FOCUS

Mai 2017

ADAMAS
Avocats associés

Loi Sapin II : Le nouveau régime du lancement d'alerte à l'épreuve de la réglementation applicable aux données personnelles

Perçu parfois comme une Cassandre des temps modernes[1], le lanceur d'alerte se manifeste aujourd'hui, à travers le monde, pour avertir les autorités compétentes, voire son prochain, des menaces qui pèsent sur l'intérêt général ou leur dévoiler des actes illicites.

Bien souvent défenseur de l'Etat de droit et dernier recours lorsque les contrôles sont défaillants, le lanceur d'alerte est pourtant fréquemment l'objet de représailles ou de sanctions de nature variée, comme en atteste l'actualité relayée par la presse internationale.

Il fallait donc qu'il bénéficie, sous réserve de respecter certaines conditions, d'une protection appropriée en France. Tel est l'un des objectifs poursuivis par la loi relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, dite « Loi Sapin II »[2]. Le premier axe de cette loi, promulguée le 9 décembre 2016, est le renforcement de la protection des lanceurs d'alerte, notamment par la définition d'un statut général de ceux-ci[3].

Comme l'a rappelé M. Michel Sapin lui-même, en sa qualité de ministre des finances et des comptes publics, lors des débats publics au Sénat, le législateur devait, à travers ce texte, « *concilier, d'une part, la protection de la liberté de communication et d'expression du lanceur d'alerte contre toute atteinte ou sanction injustifiée, et, d'autre part, la sauvegarde de l'ordre public et la protection des droits des tiers, en particulier du droit au respect de la vie privée* »[4].

L'adoption de cette loi et la récente promulgation du décret d'application relatif à ce mécanisme[5] sont donc l'occasion de rappeler les règles régissant la protection des données personnelles en la matière, en particulier à la lumière du Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 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 (ci-après le « RGDP »), qui entrera en vigueur à compter du 25 mai 2018.

---

[1] Voir notamment : « *Le « milieu du gué » de la protection législative des lanceurs d'alerte* », Anna Billard, Marc Duranton, Jean-Philippe Foegle et Tristan Martin-Teodorczyk, La Revue des droits de l'homme, Actualités Droits-Libertés, mis en ligne le 20 mai 2014, consulté le 13 avril 2017. URL : http://revdh.revues.org/752 ; DOI : 10.4000/revdh.752

[2] 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.

[3] Articles 6 à 15 de la Loi Sapin II.

[4] https://www.senat.fr/seances/s201607/s20160704/s20160704001.html

[5] Décret n° 2017-564 du 19 avril 2017 relatif aux procédures de recueil des signalements émis par les lanceurs d'alerte au sein des personnes morales de droit public ou de droit privé ou des administrations de l'Etat.

I. Présentation du nouveau régime de lancement d'alerte

A. La procédure d'alerte issue de l'article 8 de la Loi Sapin II

Aux termes des dispositions de ses articles 6 à 15, la Loi Sapin II a instauré un socle légal général du lancement d'alerte, alors qu'il n'existait jusqu'alors que des dispositifs d'alerte spécifiques et propres à certains domaines.

Dès 1982, avait été créé, au sein des entreprises, un mécanisme d'alerte en matière de santé et de sécurité à l'égard des salariés et des représentants du personnel membres du CHSCT[6]. Puis, à compter de 2002, en application de la Loi Sarbanes-Oxley[7], les filiales françaises de sociétés étrangères cotées aux États-Unis avaient également été dans l'obligation de mettre en place des dispositifs d'alerte professionnelle permettant aux salariés de signaler des fraudes ou malversations comptables ou financières.

En revanche, il a fallu attendre 2007 pour que des dispositifs d'alerte concernant « l'éthique » de l'entreprise soient progressivement introduits en droit français. Des dispositifs spécifiques ont ainsi été mis en place dans les domaines de la corruption[8], des risques sanitaires liés à des médicaments[9], des risques graves pour la santé ou de l'environnement[10], des conflits d'intérêts des responsables politiques et des agents du service public[11] ou encore de la fraude fiscale[12].

Devant ces mécanismes éparses, parfois sans véritable cohérence les uns par rapport aux autres et susceptibles de conduire à une insécurité juridique pour les lanceurs d'alerte, comme l'avait souligné le Conseil d'Etat dans son rapport du 25 février 2016[13], le législateur a souhaité instaurer un socle légal commun aux différents mécanismes d'alerte.

La Loi Sapin II a ainsi défini, de manière générale, le lanceur d'alerte comme 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, de la loi ou d'un règlement notamment, ou une menace ou un préjudice grave pour l'intérêt général, dont elle a eu personnellement connaissance[14]. Comme l'a précisé le Conseil constitutionnel[15], cette définition a vocation à s'appliquer non seulement aux cas prévus par le mécanisme mis en place par la Loi Sapin II mais également à d'autres procédures d'alerte instaurées par le législateur, le cas échéant[16].

Il sera observé que sont exclues de cette définition les personnes morales, de sorte que les syndicats, les associations ou les ONG, ne pourront bénéficier de cette qualification.

---

[6] Loi n°82-10987 du 23 décembre 1982.
[7] Section 301 (4), Public Law 107-204, https://www.sec.gov/about/laws/soa2002.pdf
[8] Loi n°2007-1598 du 13 novembre 2007.
[9] Loi n°2011-2012 du 29 décembre 2011.
[10] Loi n°2016-316 du 16 avril 2013.
[11] Loi n°2013-907 du 11 octobre 2013.
[12] Loi n°2013-1117 du 6 décembre 2013.
[13] Le droit d'alerte : signaler, traiter, protéger : Les études du Conseil d'État, 25 févr. 2016, p. 25 et s. : http://www.conseil-etat.fr/content/download/59086/527939/version/1/file/2016%20ce_etude_droit%20d%20alerte.pdf
[14] Article 6 de la Loi Sapin II.
[15] Cons. Consti., n°2016-741, 8 décembre 2016.
[16] Commentaire de la décision du Conseil constitutionnel n°2016-740 du 8 décembre 2016.

Il convient également de préciser que les faits couverts par le secret de la défense nationale, par le secret médical ou par le secret des relations clients-avocats sont « *exclus du régime de l'alerte* » défini par la Loi Sapin II, contrairement à la proposition initiale de cette loi[17]. Comme le relèvent certains auteurs[18], le secret des affaires, désormais protégé au titre de la directive sur le secret d'affaires adoptée le 14 avril 2016 par le Parlement Européen[19], n'est cependant pas visé parmi ces exceptions.

La Loi Sapin II a instauré une procédure d'alerte pour les « *personnes morales de droit public ou de droit privé d'au moins cinquante salariés* », ces dernières devant mettre en place des « *procédures appropriées de recueil des signalements émis par les membres de leur personnel ou par des collaborateurs extérieurs et occasionnels* »[20].

Les entreprises d'au moins cinquante salariés devront organiser en interne, à compter du 1er janvier 2018, c'est-à-dire à l'entrée en vigueur du décret d'application de ce mécanisme[21], une procédure permettant à leurs salariés, mais également à leurs collaborateurs extérieurs occasionnels, de lancer des alertes relatives aux manquements qu'ils constatent dans l'exercice de leurs missions.

Selon les dispositions de l'article 8 de la Loi Sapin II, le « *supérieur hiérarchique, direct ou indirect, de l'employeur* » ou le « *référent désigné* » par ce dernier sera le premier destinataire d'une alerte. Ce n'est qu'en l'absence de diligences de celui-ci « *dans un délai raisonnable* » que l'alerte pourra être adressée « *à l'autorité judiciaire, à l'autorité administrative ou aux ordres professionnels* ». Enfin, « *en dernier ressort* », à défaut de traitement par ces organismes dans un délai de trois mois, « *le signalement [pourra] être rendu public* ».

La Loi Sapin II instaure de cette façon un mécanisme en cascade, critiqué par certains comme permettant à l'employeur, premier destinataire et, le plus souvent, premier concerné, de dissimuler (ou du moins tenter de dissimuler) les faits qui pourraient lui être dénoncés. Pour d'autres, cette procédure est un moyen de lutter contre les multiples « délations » publiques relayées dans les médias qui sont de plus en plus pratiquées et qui font pression sur les autorités judiciaires et peuvent ainsi nuire au bon fonctionnement de la Justice[22]. Ce mécanisme en cascade ne s'applique toutefois pas « *en cas de danger grave et imminent ou en présence d'un risque de dommages irréversibles* »[23], notions, toutefois, sujettes à interprétation.

Le décret d'application, adopté le 19 avril et publié le 20 avril dernier, a d'ailleurs précisé le statut de ce « *référent* »[24]. Tout comme le futur délégué à la protection des données personnelles[25], issu du RGDP, le référent du mécanisme des lanceurs d'alerte doit disposer de la compétence, de l'autorité et des moyens nécessaires et suffisants pour assurer l'exercice de ses missions.

[17] http://www.assemblee-nationale.fr/14/propositions/pion3607.asp.
[18] « *Lanceurs d'alerte et entreprises : les enjeux de la loi "Sapin II"* », E. Daoud & S. Sfoggia, AJ Pénal, Février 2017.
[19] Directive du Parlement Européen et du Conseil sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites adoptée le 14 avril 2016.
[20] Article 8 de la Loi Sapin II.
[21] Décret n° 2017-564 du 19 avril 2017 relatif aux procédures de recueil des signalements émis par les lanceurs d'alerte au sein des personnes morales de droit public ou de droit privé ou des administrations de l'Etat.
[22] « *Transparence et probité de la vie économique "Alerte manquements"* », E. Derieux, Revue Lamy Droit de l'Immatériel n °33, 1er janvier 2017.
[23] Article 8 II de la Loi Sapin II.
[24] Décret n° 2017-564 du 19 avril 2017 relatif aux procédures de recueil des signalements émis par les lanceurs d'alerte au sein des personnes morales de droit public ou de droit privé ou des administrations de l'Etat – Article 4.
[25] Voir à ce titre : « *Le statut du délégué à la protection des données personnelles à la lumière des recommandations du groupe de travail « Article 29 » du 5 avril 2017* », J.-B. Chanial & C. Louwers, publié par le cabinet ADAMAS et accessible à l'adresse suivante : http://www.village-justice.com/articles/statut-delegue-protection-des-donnees-personnelles,24971.html.

B. La protection des lanceurs d'alerte issue des articles 7 et 9 à 12 de la Loi Sapin II

Pour assurer l'efficacité de ce nouveau mécanisme d'alerte, il était nécessaire de protéger les lanceurs d'alerte en question.

La Loi Sapin II confère, en conséquence, aux lanceurs d'alerte, définis par l'article 6, une protection renforcée en leur accordant, d'une part, une immunité pénale[26] et, d'autre part, une protection quant aux sanctions disciplinaires pouvant être prises à leur encontre[27].

Le nouvel article 122-9 du Code pénal dispose ainsi que « *N'est pas pénalement responsable 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* ».

Par ailleurs, le Code du travail a également été modifié pour protéger les lanceurs d'alerte. L'article L.1132-3-3 dudit Code dispose désormais, en son deuxième alinéa, qu'« *Aucune personne ne peut être écartée d'une procédure de recrutement ou de l'accès à un stage ou à une période de formation professionnelle, aucun salarié ne peut être sanctionné, licencié ou faire l'objet d'une mesure discriminatoire, directe ou indirecte, notamment en matière de rémunération, au sens de l'article L. 3221-3, de mesures d'intéressement ou de distribution d'actions, de formation, de reclassement, d'affectation, de qualification, de classification, de promotion professionnelle, de mutation ou de renouvellement de contrat, pour avoir signalé une alerte dans le respect des articles 6 à 8 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* ».

Il est également précisé par l'article 12 de la Loi Sapin II qu'« *En cas de rupture du contrat de travail consécutive au signalement d'une alerte au sens de l'article 6, le salarié peut saisir le conseil des prud'hommes dans les conditions prévues au chapitre V du titre V du livre IV de la première partie du Code du travail* ».

Ces garde-fous devraient en principe permettre aux potentiels lanceurs d'alerte de ne pas subir de répercussions négatives sur leurs carrières professionnelles. Notons, malgré tout, que les salariés pourront demeurer, en pratique, réticents à dénoncer les agissements illicites de leurs supérieurs hiérarchiques. En 2015, un sondage réalisé[28] révélait que 83% des salariés qui auraient connaissance d'un acte de corruption sur leur lieu de travail en parleraient, mais que 39% d'entre eux privilégieraient leurs collègues, alors même qu'ils n'ont pas « compétence » pour agir, plutôt que leurs supérieurs (pour 32% seulement). Le sondage montrait également que la peur des conséquences d'une alerte est, pour 39% des personnes interrogées, la raison principale de ne pas dénoncer de tels faits.

Par ailleurs, l'article 9 de la Loi Sapin II impose aux entreprises concernées que la procédure d'alerte, devant être mise en place, garantisse « *une stricte confidentialité de l'identité des auteurs du signalement, des personnes visées par celui-ci et des informations recueillies par l'ensemble des destinataires du signalement* ». En cas de divulgation de ces éléments, la personne responsable de cette divulgation s'exposera à une peine d'emprisonnement de deux ans et 30.000 €uros d'amende (150.000 €uros pour une personne morale).

[26] Article 7 de la Loi Sapin II.
[27] Articles 10 à 12 de la Loi Sapin II.
[28] « *"Lanceurs d'alerte" : quelle perception de la part des salariés ?* », Enquête Harris Interactive pour Transparency International France et Tilder, 3 décembre 2015.

De surcroît, il convient de noter que cette sanction pourra être prise en sus de celles éventuellement encourues en cas de manquement à la réglementation applicable en matière de données personnelles.

Les entreprises de plus de cinquante salariés devront donc s'assurer de mettre en place un mécanisme d'alerte efficace et sécurisé qui devra, en outre, respecter la réglementation applicable en matière de données personnelles.

II. Analyse du nouveau régime de lancement d'alerte à la lumière de la réglementation applicable en matière de données personnelles et de ses évolutions

Les dispositifs d'alerte professionnelle, en raison de leur nature, entraînent la collecte et, plus généralement, le traitement de données à caractère personnel[29] des lanceurs d'alerte et des personnes qu'ils désignent, posant ainsi la question de leur conformité à la loi n° 78-17 du 6 janvier 1978, dite loi informatique et libertés (« Loi Informatique et Libertés ») et au RGDP applicable à compter du 25 mai 2018[30].

A. Aujourd'hui : l'autorisation unique AU-004 face à la Loi Sapin II

Etant susceptibles d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat (au sens du 4° du I de l'article 25 de la Loi Informatique et Libertés), les dispositifs d'alerte doivent faire l'objet d'une autorisation préalable de la Commission Nationale de l'Informatique et des Libertés (ci-après la « CNIL »).

Dans un premier temps, la CNIL a refusé d'autoriser les dispositifs d'alerte professionnelle qu'elle a pu qualifier de « *systèmes organisés de délation professionnelle* »[31]. Toutefois, après des consultations avec ses homologues européens et les autorités américaines, la CNIL a défini, dans un document d'orientation en date du 10 novembre 2005[32], les conditions que devaient remplir les dispositifs d'alerte professionnelle pour être conformes à la Loi Informatique et Libertés.

Puis, la CNIL a élaboré une décision d'autorisation unique (AU-004) mettant en place une procédure d'autorisation simplifiée[33] pour les dispositifs d'alerte professionnelle, qui a connu différentes modifications par la suite[34]. En effet, la CNIL a dû adapter et étendre le périmètre de son autorisation unique AU-004 au regard de l'arsenal législatif mis en place en matière de dispositifs d'alerte depuis 2007[35]. C'est ainsi qu'en 2014[36], la CNIL a inclus les domaines du droit de l'environnement, de la lutte contre les discriminations, de la santé, de l'hygiène et de la sécurité au travail dans le champ de son autorisation unique.

[29] Pour rappel, constitue, selon l'article 2 de la Loi Informatique et Libertés et l'article 4 du RGDP, une donnée à caractère personnel, toute information relative à une personne physique identifiée ou identifiable, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres.
[30] Article 99 du RGDP.
[31] Le droit d'alerte : signaler, traiter, protéger : Les études du Conseil d'État, 25 févr. 2016, p. 25 et s. : http://www.conseil-etat.fr/content/download/59086/527939/version/1/file/2016%20ce_etude_droit%20d%20alerte.pdf
[32] Documentation d'orientation adopté par la CNIL le 10 novembre 2005 pour la mise en œuvre de dispositifs d'alerte professionnelle conformes à la loi du 6 janvier 1978 modifiée en août 2004, relative à l'informatique, aux fichiers et aux libertés.
[33] La CNIL peut en effet, afin de simplifier les formalités administratives des entreprises, adopter certaines procédures dites « simplifiées » qui permettent auxdites entreprises de ne procéder qu'à une déclaration de conformité par laquelle elles s'engagent à respecter le périmètre des normes ainsi édictées.
[34] CNIL, délib. n° 2005-305, 8 déc. 2005, n° AU-004 : Journal Officiel du 4 Janvier 2006. – modifiée par CNIL, délib. n° 2010-369, 14 oct. 2010 : Journal Officiel du 8 Décembre 2010. – et par CNIL, délib. n° 2014-042, 30 janv. 2014 : Journal Officiel du 11 Février 2014
[35] Loi n°2007-1598 du 13 novembre 2007 - Loi 2011-2012 du 29 décembre 2011 - Loi n°2016-316 du 16 avril 2013 - Loi n°2013-907 du 11 octobre 2013 - Loi n°2013-1117 du 6 décembre 2013.
[36] CNIL, délib. N° 2014-042, 30 Janv. 2014 : Journal Officiel du 11 Février 2014.

Cette procédure simplifiée mise en place par la CNIL reste cependant encore limitée dans son périmètre, notamment quant aux données concernées, quant aux destinataires des données et surtout quant aux finalités du traitement mis en place.

Pour bénéficier d'un engagement de conformité validé par la CNIL, les alertes ne peuvent concerner que les domaines suivants : financier, comptable, bancaire, lutte contre la corruption, pratiques anticoncurrentielles, lutte contre les discriminations, harcèlement au travail, santé, hygiène, sécurité au travail et protection de l'environnement.

Les dispositifs d'alerte portant sur d'autres domaines devront nécessairement faire l'objet d'une autorisation spécifique et les entreprises devront, dans ces hypothèses, tenir compte des délais qu'impose cette procédure pouvant aller jusqu'à quatre mois (deux mois renouvelable une fois)[37].

Or, le mécanisme des lanceurs d'alerte résultant de la Loi Sapin II a vocation à s'appliquer à différents domaines du droit, même hors du périmètre de l'entreprise. En effet, comme évoqué ci-avant, le Conseil constitutionnel a précisé que le mécanisme découlant de l'article 8 de la Loi Sapin II ne serait qu'un mécanisme parmi d'autres que le législateur pourrait mettre en place, la définition des lanceurs d'alerte issue de l'article 6 étant volontairement large. Tous les domaines ne pourront dès lors être couverts par le périmètre de l'autorisation unique AU-004.

Par ailleurs, la CNIL avait, en 2005, préconisé le respect de certaines règles dans le cadre de la mise en place de dispositifs d'alerte. Ces règles devraient également s'appliquer aux traitements issus du dispositif d'alerte de la Loi Sapin II[38].

Dans le cadre de sa documentation d'orientation, la CNIL rappelle, tout d'abord, qu'un tel dispositif ne peut être que complémentaire et facultatif. La CNIL précise à ce titre qu'un tel mécanisme ne doit pas constituer un mode normal de signalement. Il doit être limité dans son champ au risque de mise en cause abusive ou disproportionnée. Son existence doit être imposée par la loi et son application ne doit pas faire l'objet d'une obligation mais d'une simple incitation. En effet, par principe, un traitement de données personnelles ne peut être réalisé qu'avec le consentement de la personne concernée par le traitement[39]. Or, dans le cadre d'un dispositif d'alerte, la personne faisant l'objet de l'alerte ne consent pas à ce traitement. Dès lors, il est nécessaire qu'un tel dispositif résulte d'une obligation légale. La CNIL précisait ainsi que « *les dispositifs d'alerte ne peuvent être considérés comme légitimes que du fait de l'existence d'une obligation légale (législative ou réglementaire) imposant la mise en place de tels dispositifs* »[40]. Cette condition est remplie dans le cadre de la Loi Sapin II.

En outre, la CNIL préconise, dans sa documentation d'orientation, de définir limitativement les catégories de personnes concernées par le dispositif d'alerte, sur le fondement du principe de proportionnalité. Cette préconisation pourrait être contraire à l'esprit de la Loi Sapin II dont le mécanisme vise le signalement de faits illicites (« *un crime ou un délit, une violation grave et manifeste d'un engagement international ou notamment de la loi ou d'un règlement, ou une menace ou un préjudice graves pour l'intérêt général* »[41]), et non le signalement d'une personne ayant commis un tel fait. Il est à espérer que la CNIL adaptera rapidement ses recommandations à ce propos.

[37] Article 25 III de la Loi Informatique et Libertés.
[38] Documentation d'orientation adopté par la CNIL le 10 novembre 2005 pour la mise en œuvre de dispositifs d'alerte professionnelle conformes à la loi du 6 janvier 1978 modifiée en août 2004, relative à l'informatique, aux fichiers et aux libertés.
[39] Articles 6 et 7 de la Loi Informatique et Libertés.
[40] Documentation d'orientation adopté par la CNIL le 10 novembre 2005 pour la mise en œuvre de dispositifs d'alerte professionnelle conformes à la loi du 6 janvier 1978 modifiée en août 2004, relative à l'informatique, aux fichiers et aux libertés – page 2.
[41] Article 6 de la Loi Sapin II.

De plus, la CNIL préconise également dans sa documentation d'orientation la protection de l'émetteur de l'alerte. Elle rappelle en parallèle que, par principe, l'émetteur de l'alerte doit être identifié afin de responsabiliser ce dernier. Un lanceur d'alerte, sous le régime de l'autorisation unique AU-004, ne peut rester anonyme que sous certaines conditions. En revanche, la CNIL précise, tout comme la Loi Sapin II en son article 9, que l'identité de l'émetteur de l'alerte doit être traitée de façon confidentielle, le mécanisme ne devant pas inciter à recourir à des alertes anonymes. La Loi Sapin II reste cependant silencieuse quant à l'anonymat du lanceur d'alerte.

Egalement, comme pour tous les traitements de données personnelles, la CNIL impose aux entreprises mettant en place ces dispositifs d'alerte la diffusion d'une information claire et complète les concernant. L'information comprend notamment : l'identité du responsable de traitement, les objectifs poursuivis, les domaines concernés par les alertes, le caractère facultatif du dispositif, les destinataires des alertes, les éventuels transferts de données hors de l'Union Européenne, les droits des personnes identifiées par le traitement mis en œuvre. La CNIL précise également qu'une information précise quant à l'utilisation abusive de ce mécanisme doit être diffusée et qu'une telle utilisation peut exposer son auteur à des sanctions disciplinaires ou à des poursuites judiciaires. La CNIL impose également que la personne faisant l'objet d'une alerte professionnelle soit informée du traitement réalisé la concernant et ce afin de lui permettre d'exercer ses droits d'opposition ou de rectification. La personne faisant l'objet d'une alerte doit notamment être informée de l'identité du responsable de traitement, des faits qui lui sont reprochés, des destinataires de l'alerte et des modalités d'exercice de ses droits. Néanmoins, la CNIL précise que « *lorsque des mesures conservatoires sont nécessaires, notamment pour prévenir la destruction de preuves relatives à l'alerte, l'information de cette personne doit intervenir après l'adoption de ces mesures* ».

Par ailleurs, la CNIL préconise que le recueil des alertes soit réalisé par des moyens dédiés et notamment que les personnes habilitées à recueillir ces alertes soient (i) en nombre limité, (ii) spécialement formées et (iii) astreintes à une obligation renforcée de confidentialité. La Loi Sapin II, en prévoyant expressément en son article 9 que la divulgation des informations recueillies dans le cadre d'une alerte peut conduire au prononcé d'une peine d'emprisonnement de deux ans et d'une peine d'amende pouvant aller jusqu' à 30.000 €uros pour une personne physique et 150.000 €uros pour une personne morale, semble également préconiser un contrôle du recueil des alertes.

Enfin, la CNIL précise que l'ensemble des principes applicables en matière de données personnelles (finalité, proportionnalité, pertinence des données, durée de conservation des données limitée, sécurité, confidentialité des données et respect des droits des personnes concernées) doit être respecté dans le cadre de la mise en place d'un dispositif d'alerte.

B. Demain : la mise en œuvre de la Loi Sapin II et le RGDP

Le nouveau régime de lancement d'alerte mis en place par l'article 8 de la Loi Sapin II devrait impliquer une adaptation du régime actuel de l'autorisation unique AU-004, le décret d'application ayant de surcroît précisé qu'en cas de traitement automatisé des signalements mis en œuvre dans le cadre de ce mécanisme, une autorisation de la CNIL devra être obtenue[42].

Nous pouvons regretter que le décret d'application précisant les modalités et conditions relatives au mécanisme des lanceurs d'alerte instauré par l'article 8 de la Loi Sapin II n'ait pas repris *a minima* les préconisations de la CNIL susvisées. Il serait opportun que la CNIL fournisse, avant le 1er janvier 2018, une version actualisée de sa documentation d'orientation.

Il doit être rappelé, qu'en la matière, les sanctions peuvent, en théorie, être très sévères. En cas de violation par un responsable de traitement de ses obligations découlant de la Loi Informatique et Libertés, le plafond de la sanction pécuniaire prononcée par la CNIL est de 3 millions d'euros depuis le 9 octobre 2016[43]. Le RGDP, applicable à compter du 25 mai 2018, alourdira largement ce plafond puisque des sanctions pécuniaires d'un montant de 10 millions d'euros ou 2% du chiffre d'affaires annuel mondial total de l'exercice précédent (le montant le plus élevé étant retenu) ou 20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent (le montant le plus élevé étant retenu) seront alors encourues en fonction du manquement concerné[44]. Toutefois, en pratique, pour décider s'il y a lieu d'imposer une sanction pécuniaire et pour décider de son montant, plusieurs critères définis par la Loi Informatique et Libertés[45] et complétés par le RGDP[46] sont pris en compte. Dès lors, les plafonds des sanctions susvisées ne devraient être que rarement appliqués.

De surcroît, il sera rappelé que le RGDP modifiera considérablement la philosophie actuelle de contrôle des traitements de données personnelles en supprimant généralement l'obligation des formalités préalables tout en responsabilisant les opérateurs (responsable de traitement et sous-traitant)[47].

---

[42] Décret n° 2017-564 du 19 avril 2017 relatif aux procédures de recueil des signalements émis par les lanceurs d'alerte au sein des personnes morales de droit public ou de droit privé ou des administrations de l'Etat – Article 5, III.

[43] Article 47 de la Loi Informatique et Libertés modifié par la Loi n°2016-1321 du 7 octobre 2016 qui a augmenté le plafond de 150.000 euros à 3 millions d'euros.

[44] Article 83 – 4° et 5° du RGDP.

[45] Il est légalement prévu que le montant de l'amende est fixé selon plusieurs critères : - le caractère intentionnel ou de négligence du manquement, - les mesures prises par le responsable du traitement pour atténuer les dommages subis par les personnes concernées, - le degré de coopération avec la commission afin de remédier au manquement et d'atténuer ses effets négatifs éventuels, - les catégories de données à caractère personnel concernées, - la manière dont le manquement a été porté à la connaissance de la CNIL (cf. Article 47 de la Loi Informatique et Libertés).

[46] Le RGDP prévoit désormais de nouveaux critères : - la nature, la gravité et la durée de la violation, compte tenu de la nature, de la portée ou de la finalité du traitement concerné, ainsi que du nombre de personnes concernées affectées et le niveau de dommage qu'elles ont subi; - le fait que la violation a été commise délibérément ou par négligence; - toute mesure prise par le responsable du traitement ou le sous-traitant pour atténuer le dommage subi par les personnes concernées; - le degré de responsabilité du responsable du traitement ou du sous-traitant, compte tenu des mesures techniques et organisationnelles qu'ils ont mis en œuvre; - toute violation pertinente commise précédemment par le responsable du traitement ou le sous-traitant; - le degré de coopération établi avec l'autorité de contrôle en vue de remédier à la violation et d'en atténuer les éventuels effets négatifs; - les catégories de données à caractère personnel concernées par la violation; - la manière dont l'autorité de contrôle a eu connaissance de la violation, notamment si, et dans quelle mesure, le responsable du traitement ou le sous-traitant a notifié la violation; - le respect de ces mesures précédemment ordonnées à l'encontre du responsable du traitement ou du sous-traitant; - l'application de codes de conduite approuvés ou de mécanismes de certification approuvés ; - toute autre circonstance aggravante ou atténuante applicable aux circonstances de l'espèce, telle que les avantages financiers obtenus ou les pertes évitées, directement ou indirectement, du fait de la violation (cf. Article 83 – 2° du RGDP).

[47] Articles 24 et 30 du RGDP.

Tel est le principe de l'*accountability*, notion difficilement traduisible qui évoque, à la fois, l'affirmation de la responsabilité de l'entreprise mais aussi, et surtout, sa faculté à démontrer qu'elle a bien respecté les exigences réglementaires en matière de protection des données. Il constitue, par rapport à l'état actuel de la réglementation en matière de données personnelles, une des ruptures majeures introduites par le RGDP impliquant notamment l'obligation, pour les responsables du traitement et les sous-traitants, de tenir un registre des activités de traitement effectuées sous leur responsabilité.

Le RGDP précise toutefois que les traitements déjà en cours et fondés sur une autorisation accordée par une autorité de contrôle demeurent en vigueur jusqu'à ce que ladite autorisation soit modifiée, remplacée ou abrogée[48]. Il conviendra donc d'attendre la position de la CNIL quant au régime de l'autorisation unique AU-004, cette dernière ayant par ailleurs récemment annoncé la révision à venir de la Loi Informatique et Libertés à la lumière du RGDP[49].

Par ailleurs, il sera également nécessaire pour les entreprises d'adapter l'information communiquée aux personnes concernées par les dispositifs d'alerte. En effet, alors que la Loi Informatique et Libertés prévoyait la possibilité de recourir à une information réduite dans certains cas[50], cette possibilité est écartée par le RGDP. L'obligation d'information issue du RGDP a ainsi été renforcée et le contenu de cette information est désormais précisément défini aux articles 13, 14 et 15 à 22 dudit RGDP.

Toutefois, le RGDP a également prévu des exceptions à cette obligation d'information notamment « *dans la mesure où l'obligation [d'information] est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs dudit traitement* ». En pareils cas, le responsable du traitement devra prendre « *des mesures appropriées pour protéger les droits et libertés ainsi que les intérêts légitimes de la personne concernée, y compris en rendant les informations publiquement disponibles* »[51]. L'obligation d'information pourra également ne pas être fournie si « *les données à caractère personnel doivent rester confidentielles en vertu d'une obligation de secret professionnel réglementée par le droit de l'Union ou le droit des États membre, y compris une obligation légale de secret professionnel* »[52]. Dès lors, l'information des personnes visées par des alertes pourrait être adaptée aux circonstances particulières de ces mécanismes, comme le recommandait déjà la CNIL dans sa documentation d'orientation de 2005[53].

Enfin, les nouveaux droits issus du RGDP, tel que le droit à l'effacement (« droit à l'oubli ») ou le nouveau droit à l'opposition, devront également être respectés et adaptés aux dispositifs d'alerte.

Pour rappel, le droit à l'effacement[54] se définit comme le droit pour la personne concernée par le traitement de données personnelles d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant. Ce droit connaissait déjà une existence de fait, notamment au travers de l'obligation de la Loi Informatique et Libertés de ne pas conserver les données au-delà de la durée nécessaire à l'accomplissement de la finalité du traitement[55]. Ce droit est conditionné et ne s'applique que dans certaines hypothèses limitatives. Le RDGP précise à ce titre que le droit d'effacement ne s'applique pas si le traitement

[48] Considérant 171 du RGDP.
[49] https://www.cnil.fr/fr/les-enjeux-de-2017-2-disposer-imperativement-dune-nouvelle-loi-informatique-et-libertes-avant-mai-0.
[50] Article 32 de la Loi Informatique et Libertés.
[51] Article 14 5° b) du RGDP.
[52] Article 14 5° d) du RGDP.
[53] Documentation d'orientation adopté par la CNIL le 10 novembre 2005 pour la mise en œuvre de dispositifs d'alerte professionnelle conformes à la loi du 6 janvier 1978 modifiée en août 2004, relative à l'informatique, aux fichiers et aux libertés – page 7.
[54] Article 17 du RGDP.
[55] Article 6 de la Loi Informatique et Libertés.

répond à une obligation légale. Un tel argument pourrait être invoqué pour faire échec au droit à l'effacement de la personne faisant l'objet d'une alerte.

Le droit à l'opposition[56] permet à la personne concernée de s'opposer à tout moment à un traitement des données personnelles la concernant. Dans le cas des traitements nécessaires à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique ou nécessaires à la protection d'intérêts légitimes, la personne concernée peut également exercer son droit d'opposition. Toutefois, le responsable du traitement peut ne pas faire droit à la demande de la personne concernée s'il démontre qu'il existe des motifs légitimes et impérieux pour le traitement en cause qui prévalent sur les intérêts de la personne concernée ou s'il démontre que le traitement en cause est nécessaire « *pour la constatation, l'exercice ou la défense de droits en justice* ». S'agissant des dispositifs d'alerte, il pourrait ainsi être invoqué que le droit d'opposition de la personne mise en cause par l'alerte serait susceptible de porter atteinte à la constatation d'une infraction et à l'exercice de droits en justice notamment.

***

Wikileaks, Deltour, Snowden… L'actualité des lanceurs d'alerte a conduit le législateur français, comme ses homologues anglais ou américains, à unifier et généraliser les mécanismes existants en la matière.

Or, compte tenu des traitements de données personnelles découlant de ces dispositifs et au regard de la nouvelle règlementation applicable dans ce domaine, les entreprises devront adapter leurs outils internes pour se mettre en conformité avec, d'une part, les obligations de l'article 8 de la Loi Sapin II, outre, le cas échéant, les obligations anticorruption de ladite Loi Sapin II[57], et, d'autre part, les obligations du RGDP.

NB : Cet article a été rédigé à partir d'un article précédent publié par ses auteurs dans la revue Lexbase (Lexbase Hebdo édition affaires n°508 du 4 mai 2017) et complété pour prendre en compte les nouvelles dispositions du décret d'application.

Jean-Baptiste CHANIAL
Avocat Associé
Certificat de spécialisation – Mention droit des nouvelles technologies de l'informatique et de la communication
jean-baptiste.chanial@adamas-lawfirm.com
+ 33 (0) 4 72 41 15 75

Cécile LOUWERS
Avocat
cecile.louwers@adamas-lawfirm.com
+ 33 (0) 4 72 41 15 75

[56] Article 21 du RGDP.
[57] Voir à ce titre : Lettre Flash ADAMAS « *Loi Sapin II : Focus sur la mise en place de "plans anticorruption" d'ici le 1er juin 2017 – Il ne reste que quelques semaines pour se mettre en conformité…* ».