Guide de mise en œuvre de l'*AI Act*

Partie 2 : Gouvernance

Mode d'emploi et outils pour mettre en place une gouvernance de l'IA

Cigref
RÉUSSIR LE NUMÉRIQUE

numeum
Engager le numérique

Table des matières

Introduction

Dans cette période d'entrée en vigueur des règles applicables à l'espace numérique européen dans le cadre de la stratégie européenne « Décennie Numérique », les enjeux de la gouvernance sont devenus cruciaux. La mise en place d'une gouvernance dédiée apparaît essentielle pour permettre aux entreprises et aux administrations publiques, soumises à ces nouveaux textes réglementaires, de mieux les appréhender et de naviguer entre les diverses obligations qui en découlent.

En définissant et en imposant des normes de conformité et de responsabilité, l'*AI Act* vise à garantir que les modèles d'Intelligence Artificielle à usage général et les systèmes d'Intelligence Artificielle, déployés par les organisations, soient sûrs, transparents et respectueux des droits fondamentaux.

Ainsi, l'*AI Act* introduit des exigences de gouvernance rigoureuses pour encadrer leur utilisation et leur déploiement en Europe avec, pour les systèmes d'IA en particulier :

- Une **classification** selon le niveau de risque (inacceptable, élevé, limité et minimal) ;
- Des exigences de **conformité** pour les systèmes à **risque élevé** ;
- Une surveillance et des **audits** ;
- Un rôle central des **autorités de régulation** ;
- Une **gouvernance des données** et des exigences de **transparence** ;
- Une clarification des questions liées à la **responsabilité** et la **gestion des risques**.

Au-delà du risque réglementaire (particulièrement pour les systèmes d'IA à risque élevé), la gouvernance permet aux organisations, pour chaque cas d'usage – et ce point est non négligeable – d'identifier et de limiter l'ensemble des autres risques sous-jacents au développement et à l'utilisation de systèmes d'IA, par exemple ceux associés à la propriété intellectuelle, la confidentialité ou la cybersécurité.

In fine, le rôle de la gouvernance est de **poser un cadre**, **propre à chaque organisation**, **compris** et **adopté par tous**, afin de permettre et de promouvoir l'adoption et le développement de l'IA au sein de l'entreprise. Il s'agit d'un outil au service de l'innovation et non, comme on le pense trop souvent, d'un frein à cette dernière.

L'objectif de ce 3e livret du « Guide de mise en œuvre de l'*AI Act* » est d'expliquer les besoins et les spécificités de la gouvernance en matière d'IA afin que les organisations puissent appliquer au mieux les règles présentées dans le livret « Cartographie des obligations » de ce guide. Ce livret a également vocation à proposer des outils pratiques et des recommandations utiles à l'adoption d'une stratégie de gouvernance efficace.

Par ailleurs, puisqu'une « bonne » gouvernance ne doit pas s'arrêter aux portes de l'organisation concernée, un aperçu global de l'environnement institutionnel de l'IA sera présenté afin que les lecteurs puissent utiliser leur gouvernance comme outil de dialogue et d'échange avec les autres acteurs du marché et les autorités, sur le plan national comme international.

1. Comprendre la gouvernance de l'IA

1.1. Qu'est-ce que la gouvernance de l'IA ?

La gouvernance est une notion protéiforme, mais appliquée à un contexte règlementaire, et en particulier celui de l'*AI Act*, elle agit comme un outil de conformité.

Très pratiquement, la gouvernance de l'IA recouvre l'ensemble des politiques, mesures, et procédures à mettre en œuvre afin que l'organisation qui utilise ou développe l'IA puisse identifier les risques associés à un cas d'usage donné et s'en protéger. Elle permet de définir ou d'identifier :

1. Les **acteurs** (personnes et départements) impliqués dans la mise en conformité de l'IA et dans la prévention des risques de l'IA.
2. Les **lieux de concertation et d'arbitrage** qui faciliteront les échanges d'information entre acteurs et les prises de décision (comitologie).
3. Les **tâches** à entreprendre afin de se conformer à l'*AI Act* et prévenir les risques de l'IA.
4. Les **outils** et les **procédures** à mettre en place pour décliner les tâches identifiées au sein de l'organisation.
5. La **responsabilisation** de la chaîne d'acteurs de la gouvernance.

Des outils comme le RACI - matrice de répartition des responsabilités entre différents acteurs avec des niveaux de responsabilité, information et consultation attribués en fonction des tâches à accomplir – ainsi que le rétroplanning peuvent aider à clarifier ces cinq éléments et à responsabiliser les acteurs de la gouvernance.

Il est important de noter qu'il **n'existe pas un modèle unique de gouvernance de l'IA** et qu'il n'est **pas forcément nécessaire de créer de nouvelles instances et procédures**. En fonction des entreprises et de leurs secteurs d'activité, des instances de gouvernance (opérationnelles ou juridiques) sont déjà en place. La gouvernance de l'IA peut s'insérer dans ces instances et ainsi s'adapter au fonctionnement existant de l'organisation en intégrant les évolutions structurelles et règlementaires à venir. La gouvernance de l'IA, aussi importante soit-elle, ne doit pas bouleverser la structure et les modèles d'organisation des entreprises ni entraver les futurs besoins. La gouvernance doit être perçue comme une opportunité à adopter sur le long terme.

Il est donc recommandé de prendre en compte les autres instances de gouvernance de l'organisation et d'évaluer dans quels cas il est possible et pertinent de réutiliser l'existant. Par exemple, la méthodologie projet utilisée par les achats pour sélectionner un prestataire dans le cadre d'un nouveau projet, ou celle des équipes de R&D pour lancer un nouveau produit peuvent être adaptées pour choisir ou intégrer certains outils d'IA.

> Si pour certaines entreprises, il peut être pertinent de créer une gouvernance unique dédiée qui englobe l'ensemble des risques liés à l'IA de façon holistique, pour d'autres, il sera préférable de rattacher la gouvernance de l'IA aux gouvernances déjà existantes en fonction des risques identifiés (gouvernance mise en place par le Délégué à la Protection des Données personnelles (DPO), propriété intellectuelle, RH, éthique & Responsabilité Sociétale des Entreprises, etc.). Ainsi, il peut être recommandé de mutualiser les efforts et de capitaliser sur les procédures et actions déjà menées ou en cours, en particulier en ce qui concerne la gouvernance de la donnée (qui appréhende par exemple les règlements européens *Data Act* (Règlement UE 2023/2854) et *Data Governance Act* (Règlement UE 2022/868) ainsi que les exigences de

cybersécurité avec la directive NIS II (Directive UE 2022/2555) et le règlement DORA (Règlement 2022/2554)).

Dans les secteurs déjà très réglementés, comme le secteur financier ou certains secteurs industriels, cette mutualisation de la gouvernance est d'ailleurs recommandée par l'*AI Act* « *afin d'assurer la cohérence, d'éviter les doubles emplois, et de réduire au maximum les charges supplémentaires* » (Article 8.2 de l'*AI Act*).

1.2. Pourquoi implémenter une gouvernance de l'IA ?

Tout d'abord, un **cadre défini** et **connu de tous** est indispensable pour rendre opérationnelles les règles de l'*AI Act* de manière efficace et pérenne. C'est pourquoi aujourd'hui, un grand nombre d'organisations restent prudentes et peinent à s'organiser pour maîtriser le déploiement des systèmes d'IA, faute d'un cadre permettant l'identification des opportunités et des risques associés à chaque cas d'usage.

La mise en place d'une gouvernance permet également de rationaliser les efforts au sein de l'organisation et de mobiliser les différentes fonctions et départements qui ont vocation à être impliqués. La gouvernance est donc le vecteur de cette transversalité essentielle pour organiser au mieux les indispensables échanges entre les différents métiers et appréhender les différents risques.

La mise en place d'une gouvernance de l'IA répond aussi à un enjeu réputationnel pour l'entreprise. L'intelligence artificielle suscite de nombreuses inquiétudes quant à son impact sur nos sociétés. Une entreprise qui cherche à adopter l'IA a ainsi tout intérêt à gagner la confiance de son personnel, de ses clients et du marché (à tout le moins européen) en montrant « patte blanche » quant au respect des règles de l'*AI Act* mais également quant à son appréhension des risques globaux de l'IA (éthique, RSE, impacts sur l'emploi, respect des droits de propriété intellectuelle, etc.). La transparence et la responsabilisation des acteurs de l'IA vis-à-vis du public et du marché (publication de politiques, lignes directrices sur les sites internet, engagements sur l'IA Responsable, adhésions à des pactes, etc.), sont autant d'éléments de nature à rassurer, voir même à faire gagner un **avantage concurrentiel**, (ou du moins, à ne pas en perdre un).

Par ailleurs, la mise en œuvre du RGPD a permis d'éprouver la démarche et ses acquis, et a prouvé qu'une gouvernance bien pensée permet de **minimiser les coûts de mise en conformité**. Ce dernier point est fondamental car les organisations n'étant pas en mesure de complètement anticiper ces coûts à date, elles ont besoin de rassurer leurs instances de gouvernance à cet égard.

Avantage concurrentiel | **Appréhension globale du risque** | **Minimisation du coût de la conformité**

Trois grandes raisons d'implémenter une gouvernance de l'IA

2. Réduire son exposition aux risques grâce à la gouvernance de l'IA

2.1. De quels risques s'agit-il ?

La gouvernance de l'IA permet d'appréhender **tous** les risques afférents à l'IA, et ce, à chaque étape du cycle de vie d'un système d'IA : de sa conception à son développement, son entraînement, ses phases de test, sa mise en production, et sa mise sur le marché (déploiement), sans oublier son utilisation.

Les éléments ci-dessous présentent les principaux risques juridiques inhérents à l'IA auxquels il faut prêter attention, en fonction de son rôle dans la chaîne de valeur, afin d'assurer une utilisation sûre du modèle d'IA à usage général ou du système d'IA. La gouvernance, pour chaque cas d'usage, doit permettre l'identification des risques, leur évaluation et la mise en œuvre de mesures de remédiation.

Risque réglementaire

- Le non respect de l'une ou plusieurs des obligations de l'*AI Act* peut avoir des conséquences financières (sanctions) mais également réputationnelles (perte de part de marché, perte de clientèle, etc.).
- En dehors de l'*AI Act*, l'utilisation des systèmes d'IA doit être conforme aux lois et réglementations émergentes dans le monde entier (Etats-Unis, Chine, etc.).

Responsabilité

- Les règles de responsabilité du fait des produits défectueux (telles que récemment modifiées par la Directive UE 2024/2853) doivent être anticipées, tout comme les règles classiques de responsabilité contractuelle et délictuelle. En effet, les IA étant par nature difficilement prévisibles, il est possible qu'elles produisent des résultats dommageables pour des individus ou des entreprises.
- Dans le cadre de la fourniture de systèmes d'IA à des entreprises, les contrats devront être adaptés afin de prendre en compte les risques spécifiques à l'IA (comme cela avait été fait par exemple lors de l'entrée en vigueur du RGPD).

Confidentialité et protection du secret des affaires

- La particularité des systèmes d'IA est qu'ils sont entraînés en continu, y compris à partir des données entrées par les utilisateurs (input). L'environnement dans lequel l'IA évolue, s'il n'est pas ségrégé, peut également permettre à l'IA d'apprendre des données auxquelles elle a accès. Une IA qui n'implémente pas des mesures de sécurité adéquates pourrait rendre accessibles ses données confidentielles auprès d'autres clients, voire du public (appelé effet de régurgitation) – notamment parce que l'IA pourrait générer ces données d'entrée si elles sont considérées pertinentes au regard de la requête faite par un autre utilisateur.

Sécurité informatique et robustesse

- Les systèmes d'IA sont particulièrement vulnérables aux attaques cyber : attaques par manipulation (détournement du comportement du système d'IA *via* des requêtes malveillantes), par infection (contamination du système d'IA lors de sa phase d'entraînement *via* des données d'entrées ou d'entraînement), par exfiltration (vol de données utilisées par le système d'IA en production).
- Ces attaques peuvent avoir de graves conséquences sur la confidentialité des données mais également leur intégrité, leur disponibilité et/ou leur traçabilité.

Erreur

- Les systèmes d'IA se distinguent des logiciels traditionnels par leur caractère «imprévisible». Les systèmes d'IA peuvent générer des contenus faux, inexacts ou trompeurs et faire référence à des sources qui n'existent pas (appelé phénomène d'« hallucination »), notamment lorsque les jeux de données d'entraînement ne sont pas qualitatifs et sélectionnés avec soin lors de l'entraînement. Ainsi, il faut porter une attention particulière aux cas d'usage du système afin d'éviter une finalité d'utilisation critique pour l'entreprise et inclure des procédés de vérification humaine des résultats.

Protection des données personnelles

- L'utilisation de systèmes d'IA peut impliquer le traitement de données personnelles lorsqu'elles sont utilisées en données d'entrée. Aussi, de nombreuses données personnelles sont utilisées en données d'entraînement et les autorités de protection de données rappellent que cette utilisation doit être sans préjudice du respect des règles de protection des données (information, droit à la suppression, durées de conservation, etc.) et ce, quand bien même la technologie d'entraînement utilisée rendrait difficile le respect de ces règles.
- Des bonnes pratiques et recommandations ont été émises par les autorités de protection de données sur ce risque.

Discrimination et impartialité

- Les systèmes d'IA peuvent produire des résultats discriminatoires ou biaisés à l'encontre de certaines personnes ou de certains groupes de personnes si les systèmes d'IA n'ont pas été correctement entraînés (avec des données qui reproduisent des biais discriminatoires humains innés) ou s'ils ont été déployés dans un but différent de celui pour lequel ils ont été conçus. Lorsque l'utilisation du système concerne un domaine ou permet de prendre des décisions pouvant avoir un impact sur des personnes ou groupes de personnes, une vérification humaine systématique est de mise.

Transparence et explicabilité

- Une bonne compréhension du fonctionnement et des stades de développement du système d'IA est essentielle pour que l'entreprise l'intègre au mieux et anticipe les risques qui peuvent en découler.
- Par ailleurs, il est important de ne pas avoir recours aux systèmes d'IA dits « boîtes noires » (c'est-à-dire dont le fonctionnement est complètement opaque) afin que les utilisateurs puissent en cas de besoin (résultat erroné ou discriminant par exemple) comprendre ce qui a provoqué la mauvaise performance du système d'IA et ainsi y remédier.

Propriété intellectuelle

- Puisque les systèmes d'IA sont entraînés sur de larges jeux de données souvent issus de fouilles de données disponibles en ligne (« web scrapping »), il est important de s'assurer auprès du fournisseur du système ou modèle d'IA, ou du prestataire participant à la constitution des jeux de données, que l'opposition des auteurs ou détenteurs des droits de propriété intellectuelle sur ces données (s'ils l'ont exprimé) soient respectés (voir à cet égard les règles sur l'exception de fouille de données issue de la Directive UE 2019/790 ainsi que les exigences de transparence sur les sources de données imposées aux fournisseurs de modèles d'IA sous l'article 53.1 de l'*AI Act*, telles qu'elles seront précisées par les codes de pratique).
- Par ailleurs, l'utilisation des résultats doit faire l'objet d'une grande attention à cause (i) du risque de régurgitation des données d'entrée ou d'entraînement et (ii) parce qu'il n'existe pas encore à date de réponse juridique claire sur la propriété intellectuelle de résultats générés par une IA. L'utilisateur devra donc s'assurer que l'utilisation souhaitée des résultats est rendue possible par le fournisseur du système d'IA (notamment *via* les clauses du contrat qui les lie).

Au-delà des risques juridiques, la question de la frugalité de l'IA d'un point de vue environnemental doit être envisagée. En effet, l'entraînement des modèles d'IA génère une consommation significative d'énergie (électricité, eau, métaux rares, espaces artificialisés liés à la construction de centres de données, recyclage) suivant le nombre de paramètres du modèle, l'efficacité énergétique des centres de données et l'intensité carbone du réseau électrique. L'impact écologique de l'IA est au cœur des discussions, encourageant ainsi les organisations à évaluer leur propre impact environnemental, grâce à de nouvelles normes (par exemple, la norme AFNOR SPEC 2314 qui établit un référentiel général pour l'IA frugale et qui fournit une méthodologie d'évaluation environnementale des IA, ou encore une nouvelle norme de l'AFNOR, spécifique à l'impact environnemental des outils d'intelligence artificielle, qui devrait être publiée courant 2025 selon la presse spécialisée).

2.2. Comment réduire son exposition aux risques ?

L'appréhension des risques doit être faite **dans son ensemble** et non individuellement par risque car plusieurs risques peuvent être intimement liés entre eux. Par exemple, confidentialité, sécurité, protection des données ou encore, erreur et propriété intellectuelle. Il est recommandé que toute utilisation ou fourniture d'un outil d'IA fasse l'objet d'une évaluation des risques qui attribue **une notation par risque** mais également **un niveau de risque dans sa globalité**.

Il est important de noter que chaque risque doit être évalué en gardant en tête le **cas d'usage souhaité**. En effet, en matière d'IA, les risques doivent **s'apprécier** sous l'angle de la **finalité de l'IA** et non de la technologie sous-jacente (ce qui correspond d'ailleurs à l'approche adoptée par l'*AI Act*). Par exemple, pour un cas d'usage marketing, le risque de propriété intellectuelle paraît primordial alors que le risque d'erreur semble de moindre portée. À l'inverse, pour un cas d'usage financier, le risque d'erreur est de première importance.

Pour cet exercice, des outils comme des matrices de risques ou des outils de notation d'appel d'offres peuvent être utiles. Les personnes évaluant les risques devront nécessairement compléter l'exercice par l'identification des **mesures de remédiation** associées à ces risques. Si, à la suite de cet exercice d'évaluation des risques, il apparaissait que les mesures de remédiation existantes ne suffisent pas à diminuer le niveau de risque ou que, malgré leur implémentation, l'utilisation ou la fourniture d'un modèle ou système d'IA mettent à mal l'activité de l'organisme ou les droits et libertés des individus, il serait recommandé de renoncer au cas d'usage envisagé et de le réévaluer dans le futur à la lumière de nouvelles mesures.

Exemples de mesures de remédiation

3. Mettre en œuvre une gouvernance utile de l'IA

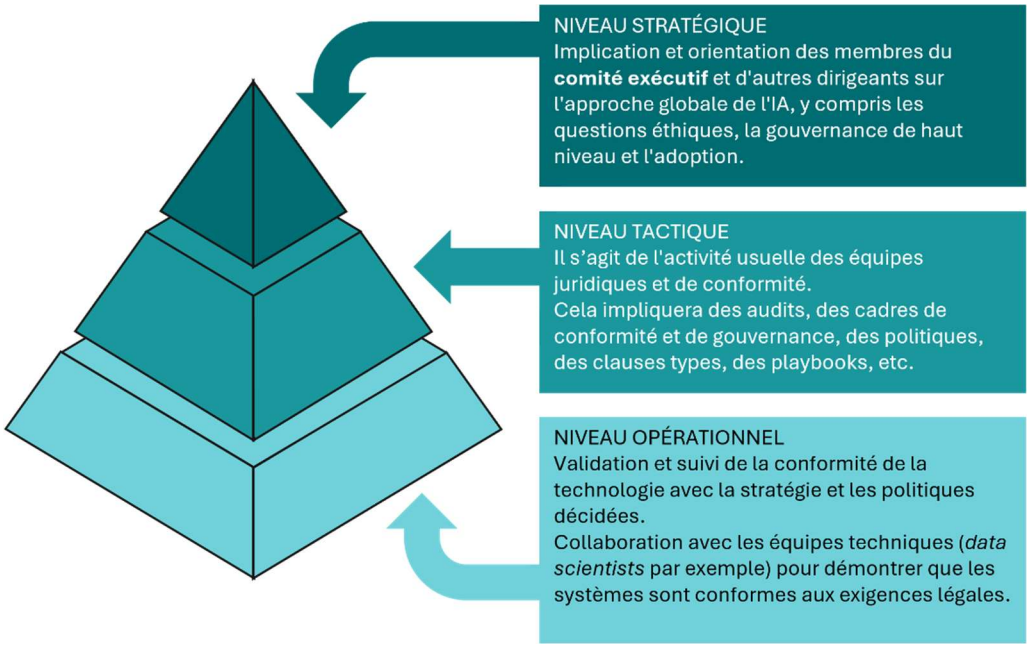
La gouvernance de l'IA devant être propre à chaque organisation, les prérequis et les outils nécessaires à sa mise en œuvre leur seront également spécifiques. Il existe cependant un certain nombre de recommandations et méthodologies couramment rencontrées au sein d'organisations ayant implémenté une gouvernance efficace qui peuvent s'appliquer à toutes.

3.1. Quels sont les prérequis ?

1- Définir une stratégie IA au sein de l'entreprise

Définir une stratégie au niveau managérial constitue un prérequis essentiel à l'établissement de la gouvernance de l'IA au sein de l'organisation. La première étape est constituée par la définition au niveau managérial du cadre général et des règles de déploiement de l'IA ainsi que de l'allocation des ressources financières et humaines nécessaires.

Cette stratégie exige d'être étayée par des principes fondamentaux couvrant des sujets tels que l'utilisation éthique, la confiance, la surveillance et le respect des normes juridiques. Appliquée de façon descendante elle pourra ensuite former et guider les décisions et la mise en œuvre de l'IA aux niveaux tactiques et opérationnels.



Pyramide de la gouvernance de l'IA

2- Disposer d'une bonne gouvernance de la donnée

La gouvernance de la donnée est un prérequis « critique » de la gouvernance de l'IA au sein d'une organisation pour les raisons suivantes :

- les systèmes d'IA dépendent fortement de la qualité et de l'intégrité des données et des informations qu'ils utilisent ;
- la gouvernance de la donnée contribue à garantir la conformité aux réglementations et aux normes éthiques ;
- une gouvernance de la donnée robuste aide à minimiser les risques opérationnels et sécuritaires.

3- Cartographier les SIA utilisés/développés par l'organisation

Pour maîtriser les risques liés à l'IA, il faut identifier les nombreux systèmes d'IA ainsi que les modèles d'IA utilisés de façon sous-jacente au sein de ces systèmes. Il est également nécessaire d'identifier les cas d'utilisation actuels et futurs de l'IA au sein de son organisation. Les définitions juridiques de l'IA ont tendance à être larges et à englober de nombreux systèmes existants. Tel que défini dans l'*AI Act* et précisé par les lignes directrices de la Commission européenne, certains systèmes complexes pourraient être qualifiés de « système d'IA ».

Une cartographie détaillée permet d'avoir une vue d'ensemble des différents systèmes d'IA et modèles d'IA utilisés dans l'organisation et ainsi d'identifier les actions prioritaires. Cet exercice de cartographie est aussi l'occasion d'interroger les équipes sur les cas d'usage d'IA afin d'identifier les IA à risque inacceptable, à risque élevé et à risque spécifique en matière de transparence ou encore les modèles à risque systémique potentiellement intégrés dans les systèmes développés ou utilisés.

Dans la plupart des organisations, les résultats des systèmes informatiques basés en dehors de l'UE finiront par être utilisés dans l'UE sous une forme ou une autre. Il peut s'agir d'une utilisation directe par

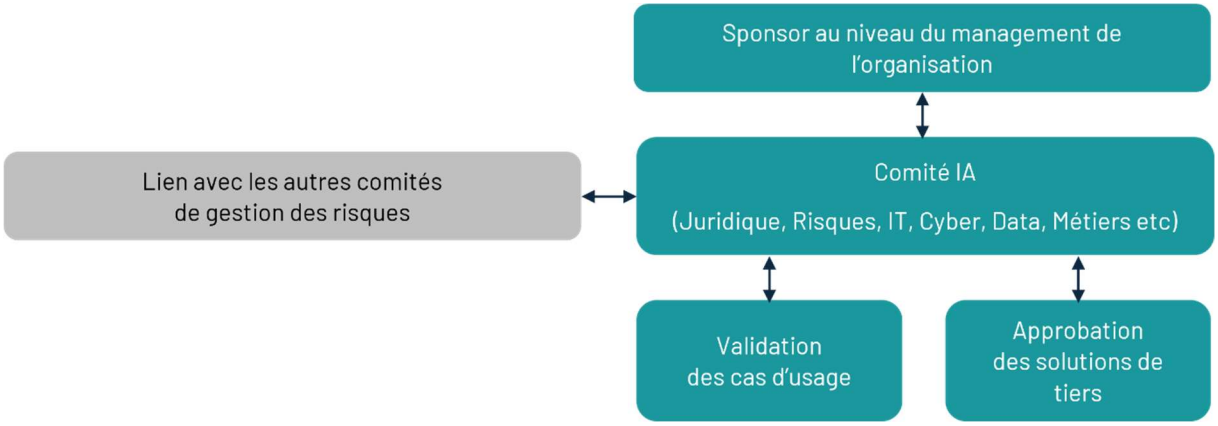
l'organisation, ou par ses clients, ses fournisseurs ou d'autres partenaires. Dans ce cas, ces systèmes situés en dehors de l'UE seront toujours couverts par la loi sur l'IA.

En ayant une compréhension complète des systèmes d'IA en place et de leurs modèles d'IA sous-jacents, l'organisation peut s'assurer que les pratiques de gouvernance sont alignées avec les objectifs stratégiques et les exigences réglementaires, évitant ainsi les écueils liés à une gestion fragmentée ou incohérente de l'IA.

4- Mettre en place une comitologie

L'étape suivante consiste à mettre en place les structures organisationnelles quotidiennes qui reprendront la stratégie IA de l'entreprise et la mettront en œuvre au niveau tactique. Pour la plupart des organisations, il existe déjà un ensemble de structures permettant de maîtriser les risques au niveau opérationnel ; il s'agit donc d'y intégrer la gouvernance de l'IA.

Idéalement, un nouveau comité de gouvernance de l'IA pourrait « s'approprier » la question des risques spécifiques liés à l'IA. Ce comité devrait comprendre des représentants des départements concernés (par exemple, juridique, données, conformité, cybersécurité, informatique, opérations) et rendre compte à un sponsor de haut niveau.



Comitologie de gouvernance de l'IA

5- Définir des procédures et règles internes

Le comité IA va être en charge de mettre en place les politiques, lignes directrices, procédures et autres règles internes spécifiques à l'IA en s'adossant sur des documents déjà existants (par exemple, charte informatique).

Attention à ne pas oublier les règles de droit du travail sur la consultation et/ou l'information des instances représentatives du personnel, le cas échéant.

3.2. Quels sont les outils de la gouvernance ?

Les outils de la gouvernance permettent de faciliter voire d'automatiser certaines tâches identifiées lors de la phase de détermination de la stratégie de la gouvernance.

La liste ci-dessous est donnée à titre d'exemple mais **les outils sont à adapter à chaque organisation**, en fonction de sa taille, de son activité, de son appétence aux risques, de la maturité des équipes et de la quantité des systèmes d'IA identifiés lors de la cartographie.

- Matrice de responsabilité (RACI) pour la définition des rôles et responsabilités en interne ;
- Rétroplanning de la mise en place des outils au vu du calendrier réglementaire d'entrée en application de l'*AI Act* ;
- Questionnaire de recensement et de qualification des outils d'IA à l'aune de l'*AI Act* ;
- Outils de consignation de la documentation technique des outils d'IA, des documents répondant aux exigences de transparence communiqués par les fournisseurs ;
- Outil d'évaluation de la maturité IA des prestataires ou de notation d'appel d'offres ;
- Outil d'évaluation des risques des cas d'usage et outils d'IA (voir chapitre sur le sujet) ;
- Modèles de clauses contractuelles afin d'encadrer les risques associés à l'IA ;
- Modèles de documentation technique pour les équipes opérationnelles et techniques si l'organisation développe des systèmes d'IA ;
- Supports de formation et sensibilisation sur la technologie et sur les risques afférents à l'IA ;
- Procédures opérationnelles standardisées (ou SOP).

3.3. Quelles sont les obligations légales de gouvernance de l'IA ?

L'approche par les risques de l'*AI Act* concernant les systèmes d'IA, oblige les entreprises à procéder à leur cartographie. Un tel exercice consiste à évaluer et surveiller les systèmes d'IA et les modèles d'IA sous-jacents en fonction de leur catégorie de risque.

Concernant les systèmes d'IA à risque élevé et les fournisseurs de modèles d'IA à usage général présentant des risques systémiques, l'*AI Act* introduit des exigences de gouvernance rigoureuses, déjà détaillées dans la partie 1 Obligation de ce guide, dans les fiches 1 à 5 de la « Cartographie des obligations applicables aux organisations selon l'*AI Act* » et listées ci-dessous :

Pour le fournisseur d'IA à risque élevé :

- ➔ **Système de gestion de la qualité**, notamment *via* les techniques, procédures et actions à implémenter tout au long du cycle de vie de l'IA ;
- ➔ **Système de gestion des risques** ;
- ➔ **Garantie de conservation de la documentation** (documentation technique, système de gestion de la qualité, déclaration UE de conformité, etc.) ;
- ➔ **Gouvernance de la donnée** afin de s'assurer de la qualité des données d'entraînement ;
- ➔ **Système de surveillance après commercialisation** du système d'IA.

Pour le déployeur d'IA à risque élevé :

- **Système de gestion de la qualité**, notamment *via* les techniques, procédures et actions à implémenter tout au long du cycle de vie de l'IA ;
- **Système de gestion des risques** ;
- **Garantie de conservation de la documentation** (documentation technique, système de gestion de la qualité, déclaration UE de conformité, etc.) ;
- **Procédures de vérification humaine.**

Pour le fournisseur de modèles d'IA à usage général présentant des risques systémiques :

- **Méthodologie d'évaluation des modèles,** en vue d'identifier et d'atténuer les risques systémiques *via* l'utilisation de protocoles et outils standardisés ;
- **Gestion et déclaration des incidents graves** au Bureau de l'IA et aux autorités nationales compétentes.

Par ailleurs, il convient de noter que l'*AI Act* comporte également des dispositions concernant les IA qui ne sont pas à risque élevé. En effet, l'article 95 prévoit que les fournisseurs de tels systèmes doivent être encouragés à établir des **codes de conduite** accompagnés de mécanismes de gouvernance afin de favoriser l'application de tout ou partie des obligations applicables aux systèmes à risque élevé en fonction du cas d'usage en question. Ces codes de conduites pourraient concerner par exemple l'éthique, l'environnement, la maîtrise de l'IA (Article 4 de l'*AI Act*) ou encore la conception inclusive et diversifiée (en termes de variété des équipes de développement et la promotion de la participation des parties prenantes à ce processus de conception inclusive des systèmes).

4. Anticiper la gouvernance institutionnelle

4.1. La gouvernance européenne

L'*AI Act* institue une gouvernance multi-niveau constituée :

- des **autorités nationales** (une autorité notifiante et une autorité de surveillance du marché au moins) pour s'assurer de la mise en œuvre de l'*AI Act* au niveau des États membres, qui pourront coopérer *via* le **Comité IA**,
- le **Bureau de l'IA** pour le développement des capacités de l'Union dans le domaine de l'IA,
- la **Commission européenne**, assistée du **Comité IA**, pour la coordination et la cohérence de l'application dans l'ensemble de l'Union,
- des **groupes d'experts** pour apporter une expertise scientifique et technique. Les attributions de ces institutions et la répartition de leurs champs de compétence sont détaillées dans le livret « Points clés de l'*AI Act* – Introduction » de ce guide.

La gouvernance articulée entre les différentes institutions suit une approche résolument axée sur la sécurité des produits, comme le rappelle le Bureau de l'IA. Il est probable qu'elle sera d'une grande complexité avec une approche très différente de celle du RGPD.

4.2. La gouvernance française

Les autorités nationales de régulation devront relever plusieurs défis dans la mise en œuvre de l'*AI Act*, en particulier face à des organisations soumises à des textes réglementaires multiples et relevant de plusieurs autorités compétentes.

Il avait été initialement envisagé que la CNIL soit l'autorité compétente en matière d'IA en France.

Aujourd'hui s'esquissent les grandes lignes d'une répartition des compétences en matière de régulation de l'intelligence artificielle en France. **Cependant, à la date de la publication de la première édition de ce guide, rien n'est encore officiellement acté.**

La presse juridique spécialisée évoque cependant un tandem stratégique : la DGCCRF serait responsable de la coordination opérationnelle entre les autorités sectorielles, tandis que la DGE assurerait un rôle stratégique en représentant la position coordonnée des autorités françaises auprès des instances européennes. La DGE est également pressentie pour assurer le lien avec le Comité de l'IA comme autorité de liaison unique.

La CNIL obtiendrait un large périmètre couvrant la biométrie, la notation sociale et le contrôle aux frontières. L'Arcom partagerait des compétences sur les interfaces trompeuses et les hypertrucages (*deep fake*). Les rôles de l'ANSSI et du PEReN seraient encore en discussion, notamment pour les infrastructures critiques et les organismes de conformité.

À date, il est important de noter qu'aucun financement supplémentaire n'est prévu dans le budget 2025 pour ces nouvelles responsabilités.

La répartition finale des compétences reste à définir pour certains secteurs comme l'éducation et les infrastructures critiques. Le budget 2026 sera un moment clé pour ajuster les moyens nécessaires.

4.3. La gouvernance internationale

Bien que l'*AI Act* soit un cadre de régulation européen, les autorités de régulation sont encouragées à collaborer avec des régulateurs d'autres régions pour gérer les **risques transfrontaliers** et harmoniser les **standards internationaux** dans la gouvernance de l'IA.

La gouvernance de l'IA est particulièrement pertinente pour les **entreprises multinationales** qui ont à composer avec un environnement législatif international en constante évolution. Celles-ci peuvent envisager différentes approches dont les deux suivantes données à titre d'exemple :

APPROCHE BASÉE SUR LES RISQUES	**Considérer l'*AI Act* comme le texte le plus contraignant** et estimer que la conformité à l'*AI Act* permettra de couvrir les impératifs imposés par d'autres pays. Cela s'explique par la volonté de l'*AI Act* de devenir un standard international de régulation comme a pu l'être le RGPD. ⊕ **Avantage :** Gain de temps et de ressources ⊖ **Inconvénient :** Risque de non-conformité sur les activités non européennes notamment en Chine ou aux États Unis
APPROCHE BASÉE SUR DES GRANDS PRINCIPES	La plupart des textes s'articulent autour de **grands principes de l'IA Responsable publiés par l'OCDE**. Il est donc possible de créer un programme de gouvernance sur cette base avec des contraintes spécifiques pour certains pays en fonction du déploiement des systèmes d'IA. ⊕ **Avantage :** Approche adaptée aux entreprises n'ayant pas leur centre d'activité dans l'UE ⊖ **Inconvénient :** Coûteux

La **normalisation (ISO/NIST)** joue un rôle clé pour faciliter l'application pratique du texte, en offrant des cadres techniques clairs et en simplifiant les démarches de conformité pour les entreprises. L'*AI Act* inclut à cet égard des dispositions intéressantes concernant la normalisation et la certification pour soutenir l'évaluation de conformité des systèmes d'IA, en particulier ceux à risque élevé. Par exemple, en application de l'Article 40 de l'*AI Act*, les systèmes et modèles d'IA conformes aux normes harmonisées sont présumés être conformes aux exigences correspondantes du règlement sur les IA à risque élevé, simplifiant ainsi la démonstration de conformité pour les fournisseurs. L'*AI Act* comprend également des dispositions pour encourager la participation des PME au processus de normalisation et instaure un mécanisme de notification s'il est constaté que des normes sont inadéquates.

5. Conclusion

La mise en place d'une gouvernance spécifique est indispensable pour aider les entreprises et les administrations publiques à comprendre et appliquer l'*AI Act*. Cette gouvernance, loin de se limiter à répondre aux obligations légales, permet également d'anticiper et de maîtriser d'autres risques comme ceux liés à la cybersécurité, la confidentialité ou la propriété intellectuelle. En définissant un cadre clair, partagé et adapté à chaque organisation, la gouvernance facilite l'adoption responsable de l'IA et favorise l'innovation.

Remerciements

Le Cigref et Numeum souhaitent remercier chaleureusement les pilotes du groupe de travail « Mise en oeuvre de l'*AI Act* » : côté Cigref, **Lionel Chaine**, DSI de BPI France et **Jean-Claude Laroche**, Directeur de Mission auprès de la Présidence du COE France d'EDF, et côté Numeum, **Katya Lainé**, CEO de TALKR.ai et **Thibault de Tersant**, *Senior executive Vice President* de Dassault Système.

Nous remercions également les différents participants, membres de nos deux associations, qui ont contribué à l'élaboration des livrets de ce guide.

Nous avons eu le plaisir d'être accompagnés tout au long de notre démarche par l'expertise de quatre grands cabinets d'avocats : August Debouzy, DLA Piper, Racine et Bird & Bird. Nous remercions plus particulièrement **Mahasti Razavi**, managing partner chez August Debouzy, **Anne-Sophie Lampe**, IT/IP Partner chez Bird & Bird, **Jeanne Dauzier** Partner et **Maria Aouad**, avocate chez DLA Piper, **Charles Bouffier**, avocat associé et **Naomi Meynle-Hamza**, juriste doctorante, chez Racine.

Rédaction :
Marine de Sury, Directrice de mission, Cigref
Anissa Kemiche, Déléguée aux affaires européennes, Numeum

Relecture : Chantal de Bardies, Directrice de la qualité des contenus, Cigref

Direction artistique et graphisme : Émilie Grange, Chargée de communication, Cigref

Cigref
RÉUSSIR
LE NUMÉRIQUE

numeum
Engager
le numérique