Document 1 de 1

LA SEMAINE JURIDIQUE
ÉDITION GÉNÉRALE

La Semaine Juridique Edition Générale n° 19-20, 7 Mai 2018, doctr. 553

Alerte professionnelle et protection des données personnelles

Etude par Noëlle Lenoir
avocate associée, Kramer Levin Naftalis et Frankel

et Alizée Dill
avocate, Kramer Levin Naftalis et Frankel

et Hélène Bérion
avocate, Kramer Levin Naftalis et Frankel

Lanceurs d'alerte

Sommaire

Aux lendemains de la publication par la Commission européenne d'une proposition de directive sur les lanceurs d'alerte, c'est peu de dire que ce sujet est à la pointe de l'actualité en Europe, mais également en France, notamment avec l'entrée en vigueur de la loi Sapin II. Or, quel que soit le canal choisi, l'alerte professionnelle est de nos jours un dispositif informatisé. Aussi logiquement, la proposition de directive sur les lanceurs d'alerte renvoie-t-elle à l'application du Règlement Général européen sur la Protection des Données Personnelles du 27 avril 2016 (RGPD). Le propos de cet article est - tout en précisant les règles de protection des données qui s'appliquent aux dispositifs d'alerte professionnelle - de faire état des tensions inévitables entre, d'une part, le droit à la vie privée et le droit à l'oubli qui en est le corollaire, et d'autre part, l'exigence de transparence, voire de publicité des manquements au droit et à l'éthique, qui sous-tend l'alerte professionnelle que ce soit pour mettre fin à une certaine impunité, ou plus généralement pour assurer la maîtrise de la gestion des risques dans le secteur public comme privé.

1. Une révolution culturelle en marche à l'ère du numérique

1. - Aux lendemains de la publication par la Commission européenne d'une proposition de directive sur les lanceurs d'alerte[Note 1] et alors que le Président de la Barclays Bank se voit sanctionné pour avoir tenté de révéler l'identité d'un lanceur d'alerte[Note 2], c'est peu de dire que ce sujet est à la pointe de l'actualité en Europe[Note 3]. Est-ce si nouveau ? Sous l'impulsion de l'Union européenne, les lanceurs d'alerte ont été appelés dès les années 70 à contribuer à la protection des travailleurs face aux risques de discrimination et de harcèlement moral[Note 4]. Dans l'esprit de la loi Sarbanes-Oxley de 2002 (SOX)[Note 5], les lanceurs d'alerte ont ensuite été promus acteurs essentiels de la gouvernance d'entreprise, en lien avec les ONG, ayant vocation à déjouer la corruption et la fraude. Dans le secteur financier, la valeur ajoutée des lanceurs d'alerte a aussi été reconnue par le droit de l'Union[Note 6]. Des règles européennes de protection des lanceurs d'alerte ont été définies pour inciter à la détection des risques pour l'environnement lors de l'exploration *off shore* de pétrole ou de gaz[Note 7]. Les récents scandales mettant en cause des personnalités ayant abusé de leur pouvoir pour s'attirer des faveurs sexuelles et le mouvement du #MeToo ont de nouveau mis en lumière l'intérêt de l'alerte pour stopper des pratiques hélas trop courantes dans certains milieux. Quant au rôle des lanceurs d'alerte en tant que contributeurs au journalisme d'investigation, il est à la mesure de l'ardente défense dont ils bénéficient dans les médias dès qu'il est question de protéger des secrets d'affaires, pourtant d'intérêt économique pour les entreprises, voire la nation[Note 8].

2. - En France, la consécration de l'alerte professionnelle participe d'un profond changement culturel. Jusqu'ici, le principe d'une telle alerte « éthique » se heurtait à de fortes réticences, alors que le *whistleblowing* correspond outre-Atlantique à une tradition juridique séculaire[Note 9]. La France revient de loin : rappelons-nous les deux délibérations de la Commission Nationale de l'Informatique et des Libertés (CNIL) du 26 mai 2005 sur les premiers « dispositifs d'intégrité professionnelle » et de « ligne éthique »[Note 10]. Leur installation s'imposait pourtant, sous peine de sanction, du fait de l'extraterritorialité des dispositions de la loi SOX applicables aux filiales des sociétés américaines et aux sociétés non américaines cotées en bourse aux États-Unis (Nasdaq et NYSE). Concernant le projet de *hotline* chez McDonald's France, la CNIL avait considéré que : « *... la mise en oeuvre par un employeur d'un dispositif destiné à organiser auprès de ses employés le recueil, quelle qu'en soit la forme, de données personnelles concernant des faits contraires aux règles de l'entreprise ou à la loi imputables à leurs collègues de travail, en ce qu'il pourrait conduire à un système organisé de délation professionnelle, ne peut qu'appeler de sa part une réserve de principe...* ». Cette réserve était assortie de suggestions de solutions alternatives pour éviter les « risques de dénonciations calomnieuses et de stigmatisation des employés objets d'une alerte éthique » (sensibilisation par l'information et la formation des personnels, audits, alerte par les commissaires aux comptes, saisine de l'inspection du travail ou des juridictions compétentes). Ni McDonald's France, ni la Compagnie européenne d'accumulateurs, qui avaient saisi la CNIL, n'avaient alors été autorisées à se doter d'un mécanisme d'alerte professionnelle.

3. - Ce n'est qu'à la suite de négociations avec la Security Exchange Commission (SEC), en charge de veiller à la mise en oeuvre de la loi SOX, que la CNIL s'est résolue à ne plus faire blocage aux dispositifs d'alerte, tout en les encadrant dans un document d'orientation[Note 11]. Les lignes directrices de ce document ont été reprises dans une délibération de décembre 2005 portant autorisation unique de traitements automatisés de données à caractère personnel mis en oeuvre dans le cadre de dispositifs d'alerte professionnelle (autorisation n°AU-004)[Note 12]. C'était par là-même anticiper la large diffusion de ces dispositifs dans les entreprises et les organismes publics. L'autorisation unique est en effet une facilité procédurale prévue pour les traitements fréquemment mis en oeuvre, les responsables de traitement n'ayant plus qu'à indiquer à la CNIL qu'ils se conforment à la norme définie par elle[Note 13].

4. - Les traitements informatisés de données personnelles issus des dispositifs d'alerte proviennent de différents canaux : supérieur hiérarchique, responsable éthique etc. - ceux à qui le lanceur d'alerte a souhaité directement s'adresser, ou les autorités publiques compétentes, la *hotline* n'étant que l'un de ces canaux. D'ailleurs, selon la CNIL, la *hotline* doit demeurer facultative et complémentaire par rapport aux autres voies de remontées de réclamations des salariés[Note 14] que sont, selon la gradation prévue par la jurisprudence de la Cour européenne des droits de l'homme (CEDH)[Note 15], le signalement auprès du supérieur hiérarchique ou son délégué, puis la saisine des autorités compétentes et enfin la publicité donnée à l'alerte. Quel que soit le canal choisi, l'alerte professionnelle est de nos jours un dispositif informatisé. Aussi logiquement, la proposition de directive sur les lanceurs d'alerte renvoie-t-elle à l'application du Règlement Général européen sur la Protection des Données Personnelles du 27 avril 2016 (RGPD) [Note 16] et de la directive du même jour sur le traitement de données à des fins de prévention et de détection des infractions pénales ou d'exécution de sanctions pénales[Note 17], soit les deux principaux textes de l'arsenal juridique de l'Union en la matière[Note 18]. La loi Informatique et Libertés est quant à elle en cours de révision par le Parlement au moment de la rédaction du présent article[Note 19].

5. - Le propos de ce dernier est de faire état des tensions inévitables entre, d'une part, le droit à la vie privée et le droit à l'oubli qui en est le corollaire, et d'autre part, l'exigence de transparence qui sous-tend l'alerte professionnelle en tant qu'elle est destinée à lever l'omerta qui, spécialement en France, a trop souvent été synonyme d'impunité. Jusqu'à présent, le fléau de la balance a penché en défaveur des lanceurs d'alerte qui, à quelques exceptions notables près, ont mis en péril leur vie professionnelle, et donc personnelle, en ayant le courage de dénoncer des comportements illégaux ou inacceptables[Note 20]. Mais, le vent pourrait tourner tant la dénonciation hâtive sinon mensongère prend également ancrage dans notre société. Les réseaux sociaux y ont leur part, le mouvement « anti-élite » en cette période de grands bouleversements étant un puissant facteur d'incitation au dénigrement. Dans ce contexte, la législation sur la protection des données personnelles constitue un rempart évitant de jeter en pâture que ce soit le lanceur d'alerte lui-même ou la personne mise en cause, dont les vies pourraient être injustement détruites.

2. L'alerte professionnelle : une obligation de portée de plus en plus extensive

6. - L'alerte professionnelle n'est pas née avec la loi du 9 décembre 2016, dite loi Sapin II[Note 21], mais c'est cette loi qui l'a véritablement consacrée en remédiant par ailleurs pour partie à la dispersion des textes, suivant les recommandations du Conseil d'État[Note 22]. L'article 16 de la loi va plus loin qu'une simple consécration : il rend le dispositif obligatoire à partir de

seulement 50 salariés dans le public comme dans le privé, les administrations de l'État, les communes de plus de 10 000 habitants et leurs établissements publics de coopération intercommunale à fiscalité propre (ex. communautés de communes ou d'agglomération), les départements et régions, l'Autorité des marchés financiers et l'Autorité de contrôle prudentiel et de résolution. Par ailleurs, selon l'article 17, les sociétés d'au moins 500 salariés, ou appartenant à un groupe de sociétés dont la société mère a son siège social en France et dont l'effectif comprend au moins 500 salariés, et dont le chiffre d'affaires ou le chiffre d'affaires consolidé excède 100 millions d'euros, doivent maintenant mettre en place un « *dispositif d'alerte interne destiné à permettre le recueil des signalements émanant d'employés et relatifs à l'existence de conduites ou de situations contraires au code de conduite de la société* », notamment par le biais d'une *hotline*.

7. - Adoptée seulement trois mois après la loi Sapin II, la loi sur le devoir de vigilance[Note 23] est venue superposer un nouveau régime d'alerte professionnelle avec des seuils différents de ceux fixés par la loi Sapin II. Sont visées toutes sociétés ayant, à la clôture de deux exercices consécutifs, au moins 5 000 ou 10 000 salariés en son sein et dans ses filiales directes ou indirectes selon que leur siège social est en France ou à l'étranger. La société Valéo Services a été l'une des premières à tirer les conséquences de la loi Sapin II, mais aussi de celle sur le devoir de vigilance en matière de *hotline* ; ce qui a conduit la CNIL, dans sa délibération du 8 février 2018 portant autorisation[Note 24], à relever la mise à disposition d'un formulaire d'alerte sur le site du sous-traitant, et non pas seulement de l'entreprise.

8. - Il est regrettable que le législateur n'ait pas cherché à assurer un minimum de coordination entre ces deux lois. Faisant fi des appels à clarifier et harmoniser les différents régimes de l'alerte éthique en France[Note 25], le dispositif de la loi Sapin II ne se substitue pas à tous les systèmes existants, telle que l'alerte instituée par la loi n° 2013-316 du 16 avril 2013 qui prévoit que le travailleur alerte immédiatement l'employeur sur les risques pour la santé ou l'environnement pesant sur les produits ou procédés de fabrication de l'entreprise[Note 26].

9. - Il faut espérer que la future directive sur les lanceurs d'alerte, qui consacre au-delà de certains seuils l'obligation de se doter d'un dispositif d'alerte dans les domaines de compétences de l'Union[Note 27], incitera à mettre un peu d'ordre dans la législation française. L'harmonisation des régimes d'alerte se fait en pratique dès lors qu'entreprises et administrations sont amenées à combiner dans un même système d'information les différents régimes de signalement. Elles le font en tenant compte de l'extension du champ d'application de l'alerte professionnelle au fil des réformes : l'alerte peut aujourd'hui être le fait aussi bien d'un employé (salarié, collaborateur occasionnel, agent public, stagiaire...) que de tout tiers (client, fournisseur, sous-traitant, actionnaire...). Le lanceur d'alerte n'a pas à vérifier si les faits qu'il entend porter à connaissance constituent une infraction. Il peut s'agir de crimes, de délits (ex. fraude, corruption, trafic d'influence, escroquerie, discrimination, harcèlement moral ou sexuel, abus de biens sociaux, détournements d'actifs)[Note 28] ou de toute autre violation de la loi ou du règlement, de la violation d'un engagement international (ex. atteinte aux droits de l'homme et aux libertés fondamentales), comme d'agissements contraires à l'éthique (ex. conflit d'intérêts de nature à jeter la suspicion sur un comportement)[Note 29]. C'est ce que reflète la définition de l'alerte donnée par la proposition de loi en discussion transposant la directive sur le secret des affaires. En effet, selon l'article L. 151-7 nouveau, introduit dans le Code de commerce, le secret n'est pas opposable[Note 30] à ceux qui révèlent « *dans le but de protéger l'intérêt général et de bonne foi, une activité illégale, une faute ou un comportement répréhensible* »[Note 31].

10. - Il est certain que l'extension de la portée juridique de l'alerte professionnelle n'aurait pas été possible sans les progrès de l'informatique, des progrès que le droit européen de la protection des données place sous haute surveillance.

3. L'alerte professionnelle, un traitement de caractère nécessairement sensible

11. - Dès 2005, la CNIL avait rappelé que la législation sur la protection des données personnelles s'applique non seulement aux traitements informatiques, mais également aux fichiers non informatisés qui y renvoient[Note 32]. De plus, la notion de traitement informatique couvre à la fois l'ensemble formé par une chaîne d'opérations depuis la collecte des données jusqu'à leur éventuelle destruction, et chacune de ces opérations prises isolément ; un traitement étant défini comme « *toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction* »[Note 33]. Ainsi, toute personne déterminant les finalités et moyens d'une, plusieurs ou de l'ensemble des opérations du traitement est responsable ou co-responsable du traitement, ce qui conditionne le partage des responsabilités en cas de faute.

12. - Par exemple, une filiale transmettant des alertes à sa société mère peut être regardée comme co-responsable du traitement à côté de la mère. Selon une jurisprudence du Conseil d'État de 2014[Note 34], elle ne l'est cependant pas lorsque l'outil de traitement de l'alerte est déployé au sein de ses filiales par la société mère qui en a déterminé les modalités (ex. nature des données, droits d'accès à celles-ci, durée de conservation). Les sociétés mères situées hors UE et y ayant des filiales sont donc, sur la base de ces critères, responsables de traitement. En outre, un nombre important d'entreprises françaises choisissent des prestataires informatiques situés dans des pays plus ou moins lointains, tels que les États-Unis, l'Afrique du Sud ou l'Inde (centres téléphoniques, gestionnaires de bases de données sur serveurs, gestionnaires de *clouds*...). Or, en cas d'incident, quel que soit le lieu d'implantation du responsable du traitement ou du prestataire, l'un et l'autre doivent apporter la preuve que le dommage ne leur est nullement imputable[Note 35].

13. - Les traitements impliquant le transfert de données hors UE (sauf à ce que le pays tiers bénéficie d'une « décision d'adéquation » de la Commission européenne)[Note 36] font l'objet d'une attention particulière du fait des difficultés d'y contrôler l'utilisation ou la réutilisation des données. Les groupes multinationaux ont clairement intérêt à se doter de règles d'entreprise contraignantes[Note 37] assurant le libre flux des données au sein des entités du groupe. À défaut, l'entreprise devra se conformer à des clauses types de protection des données adoptées par la Commission européenne ou une autorité de contrôle (la CNIL en France) ou autorisées par une telle autorité. Des clauses contractuelles différentes s'appliquent aux transferts entre sociétés mères et filiales (de responsable du traitement à responsable du traitement) ou entre sociétés et leurs sous-traitants, avec la possibilité pour les cocontractants d'insérer les clauses dans d'autres contrats, tel qu'un contrat entre le sous-traitant et un autre sous-traitant. Le RGPD prévoit que les garanties que s'engage à respecter l'entité ayant opéré des transferts de données valent pour les transferts ultérieurs au départ du pays tiers vers un autre pays tiers[Note 38], sans que l'on puisse savoir si une telle prescription n'est pas illusoire. La CNIL contrôle le contenu des contrats incluant un transfert de données vers un pays tiers. Dans une délibération du 1er décembre 2016 sur un dispositif d'alerte impliquant un transfert vers un prestataire aux États-Unis, elle a pris acte favorablement de ce que le contrat de prestation de services reprenait l'intégralité des clauses contractuelles-types de la Commission européenne[Note 39]. Certains observateurs soulignent le caractère protectionniste d'une législation qui érige des barrières autour de l'UE alors que par définition les systèmes informatiques n'ont pas de frontières. Mais, d'une part, l'Europe n'est pas seule à avoir cette démarche ; d'autre part, l'étape est nécessaire compte tenu du caractère aléatoire du contrôle des données lorsque les traitements sont éloignés de leurs utilisateurs.

14. - Sous un autre aspect, le RGPD apporte, cette fois-ci, de la simplification en supprimant les formalités préalables, déclaratives ou d'autorisation[Note 40]. Il y substitue l'autocontrôle : tout traitement susceptible d'engendrer un risque élevé pour les droits et libertés des personnes doit faire l'objet d'une analyse d'impact devant contenir « *une description du traitement et de ses finalités, une évaluation de la nécessité et de la proportionnalité, une appréciation des risques* [...] *et les mesures envisagées pour traiter ces risques ...*»[Note 41]. La future loi Informatique et Libertés prévoit que la CNIL est consultée sur les mesures à prendre face à un risque élevé lié au traitement ou aux technologies ou procédures utilisées[Note 42]. Cela pourrait être le cas des dispositifs d'alerte[Note 43]. Aussi, même en l'absence de traitements de données sensibles[Note 44], une analyse d'impact de ces dispositifs est-elle recommandée.

4. Les protagonistes de l'alerte et la protection des données personnelles

15. - Depuis l'origine, les législations sur l'alerte professionnelle ont tendu à sécuriser le lanceur d'alerte en le prémunissant contre d'éventuelles mesures de rétorsion. La proposition de directive sur les lanceurs d'alerte énumère les mesures de rétorsion susceptibles de viser aussi bien le salarié qu'un tiers lanceur d'alerte. Elle prévoit aussi des mesures de protection positives, parmi lesquelles l'assistance des autorités publiques ou encore le bénéfice du renversement de la charge de la preuve, celle-ci pesant sur l'auteur des mesures de rétorsion contestées[Note 45]. En outre, depuis la loi Sapin II, l'article 122-9 du Code pénal exonère de responsabilité pénale « *la personne qui porte atteinte à un secret protégé par la loi, dès lors que cette divulgation est nécessaire et proportionnée à la sauvegarde des intérêts en cause, qu'elle intervient dans le respect des procédures de signalement définies par la loi et que la personne répond aux critères de définition du lanceur d'alerte prévus à l'article 6 de la loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique* ». La jurisprudence aura à apprécier si cette disposition permet ou non de couvrir les cas de soustraction de données par des lanceurs d'alerte dans le but d'accréditer les faits signalés. Elle devra également déterminer comment concilier l'article 122-9 du Code pénal avec l'article226-18 du même code qui incrimine le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite[Note 46].

16. - Ces protections *ex post* des lanceurs d'alerte seraient insuffisantes si les lanceurs d'alerte n'étaient pas protégés *ex ante* par le secret gardé sur leur identité. Dans beaucoup de pays, comme le Royaume-Unis, la règle est l'anonymat ; encore que l'autorité de contrôle britannique indique qu'elle serait mieux à même de conduire une investigation si le lanceur d'alerte communiquait son identité[Note 47]. La proposition de directive sur les lanceurs d'alerte se borne quant à elle à évoquer la notion de confidentialité[Note 48]. Le seul dispositif invitant les lanceurs d'alerte en France à transmettre des signalements anonymes est celui mis en place par la Commission européenne pour encourager à dénoncer des cartels, *via* une adresse internet ou une *hotline*[Note 49]. Pour le reste, au regard du droit français, les lanceurs d'alerte ne bénéficient en général pas de l'anonymat vis-à-vis des destinataires de l'alerte[Note 50] (sous-traitant et responsable du traitement chargés spécifiquement de traiter les alertes). Leur identité ne peut être divulguée, sauf à l'autorité judiciaire, qu'avec leur consentement[Note 51]. Pour autant pour la CNIL, l'obligation pour le lanceur d'alerte de s'identifier auprès des destinataires de l'alerte, limite les risques de mises en cause abusives ou disproportionnées[Note 52]. Elle admet cependant que les alertes soient anonymes lorsque la gravité des faits, suffisamment détaillés, le justifie et moyennant l'examen préalable par leur premier destinataire de l'opportunité d'une diffusion dans le dispositif d'alerte[Note 53]. Une fois son identité connue du destinataire de l'alerte, lelanceur d'alerte est informé des suites données à son signalement[Note 54] et du fait que l'utilisation de bonne foi du dispositif ne l'expose à aucune sanction mais que, *a contrario*, une utilisation abusive l'expose à des sanctions disciplinaires et des poursuites judiciaires[Note 55]. L'expérience montre que l'absence d'anonymat est un frein au développement des signalements sur internet, intranet ou une *hotline* ; pourtant les responsables du traitement doivent s'abstenir d'encourager les lanceurs d'alerte à conserver l'anonymat[Note 56].

17. - La protection de l'identité de la personne mise en cause est tout aussi essentielle[Note 57]. Selon la CNIL, le mis en cause a le droit d'être informé qu'il est visé par une alerte, des faits reprochés et des modalités d'exercice de ses droits d'accès et rectification, et ce, dès l'enregistrement de ses données. Ce n'est que si des mesures conservatoires doivent être prises, notamment pour prévenir la destruction de preuves, que son information intervient après l'adoption de ces mesures[Note 58]. Les modalités de l'investigation menée sur la personne mise en cause répondent pour le reste aux nécessités de « *l'intérêt légitime* », au sens du RGPD, de l'entité qui traite l'alerte. La notion, aux contours volontairement vagues, permet de traiter des données, en dehors d'un cadre légal ou contractuel précis, « *compte tenu des attentes raisonnables des personnes concernées fondées sur leur relation avec le responsable du traitement* » [Note 59]. Cette notion rejoint celle retenue dans l'hypothèse soumise à la CEDH où un employeur, alerté du comportement délictuel d'un salarié, avait vérifié les fichiers sur le disque dur de l'ordinateur personnel de ce dernier hors sa présence. Dans son arrêt rendu en 2018[Note 60], la Cour a constaté que la consultation des fichiers par l'employeur du requérant répondait à un but légitime de protection des droits de l'employeur, qui pouvait donc « *légitimement* » vouloir s'assurer que ses salariés utilisent les équipements informatiques à leur disposition en conformité avec leurs obligations légales et contractuelles. Elle a relevé que si un employeur peut ouvrir des fichiers professionnels, il ne peut ouvrir ceux identifiés comme personnels qu'en présence de l'employé ; tout en notant qu'en l'espèce les fichiers litigieux n'étaient pas identifiés comme privés.

5. De la mise en oeuvre de mesures de sécurité appropriées

18. - Comme tous les traitements informatiques, ceux dont la finalité est l'alerte professionnelle sont sujets à des cyberattaques. Avant même la montée de ce risque, le droit de la protection des données a consacré le principe de la minimisation des données[Note 61]. Selon ce principe, les données collectées sur des individus doivent être limitées à ce qui est strictement nécessaire au regard de la finalité du traitement[Note 62]. La CNIL vérifie alors si les données traitées à fins d'alerte professionnelle correspondent à ce qui est utile au fonctionnement du dispositif et proportionné. L'autorisation unique AU-004, qui fixe la doctrine, de la CNIL prévoit que peuvent ainsi être collectées l'identité, les fonctions et coordonnées de l'émetteur de l'alerte, de la personne mise en cause ainsi que des personnes intervenant dans le recueil ou le traitement de l'alerte ; de même que les éléments sur les faits signalés, ceux recueillis lors de la vérification de ces faits, le compte rendu des opérations de vérification et des suites données à l'alerte[Note 63].

19. - Le deuxième moyen de prévenir les violations de données est de limiter autant que faire se peut les destinataires de l'alerte[Note 64] qui doivent être désignés, selon la CNIL, parmi ceux ayant un « *intérêt légitime* » à accéder aux données[Note 65]. Procédant à une analyse casuistique, la CNIL reconnaît qu'il en est ainsi du personnel du prestataire en charge de la réception des alertes, du responsable de l'éthique et de la conformité, des membres de la direction juridique, du directeur de l'audit interne, des responsables des ressources humaines, ainsi que des personnes en charge des investigations. Tous sont astreints à une obligation renforcée de confidentialité contractuellement définie[Note 66] ; et n'accèdent aux données que dans la stricte limite de leurs attributions[Note 67].

20. - Une troisième façon d'éviter la violation de données sur les alertes est de les rendre inaccessibles, ce qui est le cas par définition lorsqu'elles sont effacées. Là encore, l'approche de la CNIL est de réduire au strict minimum ladurée de conservation des données[Note 68]. La procédure de recueil des alertes doit préciser les dispositions prises afin de détruire les données de signalement de nature à permettre l'identification de lanceur d'alerte et des personnes visées lorsqu'aucune suite n'y a été donnée, ainsi que le délai de conservation des données limitée à deux mois à compter de la clôture des opérations de recevabilité ou de vérification[Note 69]. Lorsqu'une procédure disciplinaire ou judiciaire est engagée à l'encontre de la personne mise en cause ou de l'auteur d'une alerte abusive, les données sont conservées uniquement jusqu'au terme de la procédure. Même les données archivées, qui doivent figurer dans un système d'information distinct à accès restreint, ne peuvent être conservées au-delà des délais des procédures contentieuses[Note 70]. La problématique de la destruction des données dépasse le cadre du présent article. Mais il est un fait - regrettable - que la doctrine de la CNIL tendant à faire disparaître les informations une fois leur utilisation achevée, peut conduire à une perte de valeur en privant les chercheurs, notamment les historiens, d'un accès à la connaissance. En dehors de l'obligation de limiter les catégories de données traitées et leur durée de conservation ainsi que le nombre des destinataires des données, tout gestionnaire d'un traitement à finalité d'alerte professionnelle (responsable du traitement et sous-traitant) est tenu de prendre les mesures techniques[Note 71] nécessaires pour prévenir l'accès ou l'utilisation non autorisé ou illicite des données ou de l'équipement utilisé. La pseudonymisation et le chiffrement des données ont été encouragés par la CNIL[Note 72] avant le RGPD[Note 73].

21. - Les mesures organisationnelles préconisées par la CNIL portent sur l'authentification des utilisateurs du dispositif d'alerte avec un identifiant et un mot de passe[Note 74] à renouveler régulièrement[Note 75], et le recours à la fonction de hachage HMAC à clé secrète[Note 76]. Les habilitations doit être attribuées à l'issue de procédures formalisées, validées par le responsable du traitement, mises à jour et portées à la connaissance des utilisateurs[Note 77]. Un mécanisme de journalisationdes accès doit être mis en place pour assurer la traçabilité d'éventuels incidents ou intrusions[Note 78]. L'échange de données par messagerie et canaux sécurisés et l'utilisation du protocole HTTPS[Note 79], le gardiennage des locaux et l'existence d'un système de badges constituent autant de mesures de sécurité jugées appropriées[Note 80]. La maintenance des matériels doit être assurée. De façon plus générale, les mesures de sécurité doivent être réexaminées au regard de la réévaluation permanente des risques[Note 81].

22. - La gestion des risques informatiques est maintenant intégrée, sinon toujours parfaitement appropriée, par les opérateurs de traitements. Ce qui a changé fondamentalement, c'est l'échelle des sanctions en cas de violation des données. Les autorités de contrôle comme la CNIL peuvent désormais infliger des amendes jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires mondial, le montant le plus élevé étant retenu[Note 82]. La gestion des dispositifs d'alerte est devenue un des volets importants de la politique de conformité que les entreprises comme les administrations ont conscience de devoir très sérieusement mettre en oeuvre.

6. Responsabilités des gestionnaires des traitements à fins d'alerte professionnelle et conformité

23. - La première démarche à effectuer, une fois envisagée l'installation d'un dispositif d'alerte professionnelle est pour le responsable du traitement d'informer son personnel[Note 83] et ses collaborateurs extérieurs ou occasionnels. Cette information peut passer par son code de conduite, une campagne d'affichage sur les sites du groupe, une publication, un courriel aux salariés (voire, pour tenir compte des obligations découlant de la loi sur le devoir de vigilance, aux sous-traitants et fournisseurs avec lesquels il entretient « *une relation commerciale établie* »), des mentions ou notes d'information publiées sur le site internet et intranet du groupe, un livret à destination de ses partenaires[Note 84]... Cette information doit préciser la procédure de recueil des signalements, en définir les destinataires ainsi que les conditions de transmission des signalements à chacun d'entre eux[Note 85]. Les responsables du traitement doivent veiller à informer et consulter préalablement les institutions représentatives du personnel[Note 86] ainsi que l'inspection du travail si la procédure est intégrée au règlement intérieur ; la CNIL en prenant acte[Note 87]. La proposition de directive sur les lanceurs d'alerte détaille en outre les informations à diffuser par les autorités compétentes[Note 88] auprès du public.

24. - Outre ce devoir d'information, le responsable du traitement doit veiller au recrutement de ses sous-traitants, qui doivent présenter des « *garanties suffisantes* », ainsi qu' au contrôle de leurs prestations en matière d'alerte professionnelle comme en toute autre matière. Les contrats de prestations de services doivent contenir toutes les instructions nécessaires à la protection de la sécurité des données et définir la finalité et la durée du traitement, le type de données traitées, les catégories de personnes concernées, la répartition des droits et obligations des cocontractants[Note 89]. Au surplus, les registres

des activités de traitement, respectivement tenus par chaque responsable du traitement et chaque sous-traitant, doivent comporter toutes les spécifications du dispositif d'alerte[Note 90]. Les entreprises sont incitées à adopter des politiques internes de gestion de l'alerte, à former leurs personnels et partenaires, à auditer les systèmes d'alerte et à intégrer les résultats des audits dans la cartographie des risques. Ces exigences de conformité se fondent sur un principe d'*accountability*, à savoir la nécessité de rendre compte de ses activités et éventuels manquements qui, venu des pays de *Common law*, s'impose ainsi en France.

25. - Cette logique de conformité se conjugue avec une logique de responsabilité. En effet, les responsabilités juridiques, à la fois administrative, pénale et civile des gestionnaires de dispositif d'alertes sont potentiellement considérables[Note 91]. Toute violation de données personnelles oblige le sous-traitant à la notifier au plus vite au responsable du traitement, lequel, quant à lui, doit la notifier à l'autorité de contrôle (en France, la CNIL) si possible dans les 72 heures[Note 92]. En pratique, la CNIL se rend dans l'entreprise pour des vérifications sur place. En fonction des manquements constatés, elle peut sanctionner très lourdement l'entité fautive (V. plus haut). Cette dernière peut aussi être sanctionnée pénalement pour violation de la confidentialité des données du dispositif d'alerte professionnelle, jusqu'à deux ans d'emprisonnement et 30 000 euros d'amende[Note 93]. Si l'infraction est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement se doit de les en aviser dans les meilleurs délais. Par ailleurs, il s'expose à une action collective[Note 94].

26. - Pour conclure, la volonté du législateur européen ou français de faire de tout un chacun un collaborateur de la Justice au sens non seulement institutionnel, mais éthique, est l'une des principales marques de l'évolution culturelle à l'oeuvre. Elles répondent à une demande sociale de mettre fin à l'impunité des « puissants » et de responsabiliser les acteurs publics et économiques. Les dispositifs d'alerte sont regardés par les autorités judiciaires, dans le cadre de la lutte contre la corruption, comme l'un des moyens essentiels de prévention de ce risque.Dans le droit fil de l'approche de la justice américaine[Note 95], reflétée dans les transactions pénalesconcernant par exemple, pour ne mentionner qu'elles, Alcatel-Lucent, Technip, Total, ou Alstom, le Parquet de Nanterre a tenu compte dans l'une des toutes premières conventions judiciaires d'intérêt public, et à titre de circonstance atténuante, notamment, de la mise en place de systèmes d'alerte professionnelle[Note 96]. De même, dans ses recommandations de décembre 2017[Note 97], l'Agence Française Anti-corruption place les dispositifs d'alerte parmi les principales mesures de prévention et de détection de ce risque. Parallèlement, l'encadrement juridique de l'alerte par le droit de la protection des données est utile pour prévenir les abus d'un dispositif qui doit rester destiné à favoriser la paix sociale, et non la remettre en cause.

Note 1 *Prop. dir. n° 2018-0106, 2 avr. 2018 relative à la protection des personnes dénonçant des violations du droit de l'Union*.

Note 2 In The Guardian, *Barlcays CEO Jes Staley faces fine over whistleblower incident,* April 20, 2018 https://www.theguardian.com/business/2018/apr/20/barclays-ceo-jes-staley-facing-fine-over-whistleblower-incident

Note 3 *Avant-Propos, Les lanceurs d'alerte, Quelle protection juridique ? Quelles limites ?, ss dir. M. Disant et D. Pollet-Panoussis : LGDJ, 2017*.

Note 4 *Cons. UE, dir. 1976/207/CEE, 9 févr. 1976 relative à la mise en oeuvre du principe de l'égalité de traitement entre hommes et femmes : JOCE n° L 39, 14 févr.1976, p. 40. - Cons. UE, dir. 2000/43/CE, 29 juin 2000 relative à la mise en oeuvre du principe de l'égalité de traitement entre les personnes sans distinction de race ou d'origine ethnique : JOCE n° L 180, 19 juill. 2000, p. 22. - Cons. UE, dir. 2002/73/CE, 23 sept. 2002 relative à la mise en oeuvre du principe de l'égalité de traitement entre hommes et femmes en ce qui concerne l'accès à l'emploi, à la formation et à la promotion professionnelles, et les conditions de travail : JOCE n° L 269/15, 5 oct. 2002, p. 15. - Cons. UE, dir. 2004/113/CE, 13 déc. 2004 mettant en oeuvre le principe de l'égalité de traitement entre les femmes et les hommes dans l'accès à des biens et services et la fourniture de biens et services : JOUE n° L 373, 21 déc. 2004, p. 37. - Cons. UE, dir. 2006/54, 5 juill. 2006 relative à la mise en oeuvre du principe de l'égalité des chances et de l'égalité de traitement entre hommes et femmes en matière d'emploi et de travail (refonte) : JOUE n° L 204, 26 juill. 2006, p. 23.*

Note 5 *Sarbanes-Oxley Act, 30 juill. 2002 : Public Law 107-204.* - V. aussi *le Dodd-Franck Act, 21 juill. 2010 : Public Law 111-203.*

Note 6 *PE et Cons. UE, dir. 2013/36/UE, 26 juin 2013 concernant l'accès à l'activité des établissements de crédit et la surveillance prudentielle des établissements de crédit et des entreprises d'investissement : JOUE n° L 176, 27 juin 2013, p. 338. - PE et Cons. UE, règl. (UE) n° 575/2013, 26 juin 2013 concernant les exigences prudentielles applicables aux établissements de crédit et aux entreprises d'investissement :*

JOUE n° L 176, 27 juin 2013, p. 1. - PE et Cons. UE, règl. (UE) n° 596/2014, 16 avr. 2014 sur les abus de marché : JOUE n° L 173, 12 juin 2014, p. 1.

Note 7 *Cons. UE, dir. 2013/30/UE, 12 juin 2013 relative à la sécurité des opérations pétrolières et gazières en mer : JOUE n° L 178, 28 juin 2013.*

Note 8 *PE et Cons. UE, dir. 2016/943/UE, 8 juin 2016 sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites : JOUE n° L 157, 15 juin 2016, p. 1. - Prop. loi de transposition n° 675, AN, 19 févr. 2018.* - V. également, *La loi sur le secret des affaires menace-t-elle la liberté d'informer ? : Le Monde 27 févr. 2018. - P. Durand et E. Joly, Le « secret des affaires », une menace pour la démocratie : Libération 14 mai 2016.*

Note 9 *N. Lenoir, Les lanceurs d'alerte, une innovation française venue d'outre-Atlantique : JCP E 2015, 1492*. - V. le *False Claim Act* de 1863 sur le droit de tout citoyen d'intenter une action civile au nom du gouvernement fédéral à l'encontre de quiconque commet des fraudes à son préjudice.

Note 10 *CNIL, délib., n° 2005-110 et n° 2005-111, 26 mai 2005*.

Note 11 Document d'orientation du 10 novembre 2005 pour la mise en oeuvre de dispositifs d'alerte professionnelle.

Note 12 *CNIL, délib. n° 2005-305, 8 déc. 2005, NOR CNIX0508957X*, modifiée en dernier lieu par la *CNIL, délib. n° 2017-191, 22 juin 2017*.

Note 13 Le RGPD supprime les formalités préalables, les normes déjà adoptées par la CNIL (autorisation unique, norme simplifiée, méthodologie de référence) devenant des référentiels.

Note 14 *CNIL, délib. n° 2018-042, 8 févr. 2018. - CNIL, délib. n° 2017-160, 18 mai 2017. - CNIL, délib. n° 2016-051, 25 févr. 2016. - CNIL, délib. n°2016-113, 21 avr. 2016. - CNIL, délib. n° 2016-356, 1er déc. 2016.*

Note 15 *CEDH, gr. ch., 12 févr. 2008, n° 14277/04, Guja c/ Moldova : JurisData n° 2008-010477. - CEDH, 19 févr. 2009, n° 4063/04, Marchenko c/ Ukraine. - CEDH, 21 juill. 2001, n 2874/08, Heinisch c/ Allemagne. - CEDH, 8 janv. 2013, n° 40238/02, Bucur et Toma c/ Roumanie.*

Note 16 *Cons. UE, règl. (UE) n° 2016/679, 27 avr. 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données : JOUE n° L 119, 4 mai 2016, p. 1.*

Note 17 *Cons. UE, dir. 2016/680/UE, 27 avr. 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données : JOUE n° L 119, 4 mai 2016*.

Note 18 V. également *Cons. Europe, Conv. STE n° 108, 28 janv. 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*.

Note 19 *Doc. AN, Projet loi n° 490, 13 déc. 2017 relatif à la protection des données personnelles*.

Note 20 *S. Gibaud, La femme qui en savait vraiment trop : Le Cherche-Midi, 2014*.

Note 21 *L. n° 2016-1691, 9 déc. 2016, art. 8, relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, dite loi « Sapin II » : Journal Officiel du 10 Décembre 2016, texte n° 2.*

Note 22 *Conseil d'État, Rapport « Le Droit d'alerte : signaler, traiter, protéger », 25 févr. 2016*.

Note 23 *L.* n° *2017-399, 27 mars 2017 sur le devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre : Journal Officiel du 28 Mars 2017 , texte n° 1.*

Note 24 *CNIL délib., n° 2018-042, préc. note 14*.

Note 25 *N. Lenoir, préc. note 9, spéc. p. 48. - Conseil d'État, Rapp. préc. note 22, spéc. p. 70-72.*

Note 26 Parmi les autres régimes d'alerte subsistant : outre *CPP, art. 40, al. 2* réservé aux autorités constituées, on peut citer : *C. trav., art. L. 4131-1 ; C. pén., art. 434-1, 223-6 et 434-3 ; L. n° 2016-1917, 29 déc. 2016 de finances pour 2017, art. 109* (lanceurs d'alerte fiscaux).

Note 27 Les domaines sont les suivants : marchés publics, secteur financier (y inclus la prévention du blanchiment d'argent et du financement du terrorisme), sécurité des produits, des transports, sécurité nucléaire, santé, protection de l'environnement, protection du consommateur, concurrence, atteinte aux règles du marché intérieur et aux intérêts financiers de l'Union et même protection de la vie privée et des données personnelles et sécurité des systèmes d'information.

Note 28 *L. n° 2016-1691, art. 6.*

Note 29 V. l'évolution qu'a connu le champ de l'autorisation unique AU-004 de la CNIL au travers de délibérations successives jusqu'à la dernière en date du 22 juin 2017 n° 2017-191 prise pour tenir compte de la loi Sapin II et des derniers développements législatifs et règlementaires en matière de délinquance financière.

Note 30 *http://www.assemblee-nationale.fr/15/propositions/pion0893.asp*- À l'exception du secret médical, du secret de la défense et du secret des relations avocat/client.

Note 31 V. le texte dans sa dernière version (quasi définitive), *Doc. AN, PPL n° 893, 19 avr. 2018.*

Note 32 *RGPD, art. 2*.

Note 33 *RGPD, art. 4 (2).*

Note 34 *CE, 12 mars 2014, n° 354629 : JurisData n° 2014-004450*. - V. Ouvrage collectif, *Protection des données personnelles, se mettre en conformité d'ici le 25 mai 2018 : Editions législatives, 2017, p.140.*

Note 35 *RGPD, cons. 146, art. 24 et 82 (2).*

Note 36 Décision attestant qu'il offre un niveau de protection suffisant. Le *Privacy Shield* du 12 juillet 2016, qui permet le transfert de données aux États-Unis vers les entreprises certifiées à cet effet auprès de la *Federal Trade Commission*, résulte d'une décision d'adéquation de la Commission : *Comm. UE, déc. 2016/1250/UE, 12 juill. 2016.*

Note 37 La CNIL définit sur son site ces règles d'entreprise comme « *un code de conduite définissant la politique d'une entreprise en matière de transferts de données personnelles [et permettent] d'offrir une protection adéquate aux données transférées depuis l'UE vers des pays tiers à l'UE au sein d'une même entreprise ou d'un même groupe* ».

Note 38 *RGPD, art. 44.*

Note 39 *CNIL, délib. n° 2016-356, préc. note 14.*

Note 40 L'Article 9 du RGPD laisse une marge de manoeuvre aux États membres pour le traitement de données génétiques ou biométriques ou comportant le numéro de sécurité sociale ; ils peuvent « *maintenir ou introduire des conditions supplémentaires, y compris des limitations en ce qui concerne le traitement de ces données* ».

Note 41 *RGPD, art. 35 (7).*

Note 42 *Doc. AN, Projet loi n° 110, 12 avr. 2018, art. 70-4.*

Note 43 Sur son site internet, la CNIL cite 9 critères dont 2 s'ils sont remplis devraient conduire à réaliser une analyse d'impact : *https://www.cnil.fr/fr/ce-quil-faut-savoir-sur-lanalyse-dimpact-relative-la-protection-des-donnees-dpia*

Note 44 Données sur les origines raciales ou ethniques, les orientations sexuelles, opinions politiques, convictions religieuses ou philosophiques, appartenance syndicale, données génétiques et biométriques, condamnations pénales et infractions (*RGPD, art. 9, 10*).

Note 45 *Prop. dir. préc. note 1, art. 14 et 15*.

Note 46 Rappelons qu'Hervé Falciani, lanceur d'alerte et ex-informaticien d'HSBC qui avait soustrait des fichiers de clients de la banque, a été condamné par contumace en 2015 en Suisse pour soustraction de données et espionnage économique aggravé.

Note 47 Site de *l'Information Commissioner's Office* (ICO) sur « *protection for whistle blowers* ».

Note 48 *Prop. dir. préc. note 1, art. 5.*

Note 49 *http://ec.europa.eu/competition/cartels/whistleblower/index.html=*

Note 50 *CNIL, délib. n° 2016-356, préc. note 14*.

Note 51 *L. n° 2016-1692, art. 9*. - V. aussi *D. n° 2017-564, 19 avr. 2017, art. 5.*

Note 52 *CNIL, délib. n°2018-042, préc. note 14. - CNIL, délib. n° 2017-095, 23 mars 2017. - CNIL, délib. n° 2016-051, préc. note 14.*

Note 53 *CNIL, délib. n° 2018-042, préc. note 14. - CNIL, délib. n° 2017-191, préc. note 29. - CNIL, délib. n° 2017-095, 23 mars 2017. - CNIL, délib. n° 2016-051, préc. note 14. - CNIL, délib. n° 2016-113, préc. note 14. CNIL, délib. n°2016-356, préc. note 14*.

Note 54 *D. n° 2017-564, 19 avr. 2017, art. 5.*

Note 55 *CNIL, délib. n° 2018-042, préc. note 14. - CNIL, délib. n° 2017-160, 18 mai 2017*.

Note 56 *CNIL, délib. n° 2017-191, préc. note 29, art. 2*.

Note 57 L' « affaire » Renault est illustrative : elle débute en 2010 par l'envoi d'une lettre anonyme à la direction, suivie d'une enquête interne menée par des responsables de la sécurité qui se solde par le licenciement de trois cadres dirigeants et la plainte de l'entreprise pour « espionnage industriel, corruption, abus de confiance, vol et recel commis en bande organisée ». L'affaire est rendue publique par l'entreprise dans les médias. Or l'enquête de la DCRI n'accrédite pas les faits, mais met en cause les responsables de la sécurité du groupe pour escroquerie en bande organisée : un prétendu informateur anonyme ayant été rémunéré par eux via un intermédiaire afin de donner corps aux soupçons d'espionnage.

Note 58 *CNIL, délib. n° 2018-042, préc. note 14. - CNIL, délib. n° 2017-160, préc. note 14. - CNIL, délib. n° 2016-051, préc. note 14. - CNIL, délib. n° 2016-113, préc. note 14. - CNIL, délib. n° 2016-356, préc. note 14. - CNIL, délib. n° 2017-191, préc. note 29, art. 9*.

Note 59 *RGPD, cons. 47*.

Note 60 *CEDH, 22 févr. 2018, n° 588/13, Libert c/France : JurisData n ° 2018-002784 ; JCP G 2018, act. 290, obs. F. Sudre ; JCP G 2018, 433, note F. Marchadier*, à propos d'un agent d'une entreprise publique licencié pour avoir stocké sur son ordinateur professionnel des fichiers et de fausses attestations.

Note 61 Principe confirmé par *RGPD, art. 5(1) (c).*

Note 62 *CNIL, délib. n° 2018-042, préc. note 14. - CNIL, délib. n° 2017-160, préc. note 14. - CNIL, délib. n° 2017-095, préc. note 53. - CNIL, délib. n° 2016-051, préc. note 14. - CNIL, délib. n° 2016-113, préc. note 14. - CNIL, délib. n° 2016-356, préc. note 14. - CNIL, délib. n° 2017-191, préc. note 29, art. 3.*

Note 63 *CNIL, délib. n° 2018-042, préc. note 14. - CNIL, délib. n° 2016-051, préc. note 14. - CNIL, délib. n° 2016-113, préc. note 14. - CNIL, délib. n° 2016-356, préc. note 14*. - Il appartiendra à la jurisprudence d'apprécier la possibilité ou non d'enregistrer des données sur la santé physique ou mentale du mis en cause, ou sur sa religion, par exemple, s'il en découle certains comportements.

Note 64 *CNIL, délib. n° 2017-095, préc. note 53. - RGPD, art. 25 (2). - G29, Opinion 1/2006 "On the application of EU data protection rules to internal whistleblowing schemes in field of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime", p. 10*.

Note 65 *CNIL, délib. n° 2018-042, préc. note 14. - CNIL, délib. n° 2017-160, préc. note 14. - CNIL, délib. n° 2016-051, préc. note 14. - CNIL, délib. n° 2016-113, préc. note 14. - CNIL, délib. n° 2016-356, préc. note 14*.

Note 66 *CNIL, délib. n° 2018-042, préc. note 14. - CNIL, délib. n° 2017-160, préc. note 14. - CNIL, délib. n° 2016-051, préc. note 14. - CNIL, délib. n° 2016-113, préc. note 14. - CNIL, délib. n° 2016-356, préc. note 14. - G29, Avis 1/2006, préc. note 65, spéc. p.15*.

Note 67 *CNIL, délib. n° 2016-356, préc. note 14*.

Note 68 *RGPD, cons. 39 et art. 5(1) (e). - CNIL, délib. n° 2018-042, préc. note 14. - CNIL, délib. n° 2017-160, préc. note 14. - CNIL, délib. n° 2016-051, préc. note 14. - CNIL, délib. n° 2016-113, préc. note 14. - CNIL, délib. n° 2016-356, préc. note 14.*

Note 69 *D. n° 2017-564, 19 avr. 2017, art. 5.*

Note 70 *CNIL, délib. n° 2017-191, préc. note 29, art. 6.*

Note 71 *RGPD, art. 5(1) (f).* - V. aussi *RGPD, cons. 39.*

Note 72 *RGPD, art. 32 (1). - CNIL, délib. n° 2018-042, préc. note 14. - CNIL, délib. n° 2017-160, préc. note 14. - CNIL, délib. n° 2017-095, préc. note 53. - CNIL, délib. n° 2016-051, préc. note 14. - CNIL, délib. n° 2016-113, préc. note 14. - CNIL, délib. n° 2016-356, préc. note 14*.

Note 73 *RGPD, art. 4 (5) et 32 (1) (a*) : ces mesures de sécurité permettent de réduire considérablement le risque d'identification d'une personne.

Note 74 *CNIL, délib. n° 2018-042, préc. note 14. - CNIL, délib. n° 2017-160, préc. note 14. - CNIL, délib. n° 2016-051, préc. note 14. - CNIL, délib. n° 2016-113, préc. note 14. - CNIL, délib. n° 2016-356, préc. note 14.*

Note 75 *CNIL, délib. n° 2017-160, préc. note 14. - CNIL, délib. n° 2017-095, préc. note 53*.

Note 76 *CNIL, délib. n° 2017-160, préc. note 14. - CNIL, délib. n° 2016-113, préc. note 14.*

Note 77 *CNIL, délib. n° 2018-042, préc. note 14. - CNIL, délib. n° 2017-160, préc. note 14. - CNIL, délib. n° 2016-051, préc. note 14. - CNIL, délib. n° 2016-356, préc. note 14.*

Note 78 *CNIL, délib. n° 2018-042, préc. note 14. - CNIL, délib. n° 2017-160, préc. note 14. - CNIL, délib. n° 2016-051, préc. note 14. - CNIL, délib. n° 2016-113, préc. note 14.*

Note 79 *CNIL, délib. n° 2017-095, préc. note 53*.

Note 80 *CNIL, délib. n° 2017-095, préc. note 53*.

Note 81 *CNIL, délib. n° 2018-042, préc. note 14. - CNIL, délib. n° 2017-160, préc. note 14. - CNIL, délib. n° 2016-051, préc. note 14. - CNIL, délib. n° 2016-356, préc. note 14.*

Note 82 *RGPD, art. 83*.

Note 83 Aux termes de l'article L. 1222-4 du Code du travail, « *Aucune information concernant personnellement un salarié ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance* ».

Note 84 *CNIL, délib. n° 2018-042, préc. note 14. - CNIL, délib. n° 2017-160, préc. note 14. - CNIL, délib. n° 2016-051, préc. note 14. - CNIL, délib. n° 2016-356, préc. note 14.*

Note 85 *CNIL, délib. n° 2017-191, préc. note 29, art. 8*.

Note 86 *C. trav., art. L.2312-38*.

Note 87 *CNIL, délib. n° 2018-042, préc. note 14.*

Note 88 L'article 10 de la proposition de directive sur les lanceurs d'alerte (*préc. note 1)*, prévoit notamment une obligation de communiquer un numéro de téléphone, une adresse e-mail et postale dédiée, de mettre en oeuvre une procédure spécifique pour la notification des violations, et d'informer sur les recours et procédures prévues contre les mesures de représailles.

Note 89 *RGPD, art. 28 (1) et (3).*

Note 90 *RGPD, art. 30*.

Note 91 *D. Fatôme, Quelles actions judiciaires en cas de violation du RGPD : Comm. com. électr. 2018, dossier 18.*

Note 92 *RGPD, art. 33 (1) et (2).*

Note 93 *L. n° 2016-1691, art. 9.*

Note 94 V. *L. n° 2016-1547, 18 nov. 2016 de modernisation de la justice du XXIe siècle : Journal Officiel du 19 Novembre 2016, texte n° 1*.

Note 95 *US Federal Sentencing Guidelines, 2016, §8B2.1(5).*

Note 96 *CJIP, 15 févr. 2018* concernant la SAS Kaefer Wanner (*RPPI 2018, act. 12)*, validée par *TGI Nanterre, ord., 23 févr. 2018, n° 11245045572*. Il s'agissait de la diffusion d'une charte sur les lanceurs d'alerte et de la création d'un système (outre l'alerte interne) permettant, par téléphone et chez un prestataire indépendant, de lancer une alerte.

Note 97 https://www.economie.gouv.fr/files/files/directions_services/afa/2017_-_Recommandations_AFA.pdf.