Quand la compliance se saisit de « l'IA » : un nouvel horizon pour la fonction compliance dans l'entreprise et les CCO

Christophe Roquilly, Professeur, Directeur de l'EDHEC Augmented Law Institute, Doyen honoraire du corps professoral à l'EDHEC Business School et Vice-Président du Cercle de la Compliance

Portée par l'intelligence artificielle générative, la vague de « l'IA » est arrivée sur les rives de nombreuses entreprises et organisations. Deux remarques préliminaires s'imposent. La première porte sur le caractère discutable de la terminologie « IA », Luc Julia[1] lui-même affirmant qu'elle n'existe pas. Mais étant passée non seulement dans le langage courant, mais également dans le langage juridique comme en atteste l'IA Act publié le 12 juillet 2024 au Journal officiel de l'Union européenne (JOUE), admettons qu'il soit trop tard pour revenir sur celle-ci. Deuxièmement, il convient alors de rappeler qu'il n'y a pas qu'un type d'IA. Entre IA connexionniste et IA symbolique, entre système expert et apprentissage automatique (supervisé ou non), entre IA dite « faible » ou « étroite » et IA dite « forte », les différences peuvent être substantielles. Enfin, et pour reprendre les thèmes chers au mouvement technoréalisme, l'IA ne peut être enfermée dans les qualificatifs de « système », « outil », « algorithme » ou encore « modèle »[2].

Quoi qu'il en soit, un nombre croissant d'organisations utilisent ou vont utiliser des solutions technologiques s'appuyant sur une IA, sans parler de celles qui vont les fabriquer, parfois sur la base de « larges modèles de langage » (LLM). Et pas toujours en adoptant la bonne démarche, en particulier en matière d'identification des buts poursuivis et de risques encourus. Émerge ainsi un nouveau terrain de jeu passionnant et à enjeux pour les Compliance Officers et la fonction compliance. En effet, il met à contribution cette vision que partageait il y a un peu plus d'un an Catherine Delhaye dans les colonnes du Journal du Management Juridique[3], à savoir que le Compliance Officer sera de plus en plus un manager du risque, qui doit aussi se préoccuper de la *soft law*, contributeur à des enjeux stratégiques et recherchant la coopération.

[1] Luc Julia est un ingénieur et informaticien franco-américain, spécialisé dans l'intelligence artificielle.
[2] Voir https://www.technorealisme.org/
[3] Interviewée par Aude Dorange, Journal du Management Juridique, mai 2023, https://www.village-justice.com/articles/interview-compliance-doit-rayonner-dans-toute-organisation,46119.html

I. La fonction compliance acteur de la gestion des risques systémiques posés par les « IA »

Ces risques sont multiples (technologiques, économiques, humains, et évidemment juridiques et éthiques) pouvant se traduire par de la destruction de valeur financière, stratégique et réputationnelle. C'est d'ailleurs une approche par les risques qui prévaut dans le Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle[4]. Les « systèmes d'IA » sont en effet classés selon leur niveau de risque par rapport aux valeurs de l'Union européenne (UE), ainsi qu'à la santé, la sécurité et aux droits fondamentaux (inacceptable, haut, spécifique et minimal) et entraînent des obligations différentes selon le niveau. De plus, les « modèles d'IA à usage général » sont soumis à diverses obligations, notamment de transparence, de documentation, d'évaluation et d'atténuation des risques systémiques. Et d'autres types de risques juridiques ne sont pas à négliger, notamment en matière de droits de propriété intellectuelle.

Pour de nombreuses organisations, le terrain de jeu ne se limite pas à l'UE et il est alors impératif de s'enquérir des choix de régulation de l'IA qui ont été – ou seront – faits dans les différentes zones géographiques où l'entreprise intervient d'une manière ou d'une autre. Par exemple, aux Etats-Unis, après une ordonnance signée par le Président Biden en octobre 2023 et les initiatives prises par certaines autorités telles que la *Federal Trade Commission* (*FTC*), divers textes sont en attente et de nombreux États ont d'ores et déjà pris certaines dispositions[5]. Des pays comme la Chine ou le Royaume-Uni ont fait des choix différents, entre régulations ciblées et régulations sectorielles à venir, certes avec des doctrines étatiques différentes.

Seule une cartographie des réglementations applicables à l'entreprise en fonction de sa géographie économique et de son (ses) secteur(s) d'activité, de son statut au regard des IA (est-elle fournisseur, déployeur, utilisateur ?) et du type d'IA concerné peut permettre de répondre à une première question dans le registre de la compliance : à quoi devons-nous nous conformer ? Et comme évoqué précédemment par la citation de Catherine Delhaye ainsi que dans le livre blanc « Talented Compliance – Le Référentiel de compétences du Compliance Office sur mesure », édité par le Cercle de la Compliance en partenariat l'EDHEC Augmented Law Institute[6], la compliance n'est pas seulement la conformité à la réglementation et aux engagements souscrits par l'entreprise, et donc aux règles internes, mais elle intègre également une notion d'éthique et de respect des valeurs. La compliance en matière d'IA doit non seulement être « réglementaire », mais aussi « éthique », et donc globale. L'examen des règles de *hard law* qui commencent à émerger pour encadrer les « systèmes d'IA » met en évidence que le débat éthique est indispensable dans les entreprises notamment parce que ces règles sont parfois floues car faisant référence à des concepts ou des notions pas toujours (bien) définis : transparence, explicabilité, durabilité, bienveillance, justesse, loyauté, robustesse, proportionnalité, *etc.* L'examen des divers travaux et recommandations d'organisations comme l'UNESCO, les Nations-Unies, l'OCDE, *etc.*, peut évidemment aider, mais il n'exonère pas l'entreprise de sa propre introspection éthique pour décider, au-delà de ce qui est légal ou licite, ce qui est acceptable d'un point de vue éthique tenant compte de ses valeurs et de ses objectifs économiques.

[4] https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=OJ:L_202401689
[5] https://www.ncsl.org/technology-and-communication/artificial-intelligence-2023-legislation
[6] https://www.lecercledelacompliance.com/competences-compliance/

L'identification des risques portés par les normes juridiques et éthiques est un travail fondamental dans la chaîne de valeur de la fonction compliance. Mais la compliance, et le rôle des Compliance Officers, sont bien plus larges. Elle vise en réalité « *l'ensemble des mesures prises par l'entreprise et sa direction dans le but de répondre aux exigences posées par les lois et les règlements, ainsi que par toute autre norme ou valeur dont l'inobservance ou le non-respect risquerait d'entrainer des conséquences négatives pour l'entreprise* »[7]. Ces mesures peuvent être un dispositif de gouvernance, des process, des codes de bonne conduite, des programmes à déployer, des formations, *etc.* Elles vont nécessiter une étroite collaboration entre la fonction compliance et d'autres fonctions de l'entreprise, d'autant que la compliance en matière d'IA va devoir aussi se référer à des normes issues de corpus de règles extérieurs aux régulations et réglementations spécifiques à l'IA.

II. La place de la fonction compliance dans la gestion des risques liés aux « IA » : le dynamitage des silos

La diversité des risques juridiques et éthiques que présentent les « systèmes d'IA » – le *National Institute of Standards and Technology* (*NIST*) du *US Department of Commerce* en a dénombré une bonne dizaine en matière d'IA Générative[8] – met en évidence l'indispensable collaboration entre la fonction compliance et de nombreux autres acteurs de l'entreprise, aux différents stades du process global de compliance : identification et évaluation des risques de non-conformité (*e.g.* « shadow IT » avec des employés utilisant ChatGPT sans se soucier de la sécurité/confidentialité des données utilisées) et l'existence ou non de processus de contrôle adéquat ; mise en place de méthodes d'évaluation de ces risques en tant que partie intégrante de programmes de compliance et évaluation de l'efficacité de ces programmes, ainsi qu'amélioration nécessaire de ces méthodes et programmes dès lors que les normes juridiques en matière d'IA sont susceptibles d'évolution ; élaboration de la documentation nécessaire permettant de montrer qu'un dispositif robuste en matière de « compliance IA » existe.

La « compliance IA » est un dynamiteur de silo. Parce que, d'une part, elle ne peut pas être développée en vase clos. Lors d'une allocution en mars 2024 auprès de l'*American Bar Association*, Lisa Monaco, la *Deputy General Attorney*, a indiqué qu'elle demandait au *Department of Justice* (*DOJ*) d'intégrer l'évaluation des risques associés à l'IA dans sa politique d'évaluation des programmes de conformité des entreprises et qu'il conviendra que les Compliance officers soient informés que le *DOJ* prendra désormais en compte la manière dont le programme de conformité d'une organisation atténue le risque d'utilisation abusive de l'IA lorsqu'il évaluera le programme dans le cadre d'une résolution d'entreprise[9]. L'existence de liens entre les normes juridiques et éthiques en matière d'IA et d'autres corpus de normes requiert qu'un dispositif de « compliance IA » soit perméable aux exigences en matière de

[7] Définition inspirée des travaux de Björn Fasterling, « Compliance – Vers une formalisation », in : C. Roquilly (ed.), La contribution des juristes et du droit à la performance de l'entreprise, Joly éditions, Lextenso éditions 2011 : 321-32, et proposée par C. Collard, C. Delhaye, H.-B. Loosdregt et C. Roquilly, « Risque juridique et conformité : manager la compliance », éd. Lamy, Lamy Conformité, 2011

[8] NIST AI 600-1, « Intelligence Risk Management Framework : Generative Artificial Intelligence Profile », NIST, avril 2024, https://airc.nist.gov/docs/NIST.AI.600-1.GenAI-Profile.ipd.pdf

[9] https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-monaco-delivers-keynote-remarks-american-bar-associations

protection des données personnelles telles qu'exigées par le RGPD[10], de cybersécurité telles que portées par le Cyber Security Act de 2019[11], de gestion des données comme le prévoit le Data Act qui ne sera applicable qu'à partir de septembre 2025, sans oublier, selon le type d'organisation ou d'entreprise, les obligations en particulier issues des DMA, DSA, et les dispositions des textes à venir sur la responsabilité en matière d'IA et les produits défectueux, pour ne se limiter ici qu'aux textes de l'UE.

Ce mille-feuille normatif appelle un dispositif de compliance ayant la capacité à embrasser la dimension polysémique et multirisque de l'IA, dépassant une approche en silo « par norme juridique ». Dès lors, plus que jamais, la fonction compliance dans l'organisation doit collaborer avec de nombreuses autres fonctions et experts, comme l'ont souligné les experts du Cercle de la Compliance dans le livre blanc précité. Cette transversalité, la fonction compliance en a l'habitude : « *l'un des rôles majeurs du compliance officer est d'ouvrir les portes et de faire admettre la transversalité* »[12]. En matière d'IA, les interactions sont et seront nombreuses : DSI, Responsables Cyber, product owners, RH, Responsables Innovation, Risque, Contrôle, *etc.*, managers BU et métiers susceptibles d'utiliser des solutions intégrant une IA et, selon les organisations et l'existence ou fusion de certaines fonctions (*Chief Ethics Officer, Digital Ethics Officer, Head of Data*, Directrice ou Directeur Juridique, *Chief AI Officer*, *etc.*). L'identification de toutes les parties prenantes dans le cycle de vie de l'IA et de leurs rôles, conduira aussi à choisir la gouvernance de l'IA la plus adéquate dans laquelle le *Chief Compliance Officer* (*CCO*) doit occuper la place qui lui revient, en lien avec d'autres organes de gouvernance.

La « compliance IA » s'affirme comme une gestion de la complexité, avec ses zones grises, la rigueur et la créativité nécessaires pour que l'organisation soit en mesure de décider ce qu'elle autorise ou non au regard des risques au croisement entre les normes, les valeurs et la pérennité d'une activité économique.

[10] Concernant l'articulation entre RGPD et IA Act, voir les exposés très clairs de la CNIL : https://www.cnil.fr/fr/entree-en-vigueur-du-reglement-europeen-sur-lia-les-premieres-questions-reponses-de-la-cnil

[11] https://cyber.gouv.fr/cybersecurity-act

[12] Réf. Préc., note n°5, p. 14