SIAPARTNERS

2021

Artificial Intelligence Act
Que faut-il savoir?

Sophie Le Goff

Partner Assurance et Conformité

+ 33 6 15 29 31 83

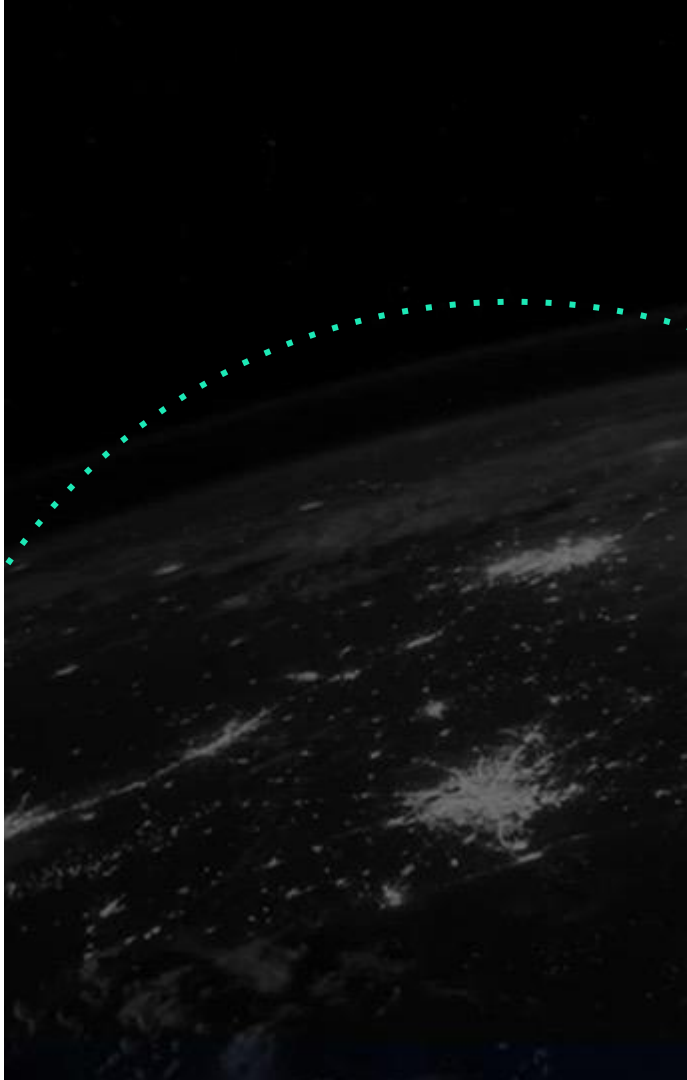
Sophie.le-goff@sia-partners.com

Jeanne Fourcade

Supervising senior Conformité

+ 33 6 82 08 26 71

Jeanne.fourcade@sia-partners.com



Artificial Intelligence Act - Introduction

Objectifs principaux:

- Veiller à ce que les systèmes d'IA mis sur le marché européen soient sûrs et respectent les droits fondamentaux des citoyens et les valeurs de l'UE
- Garantir la sécurité juridique pour faciliter l'investissement et l'innovation dans l'IA
- Renforcer la gouvernance et l'application effective de la législation existante sur les droits fondamentaux et les exigences de sécurité applicables aux systèmes d'IA
- Faciliter le développement d'un marché unique pour les applications d'IA légales, sûres et dignes de confiance et prévenir la fragmentation du marché

Amendes:

Jusqu'à **2, 4 ou 6% du chiffre d'affaires annuel mondial** , en fonction des violations constatées. Les États membres sont responsables de la conception de leur régime de sanctions.

Autorités de contrôle:

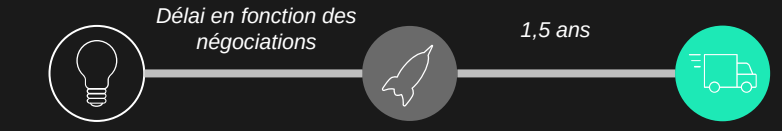
Comité européen de l'intelligence artificielle

A définir

Entreprises cibles:

- Les fournisseurs qui distribuent ou proposent des systèmes d'IA dans l'Union, que ces fournisseurs soient établis dans l'Union ou dans un pays tiers
- Les utilisateurs de systèmes d'IA situés dans l'Union européenne
- Les fournisseurs et utilisateurs de systèmes d'IA situés dans un pays tiers, où la production produite par le système est utilisée dans l'Union

Agenda:



Règlementations liées:

Le règlement sur l'IA fait partie du paquet européen de réglementation sur les données et est donc liée au DSA, DGA, DMA, etc. mais aussi au RGPD.

Artificial Intelligence Act - Apports clés

OBLIGATIONS BASÉES SUR DES CATEGORIES DE RISQUES

Les obligations prévues par le texte dépendent du niveau de risque du système d'IA utilisé (non-acceptable, élevé ou non élevé) et de l'acteur concerné (fournisseur, distributeur, utilisateur, autres). Il existe également des obligations spécifiques pour les importateurs de systèmes d'IA à risque élevé dans l'UE.

REGULATORY SANDBOXES

Les autorités nationales compétentes peuvent mettre en place des « regulatory sandboxes » qui établissent un environnement contrôlé pour tester les technologies innovantes pendant une durée limitée. Ces sandboxes sont basées sur un plan d'essai convenu avec les autorités compétentes en vue d'assurer la conformité du système d'IA et d'accélérer l'accès aux marchés. Les PME et les start-ups peuvent y avoir un accès prioritaire.

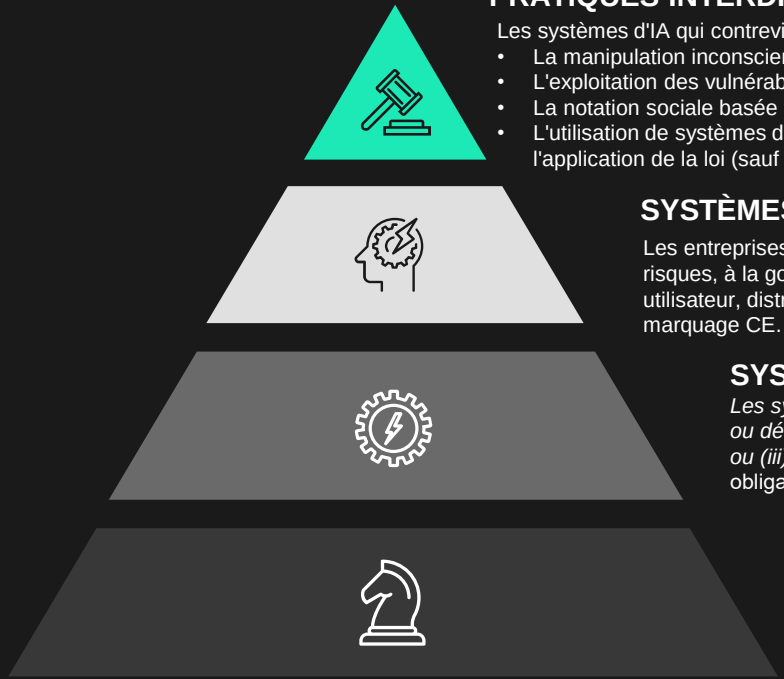
LISTE DES SYSTÈMES D'IA À RISQUE ÉLEVÉ

La liste des systèmes à risque élevé est définie et mise à jour par la Commission Européenne pour refléter l'évolution rapide des technologies.

MARQUEUR CE ET ENREGISTREMENT

Le règlement sur l'IA crée un marqueur CE pour les systèmes d'IA à risque élevé. Ce marqueur est obligatoire et est fourni par des organismes désignés. Il existe également une obligation d'enregistrer les systèmes autonomes d'IA à risque élevé dans une base de données européenne.

Artificial Intelligence Act - Impacts



PRATIQUES INTERDITES EN MATIÈRE D'INTELLIGENCE ARTIFICIELLE

Les systèmes d'IA qui contreviennent aux valeurs de l'Union européenne en violant les droits fondamentaux sont interdits, tels que :

- La manipulation inconsciente des comportements
- L'exploitation des vulnérabilités de certains groupes pour influencer leur comportement
- La notation sociale basée sur l'IA à des fins générales par les autorités publiques
- L'utilisation de systèmes d'identification biométrique à distance "en temps réel" dans des espaces accessibles au public pour l'application de la loi (sauf exceptions)

SYSTÈMES À RISQUE ÉLEVÉ *(définis et répertoriés par la Commission européenne)*

Les entreprises sont soumises à plusieurs obligations liées à la documentation, au système de gestion des risques, à la gouvernance, à la transparence ou à la sécurité, en fonction de leur qualification (fournisseur, utilisateur, distributeur et autres tiers). Ces systèmes doivent également être déclarés à l'UE et porter un marquage CE. *Voir page suivante.*

SYSTÈMES PRESENTANT DES RISQUES SPÉCIFIQUES

Les systèmes qui (i) interagissent avec les humains, (ii) sont utilisés pour détecter des émotions ou déterminer l'association avec des catégories (sociales) basées sur des données biométriques, ou (iii) générer ou manipuler du contenu (`` deep fakes ''). Pour ces systèmes, il existe une obligation d'information si le contenu est généré par des moyens automatisés ou non.

SYSTÈMES SANS RISQUE ÉLEVÉ

Création et application volontaires d'un code de conduite pouvant inclure des engagements relatifs à la durabilité environnementale, à l'accessibilité pour les personnes handicapées, à la participation des parties prenantes à la conception et au développement des systèmes d'IA et à la diversité des équipes de développement.

Artificial Intelligence Act - Focus sur les systèmes à risque élevé (1/2)

Systèmes à risque élevé

- Composant de sécurité d'un produit ou produit nécessitant une évaluation de conformité par un tiers conformément aux réglementations existantes (Dir 2009/48/EC sur la sécurité des jouets, Reg 2016/424/EU sur les téléphériques, etc)

Liste fournie à l'annexe III

- Identification biométrique et catégorisation de personnes physiques
- Gestion et exploitation des infrastructures critiques
- Éducation et formation professionnelle
- Emploi, gestion des travailleurs et accès au travail indépendant
- Accès et jouissance des services privés essentiels et des services et avantages publics
- Application de la loi
- Gestion de la migration, de l'asile et contrôle aux frontières
- Administration de la justice et processus démocratiques

NB: cette liste peut être régulièrement mise à jour par la Commission européenne

SYSTÈME DE GESTION DES RISQUES

Processus itératif continu exécuté tout au long du cycle de vie d'un système d'IA à risqué élevé (identification, évaluation des risques et adoption et test des mesures de remédiation des risques)

PRÉCISION, ROBUSTESSE ET CYBERSÉCURITÉ

Mise en œuvre des mesures et information dans les instructions

DONNÉES ET GOUVERNANCE DES DONNÉES

Formation, validation et test des ensembles de données répondant aux critères de qualité

CONTRÔLE HUMAIN

Assurer la surveillance par des personnes physiques pendant la période d'utilisation du système d'IA

DOCUMENTATION TECHNIQUE

Démonstration de la conformité aux exigences du système d'IA à risqué élevé

TRANSPARENCE ET INFORMATION DES UTILISATEURS

Conception transparente et instructions pour les utilisateurs

TENUE DE REGISTRES D'ACTIVITE

Conception et développement permettant l'enregistrement automatique des événements

Artificial Intelligence Act - Focus sur les systèmes à risque élevé (2/2)

	OBLIGATIONS DES FOURNISSEURS	OBLIGATIONS DES DISTRIBUTEURS	OBLIGATIONS DES UTILISATEURS
EXIGENCES GÉNÉRALES	• S'assurer que le système est conforme (voir la page précédente) • Prendre les mesures correctives nécessaires si le système d'IA à risque élevé n'est pas conforme	• Pas de distribution d'un système à risque élevé non conforme et si le système d'IA à risque élevé est déjà sur le marché, prendre des mesures correctives • Les conditions de stockage ou de transport ne doivent pas compromettre la conformité du système aux exigences • Vérifier que le système IA à risque élevé porte le marquage de conformité CE requis	• S'assurer de la pertinence des données entrées dans le système • Arrêter l'utilisation du système s'il est considéré comme présentant des risques pour la santé, la sécurité, pour la protection des droits fondamentaux, ou en cas d'incident grave ou de dysfonctionnement
PROCESSUS	• Disposer d'un système de gestion de la qualité (stratégie, procédures, ressources, etc.) • Rédiger la documentation technique • Évaluer la conformité • Déclaration UE et marqueur CE • Concevoir et développer des systèmes avec des capacités permettant l'enregistrement automatique des événements • Conserver les journaux générés automatiquement par le système • Mettre en place et documenter un système de suivi post-commercialisation	• Contrôle par des tiers: vérifier que le fournisseur et l'importateur du système sont en conformité vis-à-vis des obligations énoncées dans le présent règlement et que des mesures correctives ont été prises si besoin	• Conserver les journaux automatiquement générés par le système s'ils sont sous leur contrôle
TRANSPARENCE & INSTRUCTIONS	• Concevoir des systèmes transparents • Rédiger un mode d'emploi	• S'assurer que le système d'IA est accompagné du mode d'emploi et de la documentation requise	• Obligation d'utiliser et de surveiller les systèmes en suivant les instructions d'utilisation accompagnant les systèmes
INFORMATION & INSCRIPTION	• Obligation d'informer les autorités nationales compétentes en cas de risques pour la santé, la sécurité, pour la protection des droits fondamentaux ou en cas d'incidents graves et de dysfonctionnements • Enregistrer le système dans la base de données de l'UE	• Obligation d'informer le fournisseur / importateur d'un système à risque élevé non conforme et les autorités nationales compétentes	• Obligation d'informer le fournisseur / distributeur, ou l'autorité de surveillance du marché, si l'utilisateur n'est pas en mesure de joindre le fournisseur et que les systèmes présentent des risques pour la santé, la sécurité, pour la protection des droits fondamentaux des personnes sont concernés