La gestion des alertes professionnelles à la lumière du RGPD

les faits **Snowden, Mediator, LuxLeaks, nombreuses sont les affaires liées aux révélations de lanceurs d'alerte qui ponctuent l'actualité. Face à une législation éparse, la loi « Sapin II » du 9 décembre 2016 instaure un socle commun aux différents mécanismes d'alerte. La protection des données personnelles recueillies dans ce cadre nécessite d'articuler ces dispositifs avec les dispositions du RGPD.**

Aux termes de la loi « Sapin II », le lanceur d'alerte s'est vu offrir un véritable régime protecteur. Toute personne qui « *révèle ou signale de manière désintéressée et de bonne foi* » une pratique illégale ou toute menace ou préjudice grave pour l'intérêt général, dont elle aurait « *personnellement eu connaissance* », se voit reconnaître un statut lui conférant une irresponsabilité pénale et l'interdiction de toute représaille professionnelle. Ce statut est toutefois conditionné au respect d'une procédure d'alerte graduée et responsable, qui impose au salarié d'avertir en premier lieu son supérieur hiérarchique, son employeur ou un référent désigné à cet effet. La loi impose dans ce cadre aux entreprises de plus de 50 salariés, depuis l'entrée en vigueur de son décret le 1er janvier 2018, la mise en œuvre d'un dispositif de recueil de signalement interne efficace et sécurisé, garantissant une stricte confidentialité de l'identité de l'auteur, des personnes et des faits visés par l'alerte (hotline ou boîte mail dédiée, formulaire en ligne etc.) et la désignation d'un responsable du traitement de l'alerte. Ces dispositions ne sont pas sans rappeler celles prévues par le RGPD. Et pour cause, le recueil et la gestion de ces signalements impliquent nécessairement la collecte et le traitement de

Me Pierre-Randolph Dufau
Avocat à la cour
Fondateur de la SELAS
PRD avocats

données personnelles, dont les outils et principes protecteurs doivent être intégrés dès la mise en place du dispositif. À titre d'exemple, si par exception le consentement de la personne faisant l'objet de l'alerte n'a pas à être recueilli, le traitement ayant un fondement légal, ce dernier doit néanmoins respecter les principes de proportionnalité et de pertinence des données collectées dont la durée de conservation doit être limitée. Plus encore, il convient de souligner que le dispositif d'alerte mis en place doit répondre aux nouvelles exigences du RGPD en matière de sécurité et ce afin de prévenir tout détournement ou utilisation frauduleuse des données recueillies lors du signalement. Le dispositif d'alerte, qui par définition traite de données relatives à des faits susceptibles de revêtir une qualification pénale, doit ainsi être soumis à une analyse d'impact telle que prévue à l'article 35 du RGPD, à savoir une évaluation des risques encourus pour le droit des personnes concernées et les mesures envisagées pour y faire face. Enfin, tout comme l'exige le RGPD, la loi « Sapin II » impose également des opérations de sensibilisation des acteurs en interne et une documentation précise (cartographie des risques et des traitements, processus de sécurisation) démontrant les mesures organisationnelles mises en œuvre pour assurer la conformité, notamment du dispositif d'alerte.

ce qu'il faut retenir **Une approche combinée de la Loi « Sapin II » et des exigences du RGPD est indispensable pour la mise en œuvre du dispositif d'alerte. La convergence de ces textes, s'inspirant d'une méthode commune et ayant recours aux mêmes outils, permet d'assurer une meilleure couverture des risques et une rationalisation des coûts non négligeables.**

Un disque dur professionnel renommé « données personnelles » n'est pas privé

La Cour européenne des droits de l'homme (CEDH) a donné raison le 22 février dernier aux juridictions internes confirmant que l'employeur avait le droit de consulter les 1562 fichiers pornographiques, non individuellement identifiés comme privés, présents sur le disque dur d'un salarié qui avait cru astucieux de le dénommer « données personnelles ».

Direct Energie mis en demeure par la Cnil

À l'occasion de la mise en place du compteur Linky, le fournisseur d'électricité avait demandé au gestionnaire du réseau de distribution de lui transmettre les données correspondant à la consommation journalière et par demi-heure de ses clients pour élaborer leur facturation. La Cnil sanctionne le fait que ces derniers, dont les données transmises révélaient de nombreuses informations touchant à leur vie privée, n'avaient pas donné un consentement libre et éclairé.

Réserves de la Cnil sur l'application Reporty

Mise en œuvre de manière expérimentale à Nice, l'application Reporty permet à ses utilisateurs de signaler à la police « une incivilité grave (...) ou une situation critique » dont ils auraient été témoins, en transmettant leur position avec une vidéo ou un enregistrement. Pour la Cnil, si la prévention des troubles à l'ordre public peut justifier une telle atteinte à la vie privée, ce dispositif ne présente pas en l'état les garanties de proportionnalité suffisantes.