Compliance & Droits de l'Homme

Apparue dans un premier temps pour garantir la bonne application des règles et politiques en matière de concurrence, la fonction « conformité » a évolué vers des missions plus globales de suivi et de garantie de la bonne application de la règle de droit dans l'entreprise, d'édiction de politiques éthiques et de codes déontologiques propres, de contrôles assortis de sanctions en cas de manquements.

Les finalités de la 'Compliance'

En pratique, la 'Compliance' a pour mission essentielle de concourir à la gouvernance et la gestion des risques juridiques inhérents à l'activité opérationnelle de l'entreprise, au premier rang desquels figurent les éventuelles violations des droits humains générés par l'activité de l'entreprise.

La « Compliance » s'inscrit dans une démarche de prévention, détection et remédiation des risques tant juridiques que de mise en cause réputationnelle, dans un contexte où les acteurs attendent de leurs partenaires commerciaux des démarches éthiques et de conformité robustes, c'est-à-dire efficaces et flexibles.

Les réglementations de la 'Compliance'

Parmi les réglementations appartenant à la matière conformité, on compte traditionnellement la loi Sapin 2, le RGPD et la loi sur le devoir de vigilance.
Ainsi, 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 (« loi Sapin 2 ») impose des obligations en matière de transparence et de probité, parmi lesquelles :

- Une obligation préventive pour certaines entités[1] d'adopter un programme de conformité efficace et adapté s'agissant des risques de corruption et de trafic d'influence ;
- La mise en place d'une gestion des alertes permettant au lanceur d'alerte respectant le régime légal de bénéficier d'un régime de protection[2] (identité protégée, protection contre toute représailles, défaut de responsabilité pénale en cas d'atteinte à un secret protégé par la loi).

Transposée en droit français le 16 février 2022, la directive 2019/1937 du Parlement européen et du Conseil de l'Union européenne sur la protection des personnes du 23 octobre 2019 a modifié les contours du mécanisme d'alerte, deuxième pilier de l'article 17 de la loi Sapin 2. La définition du lanceur d'alerte, les critères d'application de la protection pouvant lui être accordée, ainsi que la procédure de signalement afin d'en bénéficier ont ainsi été modifiés. Le dispositif devrait entrer en vigueur le 1er août 2022.

Par ailleurs, la loi n° 2017-399 du 27 mars 2017 relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre impose à certaines sociétés[3] la mise en place d'un plan de vigilance permettant d'identifier et de prévenir les risques d'atteintes graves envers les droits humains, les libertés fondamentales, la santé et la sécurité des personnes et l'environnement, résultant tant des activités de la société mère, que des sociétés contrôlées directement ou indirectement par elle, ou des sous-traitants ou fournisseurs avec lesquelles est entretenue une relation commerciale établie, lorsque ces activités sont rattachées à cette relation.

A ce sujet, la Commission européenne a publié le 23 février 2022 sa proposition de directive sur le devoir de vigilance en matière de durabilité des entreprises afin de favoriser un comportement responsable des entreprises dans les chaines de valeur mondiales. Cette proposition de directive est susceptible d'être modifiée par les instances européennes, de sorte que son analyse doit être nuancée ; toutefois l'extension potentielle du périmètre de vigilance et les nouvelles obligations susceptibles d'être posées appellent à la mise en place de mécanismes d'anticipation de cette nouvelle réglementation.

Par ailleurs, il est important de noter que la vigilance en matière de droits humains comprend une vigilance dite 'environnementale' ; le droit à un environnement sain étant non seulement reconnu comme un droit humain mais également comme un droit permettant la jouissance d'autres droits, tels que le droit à la vie, le droit à l'alimentation ou encore le droit à la santé ou à l'eau.

1 - Un double critère cumulatif est prévu par l'article 17 de la loi Sapin II : (a) Critère du nombre de salariés : toute société employant 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 (b) Critère du chiffre d'affaires : toute société dont le chiffre d'affaires ou le chiffre d'affaires consolidé est supérieur à 100 millions d'euros.
2 - Article 6 de la loi Sapin II
3 - Cette loi concerne toute société qui emploie à la clôture de deux exercices consécutifs au moins cinq mille salariés en son sein et dans ses filiales directes ou indirectes dont le siège social est fixé sur le territoire français ou au moins dix mille salariés en son sein et dans ses filiales directes ou indirectes dont le siège social est fixé sur le territoire français ou à l'étranger.

Enfin, le règlement général sur la protection des données personnelles impose des obligations de gouvernance afférentes aux traitements de données personnelles par les entreprises. Il impose à certaines[4] sociétés la mise en place d'un registre des traitements de données personnelles, ainsi que la réalisation d'études d'impacts sur l'ensemble des droits humains de traitements particuliers[5]. Le texte, tout comme les autres réglementations de la « Compliance » est clairement ancré dans une appréhension globale du respect des droits humains, son article premier indiquant : « *Le présent règlement protège les libertés et droits fondamentaux des personnes physiques, et en particulier leur droit à la protection des données à caractère personnel.* »

'Compliance' et droits humains

On comprend aisément que la 'Compliance', en tant qu'outil de gouvernance *ex ante*, c'est-à-dire outil de gestion en amont de la réalisation du risque, est une matière juridique répondant à un besoin de facilitation du respect des droits humains. Au regard des risques actuels, de la mondialisation croissante des échanges, et de la complexité des chaines d'approvisionnement, notamment au niveau de la sous-traitance, la Compliance est un outil utile pouvant permettre de détecter des atteintes aux droits humains sa chaîne d'approvisionnement, notamment dans des zones sensibles, et d'y remédier en interne.

A titre d'exemple, la 'Compliance' tend à permettre, via le RGPD, un respect de la vie privée et de l'ensemble des autres droits fondamentaux que celle-ci conditionne, tels que le droit à la non-discrimination ou à l'épanouissement qui s'entend de « l'obligation qu'a le droit d'assurer dans l'environnement sociétal, tel qu'il est à un moment donné, la possibilité pour chacun de développer sa personnalité et de contribuer ainsi de manière originale à la construction de la société par le jeu démocratique »[6].

De la même façon, les mécanismes d'alerte favorisent une communication – interne ou externe – à même d'appréhender les risques de violation de droits humains.

Aujourd'hui, la règlementation semble tendre vers une appréhension plus globale et générale des droits humains via les mécanismes de compliance.

Ainsi, la proposition de directive sur le devoir de vigilance, en l'état, dispose de seuils d'application plus larges que ceux de la loi française sur le devoir de vigilance ; de sorte que de nombreux acteurs économiques, aujourd'hui non soumis à cette obligation, devraient à l'avenir se mettre en conformité avec les nouvelles mesures prévues par la directive. De surcroît, si les micro-entreprises et les PME sont exclues du champ d'application de la directive, elles pourraient être indirectement touchées si elles souhaitent entretenir ou conserver des relations commerciales avec des entreprises soumises à la directive.

Ou encore, le 'Digital Service Act', actuellement négocié au niveau européen, comprend en l'état des obligations d'évaluation des risques systémiques découlant, pour les très grandes plateformes, du design, du fonctionnement ou de l'utilisation de leurs services. Cette évaluation devrait notamment être réalisée *ex ante* : avant tout changement majeur apporté à leurs services. Ici encore, un mécanisme de conformité est utilisé afin de faciliter le respect des droits humains, puisque l'évaluation en question devrait notamment porter sur les risques de violation des droits fondamentaux reconnus par la Charte européenne[7].

Imane Bello,
avocate au cabinet Vigo Avocats et enseignante en éthique du numérique à Sciences Po Paris
Emmanuel Daoud,
avocat associé au cabinet Vigo Avocats

LE CERCLE DE LA COMPLIANCE

4 - . Selon l'article 30 du RGPD, l'obligation de tenir un registre de traitement doit être respectée par les entreprises ayant plus de 250 salariés. Sont également concernées par cette obligation les entreprises de moins de 250 salariés, uniquement si l'une des trois conditions visées par l'article 30.5 du RGPD est remplie : (1). Le traitement est susceptible de comporter un risque pour les droits et libertés des personnes concernées, (2) Le traitement n'est pas occasionnel, (3) Le traitement porte sur les données relatives à des infractions pénales ou sur des données sensibles (Articles 9 et 10 du RGPD).
5 - Selon l'article 35 du RGPD, la réalisation d'une analyse d'impact sur la protection des données (AIPD) est obligatoire, avant la mise en œuvre du traitement envisagé, lorsque le traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées. Le RGPD, à l'article 35.3, donne une liste de 3 types de traitements pour lesquels une AIPD est en particulier nécessaire en raison du risque élevé qu'ils sont susceptibles d'engendrer pour les droits et libertés des personnes concernées: (1) le traitement permet l'évaluation systématique et approfondie d'aspects personnels fondée sur un traitement automatisé et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire, (2) le traitement à grande échelle de données sensibles ou relatives à des condamnations pénales et des infractions, (3) la surveillance systématique à grande échelle d'une zone accessible au public. La Cnil estime, dans une délibération n°2018-326 de la CNIL, qu'un traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées si au moins deux des neuf critères visés au deuxième alinéa de l'article 1.1 de la présente délibération sont remplis. Exemple de critères : les données sont traitées à grande échelle, sont traitées des données sensibles, les données traitées concernent des personnes vulnérables (enfants, personnes âgées…). Si un traitement rempli deux de ces 9 critères, le responsable de traitement devra alors réaliser une AIPD avant de le mettre en œuvre.
6 - POULLET, « La vie privée à l'heure de la société du numérique, Larcier, 2019, §11, p. 65.
7 - En l'état du texte, article 26 (1) (b) DSA