L'AI Act

DÉCODÉ PAR L'INTELLIGENCE HUMAINE

Découvrez une réflexion portée par Cédric AUTRET consultant chez Softeam

SOFTEAM
UNE FILIALE DE DOCAPOSTE

PRÉFACE

Un livre blanc fait par l'IA sur l'IA ? Ça aurait été possible … mais ça n'aurait pas été parfait (hallucinations, biais dans l'entrainement du modèle etc.). Ici, nous vous proposons une synthèse fiable de la réglementation telle qu'elle apparait à un humain incluant les citations du texte pour vérification. Néanmoins, avant d'entamer notre plongée dans ce nouveau chapitre de la réglementation européenne, il est pour nous important de noter certains aspects qui me paraissent essentiels.

Tout d'abord, cette norme est très technique, elle approche l'IA par ses risques, cadrant ce qui doit, peut ou ne peut pas être fait mais elle oblitère l'aspect sociétal de l'implémentation des systèmes d'IA : tant que le système entre dans le cadre, est bien documenté et contrôlé rien ne vous empêche de supprimer des milliers d'emplois que ce soit par des licenciements secs, par le fait de ne plus embaucher des juniors ou des personnels moins qualifiés.
Ensuite, l'obligation de transparence imposée sur les modèles d'IA à usage général, pourrait impliquer, s'il était appliqué stricto sensu, de ne plus pouvoir utiliser un certain nombre de modèles. En effet, l'exposition des sources pourrait impliquer des poursuites judiciaires pour les sociétés en question du fait de leurs pratiques de « web crawling » massifs et de l'utilisations d'œuvres sous copyright pour l'entrainement des modèles. Nous vous invitons à suivre les affaires qui, selon les pays et les instances judiciaires vont donner des résultats différents avant qu'une jurisprudence claire n'émerge. En Europe, pour l'instant, les tribunaux semblent se baser sur l'exception pour « fouille de textes et de données » définie dans l'article 4 de la directive 2019/790.

Un autre point qui nous semble intéressant de mentionner est le calendrier. Autant avoir une date d'application rapide pour les interdictions nous semble pertinent (bien que cela pose la question de l'autorité compétente pour faire appliquer la réglementation), autant le fait d'avoir délégué aux États membres le fait de mettre en place un certain nombre d'éléments (régulateurs, bacs à sable etc.) pour le 2 août 2026 nous semble ambitieux.
À noter également que les codes de bonnes pratiques qui étaient censés être publiés pour le 2 mai 2025 l'ont été pour partie le 10 juillet 2025 (ce qui laisse une large marge de 23 jours aux acteurs avant la première vague liée aux GPAI entrant en vigueur le 2 août 2025) et les actes d'exécution de la commission concernant les bacs à sable réglementaires n'ont pas été publiés non plus (à la date du 23 juillet 2025).

Nous vous invitons désormais à découvrir la réglementation et à comprendre les enjeux autour de cette dernière au travers de notre livre blanc.

SOFTEAM
UNE FILIALE DE DOCAPOSTE

TABLE DES MATIÈRES

INTRODUCTION

L'intelligence artificielle (IA) est au cœur des grandes transformations technologiques, économiques et sociales de notre époque. Ses applications révolutionnent des domaines extrêmement variés allant de la santé à l'énergie en passant par les transports, ou encore l'éducation. Toutefois, ces avancées s'accompagnent de défis majeurs : comment garantir une IA qui respecte les droits fondamentaux ? Comment favoriser l'innovation tout en limitant les risques d'abus et de discrimination ?

Face à ces enjeux, l'Union européenne a adopté le **Règlement AI Act (UE 2024/1689)**, une législation visant à encadrer le développement, la mise sur le marché et l'utilisation des systèmes d'IA.

Ce livre blanc propose une analyse approfondie des principales dispositions de l'AI Act. Il explore d'une part les obligations des acteurs du secteur, mais aussi les opportunités que peut offrir cette réglementation pour les entreprises innovantes. Que vous exerciez des responsabilités opérationnelles en entreprise, ou que vous soyez simplement curieux de l'impact potentiel de cette norme et de l'IA de manière plus générale sur notre société, ce document vous fournira des clés pour comprendre, anticiper et saisir les opportunités liées à cette réglementation.

> **Plongez dans ce voyage au cœur de l'IA et découvrez comment l' AI Act façonne l'avenir d'une technologie qui transforme notre quotidien.**

Présentation du Règlement AI Act

Chapitre 1

SOFTEAM
UNE FILIALE DE DOCAPOSTE

1.1. Nature et champ d'application de l'AI Act

Le Règlement (UE) 2024/1689, plus connu sous le nom d'**AI Act**, est une réglementation européenne visant à établir des règles harmonisées pour le développement, la mise sur le marché et l'utilisation des systèmes d'intelligence artificielle dans l'Union européenne. Contrairement à une directive, qui nécessite une transposition dans les législations nationales, ce règlement est directement applicable dans tous les États membres, garantissant une uniformité juridique.

Le champ d'application est large et couvre :

- **Les systèmes d'IA développés ou déployés dans l'Union européenne**, indépendamment du lieu de développement. [i]
- **Les systèmes d'IA utilisés en dehors de l'UE**, si leurs sorties affectent des citoyens ou entreprises européennes. [ii]
- Les acteurs de la chaîne de valeur : **fournisseurs, déployeurs, importateurs et distributeurs** [iii] .

Les PME et les jeunes pousses sont particulièrement prises en compte, avec des dispositifs spécifiques pour réduire les charges administratives et les coûts liés à la mise en conformité. [iv]

Le règlement s'applique à la majorité des secteurs d'activité, notamment ceux touchant à la santé publique, la sécurité et la gestion des infrastructures critiques. Toutefois, les systèmes d'IA exclusivement utilisés à des fins de défense, de sécurité nationale ou de recherche scientifique sont exclus du champ d'application. [v]

Les systèmes d'IA à haut risque, tels que ceux utilisés dans des secteurs sensibles, sont spécifiquement visés par des exigences strictes pour protéger les droits fondamentaux des citoyens. [vi]

1.2. Objectifs du règlement

L'**AI Act** poursuit plusieurs objectifs clés :

- **Créer un environnement de confiance** : instaurer des règles claires pour protéger les droits fondamentaux des citoyens, y compris la vie privée, l'égalité et la non-discrimination. [vii]
- **Favoriser l'innovation** : éviter des contraintes excessives, notamment pour les petites et moyennes entreprises (PME) et les jeunes pousses (start-ups). [iv]
- **Prévenir la fragmentation** : harmoniser les législations pour garantir un marché unique fluide pour les technologies basées sur l'IA. [viii]
- **Positionner l'Europe en leader mondial** : développer une IA éthique et fiable comme modèle pour d'autres régions. [ix]

1.3. Définition des systèmes d'IA

Le règlement définit l'IA comme une famille de technologies capables d'effectuer des inférences[1], de fournir des prédictions ou des décisions, et de fonctionner avec différents niveaux d'autonomie. Ces systèmes incluent [x] :

- **L'apprentissage automatique** (exemple : réseaux neuronaux, apprentissage supervisé/non supervisé).
- **Des systèmes fondés sur des logiques ou bases de connaissances permettant l'inférence,**
- **D'autres approches statistiques ou symboliques qui remplissent ces critères.**

[1] *En intelligence artificielle (IA), une inférence correspond au processus par lequel un système d'IA utilise des données disponibles pour produire un résultat, une décision ou une prédiction. C'est un peu comme si l'IA « déduisait » quelque chose à partir de ce qu'elle a appris ou observé.*

1.4. Les catégories d'IA couvertes

Le règlement établit une classification des systèmes d'IA en fonction de leur niveau de risque. Cette approche permet de concentrer les exigences réglementaires sur les cas où les impacts sont les plus significatifs.

- **IA à risque minimal** : ces systèmes (e.g., jeux vidéo, filtres de messagerie) ne font pas l'objet d'exigences spécifiques, sauf des règles générales de transparence (ex. : informer les utilisateurs qu'ils interagissent avec une IA).
- **IA à risque limité**[xi] : ces systèmes doivent respecter des obligations de transparence. Par exemple :
  - Les systèmes générant du contenu (e.g., deepfakes) doivent être clairement identifiés comme produits par une IA.
  - Les chatbots doivent informer qu'ils ne sont pas des humains.
- **IA à haut risque**[xii] : ces systèmes peuvent avoir des impacts importants sur les droits fondamentaux ou la sécurité. Ils incluent :
  - Les systèmes utilisés dans les infrastructures critiques (e.g., transport, énergie). [xiii]
  - Les applications médicales (diagnostics, dispositifs). [xiv]
  - Les systèmes influençant l'accès à l'éducation ou à l'emploi (e.g., tri de candidatures) ainsi que ceux lié à la migration et aux contrôles aux frontières. [xv]
  - Les outils de gestion des ressources humaines. Ces IA sont soumises à des exigences strictes (documentation technique, audit, surveillance continue). [xvi]
  - Les systèmes utilisés à des fins répressives (évaluation de preuves, polygraphes ...). [xvii]
- **IA interdite** : certaines pratiques sont jugées inacceptables, notamment :
  - Les systèmes exploitant des vulnérabilités psychologiques (manipulation). [xviii]
  - La surveillance biométrique à distance en temps réel dans des espaces publics (sauf exceptions très limitées).[xix]
  - Les systèmes de notation sociale des individus par des entités publiques ou privées. [xx]

1.5. Les obligations des acteurs

Chaque acteur de la chaîne de valeur doit remplir des responsabilités spécifiques :

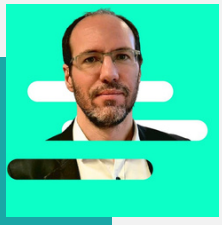
- **Fournisseurs :**
  - Réaliser des évaluations de conformité avant la mise sur le marché.[xxi]
  - Assurer la transparence et la traçabilité des systèmes.[xxii]
  - Mettre en place des mesures correctives si des risques émergent.[xxiii]
- **Déployeurs :**
  - Garantir une utilisation conforme aux instructions fournies par le fabricant.[xxiv]
  - Former leurs personnels.[xxv]
  - Faire une analyse d'impact sur les droits fondamentaux dans certains cas.[xxvi]
- **Distributeurs et importateurs :**
  - Vérifier que les systèmes d'IA respectent les exigences légales avant leur distribution.[xxvii]

1.6. Exclusions et limites

L' **AI Act** exclut de son champ d'application les systèmes développés pour [v] :

- **Les fins militaires ou de défense nationale.**
- **La recherche scientifique** avant leur mise sur le marché ou en service

Cependant, dès qu'un système est commercialisé ou utilisé pour des applications civiles, il devient soumis à la réglementation, même s'il a été initialement conçu pour des usages exclus.[xxviii]



Le regard de Cédric

Comme vous pouvez le constater, la norme est très large et, sauf cas particulier, si vous intégrez l'IA au sein de votre société, il y a de fortes chances que vous soyez concerné par ses implications. Ne tardez pas à demander à vos experts d'effectuer un diagnostic (analyse de conformité, d'impact) afin de ne pas vous retrouver à devoir engager des actions de remédiation. Vous pouvez également vous faire accompagner afin d'analyser votre situation et les actions qui peuvent en découler (typiquement la mise en place d'un modèle de gouvernance adaptée aux nouvelles contraintes)

Approche fondée sur les risques

Chapitre 2

SOFTEAM
UNE FILIALE DE DOCAPOSTE

L'un des principes fondamentaux de l'**AI Act** est son approche **fondée sur les risques**. Ce cadre garantit que les obligations réglementaires soient proportionnées au niveau de risque associé aux différents systèmes d'intelligence artificielle (IA). Cette stratégie permet d'encourager l'innovation tout en protégeant les citoyens contre des usages potentiellement nuisibles ou contraires aux droits fondamentaux.

2.1. Principe d'une approche fondée sur les risques

L'IA n'a pas les mêmes impacts dans toutes ses applications. Un système utilisé pour recommander des séries télévisées n'a pas les mêmes implications qu'un algorithme de diagnostic médical ou un outil de surveillance biométrique. En conséquence, le règlement classifie les systèmes d'IA selon leur potentiel de risque et applique des exigences croissantes en fonction de cette évaluation.

Définition des risques : les risques liés à l'IA sont définis comme la probabilité qu'un système cause des préjudices matériels (dommages physiques ou économiques) ou immatériels (discrimination, atteinte à la vie privée, manipulation psychologique). Les risques sont évalués en tenant compte :

- **De l'objectif du système.**
- **Du contexte d'utilisation.**
- **De la vulnérabilité des personnes concernées (enfants, personnes âgées, groupes marginalisés).**

2.2. Les quatre niveaux de risque

Le règlement identifie quatre catégories principales de risques associés aux systèmes d'IA, avec des obligations spécifiques pour chaque catégorie.

2.2.1. Systèmes à risque minimal

Ces systèmes présentent des impacts négligeables ou inexistants sur les droits fondamentaux ou la sécurité. Exemples :

- Jeux vidéo intégrant de l'IA.
- Outils d'optimisation de performance (e.g., recommandations pour organiser un emploi du temps).

Réglementation applicable : aucune exigence spécifique n'est imposée, mais les systèmes doivent respecter les principes généraux d'utilisation loyale et de transparence. Les développeurs sont encouragés à suivre des bonnes pratiques, mais sans obligation légale.

2.2.2. Systèmes à risque limité

Ces systèmes peuvent influencer l'expérience utilisateur ou induire des comportements, mais leurs impacts restent limités.

Exemples :

- Chatbots informatifs.
- Outils générant du contenu visuel ou audio manipulé, comme les deepfakes à usage ludique.

Exigences spécifiques [xxix]:

- **Transparence** : les utilisateurs doivent être informés qu'ils interagissent avec un système d'IA. Par exemple, un chatbot doit indiquer qu'il n'est pas humain.
- **Signalement de contenu généré** : tout contenu manipulé, comme un deepfake, doit porter une mention explicite indiquant son origine.

Ces obligations visent à garantir que les utilisateurs ne soient pas trompés par les capacités ou les intentions des systèmes.

2.2.3. Systèmes à haut risque

Les systèmes à haut risque sont ceux qui peuvent affecter significativement les droits fondamentaux ou la sécurité des personnes. Cette catégorie est au cœur du règlement, avec des exigences détaillées.

Exemples :

- Outils d'évaluation des candidatures pour l'embauche.
- Algorithmes de diagnostic médical.
- Systèmes influençant l'accès aux services publics (logement, éducation, crédit), les votes /les processus démocratiques, l'administration de la justice
- Système de gestion de l'asile et des frontières

Exigences réglementaires :

- **Documentation technique** [xxx] :
  - Fournir une description complète des objectifs, des données utilisées et des méthodologies employées.
  - Mettre en place des mécanismes pour garantir la traçabilité des décisions.
- **Gestion des risques** [xxxi] :
  - Identifier les risques potentiels avant la mise sur le marché.
  - Mettre en place des mesures pour les minimiser.
- **Surveillance continue** [xxxii] :
  - Assurer un suivi des performances du système via une journalisation.
  - Réévaluer régulièrement les risques.
- **Enregistrement dans une base de données de l'UE** [xxxiii] :
  - o Tous les systèmes à haut risque doivent être enregistrés pour permettre une transparence vis-à-vis des utilisateurs et des autorités.

2.2.4. Systèmes interdits

Certaines pratiques sont considérées comme inacceptables et sont explicitement interdites par le règlement en raison de leur incompatibilité avec les valeurs fondamentales de l'Union européenne.

Pratiques interdites :

- **Manipulation cognitive** [xxxiv] :
  - Exploiter des vulnérabilités psychologiques, comme l'utilisation de stimuli subliminaux ou de technologies qui influencent les décisions sans consentement conscient.
    Exemple : une interface cerveau-machine qui manipulerait les utilisateurs à leur insu.
- **Notation sociale** [xxxv] :
  - Toute classification des citoyens basée sur leur comportement ou caractéristiques personnelles, en vue d'en tirer des conséquences discriminatoires (comme restreindre l'accès à des services).
- **Surveillance biométrique abusive** [xxxvi] **:**
  - L'utilisation de systèmes d'identification biométrique à distance en temps réel dans des espaces publics est interdite, sauf exceptions strictes (comme la recherche d'une personne disparue dans un contexte d'urgence).
- **Reconnaissance des émotions dans les lieux de travail et les établissements d'enseignement** [xxxvii] :
  - Interdiction des systèmes d'IA visant à détecter ou interpréter les émotions des individus dans des contextes professionnels ou éducatifs, en raison des risques pour les droits fondamentaux et la vie privée.
    Exemple : un logiciel de visioconférence analysant les expressions faciales d'élèves pour évaluer leur attention en classe.
- **Catégorisation biométrique** [xxxviii] :
  - Interdiction des systèmes utilisant des données biométriques (comme le visage ou les empreintes digitales) pour inférer l'origine ethnique, l'orientation sexuelle, les opinions politiques, les croyances religieuses, ou toute autre caractéristique sensible.

    Exemple : un dispositif de contrôle d'accès différenciant les individus sur la base de leur appartenance supposée à une communauté.

- **Prédiction du risque criminel** [xxxix] :
  - Interdiction des systèmes évaluant la probabilité de commettre une infraction pénale uniquement à partir du profil ou de traits de personnalité, sans fondement factuel.
    Exemple : un outil d'IA utilisé par les forces de l'ordre pour identifier des "suspects potentiels" sur la base de leur comportement social ou de leur apparence.
- **Création ou extension de bases de données de reconnaissance faciale par moissonnage (scraping) non ciblé d'images** (internet / vidéosurveillance) [xl] :
  - Interdiction de collecter massivement des images faciales sur internet ou via des caméras de vidéosurveillance à des fins de constitution de bases de données, en raison de l'atteinte grave au droit à la vie privée et du risque de surveillance généralisée.
    Exemple : une entreprise alimentant son système de reconnaissance faciale avec des images issues de réseaux sociaux sans le consentement des personnes concernées.

2.3. Les outils pour évaluer et gérer les risques

Le règlement impose des procédures robustes pour évaluer et gérer les risques associés aux systèmes d'IA, notamment :

- **Évaluation de conformité** [xli] : les fournisseurs doivent documenter les risques et justifier les mesures prises pour les atténuer.
- **Audits** [xlii] **:** les systèmes à haut risque doivent être soumis à des audits internes et externes pour garantir leur conformité.
- **Mécanismes de correction** [xliii] : en cas de défaillance, des processus correctifs doivent être activés pour limiter les impacts.

2.4. Encourager la confiance et la sécurité

L'approche fondée sur les risques équilibre innovation et protection :

- **Encourager l'innovation** [xliv] : en limitant les contraintes sur les systèmes à faible risque, le règlement stimule les jeunes pousses et les PME.
- **Garantir la sécurité** : les obligations imposées aux systèmes à haut risque renforcent la confiance des utilisateurs, ce qui est essentiel pour l'adoption à grande échelle de l'IA.

Le regard de Cédric

L'approche fondée sur les risques de l'**AI Act** reflète une vision équilibrée et pragmatique de la réglementation. En adaptant les obligations au niveau de risque, l'Union européenne assure une protection robuste des citoyens tout en permettant à l'innovation de prospérer. D'un point de vue de l'entreprise, il convient d'intégrer et de piloter ces nouvelles contraintes de risque au même titre que n'importe quelle autre afin de se sécuriser (ne pas analyser les niveaux de risque fait ... prendre un risque), de gagner en efficacité opérationnelle (pour reprendre une terminologie du lean management : éviter le waste et le rework) et éventuellement d'avoir un facteur différenciant sur votre marché en prouvant votre capacité à être à la pointe en termes de méthode, d'organisation et de réactivité. Les chapitres suivants détailleront les exigences spécifiques pour les systèmes d'IA à usage général, d'IA à haut risque et les outils mis en place pour garantir leur conformité.

Modèles d’IA à usage général (GPIA)

Chapitre 3

SOFTEAM
UNE FILIALE DE DOCAPOSTE

3.1. Définition et portée des modèles GPAI

Un modèle d'IA à usage général (GPAI en anglais) désigne un modèle entraîné avec un volume important de données, à l'aide de méthodes variées (auto-supervisé, non supervisé, renforcement), et qui présente une généralité significative, c'est-à-dire la capacité à exécuter un large éventail de tâches distinctes de manière compétente
Ces modèles peuvent être mis à disposition via des bibliothèques, API, téléchargements ou copies physiques, et sont souvent intégrés dans des systèmes d'IA en aval.
Exemples : grands modèles de langage (LLM), modèles de génération d'images ou audio, modèles multimodaux.
Il convient de les distinguer des systèmes d'IA qui sont des applications finales incluant une interface, une logique métier ou des modules décisionnels spécifiques.

3.2. Obligations Communes pour tous les fournisseurs de GPAI

Les fournisseurs de GPAI sont soumis à des obligations minimales visant à garantir la transparence, l'interopérabilité et la sécurité juridique dans la chaîne de valeur de l'IA.

3.2.1. Documentation technique [xlv]

Les fournisseurs doivent élaborer, tenir à jour et mettre à disposition une documentation technique décrivant :

- Les capacités et les limites du modèle,
- Les moyens d'intégration (API, bibliothèques, outils),
- Les versions logicielles utilisées,
- Toute information utile pour l'évaluation des performances.

3.2.2. Transparence sur les données d'entraînement (Art. 53.1.d)

Ils doivent publier un résumé suffisamment détaillé du contenu utilisé pour l'entraînement du modèle (grands jeux de données publics/privés, sources notables), tout en respectant les secrets d'affaires.[xlvi]

3.2.3. Respect du droit d'auteur

Une politique de conformité avec la directive (UE) 2019/790 sur le droit d'auteur est requise, notamment [xlvii] :

- Identification et respect des droits réservés,
- Justification de l'usage des données extraites via text and data mining.

3.2.4. Information aux fournisseurs en aval

Les fournisseurs doivent permettre aux intégrateurs de comprendre les caractéristiques du modèle GPAI, afin qu'ils puissent respecter leurs propres obligations réglementaires.[xlviii]
Exemption : ces obligations ne s'appliquent pas aux modèles publiés sous licence libre et ouverte, avec publication des poids, architecture et usage — sauf si le modèle présente un risque systémique.

3.3 Obligations supplémentaires pour les modèles à usage général présentant un risque systémique

3.3.1. Identification d'un risque systémique [xlix]

Un modèle GPAI est considéré comme présentant un risque systémique s'il :

- Dépasse un seuil de calcul lors de l'entraînement (actuellement fixé à 10^{25} opérations en virgule flottante),
- Est désigné par la Commission (avec avis du groupe scientifique),
- Ou présente des effets graves prévisibles sur la santé, la sécurité publique, la démocratie ou l'économie.

3.3.2. Exigences Renforcées [l]

Les fournisseurs concernés doivent :

- Réaliser une évaluation approfondie, y compris via des tests contradictoires (red teaming),
- Évaluer et atténuer les risques systémiques tout au long du cycle de vie du modèle,
- Mettre en place des politiques de cybersécurité adaptées (sécurisation des poids, accès, infra),
- Signaler tout incident grave aux autorités compétentes sans retard injustifié.

3.4. Rôles du Bureau Européen de l'IA (AI Office)[li]

Le Bureau de l'IA (service de la commission) est l'autorité centrale chargée de :

- **Superviser les fournisseurs de GPAI**, notamment ceux à risque systémique,
- **Recevoir les notifications et évaluations** des fournisseurs,
- **Lancer des évaluations**, demander l'accès aux modèles (y compris API ou code source),
- **Élaborer des codes de bonne pratique** en collaboration avec l'industrie, les chercheurs et la société civile,

Le regard de Cédric

Ce régime réglementaire spécifique vise à **encadrer les modèles fondateurs** qui structurent l'écosystème de l'IA en Europe. Il cherche à garantir **la transparence, la sécurité, la conformité éthique et juridique**, tout en **encourageant l'innovation responsable**. Attention ! Les modèles GPAI sont sûrement déjà dans votre entreprise et il y a un risque non négligeable de voir de grandes sociétés américaines se détourner (être interdites ?) du marché européen du fait des contraintes apportées par la réglementation.

Et alors me direz-vous ?

- Alors si vous avez construit des systèmes autour d'un de ces modèles qu'adviendrait-il de celui-ci si, du jour au lendemain, il devenait inaccessible ?
- Êtes-vous certain d'avoir bien référencé le « shadow AI » au sein de vos services ?
- Avez-vous un processus de déclaration interne ?

Autant de questions pour lesquels je vous invite à prendre dès ce jour des mesures concrètes afin d'atténuer les risques inhérents à l'usage de produits dont on ne connait pas la pérennité

Règles spécifiques pour les systèmes d’IA à haut risque

Chapitre 4

SOFTEAM
UNE FILIALE DE DOCAPOSTE

Les systèmes d'IA à haut risque représentent la catégorie la plus encadrée par l'AI Act, en raison de leur impact potentiel sur les droits fondamentaux, la sécurité et la société. Ce chapitre explore les exigences techniques et organisationnelles imposées aux acteurs impliqués dans le développement, la mise sur le marché et l'utilisation de ces systèmes, ainsi que les mécanismes de surveillance et les sanctions prévues en cas de non-conformité.

4.1. Exigences techniques et organisationnelles

Les exigences pour les systèmes d'IA à haut risque visent à garantir leur sécurité, leur transparence et leur fiabilité tout au long de leur cycle de vie.

4.1.1. Documentation technique [lii]

La documentation technique est essentielle pour démontrer la conformité des systèmes d'IA à haut risque. Elle doit inclure :

- **Description fonctionnelle** :
  - Objectif du système et domaine d'application prévu.
  - Limitations identifiées (e.g., biais possibles, contexte d'utilisation recommandé).
- **Caractéristiques techniques** :
  - Algorithmes utilisés et leur fonctionnement.
  - Données d'entraînement et de test (source, qualité, gestion des biais).
- **Traçabilité des décisions** :
  - Documentation sur la manière dont les sorties sont générées.
  - Explication des critères de décision ou de prédiction.

Cette documentation doit être mise à jour régulièrement, notamment en cas de modifications majeures du système.

4.1.2. Gestion des données [liii]

Les données utilisées par les systèmes d'IA à haut risque doivent respecter des normes strictes :

- **Qualité des données** : elles doivent être exactes, complètes et représentatives pour éviter les biais.
- **Protection des données personnelles** :
  - Respect du RGPD (Règlement Général sur la Protection des Données).
  - Utilisation de techniques de pseudonymisation ou d'anonymisation si nécessaire.
- **Gestion des biais** :
  - o Identification proactive des biais potentiels.
  - o Mise en place de mécanismes correctifs pour réduire les distorsions dans les résultats.

4.1.3. Traçabilité [liv]

La traçabilité est un principe fondamental pour les systèmes à haut risque. Elle garantit que chaque étape du développement et de l'utilisation est documentée et auditable :

- **Registre d'utilisation** :
  - Consigner les cas d'utilisation du système.
  - Enregistrer les incidents ou erreurs rencontrés.
- **Auditabilité** : capacité à examiner le fonctionnement du système pour identifier les causes des décisions erronées ou des problèmes techniques.

4.2. Surveillance et conformité

L'**AI Act** impose des obligations spécifiques aux opérateurs impliqués dans le cycle de vie des systèmes d'IA à haut risque, pour assurer leur conformité continue.

4.2.1. Évaluation préalable de conformité [lv]

Avant la mise sur le marché ou en service d'un système d'IA à haut risque, une **évaluation de conformité** est requise. Celle-ci inclut :

- **Vérification technique** :
  - Validation des performances par rapport à l'objectif annoncé.
  - Test de robustesse face aux défaillances ou attaques.
- **Évaluation des risques** :
  - Identification des risques liés à la sécurité ou aux droits fondamentaux.
  - Mise en place de mesures d'atténuation appropriées.

Cette évaluation peut être réalisée par des tiers accrédités ou, dans certains cas, en interne par les fournisseurs.

4.2.2. Obligations des opérateurs

Les obligations varient selon le rôle de l'opérateur dans la chaîne de valeur :

- **Fournisseurs** [lvi] :
  - Assurer la conformité initiale (y compris la déclaration UE de conformité) et continuer à surveiller le système après sa mise sur le marché.
  - Fournir une assistance technique pour corriger tout problème ainsi que signaler ces non-conformités
- **Déployeurs** [lvii] :
  - Utiliser les systèmes d'IA à haut risque conformément aux notices d'utilisation, sous la supervision de personnes compétentes et formées. Ils doivent surveiller le fonctionnement des systèmes, signaler tout incident grave ou risque.
  - Informer les travailleurs, les personnes concernées (notamment dans le cadre de décisions les affectant), et coopérer avec les autorités. Les employeurs sont tenus d'informer les représentants du personnel avant tout déploiement sur le lieu de travail.
- **Distributeurs** [lviii] : vérifier que les produits sont accompagnés de la documentation requise avant leur mise en circulation.

4.2.3. Surveillance continue

Les systèmes à haut risque doivent faire l'objet d'une surveillance active une fois déployés :

- **Surveillance continue** [lix] : collecte des données pertinentes sur les performances.
- **Audits régulier** [lx] : réalisés pour s'assurer que le système reste conforme aux exigences initiales.
- **Mises à jour** [lxi] : les systèmes doivent être mis à jour en cas de nouvelles vulnérabilités ou pour améliorer leurs performances.

4.3. Sanctions en cas de non-conformité

Pour garantir le respect du règlement, des sanctions proportionnées mais dissuasives sont prévues.

4.3.1. Types de non-conformité [lxii]

Les violations peuvent inclure :

- L'absence de documentation technique ou de traçabilité.
- L'utilisation de données biaisées ou non conformes aux normes de qualité.
- La mise sur le marché d'un système non validé par une évaluation de conformité voir de systèmes explicitement interdits par le règlement

4.3.2. Sanctions [lxiii]

L'**AI Act** prévoit des amendes significatives, en fonction de la gravité de la non-conformité :

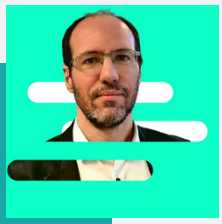
- Jusqu'à **35 millions d'euros ou 7 % du chiffre d'affaires annuel mondial** pour les infractions les plus graves (e.g. non-respect des interdictions spécifiques comme la manipulation cognitive ou la notation sociale).
- Jusqu'à **15 millions d'euros ou 3 % du chiffre d'affaires annuel mondi**al en cas de non-respect des obligations lié à une IA à haut risque
- Jusqu'à **7,5 millions d'euros ou 1% du chiffre d'affaires annuel mond**ial en cas de fourniture d'informations « inexactes, incomplètes ou trompeuses » aux organismes notifiés ou aux autorités
- Sanctions réduites pour des infractions moins graves

À noter : en règle générale, le montant le plus élevé entre le pourcentage du chiffre d'affaires annuel mondial et le montant forfaitaire est appliqué. Exception : pour les PME et les start-ups, c'est le montant le plus faible qui est retenu.

4.3.3. Mesures correctives [lxiv]

En plus des amendes, les autorités compétentes peuvent imposer :

- La suspension ou l'interdiction de mise sur le marché du système concerné.
- L'obligation de retirer le système de l'usage actif.
- La mise en conformité dans un délai défini, avec surveillance renforcée.



Le regard de Cédric

Les règles spécifiques pour les systèmes d'IA à haut risque soulignent la volonté de l'Union européenne de **protéger ses citoyens tout en encourageant une innovation responsable**. Les exigences techniques et organisationnelles, combinées à des mécanismes de surveillance rigoureux, posent les bases d'une IA fiable et digne de confiance. Toutefois, elles imposent également une **responsabilité accrue aux opérateurs, avec des sanctions strictes pour garantir leur engagement.**

Compte tenu de la sensibilité des données et des impacts des IA à haut risque, si vos systèmes sont « éligibles » vous entrez dans une zone de tolérance zéro et, comme pour le RGPD ou la cybersécurité, vous devez impérativement penser documentation, dataops (audit de qualité, plan de mitigation des biais ...), traçabilité by design, Red-teaming, tests d'attaque, procédure de notification que ce soit pour un système maison ou un système construit/fourni par un tiers.

Innovation et développement

Chapitre 5

SOFTEAM
UNE FILIALE DE DOCAPOSTE

L'un des objectifs clés de l'**AI Act** est de stimuler l'innovation en permettant le développement d'une intelligence artificielle éthique, fiable et compétitive. Ce chapitre explore les mécanismes mis en place pour favoriser l'expérimentation de nouvelles technologies, notamment à travers les bacs à sable réglementaires, et les mesures spécifiques de soutien aux petites et moyennes entreprises (PME).

5.1. Bacs à sable réglementaires

Les **bacs à sable réglementaires** (regulatory sandboxes) sont des environnements contrôlés mis en place pour permettre aux entreprises de tester des systèmes d'IA innovants dans des conditions réelles tout en bénéficiant d'un cadre réglementaire flexible. Ces espaces jouent un rôle crucial pour :

- Réduire les incertitudes liées à la conformité réglementaire.
- Encourager l'expérimentation responsable.
- Accélérer la mise sur le marché des technologies d'IA.

5.1.1. Définition et principes

Un bac à sable réglementaire est un cadre dans lequel les participants peuvent tester leurs solutions sous la supervision d'une autorité compétente. Ces tests se déroulent dans des conditions spécifiques permettant de limiter les risques pour les utilisateurs finaux. Les principes fondamentaux sont :

1. **Sécurité contrôlée** [lxv] :
    - Les tests doivent se dérouler dans des conditions qui protègent les utilisateurs contre tout préjudice.
    - Les résultats des tests doivent être documentés pour évaluer les impacts.
2. **Supervision réglementaire** [lxvi] : les autorités supervisent les tests pour garantir le respect des droits fondamentaux.
3. **Flexibilité encadrée** [lxvii] : certains assouplissements des exigences réglementaires sont accordés temporairement, dans les limites fixées par le règlement.

5.1.2. Objectifs des bacs à sable [lxviii]

1. **Faciliter l'innovation** : permettre aux développeurs de concevoir des solutions innovantes sans les contraintes immédiates de la conformité réglementaire complète.
2. **Identifier les lacunes réglementaires** : les tests peuvent révéler des besoins d'adaptation des règles existantes à des technologies émergentes.
3. **Créer un environnement d'apprentissage** : les autorités et les développeurs travaillent ensemble pour comprendre comment des solutions innovantes peuvent s'intégrer dans le cadre légal.

5.1.3. Accès aux bacs à sable [lxix]

Les bacs à sable sont principalement destinés :

- Aux start-ups et PME développant des technologies d'IA innovantes.
- Aux grands acteurs qui souhaitent tester des applications de pointe dans un cadre réglementaire contrôlé.
- Aux collaborations entre organismes de recherche et industriels.

Critères d'admissibilité : les critères ne sont pas définis par l'acte et devront être fournis par la commission via des actes d'exécutions avant l'entrée en vigueur des bacs à sable.

5.1.4. Gestion des bacs à sable

Chaque État membre est responsable de la mise en place et de la gestion de ses bacs à sable, avec un soutien du Comité Européen de l'Intelligence Artificielle (CEIA). [lxx]

5.1.5. Exemples d'utilisation possible

- **Détection médicale assistée par IA** : tester des systèmes de diagnostic dans un environnement contrôlé avant leur mise en œuvre dans des hôpitaux.
- **Mobilité autonome** : expérimenter des véhicules autonomes dans des zones géographiques spécifiques.
- **Systèmes éducatifs personnalisés** : évaluer l'impact des algorithmes d'apprentissage adaptatif sur les élèves.

5.2. Soutien aux petites et moyennes entreprises (PME)

Les Petites et Moyennes Entreprises (PME), y compris les jeunes pousses (start-ups), jouent un rôle essentiel dans l'écosystème de l'innovation en Europe. Reconnaissant les défis spécifiques auxquels elles sont confrontées, notamment en matière de ressources pour se conformer aux exigences réglementaires, l'**AI Act** prévoit plusieurs mesures de soutien visant à alléger leurs contraintes et à favoriser leur développement.[lxxi]

5.2.1. Allégements administratifs et réglementaires

1. **Documentation simplifiée** : les PME, y compris les jeunes pousses, peuvent fournir les éléments de la documentation technique requise (prévue à l'Annexe IV) de manière simplifiée. À cette fin, la Commission établira un formulaire de documentation technique simplifié ciblant spécifiquement les besoins des petites entreprises et des microentreprises.[lxxii]
2. **Système de gestion de la qualité simplifié pour les Microentreprises** : les microentreprises peuvent se conformer de manière simplifiée à certains éléments du système de gestion de la qualité requis par l'Article 17. La Commission élaborera des lignes directrices précisant les éléments concernés, en tenant compte des besoins spécifiques des microentreprises.[lxxiii]

5.2.2. Assistance technique et information

1. **Plateforme d'Information Unique** : le Bureau Européen de l'IA (Bureau de l'IA) développera et maintiendra une plateforme d'information unique fournissant des informations faciles à utiliser concernant l'**AI Act** pour tous les opérateurs de l'Union.[lxxiv]
2. **Accès Prioritaire aux Bacs à Sable Réglementaires** : les États membres accorderont aux PME, y compris les jeunes pousses, un accès prioritaire aux bacs à sable réglementaires de l'IA, sous réserve qu'elles remplissent les conditions d'éligibilité.[lxxv]
3. **Autres Mesures de Soutien Nationales** : les États membres sont encouragés à mettre en place des actions de sensibilisation, des canaux de communication dédiés pour fournir des conseils, et à faciliter l'accès aux installations d'essai et d'expérimentation pour les PME.[lxxvi]

5.2.3. Soutien financier

1. **Prise en Compte dans les Frais d'Évaluation** : les intérêts et besoins spécifiques des PME fournisseuses, y compris les jeunes pousses, doivent être pris en compte lors de la fixation des redevances d'évaluation de la conformité par les organismes notifiés, avec des frais réduits proportionnellement à leur taille et situation.[lxxvii]

Le regard de Cédric

L'accent mis par l'AI Act sur les bacs à sable réglementaires et le soutien aux PME reflète l'ambition de l'Union européenne de devenir un leader mondial de l'intelligence artificielle. En offrant des opportunités d'expérimentation tout en atténuant les contraintes pour les petites structures, le règlement vise à :

- Stimuler **l'innovation dans un cadre éthique et sécurisé.**
- Créer un **écosystème compétitif et inclusif,** où même les acteurs les plus modestes peuvent prospérer.
- Encourager une **collaboration e**ntre chercheurs, entreprises et autorités pour relever les défis technologiques et sociétaux.

Ce chapitre met en lumière le potentiel des outils d'accompagnement de l'AI Act pour transformer des idées novatrices en solutions concrètes, tout en respectant les valeurs fondamentales de l'Europe. Je vous invite à **évaluer votre éligibilité aux différents dispositifs**. En effet, ils pourraient vous permettre d'alléger considérablement la charge financière et humaine de la mise en place de nouveaux systèmes d'IA, notamment ceux potentiellement classés à haut risque, au sein de votre entreprise.

Éthique et gouvernance

Chapitre 6

SOFTEAM
UNE FILIALE DE DOCAPOSTE

L'éthique et la gouvernance sont au cœur de l'AI Act, reflétant l'ambition de l'Union européenne de promouvoir une intelligence artificielle qui soit non seulement innovante, mais également respectueuse des droits fondamentaux, de la dignité humaine et des valeurs démocratiques. Ce chapitre explore les lignes directrices éthiques qui sous-tendent le développement et l'utilisation de l'IA, ainsi que le rôle du Comité Européen de l'Intelligence Artificielle (CEIA) dans leur mise en œuvre.

6.1. Lignes directrices en matière d'éthique

Les principes éthiques de l'**AI Act** servent de cadre pour le développement et l'utilisation de l'IA dans toute l'Europe. Ces principes, inspirés par les valeurs fondamentales de l'Union européenne, visent à garantir que l'IA profite à la société tout en limitant les risques.

6.1.1. Développement centré sur l'humain

L'IA doit être conçue et utilisée pour servir les humains, non pour les remplacer ou les contrôler. Cela implique :

- Respect de la dignité humaine : les systèmes d'IA ne doivent pas exploiter les vulnérabilités psychologiques ou physiques des utilisateurs. [lxxviii]
- Renforcement des capacités humaines : l'IA doit agir comme un outil pour améliorer les compétences, l'autonomie et le bien-être des utilisateurs. [lxxix]
- Non-substitution des décisions critiques : les décisions ayant des impacts importants sur la vie des individus doivent inclure une supervision humaine. [lxxx]

6.1.2. Robustesse technique et sécurité

La robustesse technique garantit que les systèmes d'IA sont fiables et résilients face aux défaillances, erreurs ou cyberattaques. Cela inclut [lxxxi] :

- **Tests rigoureux** : les systèmes doivent être évalués pour identifier leurs limites et éviter les comportements imprévisibles.
- **Résilience aux attaques** : les mécanismes de protection contre les piratages doivent être intégrés dès la conception.
- **Sécurité des utilisateurs** : les systèmes doivent minimiser les risques de préjudices physiques, psychologiques ou économiques.

6.1.3. Transparence

La transparence est essentielle pour instaurer la confiance dans l'IA, aussi les éléments suivants sont cruciaux :

- **Comment l'IA fonctionne** : explication accessible sur leur fonctionnement via, entre autre, la notice du système.[lxxxii]
- **Que l'IA est en jeu** : information explicite lorsqu'un utilisateur interagit avec un système d'IA.[lxxxiii]

6.1.4. Diversité, équité et inclusion

Les systèmes d'IA doivent être développés pour éviter tout biais discriminatoire [lxxxiv]. Cela implique :

- **Évaluation des biais** : identifier et corriger les biais dans les données ou les algorithmes.[lxxxv]
- **Accessibilité** : promouvoir l'accessibilité à tous, notamment aux personnes en situation de handicap.[lxxxvi]

6.1.5. Bien-être sociétal et environnemental

Les systèmes d'IA doivent contribuer à un développement durable. Cela inclut :

- **Réduction de l'empreinte écologique** : fournir les moyen d'optimiser les ressources utilisées dans divers secteurs pour limiter leur impact environnemental.[lxxxvii]
- **Impact sociétal positif** : encourager les usages de l'IA qui renforcent la cohésion sociale et le bien-être collectif.[lxxxviii]

6.2. Rôle du Comité Européen de l'Intelligence Artificielle (CEIA)

Le CEIA, institué par l'**AI Act**, joue un rôle central dans la gouvernance éthique et réglementaire de l'IA au sein de l'Union européenne. Il agit comme un organe de coordination, de surveillance et de promotion des bonnes pratiques.

6.2.1. Mission du CEIA

1. **Superviser la mise en œuvre du règlement** [lxxxix]
   - Garantir une application cohérente et efficace dans tous les États membres.
   - Conseiller la Commission et les autorités nationales, notamment sur les modèles d'IA à usage général.
   - Émettre des recommandations sur toute question liée à l'application du règlement.
2. **Promouvoir l'harmonisation et la coordination au sein de l'UE** [xc]
   - Faciliter la coordination entre autorités nationales, y compris pour la surveillance du marché.
   - Encourager l'harmonisation des pratiques administratives (évaluation de la conformité, bacs à sable, essais).
   - Développer des critères communs et une interprétation partagée des concepts clés.
3. **Renforcer l'expertise et la sensibilisation à l'IA** [xci]
   - Contribuer au développement des compétences techniques et organisationnelles.
   - Soutenir la sensibilisation du public aux droits, risques et bénéfices liés à l'IA.
   - Suivre les tendances en matière d'adoption de l'IA, de compétitivité et d'évolution des compétences.
4. **Favoriser la coopération internationale** [xcii]
   - Conseiller la Commission sur les enjeux internationaux liés à l'IA.
   - Contribuer à la collaboration avec les autorités de pays tiers et les organisations internationales.

6.2.2. Activités du CEIA

1. **Élaboration de cadres de référence** [xciii] :
   - Co-construire des codes de conduite et de bonne pratique avec les parties prenantes.
   - Produire des documents d'orientation et soutenir l'interprétation du règlement.
2. **Formation et sensibilisation** [xciv] :
   - Organiser le socle de compétence nécessaire aux personnels des autorités publiques.
   - Informer le grand public sur les enjeux de l'IA et ses droits associés.
3. **Veille et recommandations** [xcv] :
   - Publier des rapports sur l'état de l'IA en Europe et formuler des recommandations d'amélioration.
   - Évaluer les expérimentations menées dans les bacs à sable réglementaires
4. **Soutien aux initiatives internationales** [xcvi] :
   - Collaborer avec des organisations internationales pour établir des normes globales d'éthique en matière d'IA.

6.2.3. Structure et fonctionnement

Le Comité européen de l'intelligence artificielle (CEIA) est composé d'un représentant par État membre. D'autres autorités, organes ou experts nationaux et de l'Union peuvent être invités à ses réunions au cas par cas, lorsque les questions examinées relèvent de leurs compétences [xcvii]. Ses décisions sont non contraignantes mais influencent fortement les politiques nationales et européennes.[xcviii]

Le regard de Cédric

L'**AI Act** propose une vision ambitieuse de l'éthique et de la gouvernance de l'intelligence artificielle. En articulant des lignes directrices claires et en établissant un organe de supervision centralisé, l'Union européenne se positionne comme un **modèle de référence pour un développement technologique respectueux des valeurs humaines et démocratiques**. Ce cadre favorise non seulement la confiance des citoyens, mais aussi l'émergence d'un écosystème d'innovation où les entreprises européennes peuvent prospérer tout en contribuant à un futur durable et inclusif.
Afin d'éviter de faire fausse route, je vous incite à **croiser votre cadre éthique avec celui du règlement**, en effet, demain, il y a un risque à ne pas pouvoir prouver sa conformité au cadre éthique européen : de la même manière qu'actuellement certains appels d'offres incluent une notion d'alignement à la taxonomie européenne (ESG), demain il est possible qu'une note d'alignement éthique soit nécessaire et potentiellement pénalisante. Ainsi on peut imaginer de manière pratique un check transparence dans la Definition of Done, prévoir en plus d'un DPO un AIEO (AI Ethics Officer) ou encore mettre un bias bounty pour inciter les collaborateurs à chercher les biais potentiels.

Interaction avec d’autres réglementations

Chapitre 7

SOFTEAM
UNE FILIALE DE DOCAPOSTE

L'**AI Act** s'inscrit dans un cadre juridique et éthique européen plus large, conçu pour protéger les droits fondamentaux et garantir un développement technologique responsable. Ce chapitre examine l'interaction entre l'**AI Act** et d'autres réglementations clés, notamment le RGPD, les dispositions relatives à l'égalité et à la non-discrimination, ainsi que les implications pour les entreprises non européennes opérant dans l'Union.

7.1. Protection des données : Relation avec le RGPD

Le **Règlement Général sur la Protection des Données (RGPD)** est une pierre angulaire du cadre législatif européen en matière de données personnelles. L'**AI Act**, bien qu'ayant un objectif différent, est conçu pour fonctionner en harmonie avec le RGPD.

7.1.1. Complémentarité avec le RGPD

Le RGPD et l'**AI Act** partagent des objectifs communs, notamment :

- **La protection des droits fondamentaux** : garantir que les données utilisées par les systèmes d'IA ne compromettent pas la vie privée ou la dignité des individus.
- **La transparence** : informer les utilisateurs sur la manière dont leurs données sont utilisées et traiter toute question liée au consentement.
- **Minimisation des données** : les systèmes d'IA doivent limiter les données utilisées à ce qui est strictement nécessaire à leur objectif.

7.1.2. Exigences spécifiques pour l'IA

L'**AI Act** introduit des obligations supplémentaires pour les systèmes d'IA, qui s'ajoutent à celles du RGPD :

- **Biais et qualité des données** : comme vu précédemment, le règlement impose des vérifications pour s'assurer que les données d'entraînement et de test sont de haute qualité et non biaisées.
- **Transparence algorithmique** : les utilisateurs doivent pouvoir comprendre pourquoi et comment leurs données influencent les décisions des systèmes d'IA.

7.1.3. Points d'attention pour les entreprises

1. **Bases légales pour le traitement** : les entreprises doivent s'assurer que toute donnée utilisée pour entraîner ou déployer des systèmes d'IA dispose d'une base légale conforme au RGPD (e.g., consentement explicite, intérêt légitime).
2. **Analyse d'impact relative à la protection des données (DPIA)** : les systèmes d'IA à haut risque doivent faire l'objet d'une analyse d'impact approfondie pour évaluer les risques pour la vie privée.
3. **Superposition des sanctions** : une violation des dispositions de **l'AI Act** concernant les données peut également constituer une infraction au RGPD, entraînant des sanctions cumulatives.

7.2. Conformité aux droits fondamentaux : égalité et non-discrimination

L'Union européenne place la protection des droits fondamentaux au cœur de sa législation, et l'**AI Act** ne fait pas exception. Le règlement introduit des dispositions spécifiques pour garantir que les systèmes d'IA ne renforcent pas les inégalités ou les discriminations.

7.2.1. Lutte contre les biais dans l'IA

Les systèmes d'IA peuvent reproduire ou amplifier des biais présents dans les données d'entraînement. L'**AI Act** exige :

- **Identification proactive des biais** : les développeurs doivent évaluer leurs données et algorithmes pour identifier tout biais potentiel.
- **Corrigibilité** : les biais identifiés doivent être corrigés pour éviter des impacts discriminatoires.
- **Documentation** : toute mesure prise pour réduire les biais doit être clairement documentée.

7.2.2. Garanties pour l'égalité

Les domaines critiques (e.g., emploi, santé, éducation, accès au crédit) sont particulièrement protégés. Les systèmes d'IA utilisés dans ces secteurs doivent respecter des règles strictes pour :

- Garantir une **égalité d'accès** aux services.
- Empêcher toute **discrimination** fondée sur des caractéristiques protégées, comme le genre, l'origine ethnique, ou le handicap.

7.2.3. Droits des utilisateurs

Le règlement renforce les droits des utilisateurs face aux systèmes d'IA :

- **Explicabilité des décisions** : les utilisateurs doivent pouvoir comprendre comment et pourquoi une décision a été prise.
- **Recours en cas de discrimination** : les citoyens doivent avoir accès à des mécanismes de recours efficaces s'ils estiment avoir été discriminés par un système d'IA.[xcix]

7.3. Coopération internationale : Implications pour les entreprises non européennes

L'impact de l'**AI Act** dépasse les frontières de l'Union européenne. Les entreprises non européennes doivent s'y conformer si elles proposent des produits ou services utilisant l'IA sur le marché européen.

7.3.1. Applicabilité extraterritoriale

L'**AI Act** s'applique :

- **Aux systèmes d'IA utilisés dans l'Union européenne**, même si le fournisseur est basé en dehors de l'UE.
- **Aux systèmes d'IA dont les résultats affectent des citoyens ou entreprises européennes**, quelle que soit leur origine géographique.

7.3.2. Exigences pour les entreprises étrangères

Les entreprises hors de l'UE doivent :

1. **Désigner un représentant légal dans l'Union européenne** : ce représentant sera le point de contact pour les autorités européennes et assurera la conformité du système avec l'**AI Act**.[c]
2. **Se conformer aux normes européennes** : cela inclut les exigences de documentation, de transparence et de gestion des risques prévues pour les systèmes d'IA.
3. **Adapter les pratiques locales** : les entreprises opérant dans des régions où les réglementations sont moins strictes devront ajuster leurs pratiques pour satisfaire aux standards européens.

7.3.3. Encouragement à une coopération internationale

L'**AI Act** incite à la création de partenariats internationaux pour :

- Harmoniser les normes globales sur l'IA.
- Faciliter les échanges de bonnes pratiques entre les juridictions.
- Éviter les conflits juridiques et promouvoir un cadre mondial cohérent.

Le regard de Cédric

L'interaction de l'**AI Act** avec d'autres réglementations, comme le RGPD ou les lois relatives aux droits fondamentaux, reflète une approche globale et cohérente de la réglementation. Cette complémentarité renforce la protection des citoyens européens tout en clarifiant les obligations des entreprises, qu'elles soient basées en Europe ou ailleurs. En intégrant des normes élevées de coopération internationale, le règlement vise également à **positionner l'Europe comme un leader de la gouvernance éthique et responsable de l'IA**. Au-delà des ambitions louables de l'Europe, on peut noter une inflation des normes, directives et autres règlements au sein de l'UE (RGPD, CSRD, NFRD, Taxonomie verte, NIS2, Ecodesign etc.) et un acteur européen bien informé, bien organisé, qui anticipe au mieux les calendriers de mise en œuvre peut avoir un avantage compétitif sur un concurrent extra-européen qui arriverait et devrait se conformer à l'ensemble des règles du jeu en une seule fois. Aussi, afin de ne pas être dépassé et laisser vos concurrents prendre des parts de marché il convient de **comprendre et doser justement l'effort à mettre sur chaque réglementation pour avoir un ratio optimal entre le coût de mise en œuvre et le risque de perdre en compétitivité.**

Mise en œuvre

Chapitre 8

SOFTEAM
UNE FILIALE DE DOCAPOSTE

Le succès de l'**AI Act** repose sur une mise en œuvre efficace et coordonnée entre les différentes parties prenantes. Ce chapitre explore les rôles des acteurs clés, les étapes du plan de transition, ainsi que les processus requis pour assurer la conformité avec le règlement.

8.1. Rôles des parties prenantes

La mise en œuvre de l'**AI Act** nécessite une collaboration étroite entre **les autorités nationales, les entreprises** et **les utilisateurs**, chacun ayant des responsabilités distinctes mais complémentaires.

8.1.1. Autorités nationales

Les autorités nationales compétentes jouent un rôle central dans l'application et la supervision du règlement. Leurs responsabilités incluent :

- **Supervision de la conformité** :
  - Contrôler les systèmes d'IA à haut risque avant leur mise sur le marché.
  - Mener des inspections ou audits réguliers pour s'assurer du respect des exigences.
- **Support aux entreprises** :
  - Fournir des guides et des outils pour aider les entreprises, notamment les PME, à comprendre et à appliquer les dispositions du règlement.
  - Établir des bacs à sable réglementaires pour encourager l'innovation dans un cadre sécurisé.
- **Coopération transfrontalière** : collaborer avec d'autres autorités nationales et le Comité Européen de l'IA pour garantir une application harmonisée du règlement dans toute l'Union.

8.1.2. Entreprises

Les entreprises, qu'elles soient fournisseurs, déployeurs ou distributeurs de systèmes d'IA, ont des responsabilités étendues :

- **Fournisseurs** :
  - Produire une documentation technique complète pour démontrer la conformité.
  - Mettre en place des systèmes robustes de gestion des risques.
- **Déployeurs** :
  - Assurer une utilisation conforme aux instructions des fournisseurs.
  - Former les personnels à l'utilisation sécurisée des systèmes d'IA.
- **Distributeurs** : vérifier que les systèmes mis sur le marché respectent les exigences du règlement (marquage CE, déclaration de conformité ...)

8.1.3. Utilisateurs

Les utilisateurs finaux, qu'ils soient individuels ou institutionnels, jouent également un rôle important :

- **Responsabilité partagée** : les utilisateurs institutionnels doivent utiliser les systèmes d'IA dans le respect des instructions fournies.[ci]
- **Signalement des problèmes** : les utilisateurs sont encouragés à signaler tout incident ou impact négatif lié à l'utilisation d'un système d'IA ; il est d'ailleurs explicitement indiqué qu'ils bénéficient du droit à la protection apporté par la DIRECTIVE (UE) 2019/1937.[cii]
- **Recours** : les utilisateurs ont le droit de demander des explications ou de contester des décisions prises par un système d'IA.[ciii]

8.2. Plan de transition

Pour faciliter une adoption harmonieuse du règlement, un plan de transition a été établi, offrant aux États membres et aux entreprises un délai d'adaptation progressif. Si les interdictions et les dispositions générales entre en vigueur le 2 février 2025 (cela inclut notamment la nécessité pour les fournisseurs et déployeurs d'avoir formé leurs personnels avant cette date), les autres obligations s'étalent dans le temps :

- **2 mai 2025** : finalisation des codes de bonne pratique pour aider les fournisseurs à se conformer.
- **2 août 2025** :
  - Application des obligations pour les fournisseurs de modèles d'IA à usage général.
  - Mise en place des dispositions relatives à la gouvernance, aux organismes notifiés et aux sanctions (y compris les amendes administratives).
- **2 août 2026** : application complète du règlement, avec toutes les infrastructures de gouvernance et d'évaluation de conformité opérationnelles sauf pour les systèmes d'IA à haut risque intégrés à des produits déjà réglementés (dispositifs médicaux, machines, jouets, etc.) dont l'entrée en application se fera le 2 août 2027

8.2.1. Délai pour les États membres

- **Transposition des mécanismes nationaux** : bien que l'**AI Act** soit directement applicable, les États membres doivent établir ou adapter leurs infrastructures nationales pour superviser son application (e.g., désignation des autorités compétentes, création des bacs à sable) avant le 2 août 2026 [civ]

8.2.2. Délai pour les entreprises

Les entreprises disposent d'un **délai transitoire** pour aligner leurs pratiques et systèmes sur les exigences de l'**AI Act**. Ce délai varie en fonction de la complexité des adaptations nécessaires :

- **Systèmes existants** : les systèmes d'IA déjà en service doivent être évalués et mis en conformité dans les deux ans suivant l'entrée en vigueur du règlement.[cv]
- **Nouveaux systèmes** : tous les systèmes mis sur le marché après la date d'entrée en vigueur doivent être immédiatement conformes.

8.3. Étapes pour la mise en conformité

La mise en conformité avec l'**AI Act** repose sur un processus structuré en plusieurs étapes, visant à garantir que les systèmes d'IA répondent aux exigences réglementaires.

8.3.1. Audit de conformité

L'audit de conformité est une étape essentielle, particulièrement pour les systèmes à haut risque :

- **Évaluation technique** :
  - Vérifier que le système fonctionne conformément à ses objectifs déclarés.
  - Identifier les risques et évaluer les mécanismes de réduction des risques.
- **Évaluation organisationnelle** : examiner les processus internes de l'entreprise (e.g., gestion des données, contrôle qualité).

8.3.2. Certification[cvi]

Les systèmes d'IA à haut risque doivent obtenir une certification avant leur mise sur le marché :

- **Évaluation initiale** : réalisée par des organismes accrédités, cette évaluation vérifie la conformité technique et éthique du système.
- **Certificat de conformité** : le certificat délivré est valable pour une durée limitée (généralement 5 ans) et peut être renouvelé après une nouvelle évaluation.

8.3.3. Rapports de conformité

Les entreprises doivent produire des rapports réguliers pour démontrer leur conformité continue :

- **Rapports techniques** : fournir des mises à jour sur la performance du système et les éventuels ajustements réalisés.[cvii]
- **Rapports sur les incidents** : toute défaillance ou tout préjudice lié à un système d'IA à haut risque doit être signalé dans les plus brefs délais aux autorités compétentes (0 à 15 jours)[cviii]
- **Mises à jour documentaires** : actualiser la documentation technique en cas de modifications majeures du système.[cix]

Le regard de Cédric

La mise en œuvre de l'**AI Act** repose sur une approche collaborative et progressive, impliquant toutes les parties prenantes. Grâce à un plan de transition structuré et à des étapes claires pour la mise en conformité, l'Union européenne vise à garantir que les systèmes d'IA soient développés et utilisés dans le respect des droits fondamentaux et des normes de sécurité. Ce cadre assure également un équilibre entre innovation et protection, offrant aux entreprises un chemin clair vers une adoption réussie du règlement. L'approche se veut progressive, mais à l'échelle d'une entreprise des urgences se profilent : Si ce n'est encore fait, je vous incite à mettre en place un comité de pilotage pluridisciplinaire afin de remédier aux non-conformités existantes (logiciel RH de recrutement basé sur l'IA ? Personnel formé ? Capacité à justifier une décision prise par le logiciel ?) et de mettre en place une gouvernance claire qui pourra adresser en temps et en heure les différents sujets ayant trait à l'AI Act.

Pour terminer...

SOFTEAM
UNE FILIALE DE DOCAPOSTE

Conclusion

L'**AI Act** marque une étape majeure dans la réglementation de l'intelligence artificielle, établissant un cadre ambitieux qui conjugue innovation technologique et respect des droits fondamentaux. Ce règlement, le premier de ce type à l'échelle mondiale, reflète la vision de l'Union européenne : construire une IA éthique, fiable et au service de la société.

Bénéfices attendus

Pour la société
L'**AI Act** offre des garanties sans précédent pour protéger les citoyens contre les usages abusifs ou risqués de l'intelligence artificielle. Grâce à des principes tels que la transparence, la lutte contre les biais et la protection des droits fondamentaux, les systèmes d'IA seront conçus pour :

- **Renforcer la confiance des utilisateurs** : informés et protégés, les citoyens peuvent interagir avec des technologies d'IA en toute sécurité.
- **Protéger la vie privée** : les exigences strictes en matière de gestion des données garantissent un respect accru de la confidentialité.

Pour les entreprises
L'**AI Act** crée des opportunités pour les entreprises innovantes tout en réduisant les incertitudes réglementaires :

- **Stimulation de l'innovation** : les bacs à sable réglementaires et les mesures de soutien aux PME permettent de tester et de développer des solutions novatrices dans un cadre sécurisé.
- **Accès au marché unique** : avec des règles harmonisées à l'échelle européenne, les entreprises bénéficient d'un environnement clair et prévisible pour déployer leurs produits.
- **Renforcement de la compétitivité** : les certifications et les garanties de conformité offrent aux entreprises un avantage concurrentiel, tant en Europe qu'à l'international.

Pour le marché intérieur
Le règlement contribue à l'unification et à la croissance du marché européen de l'IA :

- **Harmonisation des règles** : en supprimant les disparités entre les États membres, l'**AI Act** facilite les échanges et les collaborations transfrontalières.
- **Attractivité accrue** : l'Europe devient un environnement favorable pour les entreprises mondiales cherchant à développer des solutions d'IA éthiques et fiables.
- **Développement durable** : en mettant l'accent sur la durabilité et le bien-être sociétal, l'**AI Act** s'inscrit dans les objectifs à long terme de l'Union pour une croissance responsable.

Vision à long terme

Avec l'**AI Act**, l'Europe ambitionne de devenir le leader mondial en matière d'intelligence artificielle éthique et responsable. Ce règlement pose les bases d'un modèle qui pourrait inspirer d'autres régions du monde, en démontrant qu'innovation et protection des valeurs humaines ne sont pas incompatibles.
L'Europe se positionne comme un acteur incontournable de la gouvernance technologique globale, en encourageant :

- **Une IA centrée sur l'humain** : où les technologies servent les citoyens, plutôt que de les contrôler.
- **Une coopération internationale** : en travaillant avec d'autres régions pour harmoniser les normes et promouvoir des standards éthiques communs.

L'**AI Act** représente ainsi bien plus qu'un cadre réglementaire : c'est une vision d'avenir pour une intelligence artificielle au service de la société, où innovation et responsabilité avancent main dans la main. En investissant dans cette voie, l'Union européenne montre la voie pour bâtir un futur où la technologie améliore véritablement la vie de tous.

Et maintenant ?

Voici quelques actions envisageables afin de se prémunir de tout risque :

1. Faire un **diagnostic global** (cartographie des systèmes d'IA, classification ...)
2. Activer un **comité de pilotage** pluridisciplinaire
3. Adapter la compliance aux **nouvelles contraintes** (ajustement des procédures, formations ...)
4. Améliorer **la documentation** afin d'être irréprochable (traçabilité *by design*, logs de décision infalsifiables ...)
5. Mettre en place les éléments nécessaires à la **qualité de la donnée** et à la suppression d'éventuels biais
6. Anticiper la nécessité d'avoir recours à des « **organismes notifiés** » afin d'éviter la hausse inéluctable des prix quand la ressource sera très demandée
7. Actionner les leviers nécessaires afin d'être **éthique *by design*** (AIEO - AI Ethics Officer, *bias bounty* ...)
8. Profiter des **facilités** mises en place par les Etats membres (aides techniques, bacs à sable ...)
9. Rationaliser la gestion des **réglementations**
10. **Former et sensibiliser** le personnel sur ces sujets

In a nutshell, ne vous contentez pas de suivre, **soyez proactif : vous pourrez éviter des coûts et des risques**

Expertise IA chez SOFTEAM

SOFTEAM
UNE FILIALE DE DOCAPOSTE

Expertise IA Softeam

Filiale de Docaposte, Softeam a développé une forte expertise en IA au fil des années et, au-delà de cette expertise, a su tisser des liens forts au sein de notre écosystème.

Ainsi nous pouvons adresser tous vos besoins que ce soit la **mise en conformité avec l'AI Act** avec la mise en place d'une gouvernance idoine, la revue de vos architectures, la mise en qualité de vos données afin de les intégrer dans des processus liés à l'IA mais aussi l'intégration de briques du marché, le développement d'applications impliquant le développement de modèles de machine learning ad-hoc (Segmentation client, prédiction du churn, recommandation produit, reconnaissance d'objets etc.)

Nous sommes en **constante collaboration** pour ne pas dire symbiose avec d'autres acteurs comme OpenValue ou Probayes qui peuvent nous épauler sur certains aspects techniques (Databricks, modèles avancés)

Nous vous accompagnons avec une **approche pragmatique** – adaptée à votre niveau de maturité – afin de vous permettre de n'investir que sur le nécessaire dans l'optique de dégager un maximum de valeur et d'éviter l'éparpillement inhérent à la mise en place de nouvelles technologies dans un cadre non maitrisé.

Nous intervenons lors des différentes phases de gouvernance de vos projets afin d'avoir une cohérence et une vision commune : **diagnostic – conseil – implémentation / remédiation.**

Notre vision de l'AI Act

Nos experts sont les facilitateurs de **l'appropriation et l'intégration de l'AI Act**.

Comme toute mise en conformité, l'AI Act nécessite une **phase de compréhension, de formation et d'acculturation** afin de l'adopter et l'adapter à votre contexte, vos enjeux.

Nos équipes plurifonctionnelles (conseil, techniques mais aussi DPO/RSSI) vous accompagnent sur toutes les phases de mise en place : découvrir et cartographier les usages et les modèles (y compris ceux utilisant des GPAI), classifier les risques, définir la gouvernance et les rôles associés (jusqu'à un AIEO - AI Ethics Officer), documenter et effectuer la mise en œuvre de la traçabilité by design, mettre en qualité vos données (y compris la mitigation des biais), réaliser du red teaming et conduire des tests d'attaque, assister la définition d'une procédure de notification, gérer le « shadow AI », anticiper les problématiques liées à une éventuelle dépendance à des éditeurs (plan de réversibilité ...), vous préparer et vous accompagner lors des audits des organismes notifiés, et enfin vous soutenir dans l'obtention et l'usage de leviers d'appui (bacs à sable réglementaire, financements PME ...).

Le but de notre accompagnement est de rendre votre conformité plus simple : nous intégrons l'AI Act à votre gouvernance Data / Tech / conformité et aux autres obligations auxquelles vous pouvez faire face (RGPD, NIS2, ESG ...) de manière à ce que cette nouvelle contrainte ne soit pas un fardeau mais bien un avantage par rapport à vos concurrents qui n'auraient pas anticipé les changements.

Notre équipe

Nos experts sont formés tant via des certifications externes qu'en interne au sein de notre practice IA.

Des cadres expérimentés :
- Ayant déjà travaillé en environnement complexe et fortement réglementé engageant leur responsabilité
- Ayant déjà participé à et géré des projets pluridisciplinaires d'envergure (plusieurs M€)

Des consultants impliqués :
- Ayant fait le choix de rejoindre notre équipe IA

Présentation Softeam

Softeam est la filiale du conseil et services de Docaposte (Groupe La Poste).

Nous accompagnons les acteurs publics et privés dans la **mise en œuvre de leurs projets de transformation numérique**. En mobilisant des expertises sectorielles et technologiques, nous proposons une offre de conseil et de services créatrice de valeur, pour construire ensemble un **numérique responsable, durable et au service de l'intérêt général.**

Concrètement, cela se traduit dans notre attitude et dans nos engagements. Nous sommes **des partenaires de confiance** pour nos clients, en adoptant une posture d'écoute active et en coconstruisant des solutions qui répondent à leurs besoins spécifiques.

Nous sommes conscients que les défis auxquels nous faisons face sont complexes et évolutifs :
la force de notre collectif de consultants experts et engagés pour le bien commun est le socle de notre mission.

Ensemble, nous voulons faire du numérique un levier pour demain. Et cela commence justement par un bon accompagnement incluant l'IA.

Annexes

SOFTEAM
UNE FILIALE DE DOCAPOSTE

1. Extraits clés du réglement

Les annexes offrent des compléments détaillés aux chapitres précédents pour renforcer la compréhension des lecteurs et illustrer l'application concrète de l'**AI Act**. Elles comprennent des extraits clés du règlement, une liste exhaustive des pratiques interdites, et des études de cas pratiques.

1.1. Article 3 : définitions

- **Système d'IA** : tout logiciel développé à l'aide de techniques comme l'apprentissage automatique, les modèles logiques ou statistiques, qui produit des résultats influençant des environnements ou des utilisateurs.
- **Modèle d'IA à usage général** : un modèle d'IA puissant et polyvalent, capable de réaliser efficacement de nombreuses tâches différentes, même s'il est encore en phase de test ou de développement, sauf s'il est utilisé uniquement pour la recherche ou le prototypage avant sa mise sur le marché.

1.2. Article 5 : pratiques interdites

- Interdiction des systèmes exploitant des vulnérabilités des utilisateurs, comme la manipulation de mineurs ou de groupes vulnérables.
- Interdiction des systèmes de notation sociale appliqués à des individus.
- Interdiction de la surveillance biométrique en temps réel dans les espaces publics, sauf exceptions précises (e.g., menaces à la sécurité publique).

1.3. Article 10 : exigences relatives aux données

- Les systèmes d'IA doivent s'appuyer sur des données de qualité, pertinentes, représentatives et exemptes de biais.
- Obligation d'assurer la traçabilité et la documentation des données utilisées.

1.4. Article 57/58 : règles pour les bacs à sable

- Les bacs à sable permettent aux entreprises de tester des solutions innovantes avec une supervision des autorités nationales compétentes.
- Assouplissement des exigences dans un cadre sécurisé, avec un rapport final documentant les résultats des tests.

1.5. Article 99 : Sanctions

- Amendes pouvant atteindre 35 millions d'euros ou 7 % du chiffre d'affaires mondial pour les infractions les plus graves.
- Sanctions proportionnées pour les manquements moins critiques, mais dissuasives.

2. Liste des pratiques interdites

2.1. Manipulation cognitive ou exploitation de vulnérabilités

- Utiliser l'IA pour influencer les décisions des utilisateurs sans leur consentement éclairé.
- Exploiter des faiblesses spécifiques liées à l'âge, au handicap ou à des situations psychologiques.
  Exemple interdit : une application de jeux destinée aux enfants qui incite à des achats compulsifs par des mécanismes psychologiques.

2.2. Notation sociale

- Interdiction pour les autorités publiques ou privées de classifier les citoyens selon des critères comportementaux ou sociaux à des fins discriminatoires.
  Exemple interdit : une municipalité qui attribue des crédits sociaux influençant l'accès au logement ou à l'emploi public en fonction du comportement en ligne.

2.3. Surveillance biométrique abusive

- Interdiction de l'utilisation de la reconnaissance faciale en temps réel dans les espaces publics, sauf exceptions strictes (e.g., recherche de personnes disparues ou lutte contre le terrorisme, avec autorisation judiciaire).

  Exemple interdit : une caméra connectée utilisée pour surveiller les mouvements de population dans une gare sans autorisation préalable.

3. Études de cas illustrant les applications du règlement

Les études de cas suivantes montrent comment les principes et exigences de l'AI Act s'appliquent dans des scénarios réels.

3.1. Diagnostic médical assisté par IA

Contexte : une entreprise développe un système d'IA pour détecter les maladies cardiaques à partir d'imageries médicales. Ce système est classé comme à haut risque en raison de son impact sur la santé des patients.

Exigences réglementaires :

1. **Documentation technique** : l'entreprise doit fournir une description détaillée du système, des algorithmes utilisés et des limites potentielles.
2. **Analyse d'impact** : une analyse des biais dans les données d'entraînement est réalisée pour garantir que le système fonctionne pour toutes les populations.
3. **Certification** : le système doit passer un audit pour obtenir une certification avant sa mise sur le marché.

3.2. Chatbot interactif dans le service public

Contexte : un gouvernement souhaite déployer un chatbot pour fournir des informations sur les démarches administratives.
Classification : risque limité, car le chatbot n'a pas d'impact direct sur les droits fondamentaux.
Obligations :

1. **Transparence** : le chatbot doit informer les utilisateurs qu'ils interagissent avec un système d'IA.
2. **Formation des opérateurs** : les opérateurs doivent être formés pour intervenir en cas de problème ou d'escalade nécessaire.

Impacts :

- Le chatbot réduit les délais de réponse et améliore l'expérience des citoyens.
- Les utilisateurs savent qu'ils peuvent demander une assistance humaine si

3.3. Algorithme de recrutement

Contexte : une entreprise utilise un système d'IA pour trier les candidatures en fonction des compétences et des expériences des candidats.
Problème identifié : des biais dans les données historiques favorisent certains groupes au détriment d'autres.
Actions prises :

1. **Audit des données** : les données utilisées pour entraîner le modèle sont corrigées pour éliminer les biais.
2. **Supervision humaine** : les décisions finales sont prises par un recruteur humain, garantissant une égalité d'accès à l'emploi.
3. **Documentation** : une documentation détaillée des algorithmes et des ajustements est fournie.

Résultats : le système améliore l'efficacité du tri des candidatures tout en respectant les principes de non-discrimination.

Références

Toutes les références de ce livre sont consultables ici

SOFTEAM
UNE FILIALE DE DOCAPOSTE

SOFTEAM
UNE FILIALE DE DOCAPOSTE

Vous souhaitez échanger avec nos experts sur vos besoins d'accompagnement IA ?

Nos experts prennent (vraiment) le temps de vous écouter et comprendre vos enjeux, votre environnement et vos objectifs.

Contactez directement Cédric Autret via
cedric.autret@softeam.fr