer très largement sur des données construites de différentes natures (entretiens, conférences-débats) mais aussi sur des données secondaires nombreuses (rapports d'experts notamment). Il nous a semblé que la complexité du sujet ainsi que sa récence l'exigeaient.

Ainsi, nos données sont construites principalement grâce à des entretiens semi-directifs et libres (à deux chercheurs à chaque fois et d'une durée moyenne d'une heure trente par entretien). Les personnes interrogées sont toutes parties prenantes d'une réflexion sur la question du déploiement de l'alerte éthique en France. Nous avons rencontré des

M@n@gement, Vol. 11, No. 2, 2008, 113-135
Special Issue: Corporate Governance and Ethics

managers en charge de ces questions dans une grande chaîne de restauration rapide américaine (directeur des relations sociales et directeur des ressources humaines), des responsables de centrales syndicales (CGT, FO, CFDT) au niveau de quelques branches (pharmacie, métallurgie, agro-alimentaire) et au niveau confédéral ainsi que le président de la CNIL. S'ajoutent à ces entretiens formels, des participations à différentes rencontres institutionnelles avec M. Oxley, l'un des créateurs de la loi SOX, en février 2007 et avec MM. Antonmattei et Vivien en avril 2007, avec M. Medina à l'IFA en octobre 2007. Enfin, nous avons assisté, en tant qu'observateurs non participants, à une session de formation sur le whistleblowing organisée par une centrale syndicale et à destination de ses représentants cadres en octobre 2007 à Bordeaux.

A côté de la conduite d'entretiens et de la construction des données, l'originalité méthodologique relève ici de la place consacrée à l'étude de sources documentaires émanant des entreprises ou des organisations syndicales, et remises par nos interlocuteurs à l'issue des entretiens, ainsi qu'à celle de rapports produits par des institutions (ex. OCDE) ou rédigés à la demande du gouvernement français (rapport Antonmattei). En suivant Miles et Huberman (2003: 264) nous considérons que l'analyse empirique qualitative « continuellement locale » est un « instrument puissant » pour identifier des mécanismes et repérer les relations entre les événements et les processus. Nous avons procédé par adduction, en repérant des régularités stables (Koenig, 1993) et le mode de généralisation de cette recherche est de nature analytique au sens de Yin (1990). Nous avons opté pour une triangulation des méthodes de recueil de données (construites et secondaires) afin de réduire le risque de tirer des conclusions qui pourraient alors refléter seulement les biais ou les limites systématiques de telle ou telle méthode de recueil (Fielding et Fielding, 1986). Cette position se justifie notamment par le caractère relativement récent pour les acteurs du phénomène étudié et par la pluralité des positions à son encontre. En outre, en suivant les recommandations de Maxwell (2005), se donner la possibilité de confronter des données recueillies de différentes manières confère à nos conclusions plus de validité que si elles n'avaient émergé que d'une seule source ou méthode.

LES ENJEUX MANAGÉRIAUX DU DÉPLOIEMENT EN FRANCE D'UNE PRATIQUE AMÉRICAINE DE CONTRÔLE INTERNE

Introduit par la loi Sarbanes-Oxley, le *whistleblowing* —ou alerte éthique— est perçu comme une obligation imposée aux filiales françaises d'entreprises américaines ou aux entreprises françaises cotées aux Etats-Unis[5]. Le financement de l'entreprise et, partant, la réponse aux préoccupations des actionnaires, justifient l'existence du *whistleblowing,* dès lors que le contrôle introduit dans la relation d'agence entre dirigeants et actionnaires apparaît insuffisant pour garantir les

5. Aux Etats-Unis, le non respect des obligations issues de la SOX peut conduire à des sanctions qui s'exercent à deux niveaux : pour le dirigeant, sanctions civiles et pénales ; pour l'entreprise, exclusion de la Bourse.

droits des actionnaires, notamment dans leur dimension patrimoniale. Toutefois, le *whistleblowing* peut également être appréhendé comme opportunité d'agir sur les comportements, en particulier pour responsabiliser les parties prenantes, et notamment les salariés.
En d'autres termes, il apparaît nécessaire d'identifier les enjeux managériaux du déploiement de cette pratique particulière. Le premier concerne la redistribution des pouvoirs, le deuxième les légitimités distinctes de l'alerte et du contrôle et, enfin, le troisième a trait au glissement sémantique d'une pratique de contrôle interne qui devient une pratique d'alerte "éthique".

UNE REDISTRIBUTION DU POUVOIR : UN ENJEU POUR LE MANAGEMENT DE L'ACTION COLLECTIVE

Tout pouvoir s'inscrit dans une relation (Crozier et Friedberg, 1977). Détenu par un individu, il s'exerce sur une autre personne afin d'en influencer le comportement. Pour Dahl (1957: 202-203), « le pouvoir de A sur B se résume en la capacité de A d'obtenir que B fasse quelque chose qu'il n'aurait pas fait sans l'intervention de A ». Cette perspective a le mérite de rappeler que l'exercice du pouvoir n'est pas indépendant du réseau social au sein duquel il s'étend. Dans les organisations, le pouvoir consiste à « prendre des décisions qui intéressent l'ensemble » (Aron, 1972: 145) et qui « assurent la performance, dans le cadre d'obligations liées (…), quand les obligations sont légitimées par référence à leur participation à l'atteinte de buts collectifs » (Parsons, 1969: 361).
Le déploiement du *whistleblowing* fait émerger des enjeux managériaux cristallisés autour du pouvoir et des principes de coopération traditionnels. La distribution du pouvoir —ou de parcelles de pouvoir— est mise en cause, dès lors que les salariés entrent dans le jeu d'un contrôle qu'ils ne détiennent pas par délégation hiérarchique. La pratique de contrôle interne est ainsi a priori porteuse de transformations dans la mesure où elle investit les salariés de l'autorité morale de celui qui contrôle. Elle lui confère le pouvoir de contrôler en exerçant un droit d'alerter les parties prenantes en cas de constat ou de soupçon d'un dysfonctionnement. Ce pouvoir d'alerter distribué à tous les salariés affranchit, en théorie, de la seule autorité qui était, jusque-là, la leur, l'autorité hiérarchique fondée sur une légitimité rationnelle légale au sens de Weber.
Le contrôle via la pratique d'alerte, vise à déceler un comportement qui ferait courir un risque à l'entreprise. Ce contrôle introduit l'appréciation de comportements et fait appel à l'exercice de la responsabilité managériale, des dirigeants comme des encadrants de premier niveau. L'existence de cette forme de contrôle peut conduire à la recomposition des règles et des conventions formelles et informelles qui permettent la nécessaire coopération des acteurs. En particulier, la confiance entre managers et collaborateurs ou entre salariés peut être affectée, dès lors que les attentes constituées à l'intérieur d'une communauté perdent les repères quant à la définition d'un « comportement régulier, honnête et coopératif, fondé sur des normes habituellement partagées

M@n@gement, Vol. 11, No. 2, 2008, 113-135
Special Issue: Corporate Governance and Ethics

de la part des autres membres de cette communauté » (Fukuyama, 1995: 26). Toutefois, la capacité des salariés à avoir connaissance des fraudes, à les identifier, n'induit pas leur volonté d'exercer effectivement le contrôle (Moberly, 2006). Il s'agit là d'un potentiel qui ne serait pas pleinement utilisé. Deux raisons y concourent. Il s'agit d'abord de la loi du silence qui fait porter l'opprobre envers celui qui dénonce et l'évince de la communauté de travail. Ensuite, si cet obstacle est dépassé, il reste la crainte des représailles exercées par le management ou par des collègues. Cette crainte est exprimée dans la deuxième enquête européenne sur les risques de fraude en entreprise réalisée auprès des salariés de sociétés multinationales par Ernst et Young (2007). Ainsi, en France, seules 39 % des personnes interrogées « pensent que les salariés de leur société se sentiraient libres de signaler un éventuel cas de fraude dans leur entreprise », car la confidentialité de leur démarche serait suffisamment assurée. Aux Etats-Unis, l'étude de Rehg, Miceli et Van Scotter (2004) montre que les représailles à l'encontre du *whistleblower* dépendent pour une large part de la tolérance de l'organisation aux malversations. Plus cette dernière est élevée et moins les alertes sont utilisées en interne et moins les salariés ont confiance dans leurs supérieurs. Pour Weaver et Treviño (1999), ceci justifie la mise en place de programmes éthiques dans les entreprises afin d'éviter la loi du silence. Le salarié, qui se sent alors soutenu, perçoit comme acceptable de recourir à l'alerte. Le dispositif de contrôle via l'alerte tend ainsi à perturber les relations qui supportent la coopération en y insinuant les menaces de dénonciation et les craintes de représailles.

UNE JUXTAPOSITION DE L'ALERTE ET DU CONTRÔLE : UN ENJEU EN TERMES DE LÉGITIMITÉ

Avec le dispositif de *whistleblowing,* le pouvoir devient bidirectionnel. En effet, au pouvoir de contrôler pour certains, s'ajoute celui d'alerter pour tous. La transformation du contrôle interne par une base élargie de contrôleurs soulève une double question. L'une d'entre elles interroge la légitimité à détenir un pouvoir, l'autre, la légitimité à l'exercer.

La loi Sarbanes-Oxley adopte clairement le point de vue de l'actionnaire. L'idéologie capitaliste peut être considérée comme un support de légitimité. La vision de l'entreprise, l'optimisation de la valeur actionnariale en constituent le socle... à condition de faire partie du « système de croyances et de valeurs à propos de l'organisation, auquel tous les membres adhèrent » (Mintzberg, 1986 : 221). Il semble bien, du moins en France, que l'adhésion à cette représentation univoque soit loin d'être partagée et qu'il y ait débat sur la qualité des détenteurs des pouvoirs de contrôle et d'alerte.

Pour ce qui est de l'exercice du contrôle, la question de la légitimité fait intervenir les compétences à comprendre et à évaluer une situation de gestion. La qualité de l'accès du salarié à l'information —locale vs globale—, les miettes ou les ensembles d'activités qui lui sont confiées, influencent le regard porté sur sa légitimité à identifier, puis à évaluer une situation.

Dans la **Figure 1** sont exposés les enjeux de la juxtaposition de l'alerte et du contrôle interne dans un système de gouvernement que le *whistleblowing* modifie. Le caractère bidirectionnel du contrôle confié au salarié montre les liens qu'entretient cette pratique avec deux champs (celui du droit et celui de la norme), lesquels ne se rencontrent pas toujours aisément tant les socles de légitimité sur lesquels ils reposent sont fondamentalement distincts. En effet, le droit du travail est une source externe de droits et d'obligations qui s'impose aux acteurs du contrôle interne. Leur marge de liberté sur l'exercice du contrôle est d'autant plus réduite que des sanctions peuvent s'appliquer pour non respect des obligations issues du droit. Il en est différemment pour la norme sociale. Construite par les acteurs, à l'intérieur de l'organisation, elle s'appuie sur des valeurs, sur une idéologie qui accorde ou refuse aux salariés la légitimité de recourir à l'alerte.

L'intrusion de la norme sociale, porteuse d'une représentation de l'éthique, dans l'exercice du contrôle interne est susceptible de constituer une « source d'inspiration extra-juridique », à l'origine du développement d'une *soft law* (Pesqueux, 2007: 37). Celle-ci permet une « application contingente à un territoire institutionnel donné » d'une règle générale (la protection des investisseurs), et apporte une « réponse spécifique » à des enjeux particuliers dans une situation locale (les entreprises concernées, en France, par le volet *whistleblowing* de la SOX). La connexion entre les champs du droit et de la norme sociale ne semble pas aller de soi lorsqu'il s'agit de pratiques de gouvernement d'entreprise. Cependant, la contrainte dans le champ du droit existe ; les entreprises n'ont pas d'autre choix que de se mettre en conformité avec le volet *whistleblowing* de la loi SOX. Une manière pour elles, d'intégrer, d'absorber ou d'aborder la contrainte consiste à passer par la voie de la *soft law* (chartes éthiques, notamment). Il est dès lors possible d'envisager le champ d'application de la SOX comme un ensemble juridique, quelque part destiné à produire de la *soft law.*

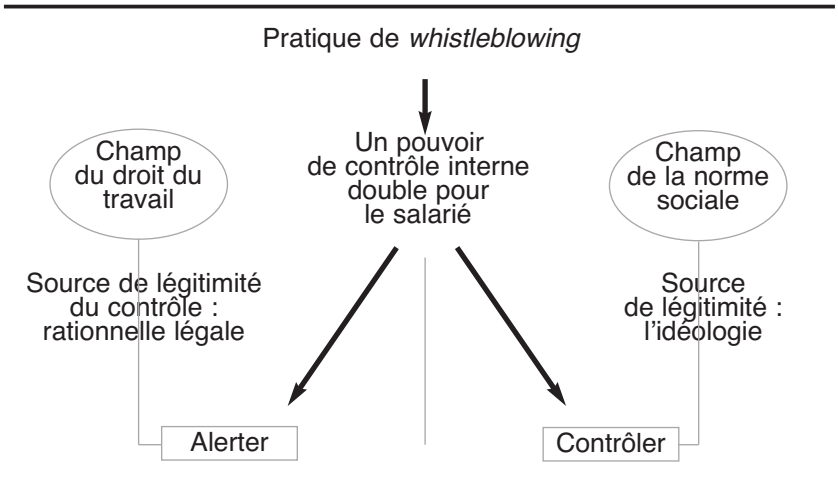

Figure 1. Le caractère bidirectionnel du contrôle interne

M@n@gement, Vol. 11, No. 2, 2008, 113-135
Special Issue: Corporate Governance and Ethics

D'UN CONTRÔLE INTERNE TRANSFORMÉ À L'ALERTE ÉTHIQUE EN PRATIQUE : L'ENJEU D'UN GLISSEMENT SÉMANTIQUE

En France, les actions de mise en conformité au *whistleblowing* se traduisent par la mise en place de dispositifs d'alerte quasi exclusivement qualifiés "d'alerte éthique". Le constat de ce glissement sémantique est suffisamment important pour que l'on s'y arrête. En effet, le caractère éthique de l'alerte pose question. Ethique par rapport à une application du droit ?, de la morale ?, de l'idéologie ? Si oui, sur quel(s) socle(s) juridique(s) ou conventionnel(s) prend-on appui ? Lors d'une récente conférence de l'ORSE (avril 2007), les responsables en charge de ces questions dans les entreprises interrogeaient : « Peut-on appréhender l'éthique, à travers les chartes, dans une dimension qui serait universelle ? ». Récemment encore, Pesqueux (2007: 37) interroge la question de l'éthique comme source de normativité dans la *corporate gouvernance,* celle-ci devenant la *soft law* de la *hard law.* Dans la même perspective, un responsable syndical, au niveau confédéral, confie « j'y vois le risque d'une privatisation du droit ».

« Salariés, héros ou délateurs ? » (de Bry, 2006: 2). Cette question souligne la représentation ambivalente du *whistleblowing* pour les parties prenantes. Alerter est perçu négativement ou, à l'inverse, manifeste un comportement héroïque du dénonciateur (Appelbaum, Grewal et Mousseau, 2006). Pour la CNIL (2005), le *whistleblowing* correspond à une alerte professionnelle, expression reprise par l'Union européenne[6] et le rapport Antonmattei/Vivien (2007)[7]. Le Cercle d'Ethique des Affaires (Eliet, 2005: 14) a retenu le terme d'alerte éthique, défini comme « un système permettant aux salariés d'alerter leurs dirigeants ou un comité spécialement constitué, sans risque d'être personnellement inquiétés, des irrégularités ou des mauvais comportements professionnels qu'ils constatent dans l'entreprise et dont ils estiment qu'ils font courir à l'entreprise un risque sérieux sur les plans financier, juridique, technique, sanitaire, sécuritaire ou quant à sa réputation ». Il est également intéressant de repérer que le glissement sémantique se retrouve dans le passage de la dénomination[8] de *hot line* ou *red line* aux Etats-Unis à *help line* en France. Ce glissement converge, selon nous, avec le passage d'une alerte conçue pour fonctionner a posteriori (après la fraude) à une alerte pensée pour agir comme un système préventif, a priori (avant la fraude).

Quelle que soit la représentation positive ou négative retenue de l'alerte éthique, les dirigeants sont tenus de déployer un dispositif d'alerte. La question du moment de l'alerte se pose et constitue un enjeu managérial car elle impacte largement celle du périmètre de l'alerte. En effet, si aux Etats-Unis, le *whistleblowing* fonctionne essentiellement comme un système d'alerte a posteriori (une fois que la fraude a été commise), son déploiement en France, compte tenu des débats et des différentes préconisations quant à sa mise en œuvre *(cf.* rapport Antonmattei et Vivien, 2007) insiste sur la dimension préventive de l'alerte. Elle apparaît ainsi non plus comme une possibilité curative mais comme un outil de gestion des risques probables dans l'entreprise. Il y a, dans ce glissement, les ingrédients d'une multiplication des

6. Avis 1/2006, adopté le 1er février 2006, relatif à l'application des règles de l'UE en matière de protection des données aux mécanismes internes de dénonciation des dysfonctionnements dans les domaines de la comptabilité, des contrôles comptables internes, de l'audit, de la lutte contre la corruption et la criminalité bancaire et financière. Le chapitre IV est consacré à l'analyse de la compatibilité des dispositifs d'alerte professionnelle avec les règles relatives à la protection des données.

7. Le rapport intitulé "Chartes d'éthique, alerte professionnelle et droit du travail français : état des lieux et perspectives" a été réalisé par un professeur de droit, P. H. Antonmattei et par P. Vivien (directeur des ressources humaines du groupe Areva), en janvier 2007.

8. Les auteurs remercient l'un des évaluateurs pour cette remarque d'ordre sémantique.

objets de l'alerte. Dans les esprits, si l'alerte devient un outil de management des risques, certains s'interrogent : pourquoi se limiter aux seuls risques financiers ? On rappellera simplement ici la position ferme de la CNIL en 2005 condamnant les positions prises en la matière notamment par l'entreprise McDonald France et demandant l'exclusion, dans le dispositif de l'entreprise, de tous les éléments susceptibles de porter atteinte à la vie privée des salariés.

Comme le montre Moberly (2006), l'attitude des salariés en matière d'alerte est à mettre en relation avec la valeur qu'ils confèrent aux effets de l'alerte éthique et avec l'évaluation des risques, pour eux-mêmes et pour l'organisation. Ainsi, la crainte des représailles, malgré des mesures collectives de protection, et la difficulté, voire l'incapacité à identifier, contacter les canaux pertinents pour porter et traiter la dénonciation, sont-elles des freins à l'exercice de l'action. En outre, les organisations préfèrent la discrétion et l'usage de canaux internes, pour révéler les fraudes, à la publicité inhérente à l'emploi de canaux externes. Pour le whistleblower, la protection contre les représailles est alors, le plus souvent, mieux assurée par le lancement de l'alerte avec recours à des voies internes. Cependant, de nombreux *whistleblowers* utilisent des canaux externes lorsqu'il leur apparaît que le rapport de pouvoir avec leur organisation ou avec le fraudeur, agit en leur défaveur. Ils recherchent alors la protection d'un espace public (Near et Miceli, 1996). Cependant, et même en dépit de fortes probabilités de représailles, l'alerte est le plus souvent lancée quand elle concerne des violations à la loi, et que le *whistleblower* estime que son action aura des effets positifs sur le dysfonctionnement (Near, Rehg, Van Scotter et Miceli, 2004).

La première partie de cette étude s'est ainsi attachée à souligner les enjeux managériaux du volet whistleblowing de la loi SOX (**Tableau 1**). Le déploiement de la pratique de l'alerte, en France, est marqué par l'influence des effets potentiellement induits par ces enjeux.

Si les acteurs que nous avons interrogés semblent affirmer de concert que les alertes effectives sont (encore) très peu nombreuses, tous s'accordent à dire que le stade embryonnaire d'aujourd'hui recèle les ingrédients d'une bombe à retardement pour demain. La seconde par-

Tableau 1. Enjeux managériaux du volet *whistleblowing* de la loi SOX

Fondements	Enjeux managériaux	Effets induits
Exercice du droit de contrôler induit par le droit d'alerter	Redistribution du pouvoir	Révision des principes de coopération (convention, hiérarchie, confiance)
Régulation du contrôle par le champ du droit Régulation de l'alerte par le champ de la norme sociale	Dualité des sources de légitimité dans la détention ou l'exercice du pouvoir	Renforcement du rôle de la *soft law* dans le contrôle interne
Appréciation des irrégularités : – selon un système de valeurs (celui des actionnaires ? celui des salariés ?) – selon des modalités temporelles variables (a priori, a posteriori)	Glissement sémantique : du *whistleblowing* à l'alerte éthique	Problème de définition du périmètre de l'alerte qui devient variable et spécifique à chaque organisation : – élargissement du champ (harcèlement...) – liens avec les chartes éthiques, par définition idiosyncrasiques

M@n@gement, Vol. 11, No. 2, 2008, 113-135
Special Issue: Corporate Governance and Ethics

tie de l'article vise ainsi à mettre en évidence ces ingrédients en montrant qu'ils sont potentiellement porteurs de changements substantiels pour le gouvernement de l'entreprise.

DU SIMPLE AMÉNAGEMENT DE LA PRATIQUE À LA POTENTIELLE RÉVOLUTION : L'EXPRESSION DE TENSIONS CONTRASTÉES

Le transfert de la pratique du *whistleblowing* dans les entreprises françaises s'inscrit dans le cadre général de mise en place d'un contrôle interne par « l'ensemble des sécurités contribuant à la maîtrise de l'entreprise. [Le contrôle interne] a pour but d'un côté d'assurer la protection, la sauvegarde du patrimoine et la qualité de l'information, de l'autre, l'application des instructions de la Direction et de favoriser l'amélioration des performances » (Ordre des Experts Comptables et des Comptables Agréés, 1977). Au-delà de la dimension comptable et financière, l'Autorité des marchés financiers[9] (2006) considère le contrôle interne comme un dispositif qui « contribue à la maîtrise des activités [de l'entreprise], à l'efficacité de ses opérations et à l'utilisation efficiente de ses ressources ». Il est susceptible de s'inscrire dans le référentiel du Committee of Sponsoring Organizations of the Treadway Commission (COSO)[10], lequel propose que le conseil d'administration, le management et le personnel de l'entreprise soient impliqués ensemble dans la mise en œuvre d'un processus de contrôle. Le contrôle interne opère ainsi comme une assurance raisonnable que les objectifs de fiabilité de l'information comptable et financière, d'efficacité et d'efficience de la conduite des opérations de l'entreprise, du respect des lois et de la réglementation applicable soient atteints.
En France, selon ses modalités de mise en œuvre et les dispositifs retenus, l'appropriation des pratiques de *whistleblowing* prend diverses formes le long d'un continuum qui s'étire de la reproduction délibérée d'une pratique à des prémices de révolution touchant au gouvernement de l'entreprise.

LE *WHISTLEBLOWING* EN FRANCE : UNE SIMPLE MISE EN CONFORMITÉ DES PRATIQUES DANS UN CADRE RÉGLEMENTAIRE AMÉNAGÉ ?

En France, la presse révèle en 2005 que les systèmes d'alerte posent des difficultés, à l'occasion d'affaires comme celle de McDonald, ou, à travers les changements de position de la CNIL qu'Antonmattei (24 avril 2007)[11] interprète comme étant des facteurs d'insécurité juridique. Le contexte changeant n'offre aux acteurs qu'une faible visibilité sur le devenir des pratiques. Ceci explique sans doute le caractère embryonnaire du déploiement du *whistleblowing* en France.
Sous contrainte d'une telle incertitude, les organisations tendent à s'en tenir à une mise en conformité, au respect d'une obligation, imposée par la logique américaine du marché financier. C'est dans cet esprit

9. L'Autorité des marchés financiers a publié en janvier 2007 une recommandation applicable aux rapports des présidents sur les procédures de contrôle interne relatifs aux exercices ouverts à compter du 1er janvier 2007. L'AMF recommande l'utilisation d'un cadre de référence et d'un guide d'application, pour partie inspirés du référentiel COSO (Committee of Sponsoring Organizations of the Treadway Commission).

10. Le COSO donne, en 1992, une définition du contrôle interne et fournit un cadre (le cube COSO) pour en évaluer l'efficacité. La loi Sarbanes Oxley oblige les sociétés cotées à évaluer leur contrôle interne. En imposant l'utilisation d'un cadre conceptuel, la SOX a favorisé l'adoption du COSO comme référentiel. Le COSO est également utilisé dans la mise en place des dispositions de la loi de sécurité financière (2003), pour les entreprises qui y sont assujetties. Pour plus de renseignements, voir le site internet du COSO : http://www.coso.org/IC.htm

11. Réunion d'échange à propos du rapport Antonmattei/Vivien (mars 2007), organisée par l'Observatoire de la responsabilité sociale des entreprises (ORSE), en présence de MM. Antonmattei et Vivien, avec l'animation de M. Médina (24 avril 2007). Les participants sont des membres de l'ORSE (ex. responsables des domaines juridique, déontologique, d'entreprises et représentants d'organisations syndicales).

que l'entreprise Kodak a déployé la procédure « consciencieusement, mais sans enthousiasme particulier », comme nous l'a confié un délégué syndical. La CNIL a été saisie, fin 2006, par les entreprises, de cinq cents déclarations de mise en place de dispositifs d'alerte professionnelle. Au cours du premier trimestre 2007, plus d'une centaine de demandes supplémentaires a été traitée, révélant ainsi la volonté grandissante des entreprises en France de se conformer aux contraintes que leur impose la loi américaine Sarbanes-Oxley de 2002. Il ne s'agit pas d'une adhésion, mais bel et bien d'une logique de conformité qui est privilégiée pour minimiser les risques de représailles.

En France, si le système se déploie peu à peu, dans les faits, les alertes effectives sont quasiment inexistantes[12] et ce mode de contrôle interne n'est précédé d'aucune expérience. Faudrait-il que les entreprises apprennent en la matière ? Si tel est le projet, quand la structure des savoirs antérieurs est faible dans un domaine, l'apprentissage y est limité car celui-ci est une fonction de ce qui est déjà connu du domaine (Cohen et Levinthal, 1990). Pour autant, dans le cas qui nous préoccupe, mettre en œuvre une telle nouvelle pratique suppose un aménagement minimum du cadre réglementaire.

Les préconisations du rapport Antonmattei peuvent d'ailleurs être appréhendées dans cette perspective. Il en va de même pour les recommandations managériales du modèle normatif de Moberly (2006) qui vise à définir strictement des procédures de *whistleblowing,* par le biais, entre autres, des canaux de révélation de la fraude et des personnes à contacter le cas échéant. Le respect des prérogatives des représentants du personnel et le recours aux dispositifs existants d'expression des salariés peuvent venir compléter l'aménagement de ce cadre. Il s'agit là de caractéristiques incitatives pour les potentiels lanceurs d'alerte. Ce dispositif est replacé dans un cadre de référence connu et accepté, celui de la protection des lanceurs d'alerte ou *whistleblowers.*

Plus généralement, l'étude des principes OCDE de gouvernement d'entreprise révisés en septembre 2004 et approuvés par les trente Etats membres montre un souhait général d'aménagement des pratiques de gouvernement d'entreprise au plus haut niveau, d'une part, et met en évidence le choix de ne pas questionner le principe même de l'alerte, d'autre part. En effet, il apparaît que la principale modification portant sur le chapitre des parties prenantes concerne la protection du salarié *whistleblower* et non une réflexion de portée managériale sur le sens même de l'alerte et sur son caractère ou non éthique. Il est, à ce propos, intéressant de remarquer que le Trade Union Advisory Committee (TUAC, 2004 : ii)[13] souligne « les progrès apportés par les Etats membres au chapitre sur les parties prenantes ». Cette instance syndicale internationale se félicite en outre du nouveau principe OCDE sur la protection des salariés témoins d'actes illicites, suivant en cela les dispositions légales instaurées par la loi Sarbanes-Oxley.

En d'autres termes, les principaux Etats industrialisés, membres de l'OCDE, et les partenaires sociaux au niveau international ont réformé, bien en amont de l'entreprise, le cadre des principes de gouvernement

12. A titre d'exemple, la direction du groupe Sanofi-Aventis annonce l'existence de trois alertes par mois en moyenne dans les entités du groupe hors Etats-Unis depuis le déploiement du dispositif en mai 2006. Les responsables « compliance/conformité », en France, déclarent traiter toutes les alertes.

13. Le TUAC est l'interface entre des syndicats de salariés et l'OCDE. Il regroupe 56 centrales syndicales affiliées dans les trente pays industrialisés de l'OCDE, représentant environ 60 millions de travailleurs.

M@n@gement, Vol. 11, No. 2, 2008, 113-135
Special Issue: Corporate Governance and Ethics

d'entreprise afin que les pratiques de gouvernement en vigueur aux Etats-Unis depuis SOX puissent être adaptées, sans entrer en conflit avec les principes affichés jusqu'alors dans les pays dits OCDE. Le choix de la simple adaptation (conformité) exclut ainsi la remise en cause plus profonde des représentations, des schémas de pensée des acteurs (Argyris et Schön, 1996), relatifs au principe même de l'alerte. Néanmoins, telle que la pratique se déploie aujourd'hui, nos investigations montrent que les ingrédients sont réunis pour un questionnement bien plus profond.

L'ALERTE ÉTHIQUE À LA FRANÇAISE : VECTEURS POUR UNE POSSIBLE RÉVOLUTION ?

Deux vecteurs apparaissent à l'analyse des dispositifs de déploiement de l'alerte en France. Ils laissent supposer que des modifications sur le gouvernement d'entreprise pourraient être bien plus profondes. Il s'agit de l'élargissement du domaine de l'alerte, d'une part, et du rôle nouveau de contrôleur du salarié, d'autre part. Selon nous, ce rôle ouvre la voie à deux configurations possibles de gouvernement d'entreprise à l'avenir, l'une tendant vers le modèle actionnarial et l'autre vers un modèle plus partenarial.

QUAND UN DISPOSITIF NOUVEAU APPARAÎT… ET QUE LE DOMAINE DE L'ALERTE S'ÉLARGIT

Le premier vecteur potentiel d'une transformation du gouvernement d'entreprise est l'introduction même de ce nouveau mode de contrôle interne. En effet, les parties prenantes (salariés, dirigeants, actionnaires) ne peuvent plus complètement agir, ni même se représenter le système de contrôle interne de leurs actions comme auparavant. Même si le système d'alerte n'est pas actionné, son potentiel de transformation sur le gouvernement d'entreprise est grand. En effet, il contient les ingrédients d'un élargissement du champ d'application de l'alerte, laquelle ne resterait plus seulement cantonnée à la sphère comptable et financière mais viendrait, plus largement, se nourrir des problèmes plus indéterminés de loyauté à l'entreprise, de respect des valeurs organisationnelles, de comportements etc. Le cas Kodak illustre tout à fait ce premier vecteur.

Dans cette dernière entreprise, la pratique de *whistleblowing* a été déployée de la manière suivante fin 2004 : une ligne téléphonique gérée par une société indépendante (numéro vert) a été mise à disposition des salariés et une lettre d'accompagnement très explicite, cosignée par le président du conseil d'administration et du président directeur général du siège de Kodak à Rochester aux Etats-Unis a été distribuée à l'ensemble des salariés dans le monde. Une petite carte (format carte de visite) qui reprend l'essentiel du dispositif a été jointe à ce courrier sous les termes : « La ligne d'assistance sur la conduite des affaires de Kodak ». Elle indique deux numéros de téléphone selon que le salarié appelle des Etats-Unis ou du reste du monde. Son

format portefeuille la destine à accompagner le salarié où qu'il soit. Il est ainsi fait appel à la vigilance constante du salarié et à son rôle de contrôleur de la conduite des affaires. Le comité de direction d'un site de Kodak en France a joint au courrier américain une lettre explicative dont il est intéressant de noter que la teneur vise à élargir le champ de l'alerte. Ci-après, des extraits des deux lettres illustrent la manière contrastée dont le siège et le site français de l'entreprise ont présenté le dispositif aux salariés.

« Nous sommes fiers du profond engagement de nos employés à se conduire en affaire selon les plus hautes normes d'éthique —une des raisons majeures de l'excellente réputation dont jouit Kodak dans le monde. Nous veillons à agir avec intégrité dans nos transactions commerciales et à nous conformer aux politiques de la société et aux lois parce que c'est ainsi qu'il faut agir. (...) Si une situation vous semble douteuse en termes d'intégrité ou de conformité, nous vous engageons à en parler d'abord à votre supérieur. Vous pouvez également en faire part à votre chef de service, à n'importe quel directeur, au service des ressources humaines ou à celui du contentieux. La ligne d'assistance sur la conduite des affaires de Kodak a été établie pour vous offrir un moyen supplémentaire de communiquer une inquiétude, de façon confidentielle, et même, anonyme » (extrait de la lettre du siège américain de Kodak).

« Ce nouveau service répond à un souci de faciliter principalement l'identification de pratiques commerciales qui ne sont pas conformes non seulement aux lois mais aussi aux valeurs de la compagnie. En tant que société manufacturière, nous sommes très peu concernés par les aspects relevant purement des pratiques commerciales ; par contre, certains aspects concernant en particulier la discrimination ou les abus de toute sorte peuvent s'appliquer à notre site » (extrait de la lettre du comité de direction en France).

Parce qu'elle s'estime peu concernée par l'usage du dispositif appliqué aux transactions commerciales, la direction du site en France prend l'initiative d'élargir le champ de l'alerte aux discriminations et abus de toute sorte, sans pour autant en préciser la nature ou les contours. Ainsi, comme le souligne Antonmattei (réunion ORSE–AREVA) l'élargissement du domaine de l'alerte, hors champs strictement comptable et financier, est envisagé de manière à « disposer d'un grand système de canal de remontée des faits, pour autant que ceux-ci nuisent gravement au fonctionnement de l'entreprise » Il ne s'agit donc pas « d'installer des corbeaux sur tous les arbres » (responsable CNIL, 2007), mais, comme l'a rappelé Antonmattei, de faire « fonctionner aussi bien en vertical qu'en horizontal un système fait pour la prévention, complémentaire à d'autres systèmes, comme celui des représentants du personnel ».

Nous défendons ici l'idée que l'élargissement du champ de l'alerte est susceptible de faire évoluer considérablement l'exercice du contrôle interne ; on passe d'un système de contrôle a posteriori pour dénoncer des dysfonctionnements à un système de contrôle a priori pour éviter que des dysfonctionnements ne se produisent. Le rapport Antonmattei/Vivien préconise sur ce point d'encourager les comportements

M@n@gement, Vol. 11, No. 2, 2008, 113-135
Special Issue: Corporate Governance and Ethics

d'anticipation et de prévention, de l'ensemble des parties prenantes de la communauté de travail. Certaines entreprises françaises se sont engagées dans la voie de la formation des dirigeants, des mandataires sociaux, des managers et des salariés afin de leur apprendre à repérer et à traiter les situations dites à risques. Le rapport présenté par l'Institut Français des Administrateurs (2007: 48-49) s'inscrit dans cette perspective alors qu'il préconise l'établissement, par le conseil d'administration, d'une cartographie des risques attachés aux différentes parties prenantes (actionnaires, clients, fournisseurs, salariés, société civile) qui affectent ou qui sont affectées par le fonctionnement de l'entreprise. Un bon système d'alerte devient alors celui dans lequel l'alerte ne se produit plus (Antonmattei et Vivien, 2007) grâce à la participation d'acteurs compétents et à l'identification et l'anticipation des risques. Un vecteur complémentaire peut être repéré pour étayer la thèse d'une transformation du gouvernement de l'entreprise. Il s'agit des salariés eux-mêmes en tant qu'acteurs du contrôle interne.

QUAND LES SALARIÉS DEVIENNENT DES CONTRÔLEURS INTERNES

Dans la perspective de la loi Sarbanes-Oxley, l'introduction des salariés, comme acteurs du contrôle interne, se traduit par de nouveaux flux d'informations susceptibles de transformer les règles de la coopération. Ainsi, aux côtés de la relation hiérarchique, managers/salariés, bien identifiée, émerge une relation de contrôle des salariés à destination des dirigeants dont il est difficile, pour les acteurs, et en l'état actuel des pratiques, de cerner le périmètre. Cela constitue, selon nous, une extension du contrôle interne. Les acteurs se trouvent placés dans une double situation, paradoxale, de contrôleur et de contrôlé. Parce qu'il est en position d'avoir à connaître la fraude, commise par les dirigeants, voire par les managers ou encore par ses pairs, le salarié est en effet incité à la révéler, au bénéfice des actionnaires (**Figure 2**).

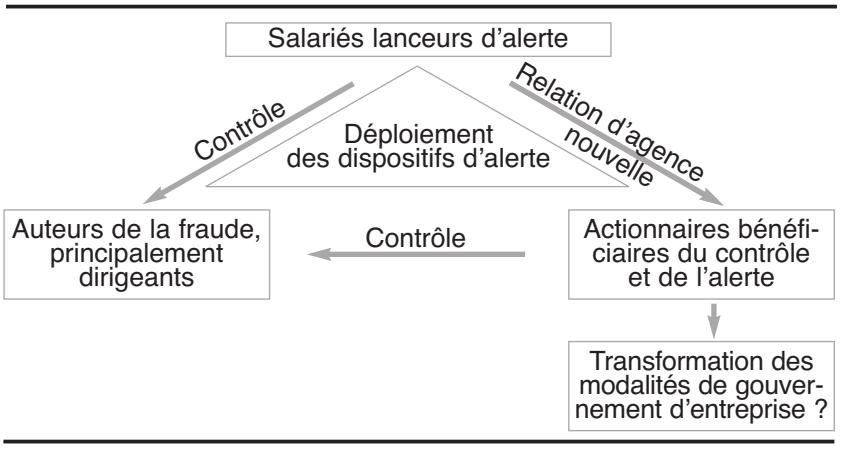

Figure 2. Exercice de l'alerte éthique : une relation triangulaire

Une relation triangulaire entre trois parties prenantes (salariés, dirigeants, actionnaires) est ainsi établie. Elle est susceptible de transformer les salariés en agents des investisseurs pour contrôler les dirigeants. Ceci est de nature, selon nos analyses, à contenir les ingrédients d'une modification plus profonde que la pratique actuelle ne le laisse paraître du gouvernement d'entreprise.

Il est intéressant de noter que, comme d'autres systèmes de contrôle, le *whistleblowing* est susceptible d'intégrer des approches fondées à la fois sur la conformité et sur le partage de valeurs. Il s'agit notamment, selon la relation triangulaire instaurée (*cf.* Figure 2) d'assurer aux salariés que la justice sera respectée, que la fraude sera sanctionnée, quel que soit le statut de son auteur (Stansbury et Barry, 2007: 245) et que le lanceur d'alerte ne subira aucune forme d'ostracisme. Cependant, dans la mesure où le contrôle interne des salariés sur les dirigeants encadre le pouvoir discrétionnaire de ces derniers, il tend à introduire, pour autant que les parties prenantes acceptent ce rôle, un mécanisme supplémentaire dans le système de gouvernement d'entreprise. L'introduction de la pratique de *whistleblowing* modifie ainsi le partage du pouvoir. La limite réside cependant dans l'acceptation ou non par les parties prenantes (salariés comme dirigeants) de cette extension du contrôle interne.

Les salariés, en tant que nouveaux acteurs du contrôle interne, peuvent exister à travers deux postures. Selon la première, ils sont susceptibles d'être instrumentalisés par les actionnaires pour servir des intérêts qui ne sont que très indirectement les leurs. Dans ce cas, nous considérons qu'ils "sont agis" et qu'une relation d'agence entre actionnaires et salariés est nouée (*cf.* Figure 2). Elle constitue la base de la légitimité du pouvoir donné au salarié de contrôler, même partiellement, ponctuellement, les dirigeants. Renforcé par cette légitimité, le salarié, en position d'agent, se plie à la règle de l'actionnaire, en position de principal, « tout en contrôlant la marge d'incertitude que lui confère son avantage en terme d'information » (Curien, 1994: 21). Le salarié assure ainsi son pouvoir à la fois vis-à-vis de l'actionnaire et vis-à-vis de ceux qu'il peut dénoncer. L'intrusion des salariés sur la scène du contrôle interne est instrumentalisée par les actionnaires afin d'affaiblir la latitude des dirigeants. Elle concourt à structurer de nouvelles relations qui transforment les règles du gouvernement d'entreprise, dès lors que les salariés participent à influencer les décisions des dirigeants et à limiter leur espace discrétionnaire (Charreaux, 1997). Le modèle de gouvernement d'entreprise reste un modèle actionnarial parce qu'il maintient l'objectif de maximisation de création de valeur pour les actionnaires. Toutefois, ce modèle est infléchi puisque la totalité des droits de contrôle sur les dirigeants n'est plus alloué aux seuls actionnaires mais partagé, même de manière occasionnelle avec les salariés-contrôleurs.

Selon la seconde posture, le salarié peut également exercer son pouvoir d'alerte afin de satisfaire ses intérêts. Le gouvernement d'entreprise est alors susceptible d'évoluer vers un modèle contractuel partenarial (Charreaux, 2002) qui prendrait davantage en compte les intérêts des salariés. A l'allocation de droit de contrôle sur les dirigeants

M@n@gement, Vol. 11, No. 2, 2008, 113-135
Special Issue: Corporate Governance and Ethics

s'ajoute alors un objectif de maximisation de la valeur pour les parties prenantes, actionnaires et salariés. Ce scénario n'est probablement pas celui de la loi Sarbanes-Oxley qui se situe davantage dans une perspective de conversion à la financiarisation de l'économie que dans une démarche sociale. Le **Tableau 2** propose une synthèse des modèles de gouvernement d'entreprise susceptibles d'émerger, selon nous, du rôle joué par le salarié-contrôleur.

L'irruption d'un dispositif d'alerte éthique bouleverse ainsi potentiellement les schémas des parties prenantes sur le fonctionnement de l'entreprise, les rôles qu'elles y jouent. Elle s'immisce dans la culture, les valeurs et les pratiques de l'organisation. Aussi les modalités de mise en place de la pratique de whistleblowing sont-elles susceptibles d'emprunter des figures variées. Comme indiqué en **Figure 3**, celles-ci se déploient le long d'un continuum compris entre la reproduction délibérée d'une pratique et les prémisses d'une modification plus radicale intégrant l'élargissement du domaine de l'alerte ainsi que le rôle nouveau de contrôleur du salarié.

Tableau 2. Effets probables du rôle joué par le salarié-contrôleur sur l'émergence de nouveaux modèles de gouvernement d'entreprise

Relation d'agence entre actionnaires et salariés	Gouvernance actionnariale Instrumentalisation de la relation d'agence par les actionnaires	Gouvernance partenariale Instrumentalisation de la relation d'agence par les salariés
Bénéficiaires d'un droit de contrôle sur le dirigeant	Actionnaires en Assemblée Générale Conseil d'administration Salariés-contrôleurs	Actionnaires en Assemblée Générale Conseil d'administration Salariés-contrôleurs
Bénéficiaires de la valeur créée dans l'entreprise	Maximisation de la valeur pour les actionnaires	Maximisation de la valeur pour un ensemble de parties prenantes (les actionnaires, les salariés)

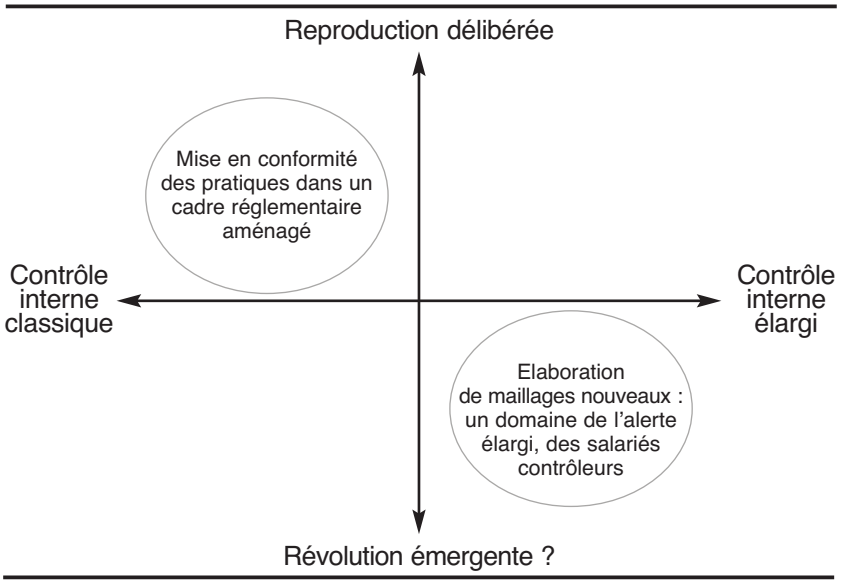

Figure 3. Les figures du déploiement des pratiques d'alerte éthique en France

Il est intéressant de noter, qu'en France, certaines centrales syndicales pressentent les bouleversements possibles des modèles de gouvernement d'entreprise. Elles se saisissent alors du problème de l'alerte pour revendiquer une redéfinition des rapports sociaux au travail. Elles développent une logique qui les conduit à instrumentaliser le dispositif d'alerte et à l'intégrer dans une démarche globale de responsabilité sociale de l'entreprise (RSE). Les syndicats appréhendent la RSE avec une exigence de responsabilité des salariés et, plus spécifiquement, celle des cadres (RSC). Cette responsabilité ne s'entend pas comme allégeance à l'entreprise et obéissance aveugle à ses prescriptions. Elle se conçoit comme un engagement du salarié qui peut l'inciter à la désobéissance organisationnelle afin de prendre en compte les intérêts, le plus souvent hors de la sphère financière, des diverses parties prenantes.
Ainsi, de la stricte observance d'une obligation venue des Etats-Unis, on observe des voies différenciées de déploiement ; reproduction aménagée versus révolution potentielle. C'est sans aucun doute pour cette raison que les Etats membres de l'OCDE ont cherché, dès 2004, à développer un discours qui dépasse le strict cadre de la reproduction ou de l'adaptation de principes et pratiques de gouvernement d'entreprise pour l'inscrire dans un débat plus large, aux contours plus flous aussi, celui de la RSE.

CONCLUSION ET DISCUSSION

Dans cet article, nous interrogeons, au regard des pratiques d'alerte dans les dispositifs de contrôle interne, les possibles transformations du système de gouvernement pour les entreprises françaises. Plus précisément, nous nous focalisons sur l'impact probable d'un dispositif particulier, le *whistleblowing* qui nous vient d'outre-Atlantique. Que se passe-t-il lorsqu'une pratique de contrôle interne américaine est déployée au sein d'entreprises françaises cotées aux Etats-Unis ou au sein de filiales d'entreprises américaines établies en France ?
Rappelons ici que le point de vue adopté par la loi Sarbanes-Oxley et le référentiel COSO est celui d'une logique de financiarisation de l'économie. Le bon fonctionnement du marché financier suppose la confiance des investisseurs, rassurés par des règles de gouvernement efficaces. Sur ce dernier point, le rapport établi par Antonmattei et Vivien (2007) rappelle que le scandale Enron a mis en lumière l'inefficacité de manière globale des mesures existantes de contrôle des comptes et de direction de l'entreprise. Dans ce contexte, la question de l'importation d'une pratique prend une dimension particulière. En effet, comme le souligne Amable (2006), en France, l'empilement, même aménagé, d'une approche américaine, ébranle notre modèle de capitalisme en affectant les équilibres sociaux et les compromis institutionnels qui les accompagnent, au détriment des salariés.
Grâce à l'analyse de la littérature, des entretiens que nous avons menés et des données secondaires recueillies, nous avons pu révéler trois enjeux managériaux liés au déploiement, en France, d'une pra-

M@n@gement, Vol. 11, No. 2, 2008, 113-135
Special Issue: Corporate Governance and Ethics

tique américaine de contrôle interne. Nous avons mis en évidence, dans la première partie, que ces enjeux concernent à la fois la redistribution des pouvoirs, les légitimités relevant du droit ou de l'idéologie, ainsi que le glissement du sens de l'alerte, de chaque côté de l'Atlantique. Puis, dans la seconde partie, nous avons tenté de dresser les figures du déploiement de l'alerte éthique en France, à travers les pratiques. Celles-ci varient de la reproduction délibérée d'une pratique à une modification plus radicale. Nous avançons l'hypothèse d'une possible révolution dans les pratiques de contrôle interne. En effet, des ingrédients contenus dans les principes qui sous tendent la pratique d'alerte nous paraissent être de nature à modifier substantiellement l'exercice de ce contrôle. Nous traitons de deux ingrédients ou vecteurs de cette transformation que sont l'élargissement du domaine de l'alerte et le rôle nouveau de contrôleur du salarié. Ils conduisent à repenser la nature des rapports sociaux dans l'entreprise, et, plus particulièrement les liens d'emploi.

Cette réflexion conserve toutefois un caractère exploratoire tant les pratiques effectives d'alerte émergent en France, même si le contexte de leur déploiement fait depuis plus longtemps l'objet d'analyses (Gressier, 2005). Cependant, nous pensons que ces premiers enseignements constituent déjà une base féconde de discussion. Celle-ci peut être organisée autour de trois idées liées. La première concerne le périmètre de l'alerte, la deuxième a trait à la question de l'articulation de cette alerte éthique avec les autres dispositifs de contrôle interne déjà existants au sein des organisations. Enfin, la troisième concerne le salarié au cœur du dispositif de contrôle et qui dispose simultanément d'un pourvoir de contrôle et d'un pouvoir d'alerte.

Le périmètre de l'alerte peut s'étendre selon deux directions suivant la perception positive ou négative du dispositif par les acteurs. Certains peuvent trouver de la satisfaction en considérant une dimension éthique au contrôle. Dans ce cas, les signaux, positifs, lancés aux actionnaires, peuvent être perçus par des parties prenantes externes et diminuer ainsi l'exposition de l'entreprise à d'éventuelles sanctions pour non respect de l'éthique (Stansbury et Barry, 2007: 243). A l'inverse, et la position initiale de la CNIL (en 2005) en est le révélateur, un dispositif d'alerte, déclenché par les salariés, à l'encontre des dirigeants, mais aussi, éventuellement, de leurs collègues, peut provoquer réticence voire hostilité. Cette perception négative s'applique au niveau des valeurs ; l'alerte consiste à dénoncer et la dénonciation, souvent associée à la volonté de nuire, est connotée négativement (Weaver et Treviño, 1999). En outre, pour ce qui est du droit français, des domaines et des niveaux d'alerte sont déjà contenus dans ce qu'on appelle le droit d'expression (ex. art. L 461-1 du Code du travail1). Il convient toutefois de préciser que si l'alerte s'exerce à un niveau individuel, le droit d'expression ci-dessus mentionné est un droit collectif.

Se pose alors la question du recouvrement, de la nouveauté de l'alerte éthique, telle que l'oriente la loi Sarbanes-Oxley, c'est-à-dire de l'articulation avec les dispositifs existants. Cette articulation se conçoit tant au plan de la cohérence des mécanismes (procédures compa-

tibles) que de leur philosophie (principes et valeurs qui les sous tendent). Cette difficulté est évoquée par le monde syndical (CGT, FO, CFDT) en particulier sous l'angle de la participation à l'élaboration des dispositifs d'alerte. Convient-il qu'il n'y ait pas de mise en place de l'alerte éthique sans voie négociée ? Certains souhaitent que ce dispositif soit un complément, après les représentants du personnel, qui tienne compte de la protection du lanceur d'alerte. D'autres considèrent que les dispositifs d'alerte, appuyés sur le droit d'expression, pourraient être étendus au-delà de la comptabilité ou de la finance, permettant ainsi aux salariés de peser sur les choix des entreprises. Enfin, et peut-être surtout selon nous, si les salariés sont placés au premier rang pour faire exister l'alerte, l'interrogation est patente sur les satisfactions qu'ils peuvent en obtenir.

L'engagement des salariés dans le contrôle interne pourrait apparaître comme une solution pour révéler l'information et réduire l'asymétrie entre actionnaires et dirigeants. En effet, les salariés, immergés dans l'entreprise, sont perçus comme des acteurs nombreux et compétents, d'autant plus susceptibles de se transformer en informateurs de pratiques illégales qu'ils sont concernés par l'avenir de leur entreprise (Antonmattei et Vivien, 2007). Toutefois, placer le salarié au cœur d'un dispositif de contrôle interne permettra-t-il de lever les difficultés pointées de manière consensuelle par les observateurs ? Comme tout système de contrôle, l'alerte éthique vise à atteindre son objectif initial —le renforcement de la confiance des actionnaires— en élaborant un dispositif qui stimule la cohérence et la prévisibilité des opérations (Stansbury et Barry, 2007: 241). En outre, l'apprentissage des salariés portant sur l'identification et la prévention des dysfonctionnements frauduleux est ainsi favorisé. Dans le même temps, toute instrumentalisation de l'alerte, qui serait perçue comme le moyen de conforter la position des dirigeants et non comme une démarche gagnant/gagnant entre parties prenantes, serait vouée à affaiblir, voire à discréditer le dispositif. A l'inverse, l'efficacité de l'alerte serait renforcée dès lors qu'un certain nombre de conditions seraient réunies. Parmi celles-ci, le périmètre des mécanismes de contrôle devrait être clairement délimité, la communication non ambigüe, et le système d'alerte éthique en adéquation avec les préoccupations des parties prenantes. Ces conditions permettraient de soutenir la coopération et de prévenir des comportements de rejet contre les dispositifs de contrôle (Stansbury et Barry, 2007: 257).

Nous voudrions, pour poursuivre la discussion, suggérer deux prolongements possibles pour cette recherche. Le premier concerne la confiance à un niveau individuel d'analyse et le second a trait au statut de l'alerte en privilégiant un niveau organisationnel d'analyse. Il nous semble qu'interroger plus avant le thème de la confiance des acteurs dans l'usage des dispositifs constitue une piste féconde. Celle-ci est entendue comme « mécanisme qui neutralise l'opportunisme et restaure la prévisibilité des comportements » (Karpik, 1998: 1045). En effet, la possibilité de recours à l'alerte éthique revêt deux facettes. Sur la première, l'alerte apparaît comme le moyen de garantir les actionnaires contre la fraude des dirigeants, de sécuriser leur investissement par une surveillance et, in fine, une moralisation des pratiques. Sur la

M@n@gement, Vol. 11, No. 2, 2008, 113-135
Special Issue: Corporate Governance and Ethics

seconde facette, l'alerte, perçue comme une menace permanente, est susceptible d'entraver l'action collective par anéantissement de la confiance. Cette dernière permet et facilite les échanges, les partages d'information, l'expérimentation, l'apprentissage collectif, c'est-à-dire la coopération qui exige un minimum d'intégration des comportements des individus et des groupes (Crozier et Friedberg, 1977).

Si l'on déplace les préoccupations au niveau organisationnel, le statut de l'alerte permet de poser d'intéressantes questions et constituerait, selon nous, le second prolongement possible de cette recherche. Dans cette perspective, l'alerte peut en effet apparaître comme un dispositif de contrôle a priori, et finalement comme un moyen d'anticiper et de gérer les risques (Medina, 2006).

Les préconisations du rapport Antonmattei/Vivien, comme les réflexions de l'ORSE ou celles de cabinets d'audit, semblent ainsi s'orienter vers une transformation du statut de l'alerte éthique, orientant, ce faisant, ses finalités. Ces réflexions mériteraient alors d'être poursuivies dans le courant théorique proposé par Charreaux (2002), qui privilégie la vision partenariale à la vision purement actionnariale de la gouvernance. Selon cette acception, le gouvernement d'entreprise se préoccupe davantage de prévenir les conflits entre les parties prenantes ; les dispositifs d'alerte pourraient ainsi être étudiés par cet éclairage. Cette voie nous semble d'autant plus riche que les administrateurs demandent aujourd'hui au conseil d'administration de réaliser des cartographies des risques RSE portés par les différentes parties prenantes (rapport IFA, septembre 2007).

Enfin, nous voudrions insister sur le manque de recul aujourd'hui en France par rapport à la mise en place et à l'utilisation de l'alerte. Reste en effet posée une question centrale ; celle de son efficacité économique. Si l'on sait que l'alerte peut diminuer les coûts de contrôle exercé par l'actionnaire (Moberly, 2006) elle peut aussi paralyser les processus collaboratifs sans garantie certaine que les intérêts de ceux pour qui elle a été pensée ne soient assurés.

Note. Cette production s'inscrit dans le cadre d'un projet financé par l'Agence Nationale de la Recherche : Le potentiel régulatoire de la RSE. Les auteurs tiennent à remercier les évaluateurs pour la qualité de leurs remarques et conseils.

Sandra Charreire Petit est professeur à l'Université Paris Sud 11. Elle y dirige le PESOR (EA 3546), mention gestion des organisations et le M2 recherche "Organisation, Stratégies et Risques". Ses recherches portent sur l'apprentissage organisationnel, le pilotage des changements et, plus récemment, sur le pilotage des systèmes éthiques dans les organisations.

Joëlle Surply est maître de conférences à l'Université Paris Sud 11 et membre du PESOR. Elle dirige le M2 professionnel "Contrôle de gestion sociale et RH". Ses recherches portent sur l'apprentissage organisationnel, la gouvernance et les questions de responsabilité sociale des organisations.

RÉFÉRENCES

■ Amable, B. 2006
Le modèle européen ébranlé, *Sciences humaines,* 176, 40-43.

■ Antonmattei, P. H., et P. Vivien 2007
Chartes d'éthique, alerte professionnelle et droit du travail français : état des lieux et perspectives, Collection des rapports officiels, Paris : La Documentation Française. Site internet : lesrapports.ladocumentationfrancaise.fr /BRP/074000335/0000.pdf

■ Appelbaum, S. H., K. Grewal, et H. Mousseau 2006
Whistleblowing: International Implications and Critical Case Incidents, *Journal of American Academy of Business,* 10: 1, 7-13.

■ Argyris, C., et D. A. Schön 1996
Organizational Learning II: Theory, Method, and Practice, Reading, MA : Addison Wesley.

■ Aron, R. 1972
Etudes politiques, Paris : Gallimard.

■ Autorité des Marchés Financiers 2006
Recommandation de l'Autorité des marchés financiers sur le "Dispositif de contrôle interne : Cadre de Référence" ifaci.com/fo/aff_file.asp?id=169

■ Berry, B. 2004
Organizational Culture: A Framework and Strategies for Facilitating Employee Whistleblowing, *Employee Responsibilities and Rights Journal,* 16: 1, 1-11.

■ Boughanmi, A., et B. Deffains 2006
Droit, gouvernance d'entreprise et structure du système financier : une analyse économétrique du cas français (1980-2004), *Finance Contrôle Stratégie,* 9: 4, 33-66.

■ Charreaux, G. (Ed.) 1997
Le gouvernement des entreprises : corporate governance, théories et faits, Paris: Economica.

■ Charreaux, G. 2002
Variation sur le thème "À la recherche de nouvelles fondations pour la finance et la gouvernance d'entreprise", *Finance Contrôle Stratégie,* 5: 3, 5-68.

■ Cohen, W. M., et D. A. Levinthal 1990
Absorptive Capacity: A New Perspective on Learning and Innovation, *Administrative Science Quarterly,* 35: 1, 128-152.

■ Crozier, M., et E. Friedberg 1977
L'acteur et le système, Paris : Seuil.

■ Curien, N. 1994
Régulation des réseaux : approches économiques, *Annales des Mines : Réalités industrielles,* octobre, 21-26.

■ Dahl, R. 1957
The Concept of Power, *Behavioral Science,* 2: 3, 201-215.

■ de Bry, F. 2006
Salariés, héros ou délateurs ? Du *whistleblowing* à l'alerte éthique, *Lettre du management responsable,* 6, octobre, 1-13.

■ de Pover, M.-F. 2006
Le "whistle blowing" anglo-saxon ou comment mettre en place un système "d'alertes éthiques" dans les pays de tradition civiliste sans créer une chasse aux sorcières ou une mesure disproportionnée par rapport à la poursuite d'un objectif légitime : la lutte contre la fraude interne, *Bulletin d'informations ALCO,* 7 : janvier, 4-14.

■ Délégation internationale pour l'audit et la comptabilité (DIPAC) 2006
Vues de presse internationale, 82, mai. Disponible électroniquement à : www.dipacint.com/content/download/660/2650/version/1/file/VDP_82.pdf

■ Eliet, G. 2005
Whistleblowing : quel système d'alerte éthique pour les entreprises françaises ?, Les cahiers de l'éthique n° 2, Paris : Cercle d'Ethique des Affaires.

■ Ernst & Young 2007
Enquête européenne sur les risques de fraude en entreprise. Paris : Ernst & Young. www.ey.com/global/content.nsf/France/Press_release_etude_fraude_04062007

■ Fayol, F. 2005
Droit d'alerte et whistleblowing : donner du sens et négocier, *Cadres-CFDT,* 414, avril, 37-43.

■ Fielding, N. G., et J. L. Fielding 1986
Linking Data, Newbury Park, CA: Sage.

■ Fukuyama, F. 1995
Trust: The Social Virtues and the Creation of Prosperity, New York : Free Press.

■ Gressier, F. 2005
Les systèmes d'alerte éthique : une conception bien désagréable de la démocratie d'entreprise, *InFOjuridique,* 50: 47-54.

■ Institut Français des Administrateurs (IFA) 2007
Les administrateurs de sociétés cotées et la responsabilité sociétale des entreprises, Paris : IFA.

■ Johnson G., K. Scholes,, R. Whittington, et F. Frery 2005
Stratégique, 7e édition, Paris : Pearson.

■ Karpik, L. 1998
La confiance : réalité ou illusion ? Examen critique d'une thèse de Williamson, *Revue économique,* 49: 4, 1043-1056.

■ Kœnig, G. 1993
Production de la connaissance et constitution des pratiques organisationnelles, *Revue de gestion des ressources humaines,* 9: 4-17.

■ Kœnig, G. 2005
Etudes de cas et évaluation de programmes : une perspective campbellienne, *Actes de la XIVe conférence de management stratégique,* Angers. www.strategie-aims.com/angers05/res/ 68-874rd.pdf

M@n@gement, Vol. 11, No. 2, 2008, 113-135
Special Issue: Corporate Governance and Ethics

■ La Porta, R., F. Lopez-de-Silanes, A. Schleifer, et R. Vishny 1999
The Quality of Government, *Journal of Law, Economics and Organization,* 15: 1, 222-279.

■ Maxwell, J. A. 2005
Qualitative Research Design: An Interactive Approach, 2e édition, Thousand Oaks, CA : Sage.

■ Medina, Y. 2006
L'alerte éthique, outil pour la GRH et le "risk management", *Lettre du management responsable,* 6, octobre, 2-7. www.esdes-recherche.net/PDF%20Lettres/YMedina.pdf

■ Ménard, C. 1997
L'économie des organisations, Paris : La Découverte.

■ Miles, M. B., et A. M. Huberman 2003
Analyse des données qualitatives, 2e édition, Bruxelles : de Boeck Université.

■ Mintzberg, H. 1986
Le pouvoir dans les organisations, Paris : Editions d'organisation.

■ Moberly, R. E. 2006
Sarbanes-Oxley's Structural Model to Encourage Corporate Whistleblowers, *Brigham Young University Law Review,* 2006 : 5, 1107-1176.

■ Near, J. P., et M. P. Miceli 1985
Organizational Dissidence: The Case of Whistleblowing, *Journal of Business Ethics,* 4: 1, 1-16.

■ Near, J.P., et M. P. Miceli 1996
Whistleblowing: Myth and Reality, *Journal of Management,* 22: 3, 507-527.

■ Near, J. P., M. T. Rehg, J. R. Van Scotter, et M. P. Miceli 2004
Does Type of Wrongdoing Affect the Whistleblowing Process?, *Business Ethics Quaterly,* 14: 2, 219-242.

■ Ordre des Experts Comptables et des Comptables Agréés (OECCA) 1977
Le contrôle interne, Etude présentée à l'occasion du 32e Congrès national, Paris, Conseil Superieur de l'Ordre des Experts Comptables.

■ Parsons, T. 1969
Politics and Social Structure, New York : Free Press.

■ Pesqueux, Y. 2007
Ethique et gouvernance : la dualité hard law/soft law, *Revue française de gouvernance d'entreprise,* 1: 35-48.

■ Rehg, M. T., M. P. Miceli, J. P. Near, et J. R. Van Scotter 2004
Predicting Retaliation against Whistleblowers: Outcomes of Power Relationships within Organizations, *Academy of Management Annual Meeting Proceedings,* SIM: E1-E6.

■ Stansbury, J. M., et B. Barry 2007
Ethics Programs and the Paradox of Control, *Business Ethics Quarterly,* 17 : 2, 239-261.

■ Trade Union Advisory Committee (TUAC) 2004
La révision des principes OCDE de gouvernement d'entreprise : une évaluation du secrétariat du TUAC, Paris : TUAC. www.tuac.org/fr/public/e-docs/00/00/01/0B/document_doc.phtml

■ Weaver, G. R., et L. K. Treviño 1999
Compliance and Values Oriented Ethics Programs: Influences on Employees' Attitudes and Behavior, *Business Ethics Quarterly,* 9: 2, 315-335.

■ Yin, R. K. 1990
Case Study Research: Design and methods, Newbury Park, CA : Sage.

CHAPITRE V

LES DISPOSITIFS D'ALERTE : LE *WHISTLEBLOWING*

LE LANCEUR D'ALERTE : QUEL RÔLE DANS LA LUTTE CONTRE LA CORRUPTION ?

Le « Plan d'action anticorruption » adopté à la fin de l'année 2010 par les chefs d'État et de gouvernement du G20[1] a mis sur le devant de la scène un acteur considéré désormais dans la plupart des enceintes internationales comme exerçant un rôle majeur dans la détection et la lutte contre la corruption : il s'agit du « donneur d'alerte » ou « lanceur d'alerte ».

Entre autres mesures contenues dans ce plan anticorruption, et destinées à exercer une fonction « d'exemplarité incitative »[2] vis-à-vis des autres États dans la lutte contre la corruption, l'une porte sur la protection de ces lanceurs d'alerte, c'est-à-dire des personnes qui, témoins d'actes illicites ou non éthiques, en informent les autorités.

Il semble désormais acquis au plan international que les lanceurs d'alerte, et plus particulièrement leur statut protecteur, doivent constituer une priorité pour tous les États engagés dans la lutte contre la corruption. Comme l'a noté l'OCDE, « le risque de corruption augmente significativement dans les environnements dans lesquels le signalement de méfaits n'est pas encouragé ou protégé »[3].

Le paradoxe veut que cette exigence, perçue comme universelle, reste encore très imparfaitement ou inégalement respectée par les États. La France en particulier, qui a pourtant joué un rôle actif au sein du G20 en assurant en 2011 la coprésidence du groupe anticorruption, ne possède pas actuellement de dispositif général protecteur des lanceurs d'alerte. Bien plus, dans notre pays, la reconnaissance des lanceurs d'alerte suscite traditionnellement de fortes réserves.

La question est de savoir si en France, la dénonciation est condamnée à rester « une pratique qui ne dit pas son nom »[4], ou si, au contraire, sous l'influence, et pourrait-on dire, la poussée du droit international, elle est conduite à prendre progressivement place au sein de notre droit positif.

Nombreux sont les débats, réflexions ou travaux de recherche qui, depuis une dizaine d'années, ont déjà abordé ce sujet. Pourtant, et avant

1. Plan adopté lors du sommet de Séoul des 11 et 12 novembre 2010. Le G20 regroupe 19 États parmi les plus industrialisés plus l'Union européenne.
2. *To lead by example* pour reprendre la terminologie du G20.
3. Note de l'OCDE sur les principes directeurs et bonnes pratiques adoptés lors de la réunion du Groupe anticorruption du G20 à Bali les 12 et 13 mai 2011.
4. Pour reprendre la formule employée par Xavier Lameyre et Maria Cardoso dans un article « La délation en droit pénal français, une pratique qui ne dit pas son nom » (*in Citoyens et délateurs, la délation peut-elle être civique ?,* Autrement 2005, p. 155 et s.).

même que ne soit posée la question du statut du lanceur d'alerte et de son éventuelle protection, tout se passe dans notre pays comme si la notion même de lanceur d'alerte avait du mal à émerger.

Il est frappant de constater qu'en France, cette notion a au départ porté sur des thématiques qui n'étaient pas directement liées aux atteintes à l'intégrité.

À l'origine, le terme de « lanceur d'alerte » désigne un simple citoyen ou un scientifique travaillant dans le domaine public ou privé et qui, confronté à un fait pouvant constituer un danger pour l'homme ou son environnement, décide de porter ce fait à la connaissance de la société civile et des pouvoirs publics. La notion a été employée en France au cours de la seconde moitié des années 1990 par des sociologues ou chercheurs spécialisés dans les risques industriels, environnementaux ou sanitaires. Leurs travaux portaient alors sur les procédés par lesquels les lanceurs d'alerte sont parvenus à faire reconnaître des dangers de nature physique ou chimique auxquels étaient exposés des salariés ou une partie de la population. Il ne s'agit pas tant, à l'origine, de pointer tel ou tel comportement individuel que de dénoncer le recours à un procédé ou l'exposition à une substance considérés comme dangereux [5].

Par la suite, le concept a pris une nouvelle dimension sous l'influence du droit anglo-saxon, à travers la notion de *whistleblowing* dont le champ d'action est plus large. En effet, il appartient au *whistleblower* [6], employé ou ancien employé d'une entreprise ou d'une agence gouvernementale de porter à la connaissance des autorités des faits non seulement susceptibles de constituer une menace contre la santé ou l'intégrité physique des citoyens, mais aussi, de façon générale, l'ensemble des comportements susceptibles de constituer une violation de la loi ou une menace contre l'intérêt général, et en particulier les délits économiques.

La notion de donneur d'alerte n'est pourtant pas inconnue du droit français, mais celui-ci est peu à l'aise lorsqu'il faut l'aborder.

Sur le plan de la sémantique, les textes emploient des qualificatifs variés, soit trop explicites, soit trop vagues. Alors que l'article 40, alinéa

5. Ainsi, un des ouvrages de référence, « Les sombres précurseurs, une sociologie pragmatique de l'alerte et du risque » par deux chercheurs à l'École des hautes études en sciences sociales, Francis Chateauraynaud et Didier Torny (Éditions de l'École des hautes études en sciences sociales, 1999), porte sur les procédés par lesquels des « lanceurs d'alerte » s'efforcent de faire reconnaître un danger, à partir de l'analyse de trois affaires : amiante, radioactivité et maladies à prions.

6. Littéralement « celui qui siffle pour donner l'alerte », terme utilisé par les Anglo-Saxons pour désigner « l'alerteur », c'est-à-dire tout individu mettant en pratique le droit d'alerte, et qui tirerait son origine de l'ancienne pratique des policiers britanniques (*bobbies*) qui, lorsqu'ils étaient témoins d'un délit, faisaient usage de leur sifflet afin d'alerter les passants et les autres policiers susceptibles de se trouver à proximité des lieux.

premier, du Code de procédure pénale utilise le terme de « dénonciation », d'autres textes recourent à des périphrases telles que « donner avis »[7], « révéler »[8], « relater ou témoigner »[9] « signaler »[10], « déclarer »[11], etc.

La plupart des juristes, de leur côté, n'emploient pas le terme de lanceur d'alerte et insistent sur la nécessité d'établir une distinction entre la dénonciation et la délation ; au mot de dénonciation, pourtant employé par les textes, ils préfèrent généralement celui, plus neutre, de signalement[12], soulignant à juste titre que la dénonciation, lorsqu'elle est prévue par des textes, porte généralement sur des faits et non sur des personnes.

Cette réticence à admettre pleinement la notion de lanceur d'alerte et à lui donner une existence juridique est discutable car elle se heurte, en particulier dans notre pays, à un certain nombre d'idées reçues.

La première idée reçue tient à l'histoire : la notion fait référence à une pratique, la dénonciation, qui possède une forte connotation négative, aussi bien dans les pays de l'Europe de l'Ouest, qui furent occupés par les nazis, que dans les pays d'Europe de l'Est, qui ont connu, jusqu'au début des années 1990, des régimes totalitaires. Or, en droit comme en fait, on constate que cette connotation négative n'est pas totalement justifiée : s'agissant des crimes, de mise en danger de la vie d'autrui ou d'atteinte à l'honneur, les dénonciations sont généralement spontanées et ne s'exercent pas dans un contexte de pression politique ou sociale forte.

Selon une deuxième idée reçue, le *whistleblowing* ferait partie de la culture anglo-saxonne et ne serait pas transposable dans les pays ayant une tradition de droit romain. Aux États-Unis notamment, il s'agirait d'un comportement admis, voire encouragé par la société, et les *whistleblowers* constitueraient en quelque sorte des « anges »[13]. Cette idée doit également être réfutée. Aux États-Unis, comme en France, il faut du courage pour dénoncer, car dans les deux pays, les risques en termes d'emploi, de réputation, sont identiques. Ceci explique d'ailleurs que, par pragmatisme, le droit anglo-saxon porte son attention sur les garanties (en termes de protection de l'emploi, de confidentialité, etc.) accordées aux lanceurs d'alerte.

7. Article 40, alinéa 2, du Code de procédure pénale.
8. Article L. 820-7 du Code commerce.
9. Article L. 1161-1 du Code du travail.
10. Article L. 2211-2 du Code général des collectivités territoriales.
11. Article L. 561-1 du Code monétaire et financier.
12. Par exemple Christian Vigouroux dans *Déontologie des fonctions publiques*, Dalloz, février 2011, p. 522 et s.
13. Pour reprendre le titre d'un documentaire diffusé sur la chaîne Arte en novembre 2007, « Du côté des anges ».

Une troisième idée reçue voudrait que le *whistleblowing* soit étranger à la culture juridique française. Or, là encore, cette idée, sous-tendue par l'opposition traditionnelle entre droit anglo-saxon et droit continental, est fausse[14].

Le droit positif français comporte en effet de nombreux dispositifs pour lesquels la dénonciation constitue une source d'information pour les autorités chargées de lutter contre la délinquance.

Le droit pénal donne même une valeur juridique élevée à la dénonciation des crimes et délits. Cette dénonciation peut constituer à la fois un élément susceptible de déclencher l'action publique (article 40, alinéa premier, du Code de procédure pénale), une obligation qui s'impose à l'ensemble des agents publics (article 40, alinéa 2, du Code de procédure pénale), et son abstention peut, en outre, dans certains cas être pénalement sanctionnée (non-dénonciation de crimes, article 434-1 du Code pénal).

Dans le domaine économique et financier, nombreux sont les dispositifs qui font de la dénonciation un élément essentiel de la révélation du non-respect de la législation. Tel est le cas en particulier de l'obligation de déclaration de soupçon qui s'impose aux professions du chiffre, aux banques, etc. ou de la procédure dite « de clémence » prévue par le droit de la concurrence.

Cependant, ces dispositifs n'ont en général ni la même portée, ni la même force que dans d'autres pays, en particulier lorsqu'ils sont mis en œuvre dans les affaires de corruption.

D'abord, ces dispositifs ont pour la plupart, un champ d'application limité. Ils s'appliquent à telle ou telle catégorie d'agents et portent sur des comportements déterminés. Ainsi, il n'existe pas en France d'obligation générale s'imposant à l'ensemble des citoyens, du secteur public comme du secteur privé, de dénoncer les manquements à la loi ou les menaces physiques ou non dont ils auraient connaissance.

Ensuite, les conséquences qui s'attachent au « cri d'alarme » en France ne sont pas aussi fortes que dans les pays ayant instauré un système de *whistleblowing*. Il n'existe pas, en général, de procédure formalisée de dénonciation, et l'absence de dénonciation, lorsqu'elle revêt le caractère d'une obligation, est rarement sanctionnée.

Enfin, comme on le verra, ils comportent de nombreuses lacunes et fonctionnent de manière imparfaite.

14. On rappellera que c'est le droit romain qui a forgé le concept de *delator* qui, à l'origine, exerçait une fonction d'accusateur dans les procès politiques destinés à éliminer les opposants de l'Empereur (cf. à ce propos l'article de Yann Rivière, « Rome impériale : les délateurs, le prince, le tribunal », *in Citoyens et délateurs*, *op. cit.*).

Ces faiblesses et carences s'expliquent difficilement. Tout laisse à penser que le lanceur d'alerte peut jouer un rôle utile, notamment pour mettre à jour des pratiques telles que la corruption.

Certains analystes relèvent que le lancement d'alerte prend toute sa valeur lorsqu'il porte sur des informations qui revêtent une importance cruciale pour l'ensemble d'une collectivité [15]. Le *whistleblowing* acquiert tout son sens lorsqu'il jette la lumière sur des risques sanitaires, industriels ou financiers.

Son utilité est également pleinement avérée lorsqu'il conduit à mettre à jour des pratiques ou des actes illégaux ou non conformes [16], que les mécanismes de contrôle internes ou externes n'ont pas permis de déceler.

Rentrent dans cette catégorie les fraudes comptables, mais également un certain nombre d'atteintes à la probité qui, comme la corruption, présentent des caractéristiques qui en rendent la détection particulièrement malaisée.

La corruption présente comme première caractéristique de relever de la criminalité dite « intelligente ». Elle fait de plus en plus appel à des montages complexes et requiert, pour être démasquée, une certaine technicité, qui implique d'être partie prenante aux montages ou de faire partie du cercle des personnes « averties » [17].

La corruption est également par définition secrète, invisible : indépendamment des difficultés de preuve, elle n'a généralement pas de traduction visible immédiate. La victime n'est souvent pas identifiée ou, comme les collectivités, n'a pas d'existence « physique ».

Enfin, la corruption relève de la criminalité en réseau : la corruption est une « relation plurielle » qui, à une certaine échelle, fait intervenir de nombreux acteurs.

Ces éléments rendent difficiles, à la fois la mise à jour des faits, leur analyse et leur qualification pénale (problème de la prescription). Avant même la recherche de la preuve, la première difficulté est de déceler

15. Cf. par exemple l'article de David Banisar *« Whistleblowing, International standards and Developments »*, mai 2006, p. 6 et s.

16. Le terme de « conformité » est une traduction réductrice de l'anglais *compliance* qui fait référence au respect d'un ensemble de normes, bonnes pratiques…, qui dépasse le seul respect de la loi.

17. Un parallèle peut ici être établi entre la corruption et une autre forme de la délinquance, celle des pratiques anticoncurrentielles (ententes, abus de position dominante…), pour laquelle la loi (loi 2001-420 du 15 mai 2001 relative aux nouvelles régulations économiques) a prévu des procédures dites « de clémence » qui conduisent à exonérer d'amende la ou les entreprises qui dénoncent ces pratiques.

l'existence des pratiques corruptrices, et la première priorité doit donc être de faciliter leur mise à jour [18].

Dans ce contexte, le lanceur d'alerte, qu'il agisse dans un cadre collectif ou individuel, qu'il soit partie prenante du système ou qu'il lui soit externe, peut être un acteur à part entière de la lutte contre la corruption.

En France, l'alerte, le signalement peuvent-ils jouer dans le domaine de la corruption un rôle équivalent à celui qui leur est imparti dans d'autres pays ? Autrement dit, un dispositif de *whistleblowing* calqué sur les mécanismes existants dans de nombreux pays, aurait-il sa pertinence dans notre pays ?

Si jusqu'à présent, le SCPC a donné une réponse réservée à l'introduction d'une dénonciation d'usage général [19], la question mérite de nouveau d'être posée en raison des évolutions récentes qui sont intervenues dans le traitement du phénomène de la corruption, avec notamment le développement de son volet préventif et la prise en compte de sa dimension internationale.

La France ne peut pas ignorer ces évolutions. Elle a ratifié l'ensemble des dispositifs internationaux contre la corruption, et a donc l'obligation d'en assurer la mise en œuvre en adaptant ses textes et en faisant évoluer ses pratiques. Par ailleurs, notre pays a mis en place un dispositif original de lutte contre la corruption qui ne se limite pas au traitement judiciaire des pratiques corruptrices, et comporte des actions préventives destinées à identifier la corruption le plus en amont possible, avant que celle-ci n'ait eu le temps de causer des dommages irréparables.

La question se pose aujourd'hui de savoir si, dans ce contexte, le lanceur d'alerte, sa reconnaissance comme son éventuel statut protecteur, peuvent constituer un outil à la fois adapté et efficace de prévention des pratiques corruptrices.

Le présent article s'efforce d'apporter des éléments de réponse à ces interrogations. Dans un premier temps, seront exposés les dispositifs de lancement d'alerte mis en place au plan international et les progrès accomplis par les États dans ce domaine (I) ; dans un deuxième temps, l'analyse sera centrée sur les dispositifs mis en œuvre en France ainsi que sur leurs évolutions les plus récentes dans le secteur public et dans le secteur privé (II).

18. Il n'est pas anodin de constater que la détection/mise à jour de la corruption constitue un chapitre à part entière des « revues de pairs » effectuées par les organisations internationales (GRECO, OCDE…) et destinées à vérifier la mise en œuvre effective des conventions anticorruption par les États parties.

19. Cf. par exemple, Rapport du SCPC 2003, p. 121 et s.

LE LANCEUR D'ALERTE : UNE PRATIQUE QUI TEND À DEVENIR UNIVERSELLE

Au plan international, le mécanisme du déclenchement d'alerte constitue désormais un outil dont l'efficacité est reconnue dans la lutte contre la corruption. Il rentre dans les préconisations des organisations internationales (A), et il est incorporé dans un nombre croissant de dispositifs nationaux (B).

Un dispositif préconisé par les organisations internationales

La plupart des conventions internationales relatives à la corruption prévoient la mise en place d'une protection des donneurs d'alerte. Certaines organisations non gouvernementales (ONG), telle que, par exemple Transparency International, préconisent également des dispositifs protecteurs.

La plupart des instruments internationaux relatifs à la lutte contre la corruption prévoient des dispositions reconnaissant l'importance des donneurs d'alerte et incitant les États parties à adopter des mesures destinées à favoriser leur mise en place et à assurer leur protection.

Les dispositions adoptées dans le cadre de l'Organisation des Nations Unies

a) La convention des Nations unies contre la corruption[20] comporte un ensemble de dispositions très complètes relatives au signalement des faits de corruption

– son article 8-4, relatif aux « Codes de conduite des agents publics », prévoit que « Chaque État partie envisage aussi… de mettre en place des mesures et des systèmes de nature à faciliter le signalement par les agents publics aux autorités compétentes des actes de corruption dont ils ont connaissance dans l'exercice de leurs fonctions » ;
– son article 13, qui traite de la « Participation de la société », prévoit dans son point 2, que « chaque État partie prend des mesures appropriées pour veiller à ce que les organes de prévention de la corruption compétents… soient connus du public et fait en sorte qu'ils soient accessibles, lorsqu'il y a lieu, pour que tous faits susceptibles d'être considérés comme constituant une infraction établie conformément à la présente convention puissent leur être signalés, y compris sous couvert d'anonymat » ;

20. Convention des Nations unies du 31 octobre 2003, dite de Mérida, signée par 154 États.

– son article 33, relatif à « la protection des personnes qui communiquent des informations », dispose que « chaque État partie envisage d'incorporer dans son système juridique interne des mesures appropriées pour assurer la protection contre tout traitement injustifié de toute personne qui signale aux autorités compétentes, de bonne foi et sur la base de soupçons raisonnables, tous faits concernant les infractions établies conformément à la présente convention ».

b) La « boîte à outils anticorruption » de l'Office des Nations Unies contre la drogue et le crime (version de septembre 2004) aborde de manière détaillée le déclenchement d'alerte et recommande des mesures légales et administratives relatives au signalement et à la protection du déclencheur d'alerte, qui comprend un système de récompense, la création d'institutions de médiation pour recevoir les plaintes, la création de hotlines, et des limites aux accords relatifs à la diffamation et à la confidentialité.

Par ailleurs, le rapporteur spécial de l'ONU sur la liberté d'opinion et d'expression s'est joint aux représentants spéciaux de la liberté d'expression et des médias de l'Organisation des États américains et de l'Organisation pour la sécurité et la coopération en Europe (OSCE) pour une déclaration sur la liberté d'expression appelant les gouvernements à adopter de meilleures protections.

Le rôle du Conseil de l'Europe

a) Les deux conventions contre la corruption adoptées par le Conseil de l'Europe en 1999 comportent des dispositions spécifiques sur les donneurs d'alerte

– La convention civile sur la corruption du 4 novembre 1999, ratifiée par 34 États, prévoit dans son article 9 que : « Chaque partie prévoit dans son droit interne une protection adéquate contre toute sanction injustifiée à l'égard des employés qui, de bonne foi et sur la base de soupçons raisonnables, dénoncent des faits de corruption aux personnes ou autorités responsables. »

– La convention pénale sur la corruption du 27 janvier 1999, qui a été ratifiée par 43 États, comporte pour sa part une disposition relative à la protection des collaborateurs de justice et des témoins (article 22).

b) Il y a lieu également de souligner le rôle joué par la Cour européenne des droits de l'homme, qui, dans le cadre de contentieux portant sur le respect de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales du 4 novembre 1950 (CESDH), a progressivement élaboré une jurisprudence favorable au lancement d'alerte et à la protection du donneur d'alerte.

La Cour européenne des droits de l'homme tend en effet à considérer que les sanctions (notamment licenciement) prises à l'encontre de magistrats ou de salariés d'organismes publics ou privés qui ont divulgué des informations « que les citoyens ont un grand intérêt à voir publier ou divulguer »[21] ou « dans un intérêt public »[22] constituent une violation à leur droit d'expression tel qu'il est garanti par l'article 10 de la convention de sauvegarde des droits de l'homme.

Dans l'une des affaires récemment jugées, elle estime « que la dénonciation par de tels agents de conduites ou d'actes illicites constatés sur leur lieu de travail doit être protégée dans certaines circonstances »[23]. Dans l'affaire Heinisch c/Germany[24], la Cour a considéré que « l'intérêt public à être informé des défaillances [dans la délivrance de soins par une société d'État] était d'une telle importance dans une société démocratique qu'il devait prévaloir sur la réputation et les intérêts commerciaux de cette dernière ».

Certains instruments régionaux tels que la **convention interaméricaine contre la corruption**[25], la **convention anticorruption de l'Union africaine**[26] ou **l'initiative anticorruption pour l'Asie-Pacifique**[27] comportent également des dispositions invitant les États parties à adopter des dispositions sur le déclenchement d'alerte et sur la protection des lanceurs d'alerte[28].

21. Affaire Guja c/Moldova, req. nº 14277/04, 12 février 2008.
22. Affaire Heinisch c/Germany, req. nº 28274/08, 21 juillet 2011.
23. Affaire Guja précitée.
24. Affaire Heinisch c/Germany précitée.
25. Convention entrée en vigueur en 1997 et ratifiée par l'ensemble des États parties à l'Organisation des États américains.
26. Convention, adoptée en juin 2003, et signée par 43 des 53 États membres de l'Union africaine. Elle est entrée en application en août 2006.
27. Initiative conduite par la Banque asiatique de développement et l'OCDE et approuvée par 25 États, mais sans caractère contraignant.
28. Respectivement à l'article III pour la première, article 5 pour la seconde et pilier 3 du Plan d'action pour l'Asie et le Pacifique.

Les travaux de l'Organisation de coopération et de développement économique (OCDE)

a) L'OCDE, dont le champ de compétence porte sur le commerce, le développement, l'innovation, la bonne gouvernance…, s'est fortement engagée dans la promotion du déclenchement d'alerte dans le secteur public comme dans le secteur privé.

– Dans le secteur public, l'OCDE procède régulièrement, depuis 2000, à une enquête auprès des administrations des États membres qui porte notamment sur les procédures d'alerte et la protection des dénonciateurs, et dont les résultats sont publiés dans « Panorama des administrations publiques ». Cette enquête fait apparaître que de plus en plus d'États membres mettent en place des mécanismes permettant aux fonctionnaires de signaler plus facilement des fautes. Ainsi, en 2009, 29 pays obligent leurs fonctionnaires à dénoncer les fautes observées et/ou ont mis en place des procédures facilitant ces alertes, contre 21 pays en 2000. Par ailleurs, près de 90 % des pays membres ont mis en place une protection pour les dénonciateurs, la plupart du temps de nature légale.

En 2003, les États membres ont adopté des « lignes directrices sur la gestion des conflits d'intérêts dans le secteur public » qui préconisent notamment « 2-3-2 b) le traitement des signalements : mettre en place des mécanismes de signalement destinés à recueillir les signalements de non-conformité, et concevoir des mesures efficaces pour encourager leur utilisation. Élaborer des réglementations et des procédures claires pour le déclenchement d'alerte, et veiller à ce que ceux qui rapportent des cas de non-respect des textes soient protégés contre d'éventuelles représailles, et que les mécanismes de signalement ne fassent pas eux-mêmes l'objet d'abus ».

– Au sein du secteur privé, les principes directeurs de l'OCDE destinés aux multinationales (juin 2000) prévoient que celles-ci devraient « II (9) se dispenser d'adopter des mesures discriminatoires ou disciplinaires à l'encontre des salariés qui rapportent de bonne foi à l'encadrement ou, si cela est approprié, aux autorités publiques compétentes, les pratiques contraires à la loi, aux lignes directrices ou au règlement intérieur de l'entreprise ».

b) L'OCDE est par ailleurs à l'initiative de la convention sur la lutte contre la corruption des agents publics étrangers dans les transactions commerciales internationales [29].

Cette convention ne comporte pas de dispositions sur le déclenchement d'alerte.

Cependant, le groupe de travail chargé du suivi de cette convention a assez rapidement intégré ce thème dans le mécanisme de suivi de la convention. C'est ainsi que dans ses rapports de suivi de phase II, le groupe de travail a recommandé à de nombreux pays d'adopter un mécanisme de protection légale du déclencheur d'alerte.

Par la suite, la convention de 1997 a été complétée en 2009 par une recommandation [30] qui a, notamment recommandé aux États parties de mettre en place des dispositifs de signalement assortis de mesures de protection pour les employés du secteur public et du secteur privé (section IX), et invité les États membres à encourager « … v) les entreprises à fournir des moyens de communication et de protection pour les personnes qui ne veulent pas commettre une infraction à la déontologie ou aux normes professionnelles sur les instructions ou sous la pression de leurs supérieurs hiérarchiques, ainsi que pour les personnes voulant signaler de bonne foi et sur la base de soupçons raisonnables des manquements à la loi, à la déontologie ou aux normes professionnelles se produisant au sein de l'entreprise, et devraient encourager les entreprises à prendre des mesures appropriées sur la base de tels signalements ».

Le thème du déclenchement d'alerte fait donc désormais pleinement partie des « standards » minimaux applicables aux États signataires de la convention de 1997.

L'initiative du G20

Dans le cadre du G20, un groupe de travail sur la corruption coprésidé en 2011 par la France et l'Indonésie a été créé en juin 2010.

À l'occasion du sommet de Séoul des 11 et 12 novembre 2010, le G20 a approuvé un plan d'action ambitieux de lutte contre la corruption, dont l'un des axes (le point 7) porte sur la protection des déclencheurs d'alerte. Dans ce cadre, à partir d'une analyse des bonnes pratiques, six principes directeurs pour l'élaboration de dispositifs protecteurs des déclencheurs d'alerte ont été proposés :

29. Convention signée le 17 décembre 1997, ratifiée par 38 pays.

30. Recommandation de l'OCDE visant à renforcer la lutte contre la corruption d'agents publics étrangers dans les transactions commerciales internationales, publiée le 9 décembre 2009.

1. Une législation claire et un cadre de travail efficace sont institués pour protéger contre les mesures discriminatoires et disciplinaires les employés qui signalent de bonne foi et sur la base de soupçons raisonnables les pratiques illégales ou de corruption aux autorités compétentes ;
2. La loi prévoit une définition des pratiques dont la révélation est protégée et des personnes bénéficiant d'une protection légale ;
3. La loi garantit que la protection dont bénéficient les déclencheurs d'alerte est robuste et compréhensible ;
4. La loi définit clairement les procédures et les circuits à suivre pour le signalement de soupçons de corruption, et encourage l'utilisation de circuits protecteurs et aisément accessibles ;
5. La loi prévoit que des mécanismes de protection efficaces ont été instaurés, en confiant à un organe spécifique disposant de la compétence et du pouvoir de recevoir et de traiter les plaintes liées à des actions de représailles et/ou des enquêtes sans justification, et en proposant une batterie de solutions ;
6. L'implantation d'une protection du déclencheur d'alerte est assortie d'actions de sensibilisation, de communication, de formation et d'une évaluation périodique de l'efficacité du dispositif de protection.

Quelle appréciation peut-on porter sur ces différents instruments internationaux ?

On observera que pour les institutions internationales à l'origine des conventions anticorruption, le déclenchement d'alerte est un instrument essentiel de lutte contre les pratiques corruptrices. Elles considèrent que celui-ci contribue à limiter les risques de corruption aussi bien au plan domestique que dans les transactions internationales.

Elles estiment également que ses enjeux dépassent celui de la lutte contre la corruption.

Ainsi, pour l'OCDE, il est le signe d'une « culture ouverte » et représente « une protection pour sauvegarder l'intérêt public et la confiance accordée aux organisations publiques »[31].

Par ailleurs, le champ d'application préconisé pour le déclenchement d'alerte est généralement très large[32]. Ainsi, par exemple, les conventions internationales recommandent que le déclenchement d'alerte s'applique indifféremment aux salariés du secteur public comme du secteur privé.

Les limites de ces instruments internationaux tiennent pour l'essentiel à leur caractère non contraignant.

31. « Panorama des administrations publiques 2009 », p. 114.
32. *Broad* est la formule le plus souvent utilisée.

Les dispositions incluses dans les conventions internationales se bornent, pour la plupart, à formuler des préconisations générales. Elles ne définissent pas directement le déclenchement d'alerte pas plus qu'elles ne précisent la nature ou les modalités qu'il doit revêtir [33].

La création des dispositifs de déclenchement d'alerte, leur gestion et le traitement des difficultés d'interprétation ou de mise en œuvre qu'ils peuvent soulever s'effectuent donc, pour l'essentiel, dans un cadre national [34].

D'autres organisations internationales ont engagé des réflexions spécifiques sur le déclenchement d'alerte dans le domaine de la corruption

En 1999, s'est tenue sous l'égide de l'OCDE une réunion d'experts des milieux syndicaux (TUAC [35]) et patronaux (BIAC [36])

Les deux organisations se sont accordées sur l'importance du déclenchement d'alerte pour dissuader et détecter la corruption et sur la nécessité d'assurer une protection des déclencheurs d'alerte, en particulier dans les pays dans lesquels il n'existe pas de culture de travail encourageant ce type de pratique, et de privilégier les mécanismes internes de détection.

Parmi les organisations internationales non gouvernementales, Transparency International (TI) est particulièrement active dans le domaine de la promotion de mécanismes visant à encourager et protéger le déclencheur d'alerte

Depuis sa création (en 1993), elle est régulièrement intervenue sur le sujet, pour, à la fois, encourager sa mise en place, mais également préconiser son encadrement, notamment la protection des déclencheurs d'alerte.

a) TI a notamment proposé en 2004 une définition très complète du déclencheur d'alerte :

« Le déclencheur d'alerte est l'individu qui a connaissance d'informations constituant des indices sérieux qu'un acte contraire aux lois et règlements ou qu'un acte contraire aux règles professionnelles propres

33. Cf. *infra,* p. 158.
34. Pour l'essentiel, car comme on l'a vu la CEDH joue un rôle essentiel dans la construction d'un cadre « supranational » sur le déclenchement d'alerte.
35. Trade Union Advisory Commitee.
36. Business and Industry Advisory Commitee.

à un secteur d'activité, a été commis ou est sur le point d'être commis, et qui veut alerter les personnes compétentes au sein de l'entreprise ou de l'organisme dont il dépend ou, lorsque cette alerte n'est pas envisageable ou qu'elle est de nature à l'exposer à un risque sérieux de représailles, les autorités administratives ou judiciaires. »

b) Pour TI, le but final du déclenchement d'alerte est de protéger l'intérêt public.

Il y parvient en informant des populations ou des organisations qu'elles ont la possibilité de prévenir un dommage, d'enquêter ou de prendre une mesure à l'encontre de ceux qui commettent des méfaits. Un des deux exemples les plus fréquemment cités pour illustrer cette démarche est celui des déclencheurs d'alerte qui ont mis à jour la dissimulation d'épidémies ou aidé à éviter la survenue de risques environnementaux ou sanitaires aux États-Unis.

Au sein du secteur privé, des études montrent que les fraudes au sein des entreprises sont plus souvent démasquées grâce aux déclencheurs d'alerte que par tout autre acteur, qu'il s'agisse des autorités de régulation, des auditeurs et des médias.

Un autre argument invoqué est que la protection du droit à dénoncer des méfaits s'apparente à la protection de la liberté d'expression et de conscience. Cette protection est également fondée sur les principes de transparence et de conformité, en particulier pour les entreprises cotées en bourse. L'affaire ENRON[37] en particulier s'est traduite pour les entreprises par de nouvelles exigences en matière de transparence financière, sociale et environnementale.

S'agissant plus spécifiquement de la corruption, les déclencheurs d'alerte jouent un rôle clé dans la mesure où la détection de la corruption est la condition préalable pour pouvoir enquêter et poursuivre.

c) TI donne également des recommandations sur le cadre législatif qui lui paraissent le mieux approprié.

En 2009, les instances de TI ont adopté une résolution sur la protection des lanceurs d'alerte qui invite « les institutions publiques et les sociétés à établir des programmes pour protéger les déclencheurs d'alerte contre les représailles, et qui comporte des canaux appropriés pour le signalement, une évaluation indépendante et des mécanismes de suivi efficaces ».

En 2010, dans le cadre d'un projet européen sur le renforcement de la protection des déclencheurs d'alerte dans l'Union européenne, TI

37. Société américaine qui au début des années 2000 avait camouflé ses énormes déficits au moyen notamment de sociétés écrans.

a proposé des principes directeurs susceptibles de guider l'élaboration d'une réglementation sur le déclenchement d'alerte.

• Un cadre législatif unique et compréhensible est plus efficace

Cette législation devrait s'appliquer au secteur public et privé, ainsi qu'aux secteurs non concurrentiels et prévoir des chaînes de signalement dignes de confiance susceptibles de recueillir les plaintes.

• La protection des déclencheurs d'alerte devrait être assurée

Les employés du secteur public comme du secteur privé ainsi que ceux qui ne font pas partie de la relation de travail traditionnelle (consultants, emplois temporaires, formateurs…) devraient être protégés des représailles lorsqu'ils signalent des problèmes de bonne foi. Ils devraient recevoir une reconnaissance professionnelle pour avoir empêché un préjudice excessif pour l'organisation ou la société. Un système de récompense, prenant en compte le contexte particulier national et légal, pourrait être instauré.

• Les signalements internes et externes devraient être protégés

Dans la mesure du possible, les signalements ou problèmes devraient d'abord être soulevés en interne et signalés au corps approprié instauré par l'organisation avec l'assurance que le déclencheur d'alerte dispose de garanties de confidentialité. Les déclencheurs d'alerte devraient également avoir la possibilité de rapporter à l'extérieur à une autorité de régulation, aux autorités de mise en œuvre ou à d'autres corps externes compétents. En dernier ressort, la révélation aux médias devrait également être protégée.

• Le respect de la réglementation est essentiel

La législation doit être effectivement appliquée et devrait être aussi robuste et consistante que possible. Pour assurer une application correcte des dispositions légales, un organe indépendant doté de suffisamment d'autonomie devrait être érigé ou désigné pour superviser l'application de la loi et recevoir les plaintes.

S'agissant plus spécifiquement de la France, TI préconise la mise en place d'un cadre juridique protecteur au profit des lanceurs d'alerte.

Une pratique largement répandue dans le monde

De nombreux États ont prévu un encadrement des dispositifs de déclenchements d'alerte, mais ceux-ci sont à différents degrés de

développement [38]. Si les motivations à l'origine de ces réglementations peuvent être très variées (1-1), une typologie des différents dispositifs existants peut être établie (1-2) ainsi qu'une évaluation de leur efficacité, notamment au regard de l'objectif de détection et de lutte contre la corruption (1-3).

Les raisons à l'origine d'un encadrement des dispositifs de déclenchement d'alerte se trouvent à l'échelle nationale ou internationale

Certains pays ont une longue tradition du déclenchement d'alerte

Ainsi les États-Unis ont, dès 1863, adopté l'*US False Claims Act* qui introduit une action de *Qui tam* [39] par laquelle un particulier peut engager une action au nom de l'État dans les cas de fraude et reçoit une récompense pour le faire. Ce type de procédé a été prévu par un grand nombre de lois aux XVIII[e] et XIX[e] siècles.

C'est l'activiste consumériste Ralph Nader qui, dans les années 1960, est à l'origine des développements modernes de la notion de déclenchement d'alerte. En 1971, il a, au cours d'une réunion à Washington, appelé les salariés des sociétés et des institutions gouvernementales à « donner un coup de sifflet » pour mettre un terme aux « bureaucraties envahissantes ou injustes ».

De nombreuses législations ont également été adoptées en réponse à des événements tragiques. Ainsi, toujours aux États-Unis, le *Whistleblower Protection Act*, adopté en 1989, est directement la conséquence de l'accident de la navette Challenger en 1986. En Grande-Bretagne, des accidents mettant en cause des ferries, des trains, des plateformes pétrolières ont conduit à l'adoption du *Public Interest Disclosure Act*.

Plus récemment, des législations ont également été adoptées à la suite de scandales financiers.

Ainsi, le *Public Interest Disclosure Act* (PIDA, 1998) au Royaume-Uni est directement lié à la faillite de la Banque du crédit commercial international (BCCI) au milieu des années 1990. C'est le cas également

38. Voir à ce propos la note de l'OCDE précitée.

39. Abréviation de l'expression latine *Qui tam pro domino rege quam pro se ipso in hoc parte sequitur* qui signifie « Celui qui poursuit en justice pour le roi aussi bien que pour lui-même ».

de la loi Sarbanes-Oxley[40] qui a été adoptée à la suite des scandales d'ENRON et de Worldcom[41].

Ces lois répondent également à une exigence nouvelle dans nos sociétés : la transparence aussi bien pour le fonctionnement des institutions publiques que pour les sociétés privées. En France par exemple, l'exigence de transparence est à l'origine de la loi du 15 mai 2001 sur les pratiques sociales et environnementales des entreprises cotées, et de la loi de sécurité financière de 2003[42]. Au Royaume-Uni, le dispositif du PIDA englobe à la fois les fonctionnaires et agents publics, les salariés du secteur privé, les stagiaires et les sous-traitants.

La pression exercée au plan international pour adopter des lois explique également la mise en œuvre de dispositifs nationaux. Le groupe de travail de l'OCDE sur la corruption, le GRECO, et le groupe d'experts de l'Organisation des Nations unies ont chacun placé la protection du déclencheur d'alerte au centre de la lutte contre la corruption. Ces organisations recommandent régulièrement aux États signataires de renforcer la protection des déclencheurs d'alerte.

L'adoption de certains dispositifs nationaux tels que, par exemple, la loi Sarbanes-Oxley a également conduit les sociétés multinationales appartenant à des sociétés américaines ou cotées aux USA à adopter des procédures de déclenchement d'alerte.

Un autre facteur réside dans la pression de la société civile. Des groupes anticorruption tels que Transparency International (TI), ou spécialisés comme le GAP (USA), le Public Concern at Work (Grande-Bretagne) et l'Open Democracy Advice Centre (Afrique du Sud) ont incité ou conseillé les gouvernements à l'occasion d'adoptions de lois.

Par exemple, TI se bat pour l'inclusion du déclenchement d'alerte dans la convention ONU et a produit une série de rapports incitant les gouvernements à adopter des dispositifs.

40. La loi Sarbanes-Oxley, dite SOX, adoptée en 2002, sur la réforme de la comptabilité des sociétés cotées et la protection des investisseurs est une loi fédérale imposant de nouvelles règles sur la comptabilité et la transparence financière.

41. Entreprise de télécommunications américaines qui a, comme ENRON, connu au début des années 2000 une faillite retentissante à la suite de manipulations comptables.

42. La loi 2003-706 du 1er août 2006 de sécurité financière a été adoptée afin de renforcer les dispositions légales en matière de gouvernance d'entreprise. Il s'agit du pendant français de la loi américaine SOX.

Une typologie des réglementations nationales sur le déclenchement d'alerte peut être établie à partir de trois critères : leur champ d'application (1-2-1), les procédures/modalités de divulgation (1-2-2) et les dispositifs de protection des déclencheurs d'alerte (1-2-3)

Le champ d'application des dispositifs de déclenchement d'alerte

En 2009, environ 50 États avaient adopté un dispositif sur le déclenchement d'alerte sous une forme ou sous une autre[43].

Une distinction peut être opérée entre deux groupes d'États : ceux qui disposent d'un dispositif spécifique sur le lancement d'alerte et ceux dans lesquels le lancement d'alerte est traité dans le cadre de lois sectorielles.

a) Parmi la première catégorie, les États qui disposent de la réglementation la plus complète sont la Grande-Bretagne[44], le Japon [45], la Nouvelle-Zélande [46], le Ghana [47] et l'Afrique du Sud [48]

Les principales caractéristiques de ces lois :

- en premier lieu, il s'agit de lois spécifiquement dédiées au lancement d'alerte, ce qui présente l'avantage de les rendre plus visibles et plus faciles à diffuser ;
- en général, leur champ d'application est plus large : dans l'idéal, une réglementation complète devrait s'appliquer à la fois au secteur public et au secteur privé. Dans les faits, seuls le Royaume-Uni, la Nouvelle-Zélande, le Ghana et l'Afrique du Sud ont adopté des lois qui couvrent les deux secteurs. Les réglementations américaine et canadienne ne s'appliquent qu'au secteur public. La réglementation japonaise s'applique seulement au secteur privé ;
- la définition des comportements couverts par le signalement est également plus étendue : la plupart de ces réglementations prévoient des définitions selon lesquelles les comportements devant être signalés ne se limitent pas à un seul domaine comme la corruption, mais s'appliquent à une large palette de comportements qui incluent la violation de la loi, les bonnes pratiques et l'éthique ;
- un autre élément important est la création de procédures qui prévoient une alerte interne. Des lois complètes sont généralement fondées sur

43. Étant précisé que, parmi les États de nature fédérale, certains États fédérés (USA) ou provinces (Canada) ont adopté des réglementations spécifiques sur le déclenchement d'alerte.
44. *United Kingdom's Public Interest Disclosure Act* (UK PIDA), adopté en 1998.
45. *Japan's Whistleblower Protection Act* (WPA).
46. *Protected Disclosures Act*, adopté en 2000.
47. *Whistleblower Act*, adopté en 2006.
48. *South Africa's Protected Disclosures Act* (PDA).

l'hypothèse que le changement de culture destiné à développer les communications internes pour prévenir les problèmes est essentiel.
– s'agissant de la protection contre les représailles, toutes ces réglementations prévoient des définitions très larges ainsi que des solutions. Dans certains pays, la protection du lanceur d'alerte peut aussi être assurée par le droit pénal[49] ;
– en ce qui concerne les recours, ces lois instaurent des voies de recours devant des organes externes, le plus souvent tribunaux ou cours ;
– enfin, la plupart des lois ont chargé un organe public d'exercer un rôle de supervision, avec un rôle de conseil aux déclencheurs d'alerte et de recevoir les signalements. Les États-Unis et le Canada ont créé de nouvelles autorités indépendantes. Les autres pays ont recours à des organes existants comme par exemple les médiateurs.

b) Les lois sectorielles

De nombreux pays ont adopté des dispositifs de protection des déclencheurs d'alerte de façon progressive. Ces dispositifs s'appliquent à certaines catégories de personnes ou à certains types d'informations. Dans certains pays, il y a à la fois des lois détaillées et des lois sectorielles pour ces domaines tels que, par exemple, la gouvernance d'entreprise.

• Les lois anticorruption

De nombreuses lois anticorruption comportent quelques dispositions sur le recueil des informations et la protection des personnes qui transmettent des informations sur des pratiques corruptrices. Les protections peuvent s'appliquer à la fois aux agents gouvernementaux et au public mais se limitent souvent à garantir l'anonymat du déclencheur d'alerte ou de l'informateur. Dans certains cas, une structure peut enquêter sur les représailles ou les menaces.

• Les textes s'appliquant aux agents publics

De plus en plus, les textes qui s'appliquent aux agents publics prévoient des dispositions qui les protègent contre des sanctions lorsqu'ils ont signalé des irrégularités.

Il s'agit soit de textes exhaustifs et spécifiques (Australie, Canada, Japon, Afrique du Sud, Grande-Bretagne, États-Unis) et/ou de dispositions spécifiques figurant dans différents textes.

49. Cas au Canada et aux USA dont les dispositions ont été modifiées par la loi Sarbanes-Oxley Act (SOX Act) qui impose une peine d'amende et/ou d'emprisonnement en cas de représailles à l'encontre d'un lanceur d'alerte qui fournit des éléments d'informations véridiques sur la commission ou possible commission d'infractions aux autorités chargées d'assurer leur respect.

La Grande-Bretagne et l'Afrique du Sud sont considérées comme ayant les systèmes légaux les plus développés. Les textes en Grande-Bretagne, Afrique du Sud et Canada prévoient que les institutions doivent adopter des procédures pour le traitement administratif des signalements internes, c'est-à-dire aux supérieurs hiérarchiques, à des conseillers et aux services de l'inspection générale.

Par ailleurs, ces procédures doivent être respectées avant qu'un lanceur d'alerte décide d'aller auprès d'un organe indépendant externe (cas au Canada, en Afrique du Sud). De même, s'agissant des signalements aux médias, les lois en Afrique du Sud et en Grande-Bretagne prévoient qu'ils doivent intervenir en dernier ressort, après la mise en œuvre des procédures internes (cas également au Canada, en Australie).

Aux USA, la loi de protection du lanceur d'alerte a été édictée en 1989[50], et, par la suite, a été complétée par les dispositions sur le *whistleblowing* dans les lois SOX et Dodd-Frank Act [51]. Ces deux lois, qui s'appliquent principalement au secteur privé, fournissent également le cadre qui protège les employés lanceurs d'alerte du gouvernement fédéral contre d'éventuelles représailles.

La loi de protection du signalement des agents publics canadien, la législation sur le lanceur d'alerte d'Australie, la loi néerlandaise sur les agents publics, la loi de protection du *whistleblower* du Japon s'inscrivent dans la même logique.

À ces textes peut s'ajouter la protection assurée par des codes éthiques internes au secteur public[52].

• Les textes sur le droit du travail : la protection du donneur d'alerte peut également être incorporée dans des textes généraux du droit du travail. Tel est le cas de l'Acte sur les travailleurs de l'environnement norvégien, ou de l'article L. 1161-1 du Code du travail français (voir infra)

• Les dispositifs pénaux

Quelques pays ont érigé en infraction pénale les représailles contre les déclencheurs d'alerte (voir *infra)*.

50. *Whistleblower Protection Act*.

51. Le *Dodd-Frank Wall Street Reform and Consumer Protection Act* a été adopté par l'administration Obama en 2010, à la suite de la crise des *subprimes* et de la crise financière et économique qui s'en est suivie, notamment afin de « promouvoir la stabilité financière des États-Unis en améliorant l'*accountability* (la responsabilisation) et la transparence dans le système financier ».

52. Cas par exemple du Code de conduite du service public d'Australie.

• Les textes sur la liberté d'expression

En Suède, l'Acte sur la liberté de la presse confère aux agents publics un droit fondamental à critiquer anonymement les actions des organes du gouvernement. De nombreux pays, comme la Moldavie en 2002, Antigua et la Barbade en 2004, l'Ouganda en 2005, la Macédoine et le Monténégro en 2006, ont adopté des dispositions sur le déclenchement d'alerte concernant les institutions publiques. Dans ces lois, la protection est toutefois limitée aux agents publics.

Autres lois

D'autres régimes, comme certaines lois relatives à l'environnement, prévoient des protections portant sur les risques environnementaux. Les lois relatives à la conformité et au secret bancaire imposent les signalements de méfaits au sein des entreprises (cas en France pour les professionnels du chiffre), en même temps qu'elles protègent contre les représailles. Il en est de même des lois en matière de droit de la concurrence.

Parmi ces lois sectorielles, certaines s'appliquent à la fois aux employés du secteur public et du secteur privé [53].

L'approche sectorielle présente des avantages : l'instauration d'une loi spécifique très complète présente l'intérêt d'accroître sa visibilité, et de rendre plus facile sa promotion par les gouvernements et les employés. Cette approche permet également de prévoir les mêmes règles et procédures aux employés du secteur public et du secteur privé, et d'assurer une stabilité et une clarté de la législation.

Mais elle comporte également de nombreux inconvénients : en premier lieu, ces lois sont parcellaires : elles ne s'appliquent qu'à un nombre limité de personnes, ne visent qu'une catégorie spécifique de comportements [54] et ne couvrent pas un grand nombre de dérives. Ensuite, elles ne sont pas bien connues en dehors de leur secteur d'activité par les salariés et les agents publics, car leur champ d'application est limité. Elles sont également principalement centrées sur les aspects qui concernent le signalement et les sanctions et par le renforcement des dispositifs internes. De plus, aucune d'entre elles ne prévoit de procédures pour des alertes internes ou standards.

On notera ici que les distinctions traditionnelles entre les lois des pays de *common law* et les pays de droit romain tendent à s'atténuer. En effet, si la plupart des lois sur le déclenchement d'alerte ont, à l'origine, été

53. Cas au Japon et en Afrique du Sud, *Dodd-Franck Act* aux USA.

54. Par exemple, le *Dodd-Franck Act* protège les lanceurs d'alerte qui fournissent des informations à la SEC sur de possibles violations à la loi sur la sécurité financière.

élaborée dans les pays ayant une tradition de *common law*, les différences entre les deux systèmes se sont fortement atténuées ces dernières années en raison du développement du droit international et du rôle joué par la Cour européenne des droits de l'homme. La plupart des pays qui ont des lois spécifiques ont une tradition de *common law,* mais l'existence de ces dispositifs s'explique davantage par l'expérience plus longue de ces pays en matière de déclenchement d'alerte. Beaucoup d'entre eux avaient d'ailleurs adopté des lois sectorielles avant d'élaborer une législation plus complète.

Les procédures et modalités du déclenchement d'alerte

a) La définition des comportements devant faire l'objet d'un signalement

Les lois spécifiques sur le déclenchement d'alerte ont généralement des définitions larges de ces comportements.

Les lois sur le déclenchement d'alerte inspirées du droit romain s'appliquent à des infractions très variées qui peuvent être la corruption, le harcèlement, le détournement de pouvoir, les évaluations du personnel, les violations des procédures administratives et internes, la gestion fausse ou frauduleuse de patrimoines publics et privés ainsi que la violation d'autres lois.

L'Acte sur la liberté d'information d'Antigua et de la Barbade [55] a l'une des listes les plus exhaustives de ces comportements.

De nombreux dispositifs nationaux comportent des dispositions spécifiques qui ont un lien avec des scandales nationaux ou les conditions historiques qui ont conduit à l'adoption de la loi. Ainsi, le PDA d'Afrique du Sud s'applique aux discriminations injustifiées. La loi japonaise sur la protection du déclencheur d'alerte mentionne explicitement les lois dans le domaine alimentaire et de la santé, le dispositif sur la pureté de l'air et sur les déchets, et les textes sur les informations personnelles.

La mauvaise gestion administrative est souvent incluse dans les dispositifs juridiques des pays qui ont des problèmes sérieux sur la capacité des agents publics à travailler efficacement [56].

Dans les lois sectorielles, en revanche, l'objet des signalements est limité au champ d'application de la loi.

De nombreux pays ont instauré des standards sur le degré d'importance du comportement devant être révélé avant que les protections

55. *Act on the Freedom of Information Antigua and Barbados*, adopté en 2004.

56. Projet de *Public Interest Disclosure Act* en cours d'examen par le Parlement indien.

ne s'appliquent. Elles exigent que l'action signalée soit importante, et n'ait pas précédemment fait l'objet d'une révélation (États-Unis par exemple).

b) Les procédures de signalement

• Le signalement

Il n'existe pas de définition légale commune sur ce qui constitue le signalement proprement dit.

– L'Organisation internationale du travail le définit comme le « signalement par des salariés ou anciens salariés de pratiques illégales, irrégulières, dangereuses ou contraires à l'éthique des employeurs ».

– La recommandation de l'OCDE du 26 novembre 2009 du Conseil visant à renforcer la lutte contre la corruption d'agents publics étrangers dans les transactions commerciales internationales prévoit la protection « contre toute action discriminatoire ou disciplinaire des employés du secteur public et privé qui signalent de bonne foi et sur la base de motifs raisonnables des soupçons d'actes de corruption d'agents publics étrangers dans des transactions commerciales internationales aux autorités compétentes ».

– La convention des Nations unies fait référence à « toute personne qui signale aux autorités compétentes, de bonne foi et sur la base de soupçons raisonnables, tous faits concernant les infractions établies conformément à la présente convention ».

– La convention civile du Conseil de l'Europe sur la corruption mentionne « une protection adéquate contre toute sanction injustifiée à l'égard des employés qui, de bonne foi et sur la base de soupçons raisonnables, dénoncent des faits de corruption aux personnes ou autorités responsables ».

• La bonne foi et les « motifs raisonnables »

Une des principales exigences prévues dans la plupart des législations est que le signalement soit fait « de bonne foi » et sur la base de « motifs raisonnables ». La protection est accordée à un individu qui fait un signalement fondé sur sa conviction que l'information révélée a satisfait une des conditions du texte, même si sa conviction est erronée.

Cette exigence est aussi prévue par la plupart des traités internationaux qui font la promotion du déclenchement d'alerte. Elle vise à prévenir l'excès de révélations abusives ou liées à du harcèlement.

Il en résulte que les individus qui font délibérément de faux signalements ne devraient pas, en principe, bénéficier d'une protection légale [57].

Certaines lois prévoient d'ailleurs des sanctions pénales en cas de fausse déclaration [58].

Certains analystes contestent cette exigence de bonne foi, car ils considèrent qu'elle peut créer un frein au déclenchement d'alerte [59], en focalisant l'attention sur le lanceur d'alerte et ses motivations, davantage que sur la qualité de l'information révélée par ce canal.

Certains tribunaux ont également, et de manière discutable, subordonné la mise en œuvre de la protection du lanceur d'alerte à sa bonne foi [60].

• Les canaux du signalement

La question des voies que doit emprunter le signalement est également un élément essentiel des dispositifs d'alerte, le principal écueil étant l'existence de procédures trop restrictives qui risquent, soit d'être dissuasives pour les lanceurs d'alerte, soit de favoriser les dénonciations informelles ou anonymes.

La loi peut prévoir un ou plusieurs canaux par lesquels les signalements peuvent être faits.

Très logiquement, il apparaît que les lois spécifiques au lancement d'alerte prévoient en général le respect de procédures internes détaillées avant que le signalement puisse être effectué auprès d'une autorité externe. À l'inverse, la plupart des lois sectorielles relatives au déclencheur d'alerte autorisent les signalements à un nombre limité d'organes externes, comme par exemple une commission nationale anticorruption.

Les signalements peuvent être internes

Le premier et plus approprié canal de signalement dans la plupart des cas de déclenchement d'alerte est l'organisation elle-même. Cela se fonde sur l'idée qu'une organisation qui fonctionne bien a la volonté d'être informée des dérives afin de prendre des mesures pour les corriger [61].

57. C'est le cas en Corée du Sud, par exemple.
58. Cas en Inde.
59. Cf. par exemple David Banisar, article précité.
60. Jurisprudence de certaines cours américaines, ou en France, comme on le verra *infra*, jurisprudence de la chambre sociale de la Cour de cassation antérieure à la création de la protection statutaire du salarié-lanceur d'alerte.
61. Idée que l'on trouve exprimée par certaines jurisprudences relatives à la protection du lanceur d'alerte, notamment celles, citées précédemment, de la Cour européenne des droits de l'homme.

S'agissant du secteur public, de nombreuses lois, telles que celles de la Grande-Bretagne, de l'Afrique du Sud, de la Nouvelle-Zélande et du Canada, encouragent ou contraignent les organisations à adopter des procédures pour un premier traitement des signalements, sous forme de mesures administratives. Les procédures sont conçues pour encourager les agents, qui ont eu connaissance des dysfonctionnements, d'être en mesure de les signaler et, pour les organes, de leur apporter une solution avant qu'ils ne prennent plus d'ampleur. Dans la plupart des cas, les employés doivent suivre ces procédures avant de saisir un organe externe, s'ils désirent être toujours protégés par la loi.

Les personnes destinataires des signalements peuvent être très variées. Cette catégorie peut inclure des directeurs, des supérieurs de rang élevé y compris des responsables d'organisations ou leurs conseillers, des juristes et des inspecteurs généraux. Par exemple, l'Acte canadien de protection du signalement par des agents publics prévoit que le responsable exécutif de toutes les organisations gouvernementales désigne un responsable senior pour recevoir et traiter ces signalements. Certaines administrations ont également de plus en plus recours à des dispositifs modernes (*hotlines*, sites Internet dédiés…) qui présentent l'avantage de rendre impersonnelle la relation entre le lanceur d'alerte et son destinataire [62].

Pour ce qui concerne le secteur privé, il n'existe pas à proprement parler de dispositions prescriptives. En France, par exemple, la mise en place d'un dispositif d'alerte éthique intervient en principe dans le cadre du règlement intérieur de l'entreprise [63].

La Chambre de commerce internationale a également établi des principes directeurs destinés aux entreprises.

Un certain nombre de sociétés ont mis en place des lignes de téléphone ou cellules d'alerte pour signaler la corruption ou d'autres méfaits au sein de leurs organisations, en particulier pour faire face aux obligations de la loi SOX et Dodd-Frank. Celles-ci peuvent être mises en place en interne, par des unités spécialisées, ou en externe, par des agences anticorruption, voire des sociétés de conseil.

Certains experts du déclenchement d'alerte pensent que ce type de canal est contreproductif.

Aux USA, une étude a montré que les employés utilisent les *hotlines* dans seulement 3 % du temps, et dans près de 80 % des cas, ils s'adressent à un directeur ou à l'encadrement supérieur.

62. Solution retenue notamment par la Commission d'éradication de la corruption d'Indonésie (site Internet), la Corée du Sud (*hotline*).

63. Dans les conditions de fond et de forme qui seront examinées *supra* dans la deuxième partie.

Les signalements externes

La plupart des lois sur le déclenchement d'alerte prévoient également, comme alternative aux signalements internes, des signalements à un organe externe à l'administration ou à l'entreprise.

De nombreuses lois spécifiques et certaines lois sectorielles prévoient des organes externes spécifiques. Par exemple, le PDA sud-africain autorise les signalements au « protecteur public » et à l'auditeur général. En Nouvelle-Zélande, le médiateur peut recevoir certaines plaintes. À Antigua, les lanceurs d'alerte peuvent faire des signalements au commissaire à l'information. On retrouve le même type de dispositif au Canada.

Lorsqu'il existe des lois sectorielles anticorruption, l'agence anticorruption est le destinataire de droit commun.

Certains pays, comme la Grande-Bretagne et l'Afrique du Sud, autorisent également les signalements à des conseillers externes ou à des syndicats représentatifs pour obtenir un avis sur leurs droits.

La révélation aux médias

Les médias (presse, télévision…) sont de plus en plus fréquemment une des voies privilégiées des alertes [64], *a fortiori* lorsque l'ensemble d'une chaîne hiérarchique, voire le personnel politique, est impliqué dans les comportements qui font l'objet du signalement. Une étude sur plus de 200 cas de fraudes aux USA entre 1996 et 2004 a fait apparaître que les médias étaient à l'origine de la révélation des fraudes dans 13 % des cas, tandis que les employés étaient à l'origine de 17 % des cas.

De nombreuses lois reconnaissent et autorisent les signalements aux médias (Canada, Grande-Bretagne, Afrique du Sud), mais le plus souvent, en dernier ressort, et si une procédure ou une série de conditions sont satisfaites. Ces exigences supplémentaires ont pour objectif de décourager les signalements publics et d'encourager les signalements internes [65]. Le rôle des médias dans le domaine du déclenchement d'alerte sera naturellement d'autant plus important qu'ils disposent du privilège légal de protéger leurs sources [66].

64. Les médias pouvant eux-mêmes, et de longue date – du moins dans les pays connaissant la liberté de la presse – jouer un rôle actif dans le déclenchement des alertes, au moyen notamment des journalistes d'investigation.

65. Exemple du Canada, notamment « lorsque l'agent public a de sérieuses raisons de penser que l'objet du signalement est un acte ou une omission qui constitue une infraction sérieuse ou constitue un risque imminent de danger substantiel et spécifique pour la vie, la santé et la sûreté des personnes, ou l'environnement » et du PIDA britannique qui prévoit différents niveaux (« gradins ») de signalement, chacun des niveaux requérant de la part du lanceur d'alerte un certain seuil de conditions à respecter pour pouvoir bénéficier de la protection légale.

66. Ce qui est le cas dans environ une centaine de pays.

Cependant, les autorités publiques sont souvent réticentes à cette utilisation des médias. Les médias, de leur côté, sont également souvent sceptiques sur les procédures requises, craignant qu'elles ne soient un moyen de limiter la liberté d'expression.

On assiste également récemment à une montée en puissance des signalements adressés à des sites Internet [67].

On ajoutera que certaines catégories d'agents publics peuvent également, de par leurs fonctions, se voir imposer certains canaux de signalement (cas des agents des services de renseignement par exemple).

• Le recours à des mécanismes destinés à encourager le signalement

Certains dispositifs donnent la possibilité aux lanceurs d'alerte de recevoir une rétribution, y compris sous une forme monétaire, pour avoir signalé des manquements, en particulier dans le cas de la fraude ou de la corruption. De nombreux spécialistes sont réticents à de telles mesures, considérant qu'ils portent atteinte aux principes de l'intérêt public de la loi. D'autres considèrent qu'elles présentent l'avantage de renforcer le statut des lanceurs d'alerte en leur donnant un rôle actif dans la lutte contre les comportements répréhensibles.

L'approche la plus extrême consiste à permettre aux particuliers-lanceurs d'alerte de se substituer au gouvernement pour recouvrer l'argent perdu ou gaspillé. C'est typiquement le cas du *False Claims Act* (FCA) américain qui autorise les particuliers à déposer plainte à la place du gouvernement pour recevoir jusqu'à 30 % des montants récupérés. Le FCA interdit aussi les sanctions contre ceux qui déposent des dossiers et autorise le versement d'une compensation additionnelle sur les montants récupérés. Plus récemment, la loi Dodd-Frank a autorisé également l'autorité américaine des marchés financiers, la *Securities and Exchange Commission* (SEC) à payer des récompenses aux particuliers qui fournissent à la Commission une information qui lui permettra de mener à bien ses investigations. Les récompenses peuvent représenter de 10 à 20 % des montants recouvrés.

Cependant, la formule la plus répandue est celle des dispositifs nationaux qui, en particulier dans certains pays d'Asie, accordent des récompenses à ceux qui ont révélé des cas de corruption.

Ainsi, en Corée du Sud, l'*Anti-corruption Act* permet aux particuliers qui révèlent des affaires de corruption de percevoir jusqu'à 30 % des

67. Certains d'entre eux ayant d'ailleurs pour spécialité la révélation de faits passés sous silence par les médias traditionnels. Rentre dans cette catégorie le site Wikileaks qui a diffusé de nombreux documents portant sur la corruption, notamment un rapport sur une importante affaire de corruption, camouflé par le gouvernement kényan.

montants récupérés, à concurrence de 2 millions de dollars US. À Taïwan, la réglementation sur la rétribution des informateurs anticorruption et leur protection prévoit sept niveaux différents de récompenses. Au Népal, l'Acte sur la prévention de la corruption autorise l'agence anticorruption à donner une « récompense appropriée à la personne qui l'assiste dans ses enquêtes, aux investigations et à la collecte de preuves relatives aux infractions punissables sous cet acte ».

Les dispositifs de protection des déclencheurs d'alerte

La question de la protection des lanceurs d'alerte est habituellement considérée comme l'élément clé d'un dispositif d'alerte efficace. Au demeurant, cette protection est préconisée par la plupart des instruments internationaux anticorruption.

Cependant, la mise en place d'une protection effective et concrète soulève en pratique de nombreuses difficultés, qui expliquent que les solutions retenues varient fortement d'un pays à l'autre en fonction de leur environnement réglementaire mais aussi sociologique. Les solutions retenues sont donc à géométrie variable.

a) La première difficulté est de déterminer les personnes susceptibles de bénéficier d'une protection

Dans certains pays du G20, le champ des personnes couvertes par la protection est très large. Ainsi, le Japon, la Corée, l'Afrique du Sud et la Grande-Bretagne ont adopté des législations de protection qui s'appliquent expressément à la fois au secteur public et au secteur privé.

Dans certains pays, la protection couvre non seulement les fonctionnaires et les employés permanents, mais également les consultants, les contractuels, les employés temporaires et les volontaires (Australie, Grande-Bretagne).

Cependant, la plupart des dispositifs sont plus restrictifs. En général, les lois de protection ne s'appliquent pas aux salariés du secteur privé.

Par ailleurs, certaines lois de protection excluent expressément certaines catégories d'agents publics du régime de protection (services de renseignement, armée).

Dans d'autres pays, les employés du secteur public qui sont impliqués dans des secteurs sensibles peuvent bénéficier d'une protection spéciale (cas aux États-Unis pour les membres des agences fédérales de renseignement).

b) Dans un deuxième temps, la question se pose de déterminer les actes (les représailles) contre lesquels cette protection est établie

Certaines lois sont très complètes. Les plus importantes protections assurées par les lois relatives au lanceur d'alerte sont l'interdiction des

discriminations et la garantie que les atteintes au statut professionnel de la personne seront réparées dans les plus brefs délais. Les définitions sont suffisamment larges pour couvrir n'importe quelle mesure de représailles [68]. L'article L. 1161-1 du Code du travail français établit également un champ de protection en matière professionnelle très large [69].

On trouve une disposition identique avec le PDA d'Afrique du Sud.

Aux États-Unis, la protection des employés est assurée, y compris contre les sanctions disciplinaires les moins sévères, comme les avertissements ou les réprimandes. En Corée, la protection s'applique aux sanctions administratives ou financières.

c) La responsabilité pénale et civile du lanceur d'alerte

Certains pays appliquent des sanctions pénales si les employés révèlent des informations relatives aux secrets d'État ou à la sécurité nationale. Les pays peuvent envisager un abandon de responsabilité pénale pour les signalements protégés, ou seulement offrir une protection si le signalement est fait à travers certains canaux [70].

Des lois de protection plus complètes peuvent aussi fournir une protection contre les injures ou la diffamation, ces actions étant particulièrement dissuasives pour les lanceurs d'alerte (Corée).

d) La confidentialité et l'anonymat

La plupart des lois sur les déclencheurs d'alerte prévoient une protection de l'identité du lanceur d'alerte, qui est gardée confidentielle, sauf si ce dernier a consenti à la révéler [71]. Certains pays prévoient d'ailleurs des sanctions en cas de révélation de l'identité du lanceur d'alerte (Inde).

Cependant, la confidentialité peut procurer un faux sentiment de sécurité. Dans la mesure où seul un petit nombre de personnes au sein d'une organisation est au courant des comportements signalés, il ne doit donc pas être difficile de les identifier. Dans de nombreux cas, les employés ont rencontré des difficultés à ce sujet. Cela explique que, par exemple, le Conseil de l'Europe (GRECO) ait recommandé que les pays assurent une plus grande protection des lanceurs d'alerte.

La confidentialité doit être distinguée de l'anonymat : il y a anonymat lorsque les signalements sont faits sans que le destinataire connaisse l'identité de l'expéditeur. En général, la protection légale prévue par

68. Cas, par exemple, de l'Afrique du Sud.
69. Voir *infra*, 2e partie.
70. Cas aux États-Unis.
71. États-Unis, Nouvelle-Zélande, Afrique du Sud.

les lois détaillées s'applique seulement aux personnes qui s'identifient comme étant à l'origine du signalement. Certaines lois sur les lanceurs d'alerte autorisent l'organe qui reçoit les signalements anonymes à les ignorer tandis que d'autres, soit leur donnent une connotation négative, soit interdisent leur utilisation.

Ainsi, la loi Sarbanes-Oxley exige que les entreprises créent des *hotlines* « anonymes, confidentielles ».

Certains dispositifs juridiques reconnaissent par ailleurs un droit constitutionnel à l'anonymat en tant que composante de la liberté d'expression [72].

L'anonymat peut également être utile dans certains cas, comme dans les systèmes juridiques dans lesquels l'État de droit n'est pas assez fort ou lorsqu'il y a des problèmes de menaces physiques ou de stigmatisation [73].

Bien que l'anonymat puisse constituer une incitation forte à l'obtention d'une récompense, un certain nombre de lois excluent les signalements anonymes (Brésil).

Mais les lois, aussi complètes soient-elles, sont loin de régler tous les problèmes. D'autres obstacles à la protection de l'anonymat peuvent être de nature culturelle.

e) La charge de la preuve

Un important problème est la charge de la preuve. La question est de savoir si l'employé est obligé de faire la démonstration que les sanctions qu'il a subies avaient un lien avec le signalement qu'il a effectué ou de placer la charge de la preuve sur l'organisation qui devra démontrer que la décision était légalement justifiée et non pas fondée sur le signalement.

Cet allégement est une réponse aux difficultés auxquelles doit faire face un employé pour prouver que les représailles étaient le résultat de son signalement, spécialement lorsque les formes de représailles peuvent être très difficiles à démontrer.

Dans cet esprit, le PDA d'Afrique du Sud, par exemple, prévoit qu'un licenciement consécutif à un signalement est présumé être un « licenciement automatiquement injuste ». Aux États-Unis, l'agence doit apporter la preuve « au moyen de preuves claires et convaincantes qu'elle aurait pris la même mesure d'ordre individuel en l'absence de signalement ». En Grande-Bretagne la charge de la preuve est fonction de la durée des fonctions de l'employé.

72. Suède, Norvège.
73. Sierra-Leone, Île Maurice.

De même, en France, l'article L. 1161-1 du Code du travail a prévu que la charge de la preuve reposait sur l'employeur.

f) La réparation des préjudices subis par le lanceur d'alerte

Les lois de protection prévoient, pour la plupart, un mécanisme de réparation pour les lanceurs d'alerte qui ont subi un préjudice. L'importance de telles dispositions a été soulignée dans une résolution de l'assemblée du Conseil de l'Europe.

Les solutions varient en fonction du préjudice. La plupart des lois prévoient un retour dans les fonctions lorsque la personne a été révoquée. Dans certains pays [74], les lanceurs d'alerte peuvent obtenir un transfert dans un poste équivalent s'il peut être démontré que des problèmes tels que du harcèlement peuvent survenir si la personne reste dans ses fonctions actuelles.

La plupart des lois sur le déclenchement d'alerte prévoient également une réparation au lanceur d'alerte dans les cas où il a subi un préjudice qui ne peut pas être réparé par une simple injonction. Cela inclut les salaires perdus, mais également une réparation du préjudice subi (cas du PIDA anglais), voire un système de dommages et intérêts.

g) Les sanctions pénales

Certains dispositifs juridiques prévoient des sanctions pénales pour les employeurs qui ont pris des mesures de représailles contre les personnes qui font des signalements [75].

Ce type de solution reste cependant encore peu répandu.

h) Les limites aux dispositifs d'alerte

Un domaine particulier qui n'est pas bien réglé par les réglementations nationales est le problème du déclenchement d'alerte en lien avec la sécurité nationale. Les organes impliqués dans la protection de la sécurité nationale sont souvent une source d'abus en raison d'excès en matière de secret et du manque de contrôles externes.

La plupart des lois échouent à traiter correctement le problème dans ce domaine, soit en l'ignorant ou, lorsqu'elles le traitent, par des procédures insuffisantes. Comme cela a été noté précédemment, de nombreux pays ont des lois relatives aux secrets d'État qui constituent un obstacle sérieux au déclenchement de l'alerte.

74. USA, Corée du Sud et Afrique du Sud.
75. Hongrie, Canada, loi Sarbanes-Oxley aux USA.

En Grande-Bretagne, le PIDA ne s'applique pas aux signalements qui violent l'Acte sur les secrets officiels. Comme cela a été noté précédemment, l'acte a été utilisé dans nombreuses affaires récentes à l'encontre de lanceurs d'alerte qui ont révélé des éléments d'intérêt public dans les médias.

Aux États-Unis, une législation particulière autorise la révélation de secrets nationaux, mais seulement aux comités de supervision du Congrès. L'*Intelligence Community Whistleblower Protection Act*, adopté en 1999, autorise les employés à rapporter aux commissions du renseignement de la Maison-Blanche et du Sénat ainsi qu'à l'inspecteur général des agences. Cependant, il procure une protection minimale aux employés du renseignement.

Au Canada, l'Acte sur la protection du signalement par les agents publics se limite à obliger le Service canadien du renseignement de sécurité (SCRS) et l'Établissement sur la sécurité des communications à adopter des procédures similaires à celles requises pour les autres départements. Les employés n'ont pas la possibilité de se plaindre auprès du commissaire à l'intégrité du service public.

Cependant, certaines lois sur le lanceur d'alerte outrepassent ces lois spécifiques. En Nouvelle-Zélande, le PDA l'emporte sur les autres lois. Cependant, dans des affaires de sécurité nationale, les signalements peuvent seulement être faits au médiateur ou à l'inspecteur général de l'intelligence et de la sécurité (cas également en Inde).

i) Les mécanismes de suivi et de supervision des dispositifs d'alerte

• Les mécanismes de suivi

Selon les pays, un organe spécifique peut être chargé de recevoir les signalements, de les traiter et/ou de recevoir et d'instruire les plaintes pour représailles, mesures discriminatoires ou disciplinaires prises contre les lanceurs d'alerte.

Plusieurs options coexistent actuellement dans le monde :

L'option de l'organe indépendant

Une solution consiste à créer un organe indépendant unique qui peut à la fois recevoir les signalements et examiner les représailles.

Le système le plus complet se trouve au Canada. En 2005, l'Acte de protection du signalement des fonctionnaires a instauré un commissaire à l'éthique du secteur public qui rapporte directement au Parlement. Ce commissaire peut recevoir des signalements, enquêter sur eux et sur les rapports de représailles venant des lanceurs d'alerte, et publier des recommandations adressées aux responsables des autorités publiques. Lorsque des violations aux droits du lanceur d'alerte sont trouvées, le tribunal peut les réparer ou prononcer des sanctions.

Aux États-Unis, le *Whistleblower Protection Act* de 1989 a érigé l'Office du conseil spécial (OSC) en qualité d'organe indépendant d'enquête. L'OSC peut enquêter sur les pratiques personnelles interdites y compris l'adoption de mesures ou la carence à prendre des mesures à la suite d'un déclenchement d'alerte. Il peut recommander des actions correctrices ou disciplinaires au sein de l'organe impliqué et apporter des cas devant le *Merit Systems Protection Board*. L'OSC peut aussi recevoir des rapports de la part des lanceurs d'alerte pour violation de la loi, gaspillage d'argent public, mauvaise gestion, abus d'autorité et danger pour la santé et la sécurité publique et les adresser à l'agence ou au procureur général dans un délai de 15 jours si cela est justifié. Il rapporte également devant le Congrès et le Président.

L'OSC semble cependant avoir éprouvé des difficultés à exercer correctement sa fonction d'assistance.

L'option du médiateur *(ombudsman)*

Une autre possibilité est de conférer les compétences de supervision au médiateur, qui habituellement est d'origine parlementaire [76]. Environ 120 pays ont instauré un médiateur. Près de 30 pays ont confié au médiateur existant la responsabilité d'appliquer la législation sur la liberté d'information.

Dans de nombreux pays, l'*ombudsman* reçoit aussi les plaintes et instruit les enquêtes portant sur des organes publics.

L'*ombudsman* a cependant une compétence limitée. D'une part, les médiateurs n'ont généralement d'autorité que sur les organes publics. De plus, ils ont des pouvoirs limités pour imposer des solutions alternatives. La plupart des *ombudsmen* s'appuient sur leur autorité morale pour contraindre les organes publics à suivre leurs recommandations. Cela peut constituer un handicap lorsque ces organes ont déjà pris une décision pour sanctionner un agent et ne veulent pas l'annuler.

En Nouvelle-Zélande comme en Irlande, les *ombudsmen* sont compétents pour recevoir des plaintes et, le plus souvent, conseiller les lanceurs d'alerte. Dans beaucoup de cas, les signalements sont faits auprès d'autres organes publics tels que le commissaire de la Police, le contrôleur et l'auditeur général ou le commissaire à la Santé et au Handicap. Les *ombudsmen* ne traitent pas des cas de sanctions.

76. Suède, Finlande, Canada, Grande-Bretagne…

L'option des organes spécialisés

De nombreux pays ont créé différents types d'organes dotés d'une compétence limitée qui peuvent recevoir des rapports sur de possibles violations de la loi ou d'autres problèmes. Certains ont aussi le pouvoir de protéger les lanceurs d'alerte et de sanctionner les discriminations. Pour l'essentiel, il s'agit d'agences anticorruption, mais quelques pays confient ces fonctions à d'autres organes tels que des commissions de la concurrence. Ils peuvent enquêter seulement pour ce qui est de leur propre domaine et dans la plupart des cas pour des crimes plutôt que pour des comportements malhonnêtes ou dangereux.

Tel est le cas, par exemple, de l'agence anticorruption (KICAC) coréenne.

Certains dispositifs prévoient que les organes anticorruption soient dotés de pouvoirs très larges (cas par exemple du projet de loi indien de révélation des intérêts publics).

L'option juridictionnelle

Une autre voie pour les signalements est de s'adresser directement aux tribunaux. Il s'agit d'une voie très coûteuse, spécialement pour les salariés qui viennent d'être licenciés et qui n'ont plus de sources de revenus pour engager une procédure. Certains pays comme la Grande-Bretagne et l'Afrique du Sud n'ont pas d'organe de supervision et s'appuient seulement sur les tribunaux pour apporter des solutions. L'inconvénient de cette approche est l'absence d'organe susceptible de recevoir des informations et d'avoir une vision générale du dispositif. Ils sont également limités en termes de champ de compétences.

La plupart des États disposant de textes spécifiques autorisent les recours des lanceurs d'alerte qui ont subi un préjudice devant des tribunaux (prud'hommes ou cours d'appel).

Le PIDA britannique autorise les recours devant les prud'hommes (environ 800 cas par an pour une centaine de décisions).

Aux États-Unis, les salariés peuvent faire un recours auprès du *Merit Systems Protection Board* et ensuite auprès de la Cour d'appel. Ce dispositif ne semble pas fonctionner très bien (depuis 1999, seulement deux cas de recours).

Au Canada, l'Acte sur le signalement des agents publics permet d'intenter un recours contre les sanctions auprès du Bureau des relations de travail du service public et du Bureau canadien des relations industrielles.

• Les mécanismes de supervision et d'évaluation

Les textes sur la protection des lanceurs d'alerte devraient bénéficier d'un accompagnement sous forme de supervision, de formation et d'évaluation. Informer les employés du secteur public ou privé de leurs droits et obligations lorsqu'ils exposent des méfaits est essentiel, comme cela a été souligné notamment dans la recommandation OCDE de 1998 sur le renforcement de l'éthique dans le service public.

Certains États du G20 ont engagé de tels efforts[77]. Certains pays du G20 ont aussi adopté des dispositions dans leurs lois[78].

Certains pays du G20, peu nombreux, ont aussi pris des mesures pour évaluer l'efficacité de leur système de protection[79].

Évaluation des lois et pratiques sur le déclenchement d'alerte

Peu d'études ont jusqu'à présent été réalisées sur l'évaluation de l'efficacité des dispositifs d'alerte existants. Les travaux disponibles se bornent en général à recenser et analyser les textes existants, mais sans réellement se poser la question de la réalité de leur fonctionnement[80]. D'une part, en effet, un grand nombre de ces dispositifs sont trop récents pour qu'il soit possible d'établir un bilan de leur efficacité. Par ailleurs, comme il a été indiqué précédemment, ces dispositifs font généralement partie d'ensembles plus vastes qui s'appliquent à la lutte contre la corruption et/ou la fraude, au droit du travail, au harcèlement dans le milieu professionnel, etc. Les évaluer en tant que tels n'a donc pas, dans ces conditions, grande signification si n'est pas pris en considération leur environnement juridique, administratif, sociologique, culturel… Les travaux qui ont été réalisés sur ce sujet, peu nombreux[81], montrent que « …les lois existantes sur le lanceur d'alerte dans la plupart des dispositifs nationaux ne fonctionnent pas aussi bien qu'espéré ou anticipé » même si « il y a des preuves que le déclenchement d'alerte prend de l'importance ».

Les quelques données disponibles confirment cette appréciation en demi-teinte.

En premier lieu, s'agissant de la mise en place de procédures de déclenchements d'alerte, aussi bien les enquêtes de l'OCDE que les « revues

77. Indonésie : programmes de promotion du signalement.
78. USA, en France, délibération CNIL du 8 novembre 2005.
79. Japon, USA.
80. Par exemple, « Panorama des administrations publiques 2009 », étude *op. cit.* de l'OCDE, qui se borne à relever que l'existence de mécanismes de *whistleblowing* « est considérée comme le signe d'une culture ouverte ».
81. On s'appuiera ici principalement sur l'étude de David Banisar, *op. cit.*

de pairs » réalisées par les organisations internationales font apparaître que la plupart des pays du G20 disposent de telles procédures, au moins dans le secteur public. Cependant, la simple existence d'une procédure ne suffit pas à garantir qu'une bonne pratique a été adoptée.

Ainsi, les États qui, comme les États-Unis, l'Afrique du Sud ou la Grande-Bretagne, ont mis en place des dispositifs de signalement très complets, connaissent de façon concomitante une forte augmentation des signalements et une augmentation des cas de représailles rapportés notamment devant les tribunaux. Ces données sont étayées par des enquêtes réalisées auprès des lanceurs d'alerte du secteur public et du secteur privé. Ainsi, une étude de 2005 dans le secteur privé a trouvé que les lanceurs d'alerte ont rapporté les représailles dans 22 % des cas tandis que 48 % ont signalé avoir reçu des retours positifs.

En Corée du Sud, 67 % des employés publics qui ont rapporté des irrégularités ont indiqué avoir été victimes de représailles.

Bien souvent, les procédures ont été adoptées davantage pour se mettre en conformité avec la loi que dans l'optique d'une amélioration des procédures et d'un changement de culture.

Une étude récente du cabinet Ernst and Young a montré qu'il y avait des différences géographiques significatives dans la perception par les dirigeants des entreprises sur l'efficacité des lanceurs d'alerte dans la réduction de la corruption, considérée comme le plus efficace en Amérique du Nord et le moins efficace en Asie.

De la même façon, si les employés semblent avoir une conscience plus développée de leur droit à une protection, une forte proportion d'entre eux reste persuadée qu'ils seront sanctionnés s'ils révèlent des violations de la légalité. Cette crainte est malheureusement justifiée si l'on considère les réactions de certaines administrations ou gouvernements face aux signalements effectués par leurs employés à des organes externes [82].

Enfin, une question à se poser est de savoir si les lois et les pratiques ont fait évoluer la perception souvent négative des lanceurs d'alerte. Une partie significative de la population persiste à assimiler les lanceurs d'alerte à des « fauteurs de troubles », des « mouchards »…

L'opinion semble cependant évoluer dans un sens positif [83].

82. Comme l'illustrent les nombreux cas de pressions exercées sur les médias pour qu'ils révèlent leurs sources…

83. Évolution reflétée par les médias : ainsi le magazine américain *Time magazine* a-t-il décerné le titre de « personnalités de l'année 2002 » à trois *whistleblowers*, respectivement Cynthia Cooper de la société Worldcom, Sherron Watkins d'ENRON et Coleen Rowley du FBI.

Des événements internationaux peuvent aussi contribuer à ces évolutions. Ainsi, le mouvement qualifié de « printemps arabe » au cours de l'année 2011, qui a conduit à la chute de plusieurs dirigeants du Maghreb et du Proche-Orient, a également été l'occasion de souligner le rôle joué par les lanceurs d'alerte dans la dénonciation des méthodes et pratiques, notamment dans le domaine de la corruption, utilisées par certains régimes autoritaires.

LE LANCEUR D'ALERTE EN FRANCE : UNE NOTION QUI PEINE À S'IMPOSER DANS LES TEXTES ET DANS LA PRATIQUE

Au sein des pays de l'OCDE, la France occupe une position intermédiaire. Elle ne dispose pas d'un dispositif spécifiquement dédié au déclenchement d'alerte, du moins dans le sens qui lui est habituellement donné dans les pays anglo-saxons.

Cependant, certaines règles, qui relèvent pour l'essentiel du droit pénal – telles que l'article 40 du Code de procédure pénale – peuvent s'en rapprocher. Ces règles soulèvent, à l'instar des dispositifs mis en place dans d'autres pays, la question de la réalité de leur mise en œuvre : on constate en effet, de façon générale, l'existence de freins importants à la pratique du lancement d'alerte, tant par les employés du secteur public que par ceux du secteur privé.

Une autre difficulté tient au fait que la France, pays de droit romain, reste marquée par une dichotomie des régimes applicables entre le secteur public et le secteur privé. Alors que dans le secteur public, le lancement d'alerte est analysé et perçu comme une obligation qui s'impose aux agents publics, dans le secteur privé, il est abordé sous l'angle de la protection des droits des salariés qui en sont les initiateurs. Dans les faits cependant, ces différences tendent à s'estomper, ce qui conduit à s'interroger sur la mise en place d'un dispositif d'ensemble applicable au déclenchement de l'alerte.

Le lanceur d'alerte dans le secteur public : contraintes des textes et faiblesses des pratiques existantes

Au sein du secteur public, le signalement a une traduction juridique qui figure à l'article 40, alinéa 2, du Code de procédure pénale. La rigueur de cette disposition contraste toutefois avec la faiblesse des pratiques.

L'article 40, alinéa 2, du Code de procédure pénale est au cœur du dispositif de signalement au sein du secteur public

Dans sa plus récente édition du « Panorama des administrations publiques » (en 2009), l'OCDE relève « qu'en 2009, 29 pays contraignent leurs fonctionnaires à dénoncer les fautes observées et/ou ont mis en place des procédures facilitant ces alertes, contre 21 pays en 2000 ».

Au sein de ces pays, la France fait partie du cercle plus restreint des États dans lesquels les agents publics sont obligés par la loi de dénoncer toute faute ou délit, y compris donc la corruption.

L'article 40, alinéa 2, du Code de procédure pénale prévoit en effet que « toute autorité constituée, tout officier public ou fonctionnaire qui, dans l'exercice de ses fonctions, acquiert la connaissance d'un crime ou d'un délit est tenu d'en donner avis sans délai au procureur de la République et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs ».

Cette disposition constitue la clé de voûte du lancement d'alerte en France dans le secteur public. La France dispose théoriquement d'un outil simple et efficace pour détecter et sanctionner les pratiques de corruption, qu'elles s'exercent au sein de la sphère publique ou, dans sa proximité, au vu et au su des agents publics. Cette disposition est rigoureuse dans son principe mais elle soulève, dans sa mise en œuvre, de nombreuses difficultés qui en limitent singulièrement la portée.

Un champ d'application très étendu

a) En premier lieu, on peut observer que les termes employés par le Code de procédure pénale, très neutres, expriment la volonté du législateur de donner une portée très large à cette disposition. En effet, alors que l'article 40, alinéa premier, dispose que « le procureur de la République reçoit les plaintes et les dénonciations et apprécie les suites à leur donner », son deuxième alinéa emploie la formule plus générale de « donne avis », ce qui met d'emblée un terme à d'éventuelles controverses sur les termes employés [84].

L'expression « est tenu » traduit également de manière suffisamment explicite l'obligation qui s'impose aux agents publics.

b) Le champ d'application de l'article 40, alinéa 2, a, en revanche, suscité davantage d'interrogations mais les réponses qui leur ont été apportées par la jurisprudence vont dans le sens d'une interprétation extensive.

• S'agissant, en premier lieu, des agents concernés par cette obligation, l'article 40, alinéa 2, vise trois catégories de personnes : les autorités constituées, les officiers publics et les fonctionnaires

Parmi les personnels de l'administration, une interprétation purement littérale aurait dû conduire à ne retenir que les agents titulaires de la fonction publique, c'est-à-dire les « fonctionnaires nommés dans un emploi

84. Alors que certains auteurs (Gérald Chalon, Xavier Lemaire et Maria Cardoso) tendent à considérer que cet alinéa s'applique à la dénonciation (entendue comme « l'acte par lequel un tiers, qui n'a pas été victime d'une infraction, la porte à la connaissance des autorités de police ou de justice » (G. Chalon), d'autres (C. Vigouroux) au contraire, considèrent que ce terme est « inadéquat » et préconise l'emploi du mot « signalement », équivalent « plus présentable » du mot *disclosure* qui est utilisé dans de nombreux pays anglo-saxons.

permanent et titularisés dans un grade de la hiérarchie des administrations de l'État, des services ou des établissements publics de l'État ou des collectivités territoriales ».

Cependant, le droit pénal ayant traditionnellement de la notion de fonctionnaire une conception très large, on considère généralement que le terme désigne non seulement les personnes qui ont été nommées dans un emploi permanent et titularisées, mais également les agents publics non titulaires.

Par ailleurs, il est habituellement admis que les détenteurs d'un mandat électif rentrent dans la catégorie des « autorités constituées » visées par l'article 40, alinéa 2, au même titre, selon la doctrine, que les juridictions, les préfets et sous-préfets et maires ainsi que les assemblées électives.

En revanche, selon une jurisprudence constante, le juge administratif estime « qu'il ne lui appartient pas, lorsqu'il statue au contentieux, de faire application du second alinéa de l'article 40 du Code de procédure pénale » [85].

Par ailleurs, le juge pénal ayant précisé que l'application de l'article 40, alinéa 2, « suppose l'exercice d'une fonction publique » [86], en sont exclus les agents de l'administration qui sont dans une situation de droit purement privé, comme par exemple les agents des services industriels et commerciaux [87], les fournisseurs de l'administration, les entrepreneurs de travaux publics, les concessionnaires de service public, les collaborateurs bénévoles de l'administration, les personnels étrangers recrutés sur contrat de droit local… Pour ces différentes personnes, le signalement reste, comme pour les particuliers, discrétionnaire et facultatif.

• Au-delà de ces personnes, il convient de noter que la plupart des textes constitutifs des autorités administratives indépendantes ou services administratifs autonomes renvoient à l'article 40 du Code de procédure pénale ou comportent une disposition équivalente

Il convient cependant de distinguer les dispositions qui sont, à proprement parler, des dispositions miroirs de l'article 40 du Code de procédure pénale, des dispositions « autonomes » qui s'appliquent à une catégorie spécifique de comportements ou d'infractions.

85. Cf. par exemple CE, 16 novembre 2007, Confédération nationale des éducateurs sportifs et salariés du sport. Le SCPC considère que cette attitude de refus adoptée par le juge administratif est discutable, car elle peut laisser prospérer des situations souvent lourdes de menaces pour le principe de légalité (cf. à ce propos l'article « Le juge administratif et les atteintes à la probité », Rapport du SCPC 2010, p. 151 et s.).

86. Cass. crim., 6 juillet 1977, *Bull. crim.,* n° 255.

87. À l'exception naturellement des directeurs et comptables conformément à la jurisprudence Jalenques de Labeau (CE, 8 mars 1957).

Dans la première catégorie, rentre par exemple l'article L. 2211-2 du Code général des collectivités territoriales qui prévoit que « conformément aux dispositions du deuxième alinéa de l'article 40 du Code de procédure pénale, le maire est tenu de signaler sans délai au procureur de la République les crimes ou les délits dont il acquiert la connaissance dans l'exercice de ses fonctions ».

De la même façon, l'article 2 de la loi du 29 janvier 1993 instituant le SCPC prévoit, sans renvoyer à l'article 40, que « dès que les informations centralisées par le service mettent en évidence des faits susceptibles de constituer des infractions, il en saisit le procureur de la République ».

Il en est de même de l'article R. 135-3 du Code des juridictions financières qui dispose que « si, à l'occasion de ses contrôles, la Cour des comptes découvre des faits de nature à motiver l'ouverture d'une action pénale, elle en informe le procureur général près la Cour des comptes, qui saisit le garde des Sceaux, ministre de la Justice, et avise le ministre intéressé ainsi que le ministre chargé des Finances »[88].

Rentrent dans la catégorie des dispositions « autonomes » les dispositions qui constituent par exemple la « déclaration de soupçon », qui s'appliquent à certaines professions à des fins de lutte contre le blanchiment d'argent (articles L. 561-1, L. 562-10 et L. 564-1 à L. 564-6 du Code monétaire et financier). Dans ce cas d'espèce, en effet, le signalement intervient dans un périmètre plus restreint :

– il ne concerne qu'une catégorie limitativement énumérée de personnes ;
– l'élément déclenchant du signalement ne se limite pas à la connaissance d'une infraction ; un simple soupçon, ou « de bonnes raisons de soupçonner » (des présomptions) peuvent justifier une déclaration ;
– les faits révélés ne constituent pas directement une infraction. Il s'agit d'opérations provenant d'une « infraction passible d'une peine privative de liberté supérieure à un an ou (qui) participent au financement du terrorisme » ;
– enfin, la déclaration doit être effectuée, non pas directement auprès de l'autorité judiciaire, mais auprès d'un service administratif [89].

c) Les faits concernés par l'obligation de signalement

Ces faits sont constitués de l'ensemble des infractions qui constituent au sens du Code pénal un crime ou un délit et ce, quel que soit leur degré

88. L'article R. 225-1 contient une disposition similaire applicable aux chambres régionales des comptes.

89. TRACFIN (traitement du renseignement et action contre les circuits financiers clandestins), service du ministère de l'Économie et des Finances, chargé de la lutte contre le blanchiment d'argent.

de gravité, qu'elles soient prévues dans le Code pénal lui-même ou dans une législation pénale annexe.

En revanche, l'expression « dans l'exercice de leurs fonctions » peut être interprétée de deux façons. La question se posait de savoir si la constatation des faits doit, au sens strict, ressortir des attributions des fonctionnaires, ou si, dans une optique plus large, porter sur l'ensemble des crimes et délits dont il peut être amené à avoir connaissance à l'occasion de l'exercice de ses fonctions. La jurisprudence a retenu une interprétation extensive de cette disposition. De manière constante, la chambre criminelle considère que l'administration satisfait « à un devoir normal » en rendant compte au procureur de la République d'une infraction qui excède le champ de ses compétences.

Des modalités de mise en œuvre très souples

a) Il convient en premier lieu de souligner que l'obligation de signalement prévue par l'article 40, alinéa 2, du Code de procédure pénale revêt un caractère personnel

Cet article n'impose pas que cette révélation soit effectuée par l'autorité hiérarchique, ni même que celle-ci en soit préalablement informée. Ainsi, un agent ne commet pas une faute en dénonçant les faits délictueux au procureur de la République sans en référer à son supérieur hiérarchique[90]. Pour autant, il n'exonère pas les personnes concernées de leur devoir de rendre compte à leur hiérarchie des constatations qu'ils ont effectuées et des suites qui paraissent devoir leur être réservées. À l'inverse, la chambre criminelle a eu l'occasion de juger que les dispositions de l'article 40 n'imposaient pas que la dénonciation soit faite par le fonctionnaire qui avait eu connaissance des faits délictueux, mais qu'elle pouvait être faite par son supérieur hiérarchique[91].

Le caractère personnel de l'obligation de dénoncer connaît toutefois une limite pour les autorités constituées sous une forme collégiale. Dans ce cas, la décision de dénonciation doit en principe émaner de l'autorité elle-même et non du fonctionnaire appartenant le cas échéant à cette institution. Ainsi, s'agissant des juridictions financières, la communication aux juridictions pénales au titre des articles R. 135-3 ou R. 241-25 intervient à la suite d'un délibéré en formation collégiale. Toutefois, elle peut être le fait du seul ministère public sur le fondement de l'article 40.

90. CE, 15 mars 1996, Guigon, *Lebon T,* p. 1109.
91. Cass. crim., 14 décembre 2000, *Bull. crim.,* n° 380.

b) Pour ce qui concerne la forme du signalement, la chambre criminelle a eu l'occasion de préciser que les renseignements fournis au procureur de la République, faisant présumer l'existence d'une infraction, ne sont astreints à aucune condition de forme [92]. Ainsi, une dénonciation peut être déposée au parquet par simple lettre ou par déclaration orale. Par ailleurs, le Conseil d'État a estimé que les ministres dans le cadre de l'organisation de leur service, peuvent préciser les modalités de mise en œuvre de l'article 40, alinéa 2.

Cependant, le dispositif de signalement dans le secteur public présente des limites et des faiblesses

Dans l'analyse à laquelle il se livre chaque année dans son rapport d'activité sur les sources d'émergence des faits de corruption, le SCPC souligne, pour la déplorer, la faible utilisation par les administrations et les établissements publics de l'article 40, alinéa 2, du Code de procédure pénale [93].

Les explications à cette situation sont multiples. Elles sont, en premier lieu, d'ordre juridique ; mais tout aussi nombreuses sont les raisons de fait qui expliquent que, au sein du secteur public, « l'on peut très légitimement se poser la question de la réalité de son application complète et de la totale transparence des décisions entourant sa transmission » [94].

Des limites d'ordre juridique

a) Ces limites tiennent, en premier lieu, à la portée de l'obligation de dénonciation

• La première difficulté tient au fait qu'aucune sanction spécifique n'est prévue en cas de non-dénonciation

De cette absence de sanctions, une partie de la doctrine a conclu que l'obligation prévue à l'article 40, alinéa 2, ne constituait qu'un simple devoir moral [95], ou qu'un simple devoir civique [96].

L'emploi de l'expression « est tenu » incite cependant la grande majorité de la doctrine à considérer qu'il s'agit d'une véritable obligation juridique, mais sans toutefois mettre un terme aux interrogations que l'on peut avoir sur la nature de cette obligation.

92. Cass. crim., 28 janvier 1992, *Gaz. Pal.* 1992, 1, 365.
93. Cf. par exemple le rapport du SCPC de 2010, p. 80 et s.
94. Rapport SCPC 2006, p. 45.
95. Cf. par exemple J.-A. Roux, S. Petit ou A. Barilari, *AJFP* 2003, p. 34.
96. Cf. P. Conte et P. Maistre du Chambon.

• En deuxième lieu, s'il n'existe pas de dispositions qui sanctionnent directement le non-recours à l'article 40, alinéa 2, il existe en droit pénal français des dispositions qui conduisent à sanctionner l'abstention face à l'obligation de dénoncer, ou les abus dans la dénonciation

• Il s'agit tout d'abord de l'article 434-1 du Code pénal relatif à la non-dénonciation de crimes.

L'article 434-1 du Code pénal punit de trois ans d'emprisonnement et de 45 000 euros d'amende « le fait, pour quiconque ayant connaissance d'un crime dont il est encore possible de prévenir ou de limiter les effets, ou dont les auteurs sont susceptibles de commettre de nouveaux crimes qui pourraient être empêchés, de ne pas en informer les autorités judiciaires ou administratives ».

Toutefois, cet article[97] ne s'applique qu'à la seule non-dénonciation de crime, excluant la non-dénonciation de délits[98]. En l'état du droit positif, la non-dénonciation de pratiques corruptrices, de nature délictuelle, ne peut donc être sanctionnée sur la base de ce texte.

• Le non-respect de l'obligation de dénoncer pourrait-il être sanctionné pour complicité sur la base de l'article 121-7, alinéa premier, du Code pénal qui dispose « qu'est complice d'un crime ou d'un délit la personne qui sciemment, par aide ou assistance, en a facilité la préparation ou la consommation » ?

La majorité de la doctrine ainsi que la jurisprudence considèrent que la complicité par abstention n'existe pas, l'article 121-7, en visant spécifiquement certains comportements, exigeant un acte positif pour que sa mise en œuvre puisse être engagée. Toutefois, certaines personnes ont pu, dès lors qu'elles disposaient de moyens légaux à même d'empêcher la commission d'une infraction, voir leur responsabilité engagée sur le terrain de la complicité, et ce du fait de leur abstention[99].

Cela conduit certains auteurs à considérer que les agents publics ont, de par la rigueur des obligations auxquelles ils sont astreints, une obligation juridique de dénoncer les actes qui font obstacle au principe

97. Ainsi que l'article 434-2 qui vise les crimes qui constituent « une atteinte aux intérêts fondamentaux… ou un acte de terrorisme ».

98. L'article 434-3 prévoit, de son côté, l'obligation de dénoncer certains délits (privation, mauvais traitements et atteintes sexuelles infligés à un mineur de quinze ans ou à une personne vulnérable).

99. Cass. crim., 28 mai 1980, *D.* 1981, IR 137, à propos du membre du directoire d'une société qui devait s'opposer à l'abus de biens sociaux commis par le président.

de légalité [100]. La non-dénonciation pourrait, pour certains d'entre eux [101], équivaloir à un acte de complicité [102].

• La question se pose, en troisième lieu, de savoir si la mise en œuvre de l'article 40, alinéa 2, du Code de procédure pénale ne trouve pas non plus un frein dans les dispositions pénales relatives à la dénonciation calomnieuse.

Ce délit est défini et puni par les articles 226-10 à 226-12 du Code pénal.

L'article 226-10 définit la dénonciation calomnieuse comme « la dénonciation, effectuée par tout moyen et dirigée contre une personne déterminée, d'un fait qui est de nature à entraîner des sanctions judiciaires, administratives ou disciplinaires et que l'on sait totalement ou partiellement inexact, lorsqu'elle est adressée soit à un officier de justice ou de police administrative ou judiciaire, soit à une autorité ayant le pouvoir d'y donner suite ou de saisir l'autorité compétente, soit aux supérieurs hiérarchiques ou à l'employeur de la personne dénoncée ».

Le risque, pour l'agent public lanceur d'alerte, de voir sa responsabilité engagée pour dénonciation calomnieuse, est réel [103], mais il ne doit pas être exagéré. D'abord, parce que cette infraction a été définie dans des termes qui en restreignent sa mise en œuvre. En effet, l'élément intentionnel de l'infraction n'est pas constitué par l'inexactitude totale ou partielle du fait dénoncé, mais par le fait que son auteur savait que les faits qu'il a dénoncés sont inexacts. Cette preuve est donc relativement difficile à apporter.

Ensuite, la jurisprudence se montre traditionnellement particulièrement exigeante. Ainsi, elle considère qu'une dénonciation légère ou téméraire ne constitue pas forcément une dénonciation faite de mauvaise foi [104]. Il en est de même si elle intervient à la suite d'une erreur [105]. En outre, la dénonciation doit, pour être calomnieuse, revêtir un caractère spontané.

100. Par exemple Gérald Chalon *in* « Le fonctionnaire et l'article 40 du Code de procédure pénale : nature et portée de l'obligation de dénoncer », *AJFP,* novembre-décembre 2003, p. 31 et s.

101. Du moins ceux qui occupent un certain niveau hiérarchique ou possèdent un minimum de compétences juridiques.

102. La récente mise en cause de certains agents publics, dans des affaires – scandale de l'amiante, notamment – où il leur est reproché de ne pas avoir empêché la commercialisation et l'utilisation de produits dangereux, notamment en alertant les autorités à même d'interdire la mise sur le marché de ces produits, milite en faveur de cette solution.

103. Comme on l'a vu *supra*, dans la première partie, le risque de mise en cause de la responsabilité du lanceur d'alerte n'est pas propre à la France.

104. Cass. crim., 22 juin 1982, *Bull. crim.,* n° 167.

105. Cass. crim., 20 juin 1963, *Bull. crim.,* n° 117.

Le fait qu'elle résulte d'une obligation légale, comme c'est le cas pour l'article 40 du Code de procédure pénale, lui ôte ce caractère de spontanéité.

b) En revanche, un problème plus sérieux est posé par la confrontation de l'obligation de dénoncer telle qu'elle résulte de l'article 40 du Code de procédure pénale avec le respect d'autres obligations incombant aux agents publics

En effet, la particularité de cette obligation est qu'elle ne s'applique pas à des citoyens ordinaires, mais à des agents publics dont certains sont placés dans une position statutaire, c'est-à-dire exercent leur activité dans une collectivité (administration de l'État ou d'une collectivité territoriale) dotée d'une mission de service public, et à ce titre soumis à un ensemble de règles et d'obligations qui contraignent chacun de leurs actes.

Classiquement, la mise en œuvre de l'article 40 soulève, au regard des règles du droit de la fonction publique, deux séries de problèmes :
- la confrontation avec les règles de la morale administrative (secret et discrétion professionnelle) ;
- la confrontation avec le principe hiérarchique.

• S'agissant de la morale administrative, il convient de distinguer les règles du secret professionnel, qui ont été établies dans l'intérêt des administrés, des règles de la discrétion professionnelle, qui visent à protéger l'intérêt du service. Ces deux règles sont prévues par le statut général de la fonction publique [106], mais l'ensemble de la doctrine tend à considérer qu'elles s'appliquent également aux agents non titulaires, non couverts par le statut général

En revanche, ces deux règles posent des problèmes différents au regard de l'article 40, alinéa 2, du Code de procédure pénale.

• Pour ce qui concerne la règle du secret professionnel, la question de sa conciliation avec l'article 40, alinéa 2, est, pour l'essentiel, réglée par les textes.

En effet, le premier alinéa de l'article 26 du statut général prévoit que « les fonctionnaires sont tenus au secret professionnel dans le cadre des règles instituées dans le Code pénal ».

Cette disposition renvoie à une règle plus générale relative au secret professionnel contenue dans le Code pénal, l'article 226-13, qui dispose que « la révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15 000 euros d'amende ».

106. Article 26 de la loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires.

Cependant, le Code pénal prévoit également, dans son article 226-14, que le secret professionnel peut être levé dans un certain nombre d'hypothèses, et notamment « dans les cas où la loi impose ou autorise la révélation du secret ». L'article 40, alinéa 2, du Code de procédure pénale constitue précisément un cas où la loi impose la révélation du secret.

Il ressort donc de la combinaison de ces dispositions que le fonctionnaire qui effectue une dénonciation dans le cadre de cet article ne peut être sanctionné sur le fondement de la violation du secret professionnel [107].

À l'inverse, si certains statuts particuliers rappellent la règle du secret professionnel, celle-ci ne revêt pas un caractère absolu, et ne doit pas constituer un obstacle à l'obligation de dénonciation prévue à l'article 40, alinéa 2, du Code de procédure pénale [108].

Ultérieurement, le fonctionnaire pourra également être délié du secret professionnel, dans l'hypothèse où il serait appelé à témoigner en matière criminelle et correctionnelle.

• En revanche, l'articulation de l'obligation de discrétion professionnelle avec l'article 40, alinéa 2, s'inscrit, avec quelques nuances, dans un schéma identique.

L'article 26, alinéa 2, du statut général prévoit que « les fonctionnaires doivent faire preuve de discrétion professionnelle pour tous les faits, informations ou documents dont ils ont connaissance dans l'exercice ou à l'occasion de l'exercice de leurs fonctions. En dehors des cas expressément prévus par la réglementation en vigueur, notamment en matière de liberté d'accès aux documents administratifs, les fonctionnaires ne peuvent être déliés de cette obligation de discrétion professionnelle que par décision expresse de l'autorité dont ils dépendent ».

Contrairement à l'alinéa précédent, ce texte ne renvoie pas au Code pénal, et il a donc appartenu à la doctrine et à la jurisprudence, de préciser les conditions de son articulation avec l'article 40, alinéa 2, du Code de procédure pénale.

On peut *a priori* considérer que l'article 40, alinéa 2, rentre dans le champ des « cas expressément prévus par la réglementation en vigueur » prévus à l'article 26, alinéa 2.

La jurisprudence a adopté une position ambiguë. Dans un arrêt du 6 juillet 1977, la chambre criminelle a en effet précisé que « si l'article 40

107. Ce qui implique naturellement qu'il se borne à communiquer au procureur de la République les seuls éléments nécessaires à la qualification du crime ou du délit.

108. Voir par exemple, l'application de la règle aux agents des impôts (Cass. crim., 30 octobre 1989, *Bull. crim.,* n° 385).

du Code de procédure pénale fait obligation à tout fonctionnaire ayant, dans l'exercice de ses fonctions, acquis la connaissance d'un crime ou d'un délit, d'en donner avis au procureur de la République, cette disposition ne saurait autoriser un agent public à enfreindre l'obligation de discrétion à laquelle il est soumis et à révéler à des particuliers des faits jugés par lui répréhensibles » [109].

De manière plus claire, plusieurs spécialistes du droit de la fonction publique estiment que l'article 40, alinéa 2, constitue bien une dérogation à l'obligation de discrétion professionnelle [110].

En revanche, la jurisprudence a apporté une réponse dénuée d'ambiguïté quant aux modalités que doit revêtir la dénonciation pour être valablement admise comme une dérogation aux règles du secret et de la discrétion.

Selon une jurisprudence constante, la dénonciation doit être adressée au seul procureur de la République ou à ses auxiliaires [111]. Dans l'arrêt Metivier [112], le juge administratif a pris soin de préciser que l'agent administratif n'a pas à rechercher des renseignements sur des événements confidentiels qu'il ne lui appartient pas de connaître. En outre, l'obligation de discrétion et de secret professionnel interdit à tout fonctionnaire de communiquer certains faits à une autre administration publique lorsque celle-ci n'est pas qualifiée pour en avoir connaissance [113].

• La confrontation de l'article 40, alinéa 2, avec le principe hiérarchique soulève également des problèmes particuliers.

En effet, le principe hiérarchique a été érigé par la jurisprudence en principe général du droit. Ce principe est également prévu par le statut général de la fonction publique, notamment à l'article 28 de la loi du 13 juillet 1983 qui dispose : « … Il [le fonctionnaire] doit se conformer aux instructions de son supérieur hiérarchique, sauf dans le cas où l'ordre donné est manifestement illégal et de nature à compromettre gravement un intérêt public… »

Quel est le rôle du supérieur hiérarchique dans la transmission des dénonciations au procureur de la République ?

109. Cass. crim., 6 juillet 1977, *Bull. crim.,* n° 255.

110. Par exemple Jean-Marie Auby, Jean-Bernard Auby, Jean-Pierre Didier et Antony Taillefait dans *Droit de la fonction publique. État, collectivités locales, hôpitaux,* « Précis Dalloz », Droit public, 4e édition, 2002, p. 305.

111. Arrêt du 6 juillet 1977 précité.

112. CE, 15 février 1961, *Lebon*, p. 124.

113. Chambre de mise en accusation, Paris, 4 juin 1954.

• Un premier point ne pose en principe plus de problème, celui de la question de savoir si le supérieur hiérarchique doit autoriser la transmission des dénonciations.

Cette solution doit être écartée. D'une part la rédaction de l'article 40, alinéa 2, est suffisamment claire. L'article 40 vise en effet tous les fonctionnaires sans distinction, et, d'autre part, il n'impose pas de formalisme préalable.

La jurisprudence du Conseil d'État comme de la Cour de cassation a statué dans ce sens.

Dans l'arrêt Guigon [114], le Conseil d'État a annulé l'arrêté d'un maire révoquant un agent de police municipal qui avait transmis au procureur certaines informations dont il avait eu connaissance lors des opérations de recensement sur le territoire de la commune sans en avertir le maire et le conseil municipal.

Dans le même sens, la chambre criminelle de la Cour de cassation a jugé qu'en dénonçant les faits délictueux au procureur, l'agent n'avait fait, « et sans qu'il ait besoin sur ce point d'une quelconque autorisation » qu'observer les prescriptions de l'article 40 [115].

• La question se pose ensuite de savoir si le supérieur hiérarchique peut imposer à ses subordonnés que les avis et informations liés à l'article 40 soient préalablement portés à sa connaissance.

La réponse à cette question semble être négative. D'une part, parce qu'elle serait contraire à la jurisprudence citée précédemment. D'autre part, car le pouvoir d'organisation dont dispose un supérieur hiérarchique ne doit pas, lui-même, contrevenir aux lois et règlements.

Mais, à l'inverse, la doctrine tend à considérer que l'agent à l'origine du signalement est tenu d'en informer sa hiérarchie [116].

• Un dernier point, plus délicat à trancher, est celui du transfert par l'agent de son obligation de dénoncer au supérieur.

114. CE, 15 mars 1996, n° 146326, précité.

115. Cass. crim., 19 septembre 2000, n° 99-83.960.

116. Cf. par exemple Gérald Chalon *in* « L'article 40 du Code de procédure pénale à l'épreuve du statut général de la fonction publique » (*AJFP*, janvier-février 2004), qui justifie cette information par « l'obligation de déférence du subordonné par rapport à son supérieur hiérarchique ». Cette position paraît devoir être critiquée, car elle conduit à remettre en question le caractère personnel de l'obligation de signalement ainsi que les modalités de transmission au seul procureur de la République telles qu'elles ont été définies par la jurisprudence. De surcroît, cette obligation d'informer semble irréaliste dans le cas où les faits signalés portent sur des comportements ou dysfonctionnements qui mettent en cause la hiérarchie.

Un fonctionnaire peut-il transmettre son avis à son supérieur hiérarchique en lui laissant le soin de saisir le procureur ?

L'article 40, alinéa 2, crée certes une obligation de nature personnelle. Cependant, celle-ci n'est assortie d'aucun formalisme procédural, et, si les agents à l'origine du signalement ne disposent pas du choix de son destinataire, ils disposent de toute liberté sur les moyens de l'atteindre.

Cette solution est celle qui a été retenue par la jurisprudence. Dans un arrêt du 14 décembre 2000 [117], la Cour de cassation a admis la possibilité de transmettre à l'autorité supérieure cette obligation « dès lors que la dénonciation au procureur par le supérieur hiérarchique des enquêteurs de la direction départementale de la concurrence, de la consommation et de la répression des fraudes (DDCCRF) des faits délictueux qu'ils avaient constatés dans l'exercice de leurs fonctions, répond aux exigences de l'article 40 du Code de procédure pénale » [118].

Toutefois, il faut déduire de cette jurisprudence que l'agent ne sera délié de son obligation que lorsque son supérieur hiérarchique aura lui-même procédé dans les plus brefs délais à la transmission au procureur de la République. Si tel n'était pas le cas, il appartiendrait alors à l'agent d'effectuer lui-même le signalement.

Ce dernier cas de figure illustre bien les difficultés pratiques auxquelles peut se heurter la mise en œuvre de l'article 40, alinéa 2, du Code de procédure pénale. Au-delà des difficultés posées par l'articulation de cet article avec d'autres dispositifs juridiques, il existe aussi des raisons de fait qui expliquent un usage relativement modéré de la dénonciation au sein du secteur public.

L'article 40, alinéa 2, reste encore, de façon paradoxale, un dispositif faiblement opérationnel

a) La sous-utilisation de l'article 40, alinéa 2, dans le domaine des atteintes à l'intégrité

• Comme il a été indiqué précédemment, l'article 40, alinéa 2, est une disposition de portée générale

Elle s'applique à l'ensemble des agents publics en raison de leur participation à l'autorité publique. Par ailleurs, elle constitue une obligation avant tout personnelle : si la Cour de cassation a admis que la communication des faits délictueux pouvait être effectuée par le supérieur hiérarchique, elle a dans le même temps considéré que cette

117.Cass. crim., 14 décembre 2000, précité.

118.Cass. crim., 14 décembre 2000, X, *AJFP* 2001-4, p. 54.

communication n'impliquait pas pour autant un transfert de responsabilité conférant à l'autorité hiérarchique un pouvoir qui ne lui appartient pas, celui d'apprécier l'autorité de la révélation. Enfin, la jurisprudence tant judiciaire qu'administrative a régulièrement rappelé que cette obligation n'était soumise à aucun formalisme, et a dégagé des solutions destinées à faciliter cette transmission, et à protéger l'auteur du signalement.

Ainsi, la juridiction judiciaire a précisé que la déclaration de bonne foi ne saurait exposer le fonctionnaire à des poursuites du chef de délégation calomnieuses. La juridiction administrative stipule, pour sa part, que le licenciement d'un fonctionnaire municipal ne peut être justifié au seul motif qu'il aurait rempli les obligations lui incombant en application de l'article 40 du Code de procédure pénale sans en référer au préalable à sa hiérarchie [119]. Cette jurisprudence semble être de nature à favoriser le recours à l'article 40 du Code de procédure pénale, à en faciliter l'usage, et à en rendre l'application très fréquente.

De surcroît, la plupart des ministères, de leur côté, rappellent régulièrement à leurs agents le contenu de cette disposition.

Le ministère de la Justice a, par plusieurs circulaires, invité les magistrats du parquet à veiller, dans leur ressort, à une stricte application des dispositions légales, certes non pénalement sanctionnables, mais pouvant servir de fondement à des poursuites disciplinaires. Il les a également invités à développer, à l'échelon local, des protocoles de signalements des faits délictueux.

Le ministère des affaires étrangères, par exemple, a, pour sa part, sur son site Intranet et par télégramme diplomatique, attiré l'attention de l'ensemble de ses agents, en poste en France et à l'étranger, sur les obligations pesant sur eux du fait de l'article 40, alinéa 2.

Enfin, l'obligation de saisine du procureur de la République est régulièrement présentée par la France comme la pierre angulaire de la détection et de la lutte contre la corruption [120].

De ces éléments, il pourrait être déduit que l'article 40 est un procédé de droit commun, un moyen efficace et très courant de mise à jour des pratiques corruptrices. Force est de constater, pourtant, que la réalité des faits est plus nuancée et que cette disposition n'est souvent pas à la hauteur des espoirs que l'on pourrait y placer.

119. CE, 15 mars 1996, n° 146326, précité.

120. Cf. par exemple « Panorama des administrations 2009 », ou même les évaluations successives de la France par le GRECO.

• Le nombre de signalements reste encore relativement faible

Depuis 2008, le SCPC s'efforce, dans le cadre de sa mission de recensement des pratiques corruptrices, de prendre en compte l'ensemble des faits qui peuvent être portés à la connaissance de l'administration sans pour autant faire l'objet d'une transmission à l'autorité judiciaire.

Dans cette optique, le SCPC a interrogé les grands corps d'inspection ou de contrôle de l'administration afin de fournir une vue aussi objective que possible de l'étendue et de la typologie des atteintes à la probité dans la sphère publique (cf. chapitre I du présent rapport).

Si les réponses apportées par les différents ministères varient fortement, qualitativement comme quantitativement, il est frappant de constater que, sur l'ensemble des cas d'atteintes à la probité relevés par l'administration, peu d'entre eux donnent lieu à des suites pénales. Par exemple, sur les seize cas relevés en 2009 par le ministère de l'Éducation nationale, alors que tous ont fait l'objet de poursuites disciplinaires (dont deux révocations), un seul a fait l'objet d'une condamnation pénale.

Le SCPC a, plusieurs reprises, observé que « dans bien des cas, malgré la caractérisation évidente du délit, les directions centrales des administrations privilégient le règlement du conflit par la voie disciplinaire plutôt que par la voie pénale. Aussi, chaque année, des infractions concernant des atteintes à la probité échappent à l'autorité judiciaire et à toute quantification »[121]. Et « l'on peut très légitimement se poser la question de la réalité de son application complète et de la totale transparence des décisions entourant la transmission »[122].

b) En réalité, nombreux sont les facteurs qui expliquent cette très faible « externalisation » des dossiers d'atteinte à la probité

Certains de ces facteurs, d'ordre juridique, ont été exposés précédemment. Ils tiennent pour l'essentiel au fait que l'obligation de signalement prévue par article 40 n'est pas assortie de sanction et doit se confronter aux autres obligations qui incombent aux agents publics. En quelque sorte l'ordre public pénal est en concurrence avec l'ordre public administratif.

Mais le faible recours à l'article 40 ne s'explique pas seulement par des raisons juridiques. Les éléments d'explication à cette situation sont également de nature technique, sociologique, voire psychologique.

121.Rapport SCPC pour l'année 2009, p. 37.
122.Rapport SCPC pour l'année 2006, p. 45.

• Sur le plan technique, le premier motif, immédiatement perceptible, tient à la nature des atteintes à la probité

Celles-ci, et notamment la corruption, sont le plus souvent des infractions dissimulées, et donc difficiles à détecter, y compris par les agents de l'administration qui sont *a priori* les mieux placés pour le faire (corps de contrôle par exemple). C'est d'ailleurs bien souvent à la suite d'une dénonciation d'une des parties prenantes aux pratiques de corruption que les faits sont mis à jour. Par ailleurs, la plupart des contrôles administratifs ne sont pas systématiques mais aléatoires, et n'ont pas pour finalité la détection des atteintes à la probité. Ils portent sur la conformité d'un ensemble d'actes ou d'opérations à des règles dont le non-respect peut par ailleurs révéler des pratiques corruptrices. C'est ici que le terme « dans l'exercice de ses fonctions » prend tout son ensemble. Il n'existe pas en France de corps de contrôle uniquement dédié à la traque des pratiques corruptrices [123], mais un ensemble de contrôles internes ou externes à l'administration, dont certains portent sur des secteurs d'activité (marchés publics, urbanisme) plus propices à la corruption ou des fonctions/disciplines (fiscalité, comptabilité publique ou privée, concurrence…) qui peuvent en constituer le support et/ou le révélateur [124]. Le hasard joue donc un rôle important, mais aussi les techniques de contrôle employées, leur étendue [125] ainsi que, très souvent la plus ou moins grande curiosité ou perspicacité des agents contrôleurs. À l'inverse, et très logiquement, l'absence de contrôles, leur réorientation, leur relâchement [126], ou, plus prosaïquement, l'insuffisante sensibilisation des corps de contrôle aux aspects pénaux de leur activité [127] créent des zones de basse pression peu propices au recours à l'article 40.

Toujours sur le plan technique, l'évolution des formes de la corruption et des moyens employés par les corrupteurs/corrompus peut aussi constituer une explication. La corruption, dans ses formes les plus contemporaines, n'est plus seulement un acte dissimulé, mais de plus en plus un acte bien

123. L'OCDE notamment ayant reproché à la France de ne pas avoir une approche « intégrée » de la lutte contre la corruption.

124. Des études économiques ont par exemple montré le lien privilégié qui existe traditionnellement entre pratiques anticoncurrentielles (ententes) et pratiques de corruption, notamment dans les marchés publics (cf. travaux d'Ariane Lambert-Mogiliansky).

125. Par exemple, le droit de suite dont disposent les juridictions financières, particulièrement précieux pour mettre à jour certaines dérives (gestion de fait) dans les satellites des collectivités publiques.

126. À titre d'exemple, le fait que depuis 2004 les agents de la DGCCRF ne participent plus systématiquement aux réunions des commissions d'appel d'offres.

127. Malgré les circulaires précitées, il apparaît que l'article 40 reste encore largement méconnu de la part des agents publics, ce qui d'ailleurs a incité le GRECO à « recommander de rappeler aux administrations publiques et à l'ensemble des agents publics l'existence et la portée de l'article 40 du CPP et faciliter son utilisation sans entrave dans les affaires de corruption » (Rapport du premier cycle d'évaluation de la France, 13-17 octobre 2003).

souvent indétectable, indécelable car dématérialisé [128] et extraterritorial [129]. Toutes formes de corruption en face desquelles les administrations et leurs méthodes de contrôle et d'investigation traditionnelles se trouvent insuffisamment armées, et qui impliquent des recherches et des démarches qui impliquent nécessairement, non seulement que l'autorité judiciaire ait été alertée, mais qu'elle ait pris des actes qui rendent possible des investigations approfondies [130].

La méthode des « indicateurs de risques », particulièrement utiles pour les pratiques relativement traditionnelles, trouve vite ses limites dans un monde sans frontières et dominé par le virtuel [131].

• Sur le plan sociologique, également, on a déjà évoqué largement les difficultés liées à la confrontation d'une norme pénale avec des dispositions et un environnement largement dominés par le droit public

Le paradoxe n'est qu'apparent et en grande partie marqué par des césures relativement artificielles. On pourrait du reste très bien imaginer que l'article 40, alinéa 2, trouve sa place davantage dans la partie « obligations » du statut général que dans le Code de procédure pénale [132]. La difficulté tient davantage dans le fait que l'obligation de signalement est, parmi l'ensemble des obligations qui s'imposent aux agents publics, l'une des rares à se traduire par une obligation individuelle à agir. Les obligations les plus importantes qui s'imposent aux fonctionnaires (obéissance, secret, discrétion, neutralité…) sont passives et le plus souvent soumises à la hiérarchie du fonctionnaire. Être un bon agent public, c'est d'abord ne pas agir dans un sens négatif avant d'agir dans un sens positif. Dans ce contexte, le signalement, qui suppose une part de liberté d'appréciation n'est pas un réflexe naturel chez les agents publics. À cela s'ajoute le poids des conservatismes ou des habitudes qui explique sans doute les risques d'inhibition déjà relevés par le SCPC [133]. Mais il y a d'autres facteurs d'explication tels que par exemple les méthodes de travail propres à

128. Cf. article sur les paris et jeux sur Internet (Rapport SCPC 2008).

129. On pense naturellement aux problèmes posés par la corruption internationale, pour lesquels, du moins dans le cas français, l'alerte institutionnelle (TRACFIN) joue un rôle essentiel, comme alternative à l'alerte individuelle, le plus souvent « privée » (salarié ou ex-salarié d'une entreprise).

130. Contraintes qui expliquent – sans pour autant la justifier – la pratique fréquente des signalements de régularisation par les services enquêteurs.

131. Cf. par exemple les développements relatifs aux *subprimes* dans le rapport du SCPC pour l'année 2008.

132. On observera que cette solution est, comme on l'a vu dans la première partie, celle retenue dans les pays dont les dispositifs sur le signalement s'appliquent indifféremment au secteur public et au secteur privé.

133. Rapport 2006, p. 48.

telle structure ou à telle administration [134] ou, plus largement la peur de perdre la maîtrise d'un dossier, qui peut être traité en interne (par la voie disciplinaire) en évitant les aléas et la médiatisation qui entourent une procédure judiciaire, ou au moyen de sanctions administratives considérées comme suffisamment dissuasives (administration fiscale, autorité de la concurrence…).

À l'inverse, une transmission à l'autorité judiciaire peut susciter chez l'agent public des craintes à l'égard d'un milieu qui lui est étranger, à la fois redouté (pour ses conséquences sur les libertés) [135] et décrié (pour sa supposée lenteur ou inefficacité). Dans de nombreuses administrations, la peur de la perte de la maîtrise d'un dossier ou d'une procédure, *a fortiori* lorsqu'il existe des sanctions alternatives (disciplinaires notamment) explique sans doute pour une large part les réticences à utiliser l'article 40, alinéa 2, du Code de procédure pénale.

• Enfin, il existe des raisons plus directement psychologiques

Le signalement nécessite de la part de l'agent public un acte positif. Il implique une démarche qui doit se traduire par un écrit ou un contact avec l'autorité judiciaire. Et c'est un acte qui peut être lourd de conséquences pour l'agent, tant au plan judiciaire que dans son activité professionnelle.

Au plan judiciaire, l'agent peut, si une suite pénale est donnée à son signalement, se voir cité comme témoin, et devenir en quelque sorte une des parties prenantes à l'affaire, voir son nom cité, exposé sous le feu des médias [136], ce qui déroge à la culture de l'anonymat et de l'« impersonnalisation » encore largement répandue encore l'administration française.

Le risque existe encore, même s'il doit être relativisé, de se voir condamné pour dénonciation calomnieuse ou même de subir une contre-offensive judiciaire [137] des personnes que son signalement aurait conduit à mettre en cause.

134. Par exemple, la crainte au sein des administrations fiscales des risques d'annulation pour détournement de procédure si des éléments de fraude fiscale apparaissaient dans une procédure initiée sur un signalement faute d'avis préalable de la commission des infractions fiscales (cf. Rapport SCPC 2006, p. 48).

135. Selon l'idée que dénoncer, c'est être déjà un peu complice, idée entretenue dans certains secteurs par des procédures telles que la procédure de clémence (un complice dénonce les autres).

136. Comme cela a, par exemple, été le cas des agents publics mis en cause dans l'affaire dite « de l'amiante », et ce avant même que leur responsabilité ne soit engagée par la justice.

137. Comme d'ailleurs les magistrats en charge du dossier. Antoine Garapon relève, à propos de l'affaire Pasqua, que « les plaintes déposées contre des magistrats par des hommes politiques se multiplient et donnent l'impression d'un corps à corps que plus rien ne peut arbitrer… » (A. Garapon, *Le Gardien des promesses. Justice et République*, Odile Jacob, 1996).

Mais le risque le plus élevé pour l'agent public qui dénonce est naturellement celui des représailles tant dans sa vie professionnelle que personnelle [138]. Les études de droit comparé montrent d'ailleurs que ce risque est récurrent, et que n'en sont pas indemnes les pays qui disposent des législations les plus robustes, c'est-à-dire qui ont prévu des dispositifs de protection des lanceurs d'alerte.

Néanmoins, la France se trouve aujourd'hui dans une situation paradoxale. Alors que la plupart des organisations internationales recommandent la protection du lanceur d'alerte, dans le secteur public comme dans le secteur privé [139], son droit positif ne comporte pas de disposition prévoyant de manière explicite la protection de l'agent public lanceur d'alerte [140].

Le risque de représailles, sous différentes formes (mutation, rétrogradation…) est loin d'être théorique pour l'agent public qui dénonce [141].

Le lanceur d'alerte dans le secteur privé : une mise en œuvre subordonnée à la protection des droits des salariés

Les salariés du secteur privé ne sont pas en France, contrairement aux salariés du secteur public, tenus de signaler les délits dont ils auraient eu connaissance. S'il n'existe pas de disposition de portée générale, certaines professions réglementées, telles que par exemple les professions du chiffre (experts comptables, commissaires aux comptes) se sont vu imposer l'obligation de signaler certaines infractions.

Cependant, la portée de ce signalement reste limitée :

– l'obligation de signaler les délits au procureur de la République ne s'applique qu'aux seuls commissaires aux comptes.

138. On peut cependant supposer – de manière empirique, car c'est une étude qui reste à faire – que l'échelle et la nature des risques varient selon que le signalement porte sur des dysfonctionnements internes à l'administration, ou qu'il concerne des dérives qui lui sont externes.

139. Cf. par exemple le Plan d'action contre la corruption du G20 précité.

140. La « protection fonctionnelle » prévue par l'article 11 de la loi n° 83-634 du 13 juillet 1983 apparaissant inadaptée dans la mesure où elle ne concerne que les faits les plus graves (menaces, violences, voies de fait, injures, diffamations ou outrages) et ne couvre pas le risque le plus fréquemment rencontré dans ce type d'affaire qui est la « placardisation » du lanceur d'alerte, même si des progrès ont été accomplis dans la protection contre le harcèlement par exemple.

141. Phénomène difficile à appréhender mais bien réel, comme en témoignent certaines affaires fortement médiatisées (cf. par exemple le cas d'un ex-responsable des services vétérinaires du Haut-Rhin s'estimant sanctionné depuis près de vingt ans pour avoir dénoncé des collègues pour des faits de corruption lors de contrôles en douane, rapporté par *L'Est Républicain* du 26 mars 2012)…

L'article L. 820-7 du Code de commerce réprime de peines contraventionnelles « le fait, pour toute personne exerçant les fonctions de commissaire aux comptes… de ne pas révéler au procureur de la République les faits délictueux dont elle a eu connaissance ».
On notera que cette obligation est, contrairement à celle figurant à l'article 40 du Code de procédure pénale, définie de façon négative, par la sanction qui s'applique en cas de non-signalement ;

– pour le reste, l'obligation de signaler qui s'applique aux professions du chiffre ne porte généralement pas sur les délits eux-mêmes, mais sur des comportements en lien avec d'éventuels délits[142] ou sur des infractions « masquantes » (faux, abus de biens sociaux…).

Par ailleurs, dans le premier cas, le signalement doit être effectué, non pas directement auprès de l'autorité judiciaire, mais auprès d'un service administratif, TRACFIN, charge à ce dernier de saisir les autorités judiciaires sur le fondement de l'article 40.

Il n'y a pas lieu, dans le cadre de cet article, de développer les problèmes très spécifiques posés par ces dispositifs de signalement, qui, au demeurant, n'ont pas pour finalité de détecter les pratiques corruptrices, mais de lutter contre le blanchiment d'argent, ou d'assurer la protection des actionnaires.

Au final, la part des signalements émanant des professionnels du chiffre représente pour l'instant une part très marginale de l'ensemble des signalements. Ces signalements trouvent leur utilité pour les schémas de corruption relativement simples, qui supposent que leurs auteurs aient effectué des opérations financières sur le territoire national ou à partir du territoire national[143].

Pour le reste, les mécanismes de signalement dans le secteur privé s'inscrivent dans des dispositifs volontaires, inclus ou non dans des chartes éthiques. Les premiers dispositifs qui se sont mis en place au sein des entreprises françaises n'en soulèvent pas moins certaines difficultés, qui tiennent pour l'essentiel, à leur conciliation avec les normes protégeant la vie privée des salariés.

142. Ainsi, en vertu de l'article L. 562-1 (11°) du Code monétaire et financier, les commissaires aux comptes et experts comptables se sont vu imposer l'obligation de déclarer les « sommes/opérations qui portent sur des sommes qui pourraient provenir… de la corruption ».

143. Par exemple, retrait ou dépôt auprès d'agences bancaires de fortes sommes en espèces destinées ou provenant de pratiques corruptrices. À titre d'illustration, les trois affaires de corruption d'agents publics étrangers jugées en France (au 10 avril 2012), ont été instruites sur la base de déclarations de soupçon adressées par les banques à TRACFIN.

Les dispositifs de signalement du secteur privé restent encore peu développés

En France, les dispositifs d'alerte professionnels sont pendant longtemps restés embryonnaires

Sur une tendance longue, on constate une faible propension des salariés du secteur privé à dénoncer les fraudes internes aux entreprises, ou les pratiques corruptrices auxquelles ses représentants pourraient se livrer. À cette situation, les motifs généralement invoqués sont de deux ordres : économiques (peur d'être licencié ou de mettre en péril l'activité économique de la société) ou d'ordre culturel (souvenir de l'Occupation, les pays latins comme la France seraient moins imprégnés que les pays anglo-saxons d'une culture de transparence et de sincérité).

La question a pu se poser également, en des termes identiques au secteur public, de savoir dans quelle mesure la dénonciation par le salarié de son employeur ou de sa hiérarchie était compatible avec le devoir de loyauté auquel il est astreint.

Jusqu'au début des années 2000, la dénonciation n'était légitimée par le Code du travail que dans des hypothèses limitées :

– signalement de mesures discriminatoires (articles L. 1132-3 et L. 1132-4 du Code du travail) ;
– signalement de harcèlement sexuel (articles L. 1153-3 et L. 1153-4 du Code du travail) ;
– signalement de harcèlement moral (articles L. 1152-2 et L. 1152-3 du Code du travail).

Mais, même dans ces cas précis, la loi n'avait pas prévu une obligation de signaler, mais seulement la protection de ceux qui acceptent de témoigner contre d'éventuelles représailles (sanction, licenciement). Autrement dit, par rapport au secteur public, et notamment à l'article 40 du Code de procédure pénale, le signalement dans le secteur privé est appréhendé dans une logique différente : alors que dans le secteur public, le signalement constitue un devoir pour l'agent public, dans le secteur privé, il est une manifestation du droit d'expression du salarié et doit, à ce titre, bénéficier d'une protection.

En dehors de ces hypothèses spécifiques, les salariés bénéficient également :

– d'un droit d'expression générale directe et collective (article L. 2281-3 du Code du travail) ;
– d'un droit de retrait « d'une situation dont ils [les salariés] avaient un motif raisonnable de penser qu'elle présentait un danger grave et imminent pour la vie ou pour la santé de chacun d'eux » (article L. 4131-3).

Ces dispositifs apparaissaient cependant insuffisants, et l'OCDE a pu relever en 2004[144] que « la loi (française) ne vient pas vraiment non plus en aide aux salariés qui, témoins de malversations, souhaiteraient en avertir les autorités compétentes ». En particulier, elle relève que « rien n'est prévu pour un salarié qui voudrait dénoncer un acte de corruption ou une fraude comptable ».

La jurisprudence a, de son côté, adopté une position qui n'a pas non plus contribué à faciliter la dénonciation par des salariés.

La question s'est en effet posée de savoir si une protection similaire à celle exposée précédemment pouvait bénéficier aux salariés qui dénoncent d'autres types d'agissements que ceux prévus par le Code du travail, et notamment des faits de corruption.

La jurisprudence y a apporté une réponse nuancée. Certes, la Cour de cassation a considéré que le fait de dénoncer à la justice des agissements caractérisant une infraction pénale (détournement de fonds[145], maltraitance de handicapés[146]) ne constituait pas en tant que telle une faute grave motivant un licenciement. Mais elle a, dans les deux cas cités, assorti cette position d'une réserve en reprochant au juge du fond de ne pas « avoir recherché si la dénonciation formulée par le salarié était mensongère ou non, et, dans l'affirmative, si le salarié avait agi de mauvaise foi »[147]. On pouvait donc considérer, *a contrario*, qu'une dénonciation de mauvaise foi pouvait constituer une faute susceptible d'entraîner un licenciement.

En revanche, la jurisprudence a fait preuve d'une grande souplesse pour ce qui concerne le destinataire des accusations. Celui-ci peut être l'inspecteur du travail[148], le parquet[149] ou encore le président-directeur général[150].

Une autre option s'est ouverte au salarié : celle de faire appel, dans le cadre du droit d'expression de l'article L. 2281-3 du Code du travail, aux structures collectives telles que les syndicats, à charge pour ces derniers de se constituer partie civile pour demander une enquête. Toutefois, cette voie reste encore peu utilisée, notamment en raison de l'encadrement tant législatif que jurisprudentiel dont fait l'objet la constitution de partie civile.

144. Dans son rapport dit de « phase 2 » sur l'application de la convention sur la lutte contre la corruption d'agents publics étrangers dans les transactions commerciales internationales.

145. Cass. soc., 14 mars 2000, n° 1285.

146. Cass. soc.,, 12 juillet 2006, n° 04-41.075.

147. *Ibidem*, décisions précitées. On observera que dans la première décision, il est reproché aux juges du fond de ne pas avoir vérifié, outre la « mauvaise foi », la « légèreté » du salarié qui dénonce.

148. Cass. soc., 14 mars 2000, n° 97-43.268, Pitron/Cunéaz.

149. Cass. soc., 12 juillet 2006, n° 04-41.075.

150. Cass. soc., 8 novembre 2006, n° 05-41.504.

De la même façon, le salarié français a pu également bénéficier des avancées significatives de notre droit dans le domaine de la protection des témoins. Ces dispositifs légaux, destinés notamment à protéger l'anonymat des témoins [151], sont toutefois subordonnés à des conditions de fond (mise en danger de la vie ou de l'intégrité physique de cette personne, des membres de sa famille ou de ses proches) et de forme (ouverture d'une procédure relative à un crime ou à un délit puni d'au moins trois ans) particulièrement lourdes et qui en rendent la mise en œuvre difficile [152].

À cela s'ajoute le fait que le salarié qui dénonce s'expose, comme dans le secteur public, au risque d'être poursuivi pour dénonciation calomnieuse (prévue par l'article 226-10 du Code pénal), même si, dans les faits, ce risque reste relativement théorique [153], ou faire l'objet d'une sanction disciplinaire sur le fondement d'un manquement au devoir de loyauté que le salarié doit à son entreprise [154].

L'ensemble de ces éléments explique que, pendant longtemps, seule une minorité d'entreprises ont mis en place des dispositifs d'alerte interne dédiés au signalement de la corruption. La plupart se sont bornées à énumérer un ensemble de règles ou valeurs éthiques ou ont considéré que les mécanismes de contrôle ou d'audit internes « de droit commun » suffisaient à faire émerger des cas de malversations ou de pratiques corruptrices.

La mise en place de dispositifs d'alerte professionnels a été stimulée par le droit international.

a) La profession de l'audit a édicté une série de normes dont certaines portent sur la déontologie et le signalement. L'une de ces normes (modalités pratiques d'application) traite de la « communication d'informations sensibles par la voie hiérarchique ou en marge de celle-ci ».

Cependant, ces normes restent des bonnes pratiques spécifiques à une profession et n'ont pas de valeur contraignante. Les organismes qui en sont les promoteurs (IIA et IFACI) prennent bien soin de préciser que la MPA 2440-3 vise à « stimuler la réflexion et qu'ils ne sont pas responsables de l'usage qui en sera fait ». En conséquence « l'auditeur

151. La principale disposition est l'article 706-60 du Code de procédure pénale, créé par la loi n° 2001-1062 du 15 novembre 2001.

152. Une autre difficulté provient du fait que l'anonymat du témoignage pouvant remettre en cause le caractère équitable du procès, la Cour européenne de Strasbourg subordonne la validité du témoignage anonyme à un certain nombre de conditions (14 février 2002, Visser c/Pays-Bas).

153. Compte tenu des exigences posées par la jurisprudence pour la mise en œuvre de ce délit.

154. Cour de cassation du 12 juillet 2006.

interne devra faire preuve de la plus grande circonspection… avant de décider de court-circuiter sa hiérarchie, et *a fortiori* de communiquer des informations à l'extérieur »[155].

De fait, la mission d'alerte de l'auditeur interne est étroitement circonscrite :

- d'une part, elle ne porte que sur les organes de décision interne (direction générale, conseil d'administration, comité d'audit) ;
- d'autre part, elle ne concerne que les faits graves commis par la direction générale et susceptibles d'affecter la continuité d'exploitation ;
- enfin, l'alerte doit être effectuée auprès du comité d'audit, mais en aucun cas auprès d'instances externes (régulateurs, commissaires aux comptes). Autrement dit, seul le signalement interne est admis.

Cette approche très précautionneuse du signalement a toutefois été influencée par la mise en œuvre, d'abord aux États-Unis puis en France, des dispositions de la loi adoptée aux USA Sarbanes-Oxley, dite SOX. Cette loi du 31 juillet 2002, intervenue peu après le scandale financier de l'entreprise ENRON, prévoit notamment l'obligation pour les entreprises américaines et leurs filiales de mettre en place des codes de conduite internes et un système de surveillance collective par déclenchement d'alerte afin de pallier la défaillance des systèmes de contrôle internes des entreprises. Par ailleurs, l'article 808 de la loi a posé le principe de protection des lanceurs d'alerte.

Les entreprises américaines avaient trois ans pour se mettre en conformité avec les nouvelles règles imposées par la Securities and Exchange Commission (SEC) pour mettre en œuvre la loi SOX. Les entreprises étrangères cotées aux États-Unis disposaient d'un an de plus.

Après plusieurs années d'incertitudes et de débats, l'Europe et la France ont adopté des textes et mis en place des dispositifs destinés à permettre aux entreprises américaines implantées en Europe ainsi qu'à leurs filiales de se mettre en conformité avec les prescriptions de la loi SOX.

C'est dans ce contexte que se sont développés les dispositifs d'alerte en France et dans les autres pays européens : ainsi, fin 2008, plus de 1 200 entreprises françaises avaient déposé une déclaration de mise place de dispositifs d'alerte.

155. Revue *Audit* n° 179, avril 2006, p. 23.

b) Le droit français s'est parallèlement engagé sur la voie d'un encadrement de « l'alerte éthique »

Cet encadrement, préconisé par le rapport Antonmattei-Vivien de janvier 2007[156], s'est traduit par un renforcement de la protection du lanceur d'alerte. À la suite de ce rapport, la loi n° 2007-1598 du 13 novembre 2007 a introduit dans le Code du travail l'article L. 1161-1 qui instaure une protection juridique du salarié lanceur d'alerte.

Cet article prévoit :

« Aucune personne ne peut être écartée d'une procédure de recrutement ou de l'accès à un stage ou à une période de formation en entreprise, aucun salarié ne peut être sanctionné, licencié ou faire l'objet d'une mesure discriminatoire, directe ou indirecte, notamment en matière de rémunération, de formation, de reclassement, d'affectation, de qualification, de classification, de promotion professionnelle, de mutation ou de renouvellement de contrat pour avoir relaté ou témoigné, de bonne foi, soit à son employeur, soit aux autorités judiciaires ou administratives, de faits de corruption dont il aurait eu connaissance dans l'exercice de ses fonctions.

Toute rupture du contrat de travail qui en résulterait, toute disposition ou tout acte contraire est nul de plein droit.

En cas de litige relatif à l'application des deux premiers alinéas, dès lors que le salarié concerné ou le candidat à un recrutement, à un stage ou à une période de formation en entreprise établit des faits qui permettent de présumer qu'il a relaté ou témoigné de faits de corruption, il incombe à la partie défenderesse, au vu de ces éléments, de prouver que sa décision est justifiée par des éléments objectifs étrangers aux déclarations ou au témoignage du salarié. Le juge forme sa conviction après avoir ordonné, en cas de besoin, toutes les mesures d'instruction qu'il estime utiles. »

Cette disposition met un terme aux incertitudes jurisprudentielles précédemment évoquées concernant l'immunité dont bénéficie le lanceur d'alerte. Elle prévoit en effet explicitement que cette immunité n'est accordée qu'aux salariés de bonne foi et que celle-ci est présumée[157]. En conséquence, la mauvaise foi du salarié ne peut pas résulter de la seule circonstance que les faits dénoncés ne sont pas établis.

156. « Chartes d'éthique, alerte professionnelle et droit du travail français : état des lieux et perspectives » : rapport établi par MM. Antonmattei et Vien et remis à M. Gérard Larcher, ministre délégué à l'Emploi, au Travail et à l'Insertion professionnelle des jeunes, janvier 2007.

157. Solution sur laquelle s'est également alignée la jurisprudence de la Cour de cassation sur le harcèlement moral (cf. par exemple Cass. soc., 10 mars 2009, n° 07-44.092, *Bull.* 2009).

On peut considérer que ce texte, à l'instar des dispositions précédemment évoquées relatives au harcèlement moral, sexuel et à la lutte contre la discrimination, s'inscrit « dans un mouvement législatif plus large qui tend à protéger le droit d'expression des salariés, lorsque celui-ci est exercé aux dépens d'autres salariés ou de supérieurs hiérarchiques, pour la défense d'un intérêt public » [158].

Cette disposition ne répond pas seulement à l'intérêt du salarié, mais également à celle de l'employeur. Comme le relève la Cour de cassation [159], « cette immunité doit également être mise en relation avec les obligations qui pèsent sur l'employeur pour prévenir et traiter les agissements [de harcèlement moral]… ».

Cette solution correspond à celle retenue dans les pays ayant instauré une protection du lanceur d'alerte. Elle est également conforme aux préconisations de la plupart des organisations internationales en la matière, et en particulier du Conseil de l'Europe [160] et du groupe de travail de l'OCDE contre la corruption qui, au regard du faible nombre de dénonciations par des salariés des entreprises françaises en matière de corruption et autre délits de la vie des affaires, avait recommandé à la France d'introduire des « mesures de protection plus fortes pour les salariés qui révèlent des faits suspects de corruption, de façon à encourager ces personnes à déclarer de tels faits sans la crainte de représailles de licenciement » [161].

Il n'existe pas pour l'instant de mécanismes d'évaluation de ces dispositifs existants en France. Ainsi, le SCPC relevait en 2006 « qu'une tonalité négative ou dubitative est de rigueur ». L'explication principale en est que « les modalités de mise en œuvre de l'alerte interne diffèrent grandement d'une entreprise à l'autre ». Selon les entreprises, cette mise en œuvre peut se traduire par la création d'une ligne téléphonique dite éthique ou d'une adresse spécifique à laquelle les salariés peuvent envoyer une révélation écrite.

D'autre part, à l'instar du secteur public, le risque est celui d'un traitement purement interne. Dans le secteur privé comme dans le secteur public, on trouve les mêmes réticences et résistances à la dénonciation, comme en témoignent d'ailleurs certaines enquêtes.

158. Commentaire fait à propos de la protection de l'auteur du signalement des cas de harcèlement moral (art. L. 1152-2 du Code du travail), dans *Jurisprudence sociale Lamy*, n° 306, 27 septembre 2011, p. 6.

159. Rapport de la Cour de cassation de 2009, rapporté dans article précité.

160. Article 9 de la convention civile contre la corruption.

161. Recommandation n° 5 du Rapport de phase 2 sur la France.

Ces réticences s'expliquent également par l'existence d'un cadre juridique particulièrement strict.

La mise en place d'un dispositif d'alerte est soumise à d'importantes contraintes juridiques

Les dispositifs d'alerte, qui ont émergé sous l'influence du droit américain, constituent un concept nouveau pour le droit continental, et en particulier pour le droit français. De fait, il n'existe pas de définition des dispositifs d'alerte, pas plus qu'il n'existe de dispositif juridique les régissant. Toutefois, les dispositifs d'alerte n'échappent pas totalement au droit. « Ils se trouvent même au cœur d'une interpénétration complexe de différents champs juridiques (droit du travail, droit pénal des affaires, loi informatique et libertés, etc.) » [162].

Cependant, en France, le débat s'est principalement porté sur le terrain de la protection des libertés individuelles. Ces dispositifs nécessitant en effet, pour la plupart, la création de fichiers nominatifs, la question s'est posée très rapidement de leur compatibilité avec les prescriptions de la loi informatique et libertés [163].

Dans un premier temps, la Commission nationale de l'informatique et des libertés (CNIL) et certains tribunaux ont marqué leur hostilité face à ce type de dispositifs

Ainsi, en mai 2005, la CNIL a rejeté deux demandes d'autorisation pour la mise en œuvre de dispositifs d'intégrité [164], aux motifs notamment qu'ils pourraient « conduire à un système organisé de délation professionnelle », « que la possibilité de réaliser une "alerte éthique" de façon anonyme ne pourrait que renforcer le risque de dénonciation calomnieuse ». Au surplus, la commission a estimé que ce dispositif était « disproportionné au regard des objectifs poursuivis et… que d'autres moyens prévus par la loi existent d'ores et déjà afin de garantir le respect des dispositions légales et des règles fixées par l'entreprise ».

Enfin, la commission a relevé que les employés objets d'un signalement ne seraient, par définition, pas informés dès l'enregistrement de données mettant en cause leur intégrité professionnelle ou de citoyen, et n'auraient

162. Circulaire de la Direction générale du travail n° 2008-22 du 19 novembre 2008 relative aux chartes éthiques, dispositifs d'alerte professionnelle et au règlement intérieur.

163. Loi n° 78-17 du 6 janvier 1978 ; le respect de cette loi est assuré par une autorité administrative indépendante, la Commission nationale de l'informatique et des libertés (CNIL).

164. Demandes formulées respectivement par la société Mc Donald's France et par la Cie européenne d'accumulateurs.

donc pas les moyens de s'opposer à ce traitement de données les concernant »[165].

La position de la CNIL s'est par la suite assouplie afin de permettre une harmonisation des pratiques françaises avec les exigences formulées par les autorités américaines.

Elle a publié le 10 novembre 2005 un document d'orientation précisant les conditions que doivent remplir les dispositifs d'alerte professionnelle pour être conformes à la loi du 6 janvier 1978. Dans ce document, la CNIL indique « qu'elle n'a pas d'opposition de principe à de tels dispositifs dès lors que les droits des personnes mises en cause directement ou indirectement dans une alerte, sont garantis au regard des règles relatives à la protection des données personnelles ».

Les entreprises doivent pour cela s'engager à respecter un ensemble de règles :

– restreindre le champ du dispositif d'alerte au domaine comptable, du contrôle des comptes, bancaire et de la lutte contre la corruption. La mise en place de dispositifs d'alerte est acceptable quand elle répond soit à une obligation législative ou réglementaire de droit français visant à l'établissement de procédures de contrôle interne (domaine bancaire par exemple), soit à un intérêt dont la légitimité est bien établie (domaine comptable, contrôle des comptes, mais aussi lutte contre la corruption) ;
– ne pas encourager les dénonciations anonymes.

La CNIL privilégie à l'anonymat une identification de l'émetteur de l'alerte et un traitement confidentiel de celle-ci. En cas d'alertes anonymes, la CNIL préconise que le traitement de ces alertes fasse l'objet de « précautions particulières ».

• Mettre en place une organisation spécifique pour recueillir et traiter les alertes : une organisation spécifique doit être mise en place au sein de l'entreprise pour traiter ces questions, notamment en limitant autant que possible la circulation des informations.

• Informer la personne concernée dès que les preuves ont été préservées, afin qu'elle puisse demander à exercer ses droits d'opposition, d'accès et de rectification.

• Enfin, le recours au dispositif d'alerte doit rester facultatif et doit intervenir en complément des autres canaux d'alerte existants : hiérarchie, commissaires aux comptes, représentants du personnel, autorités publiques.

165. Délibérations CNIL n° 2005-100 et 2005-111.

Ce document d'orientation a servi de base à l'avis, adopté le 1er février 2006, par le groupe des autorités européennes de protection des données personnelles – dit groupe de l'article 29 [166].

Par la suite, la CNIL a, par délibération du 8 décembre 2005 [167], adopté une décision d'autorisation unique de traitement automatisé de données à caractère personnel mis en œuvre dans le cadre de dispositifs d'alerte professionnelle [168].

La durée de conservation des données ne doit pas excéder deux mois à compter de la clôture des opérations de vérification si aucune suite n'est donnée. Si une procédure est engagée, les données sont conservées jusqu'à son terme. L'information des personnes impliquées par ce dispositif ainsi que les mesures de sécurité mises en œuvre sont définies de manière précise.

La procédure de mise en œuvre du dispositif d'alerte professionnelle a été précisée par une circulaire du ministère du Travail du 19 novembre 2008 [169].

Cette circulaire rappelle que l'alerte professionnelle peut être mise en place par décision unilatérale de l'employeur ou par voie négociée (au niveau de la branche, du groupe, de l'entreprise ou de l'établissement).

Pour être licite, le dispositif doit avoir fait l'objet d'une déclaration ou d'une autorisation de la CNIL, au titre de l'article 25-I-4° de la loi du 6 janvier 1978 modifiée.

En application de la délibération du 8 décembre 2005, cette formalité s'accomplit :
- soit par une déclaration d'engagement de conformité à la décision d'autorisation unique du 8 décembre 2005 (lorsque les dispositifs d'alerte sont mis en place en réponse à une obligation légale) ;
- soit après autorisation formelle de la CNIL, si le dispositif d'alerte est mis en place en l'absence d'obligation législative ou réglementaire ou établit une procédure de contrôle interne de faits portant sur d'autres domaines que financier, comptable, bancaire et de lutte contre la corruption.

166. Avis du 1er février 2006 sur les dispositifs d'alerte professionnelle dans les domaines bancaire, comptable, du contrôle interne des comptes, de l'audit et de la lutte contre la corruption et les délits financiers.

167. Délibération CNIL no 2005-305 du 8 décembre 2006, publiée au *JO* no 3 du 4 janvier 2006.

168. L'autorisation unique no 4 concerne les dispositifs d'alerte professionnelle qui permettent aux employés de signaler à leur employeur des comportements qui seraient contraires aux règles de droit français applicables dans les domaines financier, comptable, bancaire et de la lutte contre la corruption et d'organiser la vérification de l'alerte au sein de l'organisme concerné.

169. Circulaire de la Direction générale du travail no 2008-22 du 19 novembre 2008, précitée.

Le dispositif doit faire aussi l'objet d'une consultation du comité d'entreprise au titre de l'article L. 1222-4 du Code du travail (dispositif permettant le contrôle de l'activité des salariés) et éventuellement consultation du comité d'hygiène, de sécurité et des conditions de travail (CHSCT).

Les salariés doivent enfin être informés individuellement de la mise en place du dispositif, de ses caractéristiques (champ d'application, identité du responsable, protection du lanceur d'alerte, confidentialité du traitement, cas des alertes anonymes…) au titre de l'article L. 1222-4 en application de la loi informatique et libertés.

Les contrôles exercés sur les dispositifs d'alerte

Dans sa circulaire du 19 novembre 2008, le ministère du Travail a rappelé que trois types de contrôles étaient susceptibles de s'exercer sur les dispositifs d'alerte :

a) Un contrôle administratif exercé par l'inspection du travail

La DGT rappelle tout d'abord que « le système d'alerte étant dépourvu de caractère obligatoire, il ne relève pas de la discipline et, par conséquent, n'entre pas dans le champ du règlement intérieur ». En revanche, il appartient aux inspecteurs du travail de rappeler, le cas échéant, aux employeurs les prérogatives des institutions représentatives du personnel (par exemple, information et consultation du comité d'entreprise), et de vérifier la conformité des dispositions de l'alerte professionnelle au Code du travail (par exemple, information individuelle, contenu non discriminatoire…).

b) Le contrôle par le juge judiciaire

Le non-respect des obligations tirées de la loi du 6 janvier 1978 peut être pénalement sanctionné. Le juge vérifie également la conformité du système mis en place aux dispositions de la délibération du 8 décembre 2005, tant dans ses aspects procéduraux que sur le fond. Ainsi, la Cour de cassation a rappelé que le non-respect des formalités préalables auprès de la CNIL rendait le dispositif et les preuves ainsi recueillies inopposables [170].

S'agissant du contenu des dispositifs d'alerte, plusieurs décisions ont enjoint le retrait de dispositifs d'alerte à raison « de la seule existence d'un dommage potentiel imminent pour les libertés individuelles de salariés victimes de dénonciations anonymes recueillies par le biais d'un dispositif privé échappant à tout contrôler » [171] ou la suspension de la diffusion d'un

170. Cass. soc. 6 avril 2004, n° 01-45.227.

171. Ordonnance de référé 09/2005 du TGI de Libourne.

questionnaire intitulé *business ethics* que les salariés avaient l'obligation de remplir, alors que la délibération de la CNIL du 8 décembre 2005 avaient précisé que ne pourraient bénéficier du régime d'autorisation unique « que les dispositifs d'alerte ne présentant pas un caractère obligatoire » [172]. De même, le juge peut annuler un dispositif d'alerte non conforme et ordonner que les données recueillies soient détruites.

Ainsi, par décision du 8 décembre 2009, la chambre sociale de la Cour de cassation a estimé que le code éthique, comprenant un dispositif de « lanceur d'alerte », élaboré par l'entreprise Dassault Systèmes, n'était pas conforme au régime simplifié d'autorisation défini par la CNIL dans sa délibération du 8 décembre 2005. Au cas d'espèce, elle a considéré, d'une part que ce dispositif sortait du cadre prévu par la loi, et d'autre part, qu'il ne prévoyait aucune mesure d'information et de protection des personnes répondant aux exigences de la loi du 6 janvier 1978 et de la délibération du 8 décembre 2005 [173].

À l'inverse, le juge validera un dispositif d'alerte qu'il estimera conforme à la délibération de la CNIL [174].

Au-delà de la loi informatique et libertés, le juge est susceptible également de vérifier la conformité de ces dispositifs aux règles de droit commun, et notamment aux dispositions protectrices des droits et libertés [175].

c) Le contrôle exercé par la CNIL

La circulaire du 19 novembre 2008 rappelle que la CNIL est, depuis la loi du 6 août 2004, dotée de pouvoirs de sanctions administratives et pécuniaires importants. Au-delà de l'avertissement, la CNIL peut désormais, après une mise en demeure infructueuse, retirer l'autorisation attribuée, ordonner une amende. Le montant des sanctions pécuniaires peut atteindre 1,5 millions d'euros pour une personne morale et 300 000 euros et cinq ans d'emprisonnement pour un individu et par infraction. En cas d'atteinte grave et immédiate aux droits et libertés, le président de la CNIL peut demander en référé au juge d'ordonner toute mesure de sécurité utile. La CNIL peut, de sa propre initiative, se rendre dans tout local professionnel et vérifier sur place et sur pièces les fichiers. Elle peut se saisir de son propre fait d'affaires qui entrent dans le domaine de compétence qui lui est attribué.

172. Ordonnance de référé 12/06 du 27 décembre 2006 du TGI de Nanterre.

173. Cass. soc., 8 décembre 2009, n° 2524.

174. TGI Lyon, 09/2006 du 19 septembre 2006.

175. Par exemple l'article L. 1121-1 du Code du travail qui dispose que « Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché ».

Un premier bilan montre que fin 2008, 1 200 professionnels se sont engagés à respecter le cadre fixé par la CNIL dans le domaine des alertes professionnelles. La plupart de ces déclarations étaient le fait de filiales de sociétés américaines concernées par la loi SOX.

La CNIL a procédé à 300 contrôles de conformité en 2008. À partir des contrôles qu'elle a menés, elle relève un très faible recours des salariés aux dispositifs d'alerte professionnelle. C'est dans le cas de la mise en œuvre de tels dispositifs qu'elle constate le plus de manquements aux obligations légales, notamment à l'obligation de porter à sa connaissance la mise en œuvre de ce type de traitement [176].

Plus largement, elle relève, dans le rapport qu'elle a rédigé en 2008, que « la tendance qui se dégage paraît toutefois indiquer que ces dispositifs ne présentent guère d'utilité au regard des dispositions du Code du travail ou de l'utilisation, classique, de la voie hiérarchique afin de signaler ces dysfonctionnements… Dans les faits, les entreprises adossent leur dispositif d'alerte professionnelle à leur code de conduite, généralement rédigé par leur société mère, dont l'objet est plus vaste que le champ de l'autorisation unique de la CNIL ». Et la CNIL de conclure : « Les procédures d'alerte professionnelle apparaissent comme des dispositifs importés qui ne correspondent pas à la réalité sociale des entreprises françaises. »

*

Au terme de ce panorama, le constat qui s'impose est le décalage qui existe entre les discours sur le lanceur d'alerte, notamment au sein des enceintes internationales, et les difficultés juridiques ou pratiques que soulève sa mise en place dans tous les pays du monde.

Les discours balancent bien souvent entre une vision idéalisée du dénonciateur, celle du lanceur d'alerte justicier, et une vision dépréciative du lanceur d'alerte perçu comme un délateur.

L'approche des organisations internationales semble toute entière construite autour du syllogisme suivant : 1) Le signalement est utile pour la détection et la lutte contre la corruption ; 2) Le lanceur d'alerte prend des risques personnels en signalant la corruption ; 3) Il est donc nécessaire de protéger le lanceur d'alerte.

L'analyse des dispositifs existants, en France et dans d'autres pays, montre en vérité qu'il n'existe pas de modèle idéal. Il n'est pas de pays où la mise place d'un dispositif de signalement n'ait pas soulevé de débats. Il n'est pas non plus de pays où ne soit pas posée la question du champ du

176.Communiqué CNIL du 26 juin 2006.

signalement, de son destinataire, ainsi que du statut du lanceur d'alerte, de l'étendue de sa protection et de sa responsabilité éventuelle.

En France, en particulier, comme on l'a vu, la mise en place d'un dispositif d'ensemble se heurte à une double difficulté.

Une première difficulté tient au dualisme juridique et culturel entre les secteurs public et privé, ce qui traduit par le fait que le signalement, qui est un devoir pour les agents publics, est un droit pour les salariés des entreprises.

Au sein de chacun de ces secteurs, le signalement est en opposition avec d'autres devoirs au sein du secteur public (obéissance, réserve, discrétion…) et en opposition avec d'autres droits dans le secteur privé (libertés syndicales, protection de la vie privée…).

S'il semble, dans ces conditions, difficile d'envisager des mécanismes de signalement et de protection du lanceur d'alerte commun à l'ensemble des salariés, à l'instar par exemple du dispositif américain[177], des voies d'amélioration sont possibles, tant dans le secteur public que dans le secteur privé.

Pour les deux secteurs, une première mesure pourrait consister à étendre le délit de non-dénonciation de crime à la non-dénonciation de délit, ce qui inclurait les atteintes à la probité.

Cette mesure aurait pour effet de conférer au signalement le caractère d'une obligation, dont le non-respect se traduirait par la mise en jeu de la responsabilité du lanceur d'alerte qui se tait et/ou s'abstient. Elle présente toutefois l'inconvénient d'ouvrir le champ de l'obligation de signalement d'une manière tellement large qu'elle serait difficilement gérable par les parquets.

S'agissant du secteur public, la principale novation devrait porter sur l'article 40, alinéa 2, du Code pénal, pour lequel il conviendrait de prévoir :

- de lever les ambiguïtés sur son champ d'application, en spécifiant expressément, comme cela a été préconisé dans le rapport 2010[178], qu'il s'applique aux autorités exerçant des fonctions juridictionnelles ;
- de le compléter par une disposition miroir de l'article précédent, prévoyant que l'absence de signalement peut être pénalement sanctionnée.

177. Encore que ce dernier prévoit, comme on l'a vu, des régimes spécifiques pour certains agents, appartenant par exemple aux services de renseignements.

178. Rapport du SCPC 2010, p. 155.

Il conviendrait également de prévoir une disposition relative à la protection de l'agent public lanceur d'alerte. Cette protection pourrait être assurée par une extension du champ de la protection statutaire dont bénéficient les fonctionnaires (article 25 du statut général), qui pourrait s'inspirer du contenu de l'article L. 1161-1 du Code du travail.

Au-delà, est-il possible et souhaitable d'aller plus loin en France, en prévoyant par exemple, comme cela est le cas dans certains pays (États-Unis, Corée du Sud), des mécanismes d'incitation, y compris sous une forme financière, à la dénonciation ? Certes, ce type de mécanisme n'est pas totalement inconnu de notre droit, encore pour l'essentiel sous une forme négative [179].

Il y a fort à parier cependant que l'instauration en France d'un dispositif permettant de « récompenser » les personnes signalant des faits de corruption, pourrait susciter, si ce n'est des réactions de rejet, à tout le moins des débats au sein de l'opinion comme chez les spécialistes [180].

Indépendamment des aspects éthiques ou juridiques, on peut se demander si l'octroi d'une « récompense » ou d'une « prime » aux lanceurs d'alerte apporterait un réel progrès à la lutte contre la corruption.

Les résultats obtenus au moyen des dispositifs de signalement existants sont, comme on l'a vu, contrastés. Pour ce qui est du cas français, le SCPC a, régulièrement, exprimé ses interrogations sur le fonctionnement effectif de l'article 40, alinéa 2, du Code de procédure pénale. Dans le secteur privé, les contrôles réalisés par la CNIL montrent que, si les dispositifs d'alerte se sont multipliés, les salariés répugnent encore à les utiliser.

Le cœur du problème, en définitive, est que la mise en place d'un dispositif d'alerte ne suffit pas, en tant que tel, à assurer une lutte efficace contre les pratiques corruptrices. L'alerte ne peut, en effet, être considérée indépendamment de son destinataire. D'autre part, il peut être utile de se poser la question de son efficacité dans le domaine de la lutte contre la corruption.

Sur le premier point, soulever la question du destinataire de l'alerte conduit à se poser la question des suites qui lui seront données. Selon les pays, le signalement ou l'alerte doit être effectué auprès du supérieur hiérarchique ou auprès d'une instance externe, magistrat du parquet le plus souvent.

179. Par exemple sous forme d'exemption ou de réduction de peine (dont le champ a été étendu par la loi n° 2004-204 du 9 mars 2004, Perben II), ou bien encore dans le cadre d'une procédure dite de clémence prévue par le droit de la concurrence.

180. Si l'on songe par exemple aux débats qui ont entouré l'encadrement par la loi (art. 3 de la loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité) de la « rétribution » des indicateurs de la police.

Lorsque le signalement est effectué en interne, la question est celle de « l'externalisation » ou non des faits qui ont été relevés, et donc de savoir si une collectivité de travail, publique ou privée, dispose de la capacité à apprécier la nature et la gravité des faits qui sont portés à sa connaissance. En France, la réponse est loin d'être évidente, malgré la clarté des textes. Ainsi, le SCPC a-t-il eu l'occasion d'observer, tout au long de ses rapports annuels, la frilosité des administrations à saisir le juge pénal de faits qui peuvent parfois revêtir une certaine gravité. La CNIL a de son côté relevé la même attitude timorée des salariés du secteur privé.

La révélation à une instance externe soulève en revanche une question d'une autre nature qui est celle des prérogatives dont dispose cette instance dans la lutte contre la corruption. Ainsi, en France, l'alinéa 2 de l'article 40 ne peut se concevoir indépendamment de son alinéa premier qui prévoit que « le procureur est le destinataire des plaintes et dénonciations ». Autrement dit, les suites données au signalement sont subordonnées au pouvoir d'opportunité des poursuites dont dispose le parquet. Il appartiendra à ce dernier, lorsqu'il recevra une dénonciation, d'ouvrir une enquête, une information judiciaire, ou de classer sans suite. Or, comme l'illustre le cas français, le rôle du parquet dans les affaires de corruption, domestiques ou internationales [181], est souvent essentiel. Ainsi donc, l'efficacité du signalement, c'est-à-dire concrètement l'ouverture d'une enquête, rejoint le thème plus vaste, et régulièrement débattu, de l'indépendance du parquet, de sa plus ou moins grande autonomie vis-à-vis de sa hiérarchie et du degré d'ouverture de l'autorité politique vis-à-vis du traitement d'affaires fréquemment « sensibles »…

Enfin, au-delà des aspects juridiques ou plus largement de politique pénale, c'est bien l'efficacité technique de l'alerte qui se trouve posée. À cet égard, plusieurs études, et notamment l'enquête annuelle sur la fraude dans les entreprises réalisées par le cabinet PricewaterhouseCoopers (PwC), montrent une évolution des procédés ou canaux permettant de la mettre à jour. Alors qu'en 2007 PwC relevait que les entreprises portaient leurs efforts sur certains aspects gravitant autour de la culture d'entreprise (code de conduite, y compris les systèmes d'alerte), il note, dans son rapport pour 2011, que « de moins en moins de fraudes sont découvertes par l'audit interne… les entreprises ont franchi une nouvelle étape dans leur démarche de lutte contre la fraude en développant des contrôles automatisés d'identification des transactions inhabituelles. La mise en œuvre de ces contrôles permet aujourd'hui de raccourcir le délai nécessaire pour identifier une fraude et en conséquence de réduire le coût qui y est associé ».

181. Dans le domaine de la corruption internationale, on rappellera que le parquet dispose, en vertu des articles 435-6 et 435-11 du Code pénal, du monopole des poursuites.

Cette situation traduit certainement une évolution des formes de la corruption. Celle-ci recourt à des procédés de plus en plus élaborés, à la fois dématérialisés et délocalisés, qui en rendent difficile la détection, y compris au sein même de l'entreprise, et dans le milieu professionnel où évoluent les auteurs des pratiques corruptrices [182]. Par ailleurs, les entreprises se sont également efforcées d'améliorer leurs dispositifs de lutte contre ce type de pratiques afin de les identifier le plus en amont possible et sous des formes qui évitent de leur donner une trop forte résonance médiatique. Nombreuses sont celles qui semblent aujourd'hui considérer que le signalement n'est en définitive, dans la panoplie anticorruption, qu'un remède ultime, de dernier recours, qui n'est utilisé (souvent par crainte du scandale, de l'atteinte à la réputation de la société) que lorsque les autres procédures internes (audits, codes de conduite), n'ont pas fonctionné correctement.

Beaucoup de chemin reste donc encore à parcourir pour que, dans le secteur public comme dans le secteur privé, le lanceur d'alerte devienne un acteur à part entière de la lutte contre la corruption.

182. Situation illustrée par l'affaire dite de « la Société générale » début 2008, qui s'est concrétisée par une fraude de grande ampleur, en dépit de dispositifs d'audit internes.