



Le lanceur d'alerte dans les entreprises, tout un programme



Le Figaro (François Bouchon)

La loi Sapin 2 lui prévoit un statut dédié avec une procédure spécifique à mettre en œuvre pour assurer la confidentialité. Mais plusieurs questions restent en suspens comme la problématique des données personnelles et de la personne à qui confier l'alerte.

Votée en décembre dernier, la loi Sapin 2 contre la corruption a notamment créé le statut de lanceur d'alerte. « Un lanceur d'alerte est une personne physique qui révèle ou signale, de manière désintéressée et de bonne foi, un crime ou un délit, une violation grave et manifeste d'un engagement international régulièrement ratifié ou approuvé par la France, d'un acte unilatéral d'une organisation internationale pris sur le fondement d'un tel engagement, de la loi ou du règlement, ou une menace ou un préjudice grave pour l'intérêt général, dont elle a eu personnellement connaissance », définit ainsi le législateur. Dans cette définition longtemps débattue auprès du Parlement, c'est la notion d'intérêt général qui fait la différence avec la délation. Mais dans un pays où le spectre du licenciement ou du chantage reste important pour les employés, la question du lanceur d'alerte reste complexe.



« Le principe retenu par la loi est celui de la cascade, avec trois niveaux d'alerte » explique à WanSquare Sophie Scemla, associée en charge du département droit pénal des affaires et compliance chez Evershed Sutherland France. Ainsi, le premier niveau concerne la divulgation en interne, le lanceur d'alerte pouvant communiquer l'information à un référent ou à sa hiérarchie directe. Si, « dans un délai raisonnable, qui n'est pas encore défini », souligne Sophie Scemla, il n'y a rien de fait au niveau de l'entreprise, le lanceur d'alerte peut alors se tourner vers des autorités administratives, professionnelles ou judiciaires. Enfin, au-delà d'un délai de trois mois après le premier signalement, le lanceur d'alerte peut porter sur la place publique sa découverte. Cela semble bien encadré et pourtant tant la procédure d'alerte que le statut même de lanceur d'alerte posent des questions.

La première relève de la confidentialité de l'identité du lanceur d'alerte mais aussi des faits visés par l'alerte. La Cnil, n'a pas encore pris position concernant ce point et les données personnelles du lanceur d'alerte. Or, lorsque les entreprises mettent en place des systèmes de compliance et des procédures d'alerte, la Cnil doit en être informée. S'il existe déjà une procédure d'alerte dans l'entreprise, il faut faire une demande d'autorisation à la Cnil ou remplir la déclaration d'autorisation unique (formulaire AU004) applicable uniquement à 5 domaines bien précis : finance et comptabilité, corruption, discrimination au travail, hygiène au travail et la protection de l'environnement. Mais si l'entreprise n'a encore rien fait, autant être vigilant. « Comme la Cnil n'a pas encore pris position par rapport au statut de lanceur d'alerte, et pour éviter tout problème, nous recommandons à nos clients de faire une demande d'autorisation », explique [Gaëtan Cordier](#), associé en charge du département données personnelles, chez [Eversheds Sutherland France](#).

Autre problématique, la procédure d'alerte en elle-même. Car même si le lanceur d'alerte doit respecter les trois stades, encore faut-il savoir à qui vraiment s'adresser. En effet, au premier stade, le lanceur d'alerte doit divulguer l'information à son supérieur hiérarchique ou à un référent. S'il s'adresse au supérieur hiérarchique, cela pose plusieurs questions. « Un problème pourrait alors se poser dans le cas où un employé d'une entreprise française constate un problème dans un pays lointain. Son supérieur hiérarchique risque en effet d'être dans le pays en question et donc de ne pas relever du droit français », lance ainsi Philippe Desprès, associé en charge du département droit social chez Evershed Sutherland France. Sans compter que le supérieur hiérarchique peut être la personne visée par l'alerte.

Aussi, l'une des meilleures solutions est que l'entreprise désigne un référent, si possible externe à l'entreprise, « peu d'employés étant prêts à prendre la responsabilité d'un tel rôle », assure Sophie Scemla. Mais « la loi n'impose rien sur ce point alors même que la question du référent risque d'être stratégique dans les entreprises », estime Claire Olive-Lorthioir, co-présidente de la commission gouvernance et éthique du Cercle Montesquieu. Le référent doit en effet être une personne ayant les compétences nécessaires à une bonne écoute, la qualité et le courage quant à la confidentialité de l'information ce qui nécessite aussi une indépendance et une autonomie. « Ce sera le chef d'orchestre, il travaillera comme un chargé de projet et organisera le retro planning quant à la suite des opérations. Il devra permettre ainsi le traitement rapide de l'alerte », souligne encore Claire Olive-Lorthioir. Reste à savoir qui pourra porter cette casquette. Cela peut en effet être le directeur juridique ou de compliance d'une entreprise, mais rien n'empêche que ce soit la RH ou même un syndicat. Cela peut aussi être un prestataire externe, les avocats pouvant jouer ce rôle, tout comme les plateformes de recueil d'informations sensibles et d'alertes, comme par exemple la société Ethicpoint. Les décrets d'application, qui devraient bientôt sortir, devraient donner plus d'indication.

La procédure d'alerte et les conditions de « travail » du lanceur d'alerte nécessitent donc une adaptation des entreprises, encore peu habituées à ce type de démarches. Et pour celles n'ayant pas encore mis en place ce type de dispositif « c'est un véritable levier pour elles, car cela leur permettra de prouver leur lutte active contre



[Visualiser l'article](#)

la corruption », explique Claire Olive-Lorthioir. C'est aussi l'occasion de mettre en place une communication entre les différents services et renforcer les liens dans l'entreprise ». Reste que la mise en œuvre d'un tel changement d'état d'esprit dans les entreprises risque de prendre du temps.