Construire une gouvernance numérique efficace en entreprise : enjeux et méthodes

Emmanuel Daoud, Administrateur du Cercle de la Compliance, Avocat associé, Cabinet Vigo
Flora Brac de la Perriere, Avocate counsel, Cabinet Vigo
(Juin 2025)

À mesure que l'intelligence artificielle s'immisce dans les entreprises, instaurer une gouvernance du numérique devient un impératif stratégique.

Elle consiste à définir un ensemble de processus, de règles et de structures permettant de gérer les risques liés aux technologies et aux données, dans un environnement juridique dense, mouvant et exigeant.

Gouverner le numérique revient ainsi à piloter l'entreprise dans un cadre normatif d'une complexité inédite, tout en accompagnant sa transformation dans un contexte incertain et déroutant.

Elle s'impose désormais comme une évidence, conditionnant la performance, la compétitivité et la capacité des entreprises à évoluer de manière responsable.

I. Les nouveaux visages du risque juridique du numérique

Cette gouvernance doit en premier lieu reposer sur une compréhension fine et transversale des risques juridiques. Cela implique de savoir articuler la réglementation applicable à la protection des données à caractère personnel (RGPD[1], loi Informatique et Libertés[2]), à la cybersécurité (directive NIS 2[3], règlement DORA[4]), à l'intelligence artificielle (AI Act[5]), ainsi qu'à toute autre règle relative à l'éthique des usages du numérique.

Le numérique est en effet désormais l'objet d'une mille-feuille législatif d'une complexité inédite, mêlant droit impératif (règlement européen, loi etc.), normes de droit souple des autorités (CNIL, CEPD etc.), de portée générale ou sectorielle, nationale ou internationale. Cette densité normative en constante expansion, étend les hypothèses dans lesquelles la responsabilité de l'entreprise peut être juridiquement engagée.

[1] 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).
[2] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles,
[3] Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union
[4] Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 relatif à la résilience opérationnelle numérique du secteur financier
[5] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 **établissant des règles harmonisées sur l'intelligence artificielle**

Par ailleurs, la massification des traitements de données personnelles, l'essor de l'intelligence artificielle, ou encore l'augmentation des cyberattaques transforment profondément la nature, la gravité et le nombre de risques juridiques liés au numérique.

Chaque choix technologique devient porteur d'implications multiples, susceptibles d'engager l'organisation bien au-delà du seul champ opérationnel.

Réputation, confiance des utilisateurs et des partenaires, croissance économique, tels sont les enjeux d'une bonne gouvernance du numérique.

Le droit, dans ce contexte, ne constitue plus un simple garde-fou. Il devient une grammaire permettant de structurer, en toute sécurité, les choix technologiques de l'entreprise.

II. L'impératif d'une gouvernance incarnée

Toute gouvernance suppose également une architecture décisionnelle claire et lisible.

En matière numérique, l'un des écueils majeurs tient à la tentation, pour les opérationnels, d'aborder les enjeux de manière compartimentée, à travers le prisme de leurs expertises respectives.

La gouvernance numérique ne saurait pourtant se construire en silos.

La Direction des systèmes d'information (DSI) ne peut, par exemple, définir seule les mesures de cybersécurité applicables : celles-ci doivent être pensées en concertation étroite avec la direction juridique, le Délégué à la protection des données (DPO) et, lorsque cela est pertinent, le référent « intelligence artificielle » de l'entreprise.

Une réflexion commune doit s'articuler au regard de l'obligation de sécurité des traitements de données à caractère personnel (article 32 du RGPD), des obligations de sécurité des systèmes d'information et des réseaux définies par la directive NIS 2, par le règlement européen DORA si applicable, ainsi qu'avec l'obligation de robustesse des systèmes d'IA posée par l'AI Act (article 15).

Cette transversalité dans les échanges conditionne non seulement la cohérence des dispositifs, mais aussi leur pertinence.

Le pilotage de la gouvernance numérique peut être confié à un comité *ad hoc*, spécifiquement dédié aux enjeux technologiques. Ce dernier peut, le cas échéant, s'inscrire dans une structure plus englobante, telle qu'un comité d'éthique des affaires, lui-même rattaché à la direction générale.

Pour être capable de conjuguer les impératifs *business,* les exigences techniques, et les cadres normatifs, ce comité doit intégrer des profils hybrides dont des ingénieurs et des juristes.

Plus encore, un mandat clair doit lui être octroyé pour influer sur les projets structurants de l'entreprise, dès leur genèse.

III. Méthodologie pour une gouvernance efficace

L'efficacité d'une gouvernance tient aussi à la qualité de la méthode employée.

La maîtrise des actifs numériques de l'entreprise est au cœur de toute gouvernance numérique efficace. La cartographie de ces actifs est ainsi la première étape à suivre. Elle permet de recenser les éléments immatériels à valeur stratégique détenus ou exploités sous forme numérique, par l'entreprise.

Il peut s'agir de données (personnelles, sensibles, industrielles), d'infrastructures et de systèmes (ERP, cloud, IA), de contenus digitaux (sites, algorithmes, médias) ainsi que de droits associés (brevets, licences, noms de domaine). Cette cartographie, qui évolue de façon constante au gré des projets de l'entreprise, permet notamment d'identifier les flux de données, les technologies déployés, les fournisseurs, ainsi que les réglementations applicables.

Les règles internes applicables à ces actifs ainsi qu'à l'usage des outils et du système d'information, y compris à l'IA, peuvent ensuite être intégrées au sein de la Charte informatique opposable aux salariés, annexée au règlement intérieur. Sécurité, confidentialité, transparence, non-discrimination sont autant de principes, parmi d'autres, qu'il convient de décliner de manière opérationnelle à l'utilisation d'internet, des ordinateurs, smartphone, ou encore de logiciels y compris ceux intégrant de l'IA, etc. La centralisation de l'énoncé de ces règles au sein de la Charte informatique permet à celles-ci d'être lisibles, et d'octroyer à ce cadre une force contraignante.

L'élaboration de politiques et procédures détaillées, propre à chaque domaine de conformité du numérique (RGPD, IA, cybersécurité etc.) est également déterminante pour un usage sécurisé des technologies.

L'acculturation est en outre un pilier essentiel d'une bonne gouvernance du numérique. Une compréhension des enjeux du numérique par les instances dirigeantes et les opérationnels, garantit une gouvernance efficace et profonde.

Dans cette dynamique, les cabinets d'avocats jouent un rôle clé. Pour être réellement aidants, ils doivent eux-mêmes disposer d'une expertise en compliance suffisamment large et transversale, leur permettant d'articuler les exigences juridiques issues de cadres multiples — RGPD, AI Act, NIS 2, DORA, entre autres — et d'en proposer une lecture cohérente et opérationnelle. Leur positionnement leur permet de faire le lien entre les différentes directions de l'entreprise (juridique, DSI, conformité, éthique, etc.), d'identifier les synergies entre les domaines réglementaires et de veiller à leur traitement mutualisé. Ils renforcent ainsi la cohérence et l'efficacité des stratégies numériques.

IV. Conclusion : gouverner pour mieux transformer

En définitive, la dépendance croissante des entreprises aux technologies de l'information, notamment à l'IA, impose de repenser la gouvernance du numérique.

Mettre en place une bonne gouvernance du numérique revient à doter l'entreprise d'un cap et d'une boussole, dans un contexte où la pression réglementaire s'intensifie, où les parties prenantes accordent une importance croissante à la conformité, et où l'IA transforme en profondeur les pratiques professionnelles.

Elle nécessite notamment d'investir dans les compétences, de revisiter les circuits de décision, et d'adopter des méthodes de mise en conformité adaptées à la complexité réglementaire.

Mettre à jour sa gouvernance du numérique engage une vision : celle d’un usage du numérique maîtrisé, au service d’une transformation et d’une performance durable de l’entreprise.