Droit, éthique et responsabilité

TL;DR

- **Le droit conditionne le projet dès le départ :** pas après. RGPD, AI Act, responsabilité managériale - ces cadres définissent ce qui est légal, ce qui est risqué, et qui paie quand ça déraille.
- **Il existe des usages IA interdits en Europe :** et des catégories de données à statut spécial. Avant tout projet - vérifier le niveau de risque AI Act et le droit légal d'utilisation des données.
- **Le manager qui signe est responsable :** pas le fournisseur du modèle. La responsabilité ne se délègue pas à l'algorithme. Leur responsabilité est, pour la plupart des cas, rejetée.

1) Le cadre global - ce qui s'impose à tous

Le RGPD appliqué aux projets IA - 3 questions fondamentales

Tout projet IA impliquant des données personnelles engage le RGPD. Pas le RGPD en général - le RGPD sur le cas d'usage précis que vous déployez.

Question	Ce qu'elle signifie concrètement
Pourquoi ces données ?	La finalité doit être déclarée, précise et respectée. Entraîner un modèle RH à prédire les démissions - le consentement initial couvre-t-il cet usage ?
Est-ce qu'on en prend trop ?	Le principe de minimisation impose de n'utiliser que ce qui est strictement nécessaire. Toute donnée superflue est une exposition juridique.
Jusqu'à quand ?	La durée de conservation - un modèle entraîné sur des données personnelles ne les conserve pas indéfiniment. Un calendrier de suppression s'impose.

> Principe clé : le consentement doit couvrir l'usage précis. Utiliser des données clients collectées pour la facturation pour entraîner un modèle de recommandation constitue un détournement de finalité. C'est illégal.

L'AI Act - la classification des risques

Le règlement européen sur l'IA (en vigueur depuis août 2024) classe tous les systèmes d'IA en quatre niveaux de risque. La classification détermine les obligations applicables. Connaître le niveau de son projet avant de le lancer est une responsabilité managériale non négociable.

Niveau	Usages et obligations
Interdit	Notation sociale généralisée, manipulation cognitive subliminale, reconnaissance biométrique en temps réel dans l'espace public. Ces usages sont illégaux sur le territoire européen.
Haut risque	RH et recrutement, crédit et scoring, santé, éducation, justice, infrastructure critique. Obligations : audit de conformité, documentation technique, supervision humaine obligatoire, inscription au registre européen.
Risque limité	Chatbots, deepfakes, systèmes de recommandation. Obligation de transparence - informer l'utilisateur qu'il interagit avec une IA.
Risque minimal	Filtres spam, recommandations basiques, jeux vidéo. Aucune obligation spécifique.

> Les secteurs dans lesquels vous allez travailler - RH, finance, santé, éducation - sont exactement les secteurs à haut risque sous l'AI Act. Avant tout déploiement dans ces domaines : vérifier les obligations qui s'appliquent.

Les données sensibles - catégories particulières

Certaines catégories de données bénéficient d'un régime de protection renforcé sous le RGPD. Les utiliser dans un projet IA sans précautions spécifiques expose l'organisation à des sanctions sévères.

Catégorie	Exemples d'exposition dans un projet IA
Données de santé	Modèle prédictif sur des dossiers patients, analyse de prescriptions, détection de pathologies.
Données biométriques	Reconnaissance faciale, analyse vocale, empreintes utilisées pour l'authentification.
Origine ethnique	Modèle RH entraîné sur des données historiques reproduisant des discriminations.
Opinions politiques	Analyse de contenu pour profilage ou ciblage publicitaire.

> **Chiffres clés**
>
> - **Sanctions RGPD :** jusqu'à 4% du chiffre d'affaires mondial annuel ou 20 M€, selon le montant le plus élevé.
>   **Sanctions IA Act :** jusqu'à 35 M€ ou 7 % du chiffre d'affaires mondial annuel, selon le montant le plus élevé
> - **Cloud Act (2018) :** des données hébergées chez AWS, Azure ou Google Cloud peuvent être requises par le gouvernement américain même si les serveurs sont en Europe. Ce n'est pas qu'un sujet politique - c'est une responsabilité juridique.

2) Le cadre corporate - ce que les organisations font concrètement

Le DPO - Délégué à la Protection des Données

Rôle obligatoire pour toute organisation traitant des données personnelles à grande échelle. Le DPO est le garant de la conformité RGPD en interne et l'interlocuteur officiel de la CNIL.

Règle opérationnelle : tout projet IA impliquant des données personnelles doit être soumis au DPO avant lancement. L'ignorer n'est pas une option - c'est une faute managériale qui peut engager la responsabilité personnelle du décideur.

Toutes les organisations ne disposent pas nécessairement d'un DPO. Certains secteurs en imposent un. Le DPO ne traite pas nécessairement les sujets d'IA, une personne tierce peut en être nommée responsable.

La charte IA interne

Premier outil managérial concret issu du cadre légal. La charte IA définit les règles d'usage de l'IA au sein de l'organisation.

Question	Ce que la charte y répond
Quoi ?	Cas d'usage autorisés et cas d'usage interdits dans l'organisation.
Qui ?	Qui peut déployer un outil IA, qui valide, qui supervise.
Comment ?	Règles de gestion des données, supervision humaine, traçabilité.
Avec quelles conséquences ?	Sanctions internes en cas de non-respect.

La charte IA n'a aucune valeur juridique en elle-même. Elle sert à titre d'une nécessité de formalisation des usages / formation. La charte IA peut-etre rattachée au règlement intérieur de l'entreprise et devenir dans ce cas là elle devient plus engageante en matière de responsabilité.

Les 3 acteurs responsables - qui paie quand ça déraille

La responsabilité dans un déploiement IA est partagée entre trois acteurs distincts. Comprendre cette chaîne est indispensable avant de signer quoi que ce soit.

01 Le fournisseur du modèle

Responsable de la conformité du modèle de base, de la documentation technique et des certifications. OpenAI, Anthropic, Mistral - chacun a ses obligations réglementaires.

02 L'organisation qui déploie

Responsable de l'usage qu'elle fait du modèle, des données qu'elle y injecte, des décisions qu'elle laisse le modèle prendre ou influencer.

03 Le manager qui signe

Responsabilité managériale et potentiellement juridique si le projet cause un préjudice. Le modèle ne signe pas. Vous, oui.

> Question clé : à quel seuil garde-t-on un humain dans la boucle ? Pour les systèmes à haut risque sous l'AI Act, c'est une obligation légale. Pour tous les autres, c'est une nécessité managériale.

Les cadres réglementaires sectoriels

Au-delà du RGPD et de l'AI Act, deux secteurs ont des obligations supplémentaires directement pertinentes.

Secteur	Cadre et obligations spécifiques
Santé - HDS	Certification obligatoire en France pour tout projet IA traitant des données de santé à caractère personnel. Un projet IA sur des données patients sans hébergeur certifié HDS est illégal.
Finance - DORA	Digital Operational Resilience Act. En application depuis janvier 2025. Impose aux banques, assurances et sociétés d'investissement des exigences de résilience numérique et d'audit des prestataires IA.

3) Le cadre individuel - les 3 questions du manager

Les 3 questions à poser avant tout projet IA

Quel que soit l'outil, le prestataire ou le budget - posez ces trois questions avant de lancer n'importe quel projet IA impliquant des données.

01 Mes données sont-elles personnelles ou sensibles ?

Et ai-je le droit légal de les utiliser pour ce cas d'usage précis - pas pour d'autres usages, celui-ci. Si la réponse n'est pas clairement oui, le projet n'est pas prêt.

02 Mon projet est-il classé haut risque sous l'AI Act ?

Si oui : audit de conformité, documentation technique, supervision humaine obligatoire. Ces obligations s'appliquent avant le déploiement.

03 Si le modèle se trompe - qui est responsable ?

Nommer explicitement la personne responsable dans l'organisation avant de lancer. Pas après un incident. Avant. C'est une décision managériale, pas technique.

Le droit à l'explication et la transparence algorithmique

Toute personne impactée par une décision automatisée a le droit de savoir pourquoi. Cette obligation s'applique à toute décision IA qui concerne directement une personne - recrutement, crédit, accès à un service.

Pour les chatbots et systèmes génératifs : obligation d'informer l'utilisateur qu'il interagit avec une IA. Le silence constitue une violation réglementaire.

Propriété intellectuelle et IA - le sujet qui vous concerne maintenant

Quand vous utilisez ChatGPT pour rédiger un mémoire, une thèse, un rapport de stage - qui est l'auteur du contenu produit ? Le droit d'auteur sur les créations générées par IA est une question non encore tranchée définitivement. En France, la protection par le droit d'auteur requiert une création originale issue d'un effort humain.

Ce que ça change pour vous concrètement : l'usage d'un modèle génératif dans un travail académique engage votre responsabilité sur l'exactitude, l'originalité et la conformité aux règles de votre établissement - pas celle du modèle.

À retenir

- Ces trois questions sont votre bouclier. Les poser avant de signer, avant de déployer, avant de valider - c'est le minimum de toute décision managériale responsable.
- Le droit ne disparaît pas parce qu'on ne le connaît pas. L'ignorance n'est pas une défense recevable devant la CNIL ou un tribunal.

4) La grille Valeur × Risque × Dépendance enrichie

Depuis la séance 1, vous utilisez cette grille pour analyser tout projet IA. En Séance 4, la dimension Risque s'enrichit d'une nouvelle dimension : une couche juridique concrète.

Dimension	Ce qu'elle révèle après S4
Valeur	Ces gains tiennent-ils si on intègre les coûts de conformité, les obligations d'audit et les risques de sanctions ? La valeur attendue doit être recalculée net des contraintes juridiques.
Risque	Le risque n'est plus seulement technique. Il est juridique - RGPD, AI Act - et personnel. Le manager qui signe est potentiellement responsable civilement et pénalement.
Dépendance	Héberger chez un opérateur américain crée une dépendance juridique au Cloud Act. Choisir un hébergeur non certifié HDS pour des données de santé est une infraction. La dépendance a une dimension légale.

> Un projet qui optimise la Valeur sans analyser le Risque juridique et la Dépendance légale n'est pas un projet complet. Toujours les trois - simultanément.