Comprendre et anticiper le futur règlement européen sur l'intelligence artificielle

IMPACT AI

INTRODUCTION

Les risques associés à l'utilisation de techniques d'Intelligence Artificielle (IA) et notamment d'Apprentissage Automatique Statistique posent de nombreuses questions. Notamment, comment s'assurer qu'un modèle entraîné n'est pas utilisé en dehors de son domaine de validité, qu'il n'est pas biaisé, et que son utilisation ne pose pas de problème conséquent en termes de fiabilité, de sécurité, ou d'équité ?

Ces questions ont naturellement amené les organisations nationales et internationales de normalisation, les organismes de certification, et les gouvernements, à définir des normes, des référentiels, des règlements, dont le respect garantirait un usage "responsable" des techniques d'Intelligence Artificielle. Si les normes et référentiels de certification font parfois l'objet d'un choix volontaire de chaque acteur du domaine (permettant d'améliorer ses procédés de conception, développement, évaluation et maintenance des applications qu'il développe, et de donner un gage de qualité à ses clients et autres partenaires), les règlements issus par les Etats ont force de loi et devront impérativement être respectés. Certains secteurs imposent également des certifications réglementaires, tels que la santé ou les composants de sécurité, et l'IA présente dans ces dispositifs ne devra pas porter atteinte au respect des exigences spécifiques.

De très nombreuses initiatives de règlementation ont émergé ces dernières années afin de contrôler les impacts de l'IA dans les activités de différents secteurs industriels. Lancées en parallèle et avec parfois des objectifs et méthodes distinctes selon les secteurs, elles reflètent néanmoins des préoccupations en essence similaires. En avril 2021, la Commission Européenne a présenté sa proposition de réglementation sur l'IA. Il s'agit d'instaurer le tout premier cadre juridique sur l'IA au niveau mondial et constitue à ce jour le texte le plus avancé et le plus exigeant. Un texte de compromis est en cours de validation. Les amendements du Parlement Européen et les réunions entre des représentants du Parlement, du Conseil et de la Commission qui auront lieu début 2023 vont également modifier la proposition de texte, ce qui suggère une mise en application fin 2024 ou début 2025. Les différents acteurs du domaine disposent donc d'environ 2 ans pour assurer la mise en conformité de leurs processus.

L'objectif de ce document (kit) est de donner quelques clés de compréhension et recommandations aux acteurs se lançant ou en cours d'élaboration de leur démarche sur ce sujet. Il reflète la compréhension et l'expérience des membres du collectif Impact AI et complète les documents précédemment édités : le guide pratique pour une IA digne de confiance (2020) et les fiches pratiques pour une IA responsable (2022). 10 recommandations (commandements) pour la mise en conformité sont énoncées, suivies par de multiples informations utiles pour avancer dans la démarche.

Au-delà de l'aspect réglementaire, nos membres investissent dans le développement et favorisent l'usage de l'IA responsable et de confiance pour assurer un impact positif de l'IA sur la durée. Rejoignez-nous pour contribuer au développement d'une intelligence artificielle éthique et responsable en France !

A propos d'Impact AI

Impact AI est le Think & Do Tank de référence pour l'intelligence artificielle éthique en France. Notre mission est de fédérer l'ensemble des acteurs de l'écosystème : entreprises, startups, institutions, organismes de recherche ou de formation, acteurs de la société civile, pour faire avancer les usages, partager l'état de l'art et favoriser l'adoption de l'IA responsable. Plus d'informations sur www.impact-ai.fr

Dix recommandations pour la mise en conformité de l'IA

IMPACT AI

1. Choisir une définition de l'IA et définir le périmètre des systèmes IA à considérer

A l'heure actuelle, les différents règlements en cours de rédaction utilisent chacun leur propre définition de ce qu'est une IA. En attendant leur souhaitable convergence, nous recommandons à chaque acteur de choisir une définition parmi les définitions existantes et de l'utiliser pour délimiter l'ensemble des applications à mettre en conformité. Une première approche peut consister à cibler les systèmes à base d'apprentissage automatique (machine learning) ou les systèmes d'IA définis et répertoriés dans la liste fournie à l'annexe III de l'AI ACT mise à jour régulièrement par la Commission européenne.

Pour aller plus loin :

- ➔ Découvrez la définition de l'IA et les principes sur l'IA de l'OCDE
- ➔ Glossaire IA

2. Dresser et maintenir un inventaire des systèmes à base d'IA

L'étape suivante consiste à établir un inventaire des solutions développées ou utilisées (systèmes et cas d'usage) et attribuer les responsabilités en termes de mise en conformité. La mise en place d'une procédure permettant de répertorier les nouveaux systèmes d'IA potentiels est également nécessaire.

3. Sensibiliser aux risques et aux limites de l'IA ciblés par l'AI Act et les autres réglementations

En pratique, les contraintes imposées par l'AI Act ou les autres réglementations vont devoir s'appliquer tout au long du cycle de vie des applications, de la conception à la maintenance, et concerner tant les concepteurs d'IA que les utilisateurs, les distributeurs ou encore les fournisseurs. Les services supports (juridique, qualité, achats, ...) seront aussi concernés par ces réglementations. Il est donc nécessaire de sensibiliser l'ensemble des parties prenantes concernées au contenu de ces réglementations et aux règles de fonctionnement que leur respect imposera.

Pour aller plus loin :

- ➔ AI ACT - Que faut-il savoir ?
- ➔ Comment l'AI Act vous impacte ? une étude Deloitte
- ➔ Q&A : les nouvelles règles encadrant l'intelligence artificielle
- ➔ La proposition du règlement européen sur l'intelligence artificielle
- ➔ La réponse collective d'Impact AI au projet de règlementation européenne sur l'IA publiée le 06.08.2021 ici.
- ➔ Les autres règlementations liées à l'IA :
    - Cyber Resilience Act
    - Data Gouvernance Act
    - Data Act
    - Liability Rules for Artificial Intelligence

4. Mettre en place un processus de gestion du risque

La gestion du risque est un élément crucial pour assurer la conformité réglementaire d'un système d'IA. Pour chaque système, il sera donc nécessaire d'établir une stratégie permettant d'identifier les risques associés à son utilisation, d'estimer la criticité de ces risques, et de mettre en place des stratégies adaptées pour leur traitement. Les processus doivent être mis en place et appliqués dès les premières

étapes de la conception des systèmes. L'analyse de risque doit être mise à jour à chaque étape de développement du système d'IA. Toutes les personnes impliquées dans le développement doivent y être sensibilisées. Le choix d'outils adaptés, selon les types de risques à traiter, est aussi à considérer.

Pour aller plus loin :

- ➔ Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment
- ➔ Un article sur le standard ISO pour la gestion des risques liés à l'IA en cours d'élaboration
- ➔ Un cadre de gestion de risque proposé par NIST
- ➔ Un standard IA responsable proposé par Microsoft
- ➔ La certification des processus pour l'IA proposée par LNE

5. Identifier les risques spécifiques à chaque système d'IA

L'une des étapes essentielles de la gestion du risque nécessitera l'identification des risques associés à l'utilisation et au maintien en conditions opérationnelles du système d'IA. Ces risques devront prendre en compte autant les aspects liés à la sécurité et la cybersécurité, que le respect des droits fondamentaux des personnes impactées (équité, non-discrimination, etc.). Il ne s'agira donc pas seulement de repérer les potentielles sous-performances de l'IA, mais bien de se focaliser sur les comportements qui pourraient avoir un impact préjudiciable. L'identification du risque devra être documentée et structurée, de façon à pouvoir guider efficacement le traitement du risque.

Pour aller plus loin :

- ➔ Quelques exemples des méthodes d'analyse de risque
- ➔ Un modèle d'analyse d'impact et le guide d'utilisation proposé par Microsoft

6. Définir une approche sur le stock (systèmes d'IA déjà déployés) pour mettre en conformité

En parallèle, il sera nécessaire de vérifier ou mettre en conformité les systèmes d'IA déjà déployés. La démarche doit être définie et un planning global établi afin d'atteindre l'objectif de mise en conformité dans les temps impartis. Commencer par qualifier et si possible quantifier le niveau de risque des systèmes pour aider à prioriser les actions à mener afin d'assurer que les systèmes les plus importants sont traités dans l'ordre approprié.

7. Mettre en place et contrôler l'usage des bonnes pratiques

Le cadre règlementaire et normatif pour l'IA étant en cours de création, il n'existe pas aujourd'hui de méthodes d'audit ou de certification garantissant la conformité au règlement européen sur IA. Dans les cas d'usage à risque élevé, selon la catégorisation adoptée par l'AI Act par exemple, il est préférable et potentiellement moins coûteux d'adopter au plus tôt les bons réflexes en matière de conception et de gouvernance des applications d'IA, plutôt que de devoir tout repenser à l'entrée en vigueur du règlement sur l'IA ou en réaction à un dommage causé. Des outils existent pour favoriser l'usage de l'IA responsable et de confiance. Il est serait astucieux de mettre en place un référentiel d'IA Responsable au niveau de l'entreprise avec une charte éthique, un code de conduite, des principes partagés, etc. L'accompagnement peut être réalisé par des organismes tiers, capables d'auditer les méthodes mises en œuvre dans l'entreprise et proposer des recommandations d'ajustement permettant d'améliorer, par exemple, la traçabilité documentaire, la gestion des données ou les méthodes de gestion du risque.

Pour aller plus loin :

➔ Boîte à outils Impact AI
➔ Le guide IA de confiance et les Fiches pratiques Impact AI

8. Former les personnes concernées

Au-delà de la sensibilisation initiale, les personnes concernées devront être formées aux méthodes d'analyse et de traitement des risques mises en place. Cela peut commencer par acculturation aux enjeux éthiques, à la gestion des risques et aux obligations réglementaires. Lorsque le traitement des risques nécessite l'utilisation d'outils, les personnes en charge de ce traitement devront être formées à l'utilisation de ces outils et à la bonne interprétation de leurs résultats.

Pour aller plus loin :

➔ Regardez les formations suivantes :

- Objectif IA - Une formation gratuite accessible en ligne
- AI Business School pour les dirigeants d'entreprises
- Le catalogue de formations en IA proposé par Impact AI
- Consulter la liste des formations à l'IA responsable proposée par Impact AI
- Study Harvard publication on principled AI
- Formation Digital Ethics - Good Algo
- Formations LNE sur l'évaluation
- Les contenus explor'IA

9. Faire de la veille règlementaire et technologique

Comme déjà indiqué, les règlements sont loin d'être figés. Les différentes propositions vont évoluer, idéalement devenir plus cohérentes entre elles et imposer des obligations proportionnées aux risques à traiter. Par ailleurs, de nombreux acteurs développent des outils susceptibles de contribuer à l'amélioration des systèmes et des processus en vue de l'arrivée de l'AI Act.

Pour aller plus loin :

➔ Quelques recommandations pour obtenir des informations sur l'évolution de la politique d'IA dans l'Union Européenne, sur l'évolution de la liste des cas d'usage à haut-risque et sur les outils :

- Newsletter ActuIA
- DataEthics.eu Newsletter
- Le bulletin d'information EuropeanAI

10. Comprendre et suivre la préparation des normes, des certificats et des labels

Les normes peuvent être considérées comme des guides techniques pour la conception ou le test d'un produit. Respecter une norme peut alors représenter un certain gage de qualité, et les normes dites "harmonisées" (reconnues au Journal Officiel) permettront d'obtenir présomption de conformité à l'AI Act. Faire apposer un label ou une certification volontaire sur son système d'IA ou ses processus liés au développement de ce dernier peut rassurer ses clients ou utilisateurs finaux. Toutefois, il est essentiel de comprendre le caractère obligatoire ou volontaire de tous ces outils, leur articulation, ainsi que leur valeur apportée pour la réussite de la commercialisation des applications IA.

Pour aller plus loin :

➔ Normalisation, qui est concerné ? Présentation AFNOR
➔ Une présentation pour comprendre les standards et les certificats
➔ Pour aller plus loin sur les certifications, les labels et les normes vous pouvez lire cet article

15 DÉCEMBRE 2022