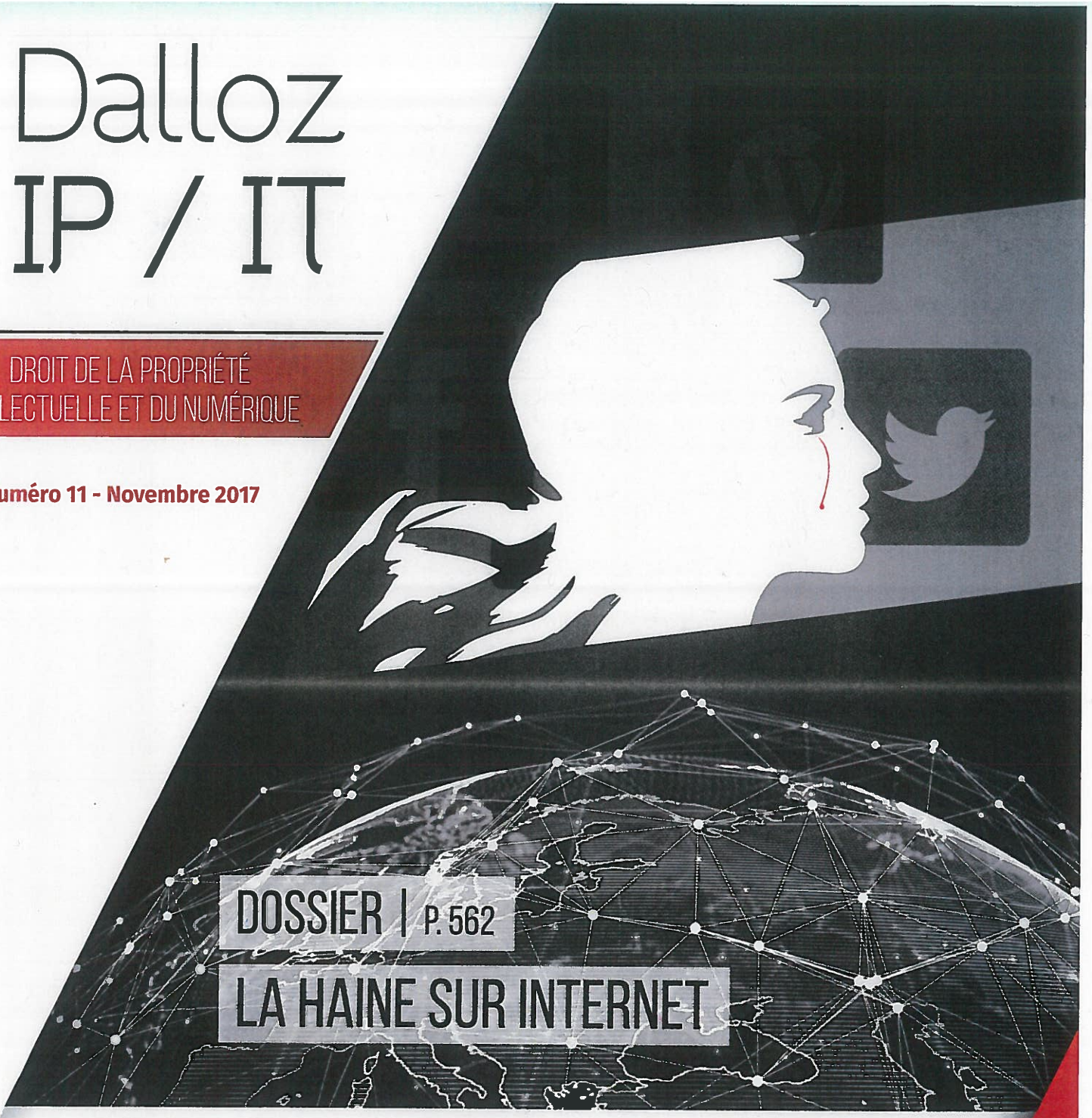
Dalloz IP / IT

DROIT DE LA PROPRIÉTÉ INTELLECTUELLE ET DU NUMÉRIQUE

Numéro 11 - Novembre 2017

9 782997 517112



DOSSIER | P. 562

LA HAINE SUR INTERNET

PRATIQUES

Loi Sapin II, loi vigilance et RGPD. Pour une approche décloisonnée de la *compliance*

Géraldine Péronne et Emmanuel Daoud

TEXTES ET DÉCISIONS

L'extension aux « webradios » de la licence légale relative aux phonogrammes du commerce est conforme à la Constitution

Cons. const. 4 août 2017

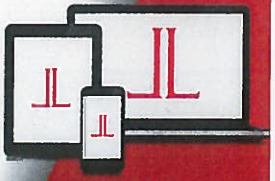
Tristan Azzi

TEXTES ET DÉCISIONS

Absence de déclaration (simplifiée) à la CNIL et recevabilité de la preuve

Soc. 1er juin 2017

Patrice Adam



Version numérique incluse

DALLOZ

LOI SAPIN II, LOI VIGILANCE ET RGPD
POUR UNE APPROCHE DÉCLOISONNÉE DE LA *COMPLIANCE*

Géraldine Péronne
Avocat au barreau de Paris - Cabinet Vigo – Docteur en droit

Emmanuel Daoud
Avocat au barreau de Paris - Cabinet Vigo

L'année 2018 sera l'année de toutes les sanctions pour les entreprises. Rien moins que trois textes imposent des obligations nouvelles aux entreprises dont la violation pourra être sanctionnée l'année prochaine : 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, dite loi « Sapin II », la loi n° 2017-399 du 27 mars 2017 relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre, dite loi « Vigilance » et, enfin, le règlement général sur la protection des données à caractère personnel du 27 avril 2016, dit « RGPD ». De sources différentes et de champ d'application matériel et territorial distincts, ces trois instruments adhèrent toutefois à la même philosophie, celle de la *compliance*. La notion a été définie comme « l'ensemble des processus qui permettent d'assurer le respect des normes applicables à l'entreprise par l'ensemble de ses salariés et de ses dirigeants, mais aussi des valeurs et d'un esprit éthique insufflé par les dirigeants »[1] ou plus prosaïquement comme « l'expression de la volonté des pouvoirs publics d'imposer des règles dont ils n'ont pas la force d'assurer l'effectivité »[2].

La *compliance* voit son importance considérablement renforcée à la lumière de ces nouveaux textes : la loi Vigilance impose de nouvelles règles aux sociétés qui se rendraient coupables de violations, entre autres, de droits humains, libertés fondamentales et atteintes à l'environnement, ces dernières pouvant voir leur responsabilité civile engagée[3]. La loi Sapin II[4] pose un nouveau cadre juridique de lutte contre la corruption dont la violation peut être sanctionnée par une amende administrative de 200 000 € pour les personnes physiques et d'un million d'euros pour les personnes morales[5]. Le RGPD[6], quant à lui, réforme le droit des données à caractère personnel dont la violation est sanctionnée par une amende administrative pouvant aller jusqu'à 4 % du chiffre d'affaires mondial de l'organisation concernée[7].

Comment les entreprises concernées doivent-elles appréhender ces mutations ? La mise en conformité peut-elle passer par une approche combinée de ces différents textes, permettant de rationaliser les efforts humains et financiers, sans pour autant céder à un pragmatisme dévoyé ? Rapidement, des points de convergence se font jour entre la loi Sapin II, la loi Vigilance et le RGPD. On observe en effet l'émergence de réglementations d'application concomitante, ayant pour objet la *compliance* et faisant peser sur les entreprises un risque de sanctions

1 Le Cercle de la *compliance*. Consulter http://www.cercledela-compliance.com/.

2 M.-A. Frison-Roche, Le droit de la *compliance*, D. 2016. 1871.

3 V. not. S. Schiller, Exégèse de la loi relative au devoir de vigilance des sociétés mères et entreprises donneuses d'ordre, JCP 2017. Doctr. 622.

4 V. not. le dossier : La loi « Sapin II » à hauteur des enjeux ?, AJ pénal 2017. 61.

5 Cette sanction pécuniaire pourra être prononcée par la commission des sanctions de l'Agence française anticorruption (AFA) nouvellement créée (art. 17, V, de la loi Sapin II).

6 V. not. le dossier : Les grands axes du règlement (UE) 2016/679 sur les données personnelles, Dalloz IP/IT 2016. 566.

7 Cette sanction pourra être prononcée par la Commission nationale de l'informatique et des libertés (CNIL).

pécuniaires très élevé. Ces éléments invitent à une approche décloisonnée des textes impliquant d'identifier plus précisément les points de jonction et éventuellement de friction, aux fins d'une application articulée de la loi Vigilance, de la loi Sapin II et du RGPD. La mise en œuvre combinée des obligations issues de ces réglementations est possible (I). Plus encore, les obligations apparaissent enchevêtrées, de telle manière qu'une analyse croisée des textes semble s'imposer (II).

I - LA POSSIBILITÉ D'UNE APPLICATION COMBINÉE DES OBLIGATIONS

Il existe des points de convergence naturels entre les obligations issues des lois Vigilance, Sapin II et RGPD quant à la méthode, qui est identique (A) et quant aux outils et ressources utilisés, qui sont similaires (B).

A - La convergence des méthodes

Les méthodes convergent autour de la notion clé de « responsabilisation » des acteurs économiques qui induit une forme d'autorégulation caractéristique de la *compliance* (1) et dans la volonté des législateurs de viser le plus grand nombre d'acteurs possibles (2).

1 - La responsabilisation des acteurs économiques

Tant la loi Vigilance, que la loi Sapin II et le RGPD participent de la responsabilisation des acteurs économiques. Il n'y a en cela rien d'étonnant dès lors que l'esprit de la *compliance*, qui traverse ces textes, est bien d'insuffler aux dirigeants de sociétés la volonté de se mettre en conformité, afin d'anticiper des risques multiples : sanctions administratives, sanctions pénales, engagement de responsabilité civile et atteinte à la réputation, notamment. Au sein du RGPD, cette autorégulation est particulièrement explicite : « [...] le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement. Ces mesures sont réexaminées et actualisées si nécessaire »[8].

Les données à caractère personnel ont longtemps été le parent pauvre de la *compliance*, et ce pour plusieurs raisons : des raisons culturelles d'abord, la *compliance* a vu le jour aux États-Unis dans le secteur bancaire et financier. Le droit des données à caractère personnel, du fait de sa relation étroite avec le droit à la vie privée, qui n'est pas consacré de la même manière aux États-Unis qu'en Europe[9], ne fait pas partie des matières historiques de la *compliance*, telles que les pratiques anticoncurrentielles, la corruption et le blanchiment d'argent. La faiblesse des sanctions, en cas de violation des données à caractère personnel, pouvait ensuite expliquer le faible intérêt des entreprises pour la matière et une certaine réticence à l'intégrer dans des programmes de *compliance* déjà lourds et coûteux.

Ce temps est révolu. À l'aune du RGPD, la place des données à caractère personnel dans le champ de la *compliance* ne fait plus aucun doute[10] : la responsabilisation des acteurs est consacrée, les outils sont adaptés et les sanctions dissuasives.

Dans le cadre de la loi Sapin II et la loi Vigilance, la nécessité d'avoir à rendre compte, expliquer et démontrer que les mesures sont prises afin d'assurer la conformité, se traduit par l'obligation pesant sur les sociétés d'élaborer des documents spécifiques tels qu'une cartographie des risques et de mettre en œuvre des mesures organisationnelles particulières, un dispositif d'alerte notamment. Ces trois textes partagent ainsi une méthode commune, qui correspond à une approche par les risques ayant pour objectif de prévenir leur survenance et si le risque se concrétise, de mieux en appréhender les effets. Naturellement, une telle approche pose aussi la question de la difficulté d'appréciation du niveau de

8 RGPD, art. 24.1. V. aussi le consid. 74.

9 Sur ce point, v. C. Castets-Renard, Quels liens établir entre les USA et l'UE en matière de vie privée et protection des données à caractère personnel ?, Dalloz IP/IT 2016. 115.

10 En ce sens, A. Debet, Les nouveaux instruments de conformité, Dalloz IP/IT 2016. 592 ; W. Maxwell et S. Taïeb, L'*accountability*, symbole d'une influence américaine sur le règlement européen des données personnelles, Dalloz IP/IT 2016. 123.

risque, pour lequel aucun des textes ne fournit de véritables critères.

En tout état de cause, tant la loi Vigilance, la loi Sapin II que le RGPD conduisent à une responsabilisation des acteurs à marche forcée. Tout défaut de conformité sera susceptible de faire l'objet de sanctions lourdes. Le changement de philosophie est patent, l'adhésion spontanée des entreprises à un programme de conformité cède la place à une soumission des acteurs à des obligations juridiquement contraignantes [11].

2 - Le rayonnement de la législation

La loi Sapin II, la loi Vigilance et le RGPD ont, en outre, une conception large de la conformité puisque ces textes étendent les obligations de mise en conformité à d'autres entités que la seule organisation visée principalement par les textes. Ainsi, tant la loi Vigilance que le RGPD s'appliquent aux sous-traitants et fournisseurs des sociétés visées. La loi Vigilance précise qu'elle vise « [...les] activités des sous-traitants ou fournisseurs avec lesquels est entretenue une relation commerciale établie, lorsque ces activités sont rattachées à cette relation ». Sur ce point, une clarification est attendue quant au sens à donner à la notion de « relation commerciale établie » qui conditionne le champ d'application de la loi.

Le RGPD encadre également très précisément la relation contractuelle entre le responsable de traitement de données et le sous-traitant ainsi que les relations entre le sous-traitant et ses propres sous-traitants, en prévoyant des dispositions contractuelles spécifiques protectrices des données à caractère personnel [12].

La loi Sapin II peut s'étendre, quant à elle, aux filiales ou sociétés contrôlées par les sociétés visées par le texte [13].

L'objectif commun est de conférer la portée la plus étendue possible au RGPD, à la loi Sapin II et à la loi Vigilance et, partant, de faire rayonner la *compliance* très largement, les sous-traitants et filiales visées pouvant être situés sur le territoire d'États étrangers et hors Union européenne [14].

La mise en œuvre des nouvelles règles de *compliance* peut ainsi s'avérer particulièrement complexe et coûteuse pour les entreprises assujetties à ces obligations. Ces contraintes supposent que la communication d'informations, l'analyse des relations entre la société mère et les filiales et sous-traitants se fassent en prenant en considération les dispositions de la loi Sapin II, de la loi Vigilance et du RGPD et ce, afin de rationaliser les efforts. Outre ces éléments de méthodologie communs, les outils qui doivent être mis en œuvre par les organisations soumises à la loi Vigilance, la loi Sapin II et le RGPD présentent de grandes similarités.

B - La similarité des outils et des ressources

La mise en œuvre des obligations figurant dans les lois Sapin II, Vigilance et le RGPD repose sur des outils d'analyse du risque identiques, tels que l'audit, la cartographie des risques, la sensibilisation des acteurs [15] (1), mais aussi sur des personnes ressources en charge du pilotage de la *compliance* (2).

1 - Sur l'analyse du risque

La loi Sapin II, au même titre que la loi Vigilance, impose la réalisation d'une cartographie des risques qui doit permettre « d'identifier, analyser et hiérarchiser les risques » [16]. Si le RGPD n'exige pas *stricto sensu* la réalisation d'une cartographie des risques, il impose en revanche au responsable de traitement la réalisation d'une analyse d'impact pour les traitements « susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques ».

Or, cette étude d'impact correspond très exactement à une cartographie des risques. Il s'agit en effet, pour un traite-

11 V. not. sur ce point X. Boucobza et Y.-M. Serinet, Loi « Sapin II » et devoir de vigilance : l'entreprise face aux nouveaux défis de la compliance, D. 2017. 1619.

12 RGPD, art. 28. On précisera que le sous-traitant au sens du droit des données à caractère personnel, fait l'objet d'une définition spécifique (art. 4, 8) du RGPD.

13 Art. 17, I-2°, de la loi Sapin II : « [...] Lorsque la société établit des comptes consolidés, les obligations définies au présent article portent sur la société elle-même ainsi que sur l'ensemble de ses filiales, au sens de l'article L. 233-1 du code de commerce, ou des sociétés qu'elle contrôle, au sens de l'article L. 233-3 du même code [...] ».

14 Sur le champ d'application territorial des textes, v. not. M. Segonds, Les apports de la loi du 9 décembre 2016 à l'anticorruption, Dr. pénal févr. 2017. Étude 4 ; O. Boskovic, Brèves remarques sur le devoir de vigilance et le droit international privé, D. 2016. 385.

15 Cette obligation figure expressément dans la loi Sapin II qui impose « un dispositif de formation destiné aux cadres et aux personnels les plus exposés aux risques de corruption et de trafic d'influence » (art. 17, II-6°).

16 Art. 1er de la loi Vigilance et art. 17, II-3°, de la loi Sapin II.

ment de données, de décrire les opérations de traitement, d'évaluer la nécessité et la proportionnalité de ces opérations, d'évaluer le risque pour les droits et libertés des personnes concernées et les mesures envisagées pour y faire face [17].

En outre, on devine que l'identification d'un traitement présentant « un risque élevé pour les droits et libertés » aura supposé au préalable une cartographie des risques, même simple, au sein de l'organisation, permettant de mettre en évidence ce risque.

En l'occurrence, la CNIL a élaboré une méthodologie détaillée relative à l'élaboration de l'étude d'impact et plus précisément à l'identification et l'évaluation du risque en matière de données à caractère personnel, qui pourrait nourrir la réflexion pour tout type de cartographie des risques [18]. De même, les labels développés par la CNIL et le label « gouvernance », notamment, fournissent par le biais de leur cahier des charges, des clés d'analyse précieuses, qui pourraient inspirer les entreprises pour la mise en œuvre des lois Sapin II et vigilance.

De toute évidence, au regard de ces développements, il serait pertinent de procéder à une cartographie des risques commune, qui implique une analyse des risques couverts par la loi Sapin II, la loi vigilance et le RGPD. Si ce dernier texte ne prévoit pas expressément de cartographie des risques, à la lumière de ce qui précède, cette analyse apparaît pourtant indispensable. En outre, sur un plan pratique, les entreprises ne devraient pas être obligées, en ces temps de restrictions budgétaires, à réaliser deux fois le même exercice.

2 - Sur la personne en charge de la *compliance*

L'élaboration d'un programme de *compliance* et sa mise en œuvre ne se conçoivent pas sans une personne « pilote », en charge de la mise en musique des ressources matérielles et humaines.

À cet égard, le RGPD est très disert sur la fonction et les missions de la personne « pilote », garante de la protection des données à caractère personnel. Les indications sont en effet très précises et même contraignantes. La désignation d'un délégué à la protection des données ou *Data Protection Officer* est même rendue obligatoire pour certaines organisations [19].

Le RGPD crée un véritable statut pour le délégué qui doit être mis à l'abri des conflits d'intérêts, dont l'indépendance est consacrée et qui est soumis au secret professionnel ou à une obligation de confidentialité [20]. Le délégué à la protection des données a une mission d'information et de conseil et doit « contrôler le respect » du règlement, tout en faisant office de « point de contact » avec la CNIL [21].

Rien de tout cela dans le cadre de la loi Sapin II qui prévoit certes la désignation d'un « référent », mais n'y ajoute aucune précision de nature à éclairer sur le statut ou les missions de celui-ci. Ce rôle doit-il dès lors être confié à un *Chief Compliance Officer*, à un juriste ou à une personne dont le profil et le titre restent à créer ?

La loi Vigilance, quant à elle, ne fait même pas mention d'un quelconque « référent ». Pour autant, une personne dédiée à la mise en conformité semble également s'imposer. La question est de savoir si le référent Sapin II peut également être le référent loi Vigilance. Rien ne semble s'y opposer, et compte tenu des liens entre ces deux lois, il s'agit d'une faculté qu'il faut considérer, surtout dans les entreprises qui ne seraient pas des multinationales.

Quid du délégué à la protection des données ? Pourrait-il également être en charge de la conformité sous l'égide de la loi Sapin II et de la loi Vigilance ? Le RGPD octroie la possibilité au délégué d'exercer d'autres missions ou tâches si celles-ci n'engendrent pas de conflits d'intérêts [22]. Toutefois, la difficulté résidera sans doute dans la charge de travail occasionnée qu'il serait déraisonnable de confier à une seule personne, sans évoquer la nécessité

17 RGPD, art. 35.

18 Consulter https://www.cnil.fr/fr/etude-dimpacts-sur-la-vie-privee-suivez-la-methode-de-la-cnil.

19 RGPD, art. 37.

20 RGPD, art. 38.

21 RGPD, art. 39.

22 RGPD, art. 38.6.

pour le délégué d'être doté d'une expertise dans chacun des domaines visés.

Il reste que la précision du droit des données à caractère personnel sur la définition du statut du délégué à la protection des données fait réfléchir. Sur ce point comme sur d'autres, les interprètes des lois Sapin II et Vigilance ne peuvent qu'envier la sophistication du droit des données à caractère personnel, dont le RGPD aussi détaillé que précis, est la figure de proue.

À cet égard, on observera que l'obligation de confidentialité ou de secret professionnel qui est imposée par le RGPD au délégué à la protection des données serait également indiquée pour le « référent » en charge de la mise en œuvre de la loi Sapin II, compte tenu de la confidentialité qui doit entourer le recueil des signalements [23].

Il n'y a donc pas lieu de dresser des cloisons là où il n'y en a pas. Si la loi Sapin II, la loi Vigilance et le RGPD présentent des différences inhérentes à leur champ d'application matériel distinct, celles-ci ne permettent pas d'occulter leurs points de convergence nombreux.

II - LA NÉCESSITÉ D'UNE APPLICATION CROISÉE DES OBLIGATIONS

Les obligations issues de la loi Vigilance, de la loi Sapin II et du RGPD présentent des points communs qui doivent conduire à appliquer ces textes ensemble. Si l'on pousse l'analyse plus avant, on observe une imbrication des champs d'application, la transversalité des données à caractère personnel conduisant à une nécessaire prise en considération des règles du RGPD dans la mise en œuvre de n'importe quel programme de *compliance* (B) et plus encore dans le cadre des lois Vigilance et Sapin II où les données à caractère personnel pourraient bien constituer un domaine d'application des mesures de *compliance* (A).

A - Les données à caractère personnel comme objet de la compliance *dans la loi Vigilance et la loi Sapin II ?*

Les données à caractère personnel constituent le champ d'application matériel unique du RGPD, qui a ainsi pour objet la protection des données. La loi Vigilance, dotée d'un objectif plus large, pourrait bien également avoir pour objet d'assurer la protection des données à caractère personnel.

La loi Vigilance prévoit la mise en œuvre d'un plan comportant « les mesures de vigilance raisonnable propres à identifier les risques et à prévenir les atteintes graves envers les droits humains et les libertés fondamentales, la santé et la sécurité des personnes ainsi que l'environnement, résultant des activités de la société et de celles de sociétés qu'elle contrôle au sens du II de l'article 233-16 [...] ».

Le champ d'application matériel du devoir de vigilance apparaît à la fois large, puisque la loi vise tous « les droits humains et les libertés fondamentales » et flou, puisqu'il ne concerne que les « atteintes graves », pour lesquelles la loi ne fournit aucun critère permettant d'apprécier le degré de gravité requis [24].

Une des questions qui se pose est dès lors de savoir si une atteinte aux données à caractère personnel est susceptible d'entrer dans le champ d'application de la loi Vigilance.

S'agissant du premier critère, relatif au champ d'application matériel de la loi, l'article 8, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne et l'article 16, paragraphe 1, du Traité sur le fonctionnement de l'Union disposent que « toute personne a droit à la protection des données le concernant ». Ce caractère fondamental du droit à la protection des données personnelles est

23 Art. 9 de la loi Sapin II.

24 Sur le caractère flou des termes de la loi, les commentateurs sont quasiment unanimes, v. not. J. Heinich, Devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre : une loi finalement adoptée, mais amputée, Dr. sociétés 2017. Comm. 78. V. toutefois *contra*, P. Mougeolle, Sur la conformité constitutionnelle de la proposition de loi relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre – Responsabilité sociale des entreprises (RSE), Rev. dr. homme, Actualités Droits-Libertés, 2017, p. 4, qui associe les atteintes graves à la notion d'ordre public international « bien reconnue par les juridictions françaises » et donne quelques exemples parmi lesquels les atteintes aux données à caractère personnel ne figurent pas.

encore rappelé dans le premier considérant du RGPD [25]. Le premier critère d'application de la loi Vigilance est donc rempli.

S'agissant du second critère relatif au degré de gravité de l'atteinte, il est aisé d'envisager une atteinte au droit à la protection des données qui atteindrait un seuil de gravité l'inscrivant dans le champ de la loi Vigilance. Une faille de sécurité qui porterait sur les données de santé de milliers de personnes ou sur d'autres données sensibles pourrait sans aucun doute revêtir cette caractéristique.

Dès lors, on peut raisonnablement penser que la loi Vigilance couvre les violations du droit des données à caractère personnel.

Qu'en est-il de la loi Sapin II ? Aux termes de son article 8, toute alerte relative à « un crime ou un délit, une violation grave ou manifeste d'un engagement international régulièrement ratifié ou approuvé par la France, d'un acte unilatéral d'une organisation internationale pris sur le fondement d'un tel engagement ». Or, l'atteinte portée aux données à caractère personnel peut constituer un délit sanctionné conformément aux articles 226-16 à 226-30 du code pénal.

Tout porte à croire que les données à caractère personnel entrent dans le champ des lois Vigilance et Sapin II et pourront donc faire l'objet d'alertes.

La loi Sapin II et la loi Vigilance prévoient en effet toutes deux la mise en place d'un dispositif d'alerte destiné à permettre le recueil des signalements [26].

La mise en œuvre des dispositifs d'alerte prévus par ces textes n'est pas sans susciter quelques interrogations. Au sein de la loi Sapin II, d'abord, l'article 8 et l'article 17 de la loi posent difficulté car ils s'articulent mal. En effet, ils ne visent ni les mêmes personnes ni le même objet [27]. La loi Vigilance, ensuite, prévoit un dispositif d'alerte pour le champ d'application matériel de la loi, mais la portée de celle-ci étant étendue et ses contours flous, l'objet du dispositif semble couvrir également au moins partiellement celui de la loi Sapin II. La mise en place de ces dispositifs dans les entreprises ne sera donc pas aisée.

L'analyse précédente conduit à inclure les atteintes portées aux données à caractère personnel dans le périmètre du dispositif d'alerte de la loi Sapin II, du moins de son article 8. Ne conviendrait-il pas alors, pour être parfaitement cohérent, d'inclure la protection des données à caractère personnel dans le code de conduite de la société dont toute violation entre dans le champ du dispositif d'alerte au sens de l'article 17 de la loi Sapin II ?

En conséquence, si les données entrent dans le champ d'application de la loi Vigilance et de la loi Sapin II, comme cela semble être le cas, en l'absence d'indications plus précises quant à la portée de ces lois, les sociétés qui sont assujetties à ces textes doivent impérativement mener un programme de *compliance* intégrant la problématique des données à caractère personnel. Cela implique naturellement une parfaite connaissance des obligations issues du RGPD.

B - Les données à caractère personnel comme moyen de la compliance

Les données à caractère personnel doivent être prises en compte dans la mise en œuvre de tout programme de *compliance* dès lors qu'elles en constituent la matière première.

En effet, de tels programmes procèdent de la collecte de données et notamment de données à caractère personnel. C'est précisément le cas des dispositifs d'alerte prescrits par la loi Sapin II et la loi Vigilance, pour lesquels l'enjeu de la protection des données est particulièrement prégnant.

Dans ce cadre, les données à caractère personnel sont des vecteurs de la *compliance* en tant qu'elles permettent la mise en œuvre du programme de *compliance*.

25 Considé. 1 : « La protection des personnes physiques à l'égard du traitement des données est un droit fondamental ».

26 Art. 1er de la loi Vigilance, art. 8 et 17, II- 2°, de la loi Sapin II.

27 Sur ce point, v. E. Daoud et S. Sfoggia, Lanceurs d'alerte et entreprises : les enjeux de la loi Sapin II, AJ pénal 2017. 71.

Cela suppose toutefois que leur usage soit encadré, conformément aux dispositions du RGPD.

Le RGPD ne prévoit aucune disposition spécifique aux dispositifs d'alerte, de sorte que son régime est soumis aux principes généraux applicables aux traitements de données. L'autorisation AU-004 de la CNIL relative aux traitements de données à caractère personnel mis en œuvre dans le cadre des dispositifs d'alerte a récemment fait l'objet de modifications afin de s'adapter à la loi Sapin II[28]. Son champ d'application est désormais calqué sur celui de la loi Sapin II, ce qui facilite la mise en œuvre du dispositif[29]. L'autorisation détermine les données à caractère personnel qui peuvent être collectées tout en précisant qu'elles doivent être formulées de manière objective, être en rapport direct avec le périmètre du dispositif et strictement nécessaires à la vérification des faits allégués.

Outre les dispositifs d'alerte, des données à caractère personnel sont également collectées dans le cadre des investigations internes ou audits menés dans les sociétés. Il convient dès lors de s'assurer que ces données sont collectées et traitées conformément aux règles et principes classiques de loyauté, de licéité, de proportionnalité, de minimisation des données, de conservation des données, etc.[30].

De même, des registres peuvent être créés visant à recenser les sous-traitants et les fournisseurs aux fins de mise en œuvre des obligations résultant de la loi Sapin II et de la loi Vigilance[31]. Il conviendra notamment de veiller aux zones de commentaires libres qui sont particulièrement encadrées par la CNIL. Il s'agit de ne pas faire apparaître de données sensibles au sens du RGPD (sur l'origine raciale ou ethnique, sur les opinions politiques ou religieuses, etc.) et plus généralement de ne pas formuler d'observations qui contreviendraient aux principes généraux précités.

Les données à caractère personnel doivent ainsi faire partie intégrante des programmes de conformité dès lors qu'elles entrent dans le champ matériel des lois Vigilance et Sapin II, mais également être protégées dès lors qu'elles sont utilisées pour mener à bien de tels programmes.

28 Délib. n° 2017-191 du 22 juin 2017 portant modification de la délibération n° 2005-305 du 8 déc. 2005 portant autorisation unique de traitements automatisés de données à caractère personnel mis en œuvre dans le cadre de dispositifs d'alerte professionnelle (AU-004). Subsiste une interrogation relative à l'application de cette autorisation : la survivance du régime des autorisations de la CNIL après l'entrée en vigueur du RGPD n'est pas acquise.

29 V., A. Balducci et E. Drouard, Loi « Sapin II » et dispositifs d'alertes professionnelles autorisés par la CNIL : quelle compatibilité ?, RLDI n° 133, janv. 2017.

30 V. le chap. II du RGPD.

31 V. not. E. Breen et A. Guttierrez-Crespin, Programmes de compliance : dix bonnes pratiques observées en France, *in La compliance : un monde nouveau*, éd. Panthéon-Assas, Paris II, 2016, p. 121, qui évoque comme bonne pratique la tenue d'un registre informatique des parties tierces.

CONSEILS PRATIQUES

Les lois Sapin II, Vigilance et le RGPD s'inspirent d'une méthode commune, ont recours aux mêmes outils et prévoient des obligations qui s'imbriquent les unes dans les autres. Ce constat milite pour une approche décloisonnée de la *compliance*. Rapprocher ces textes ne signifie pas méconnaître les différences de fond liées à leur domaine d'application distinct, dénaturer leurs dispositions ou recourir à des raccourcis simplistes, mais cela relève au contraire d'une analyse de raison qui consiste à appréhender ces textes de manière transversale afin de mettre à profit un certain voisinage.

Concrètement, il convient de mettre en commun les actions et les outils : réaliser des audits en tenant compte des exigences de la loi Vigilance, de la loi Sapin II et du RGPD, réaliser une cartographie des risques incluant les risques couverts par ces trois textes, procéder à des opérations de sensibilisation et de communication communes, instaurer un dialogue efficace entre les *Chief Compliance Officer, le Data Protection Officer* et les autres référents *compliance* désignés au sein de l'entreprise, etc.

Les bénéfices qui découlent de cette approche holistique sont significatifs : l'entreprise s'assure une meilleure couverture du risque ainsi qu'une rationalisation des coûts non négligeable.