Temps de lecture estimé : 8 minutes

Le règlement européen sur l'intelligence artificielle[1] ou **AI Act** a été conçu pour encadrer le développement et la mise sur le marché de systèmes d'intelligence artificielle (ci-après SIA) au sein de l'Union européenne, de façon à protéger les droits humains et la sécurité des utilisateurs. L'objectif de l'AI Act est d'aboutir à une IA « **digne de confiance** ». Il concerne toutes les entreprises qui fournissent ou utilisent des SIA.

Entré en vigueur le 1er aout 2024, l'AI Act se précise mois après mois, au gré des **lignes directrices fournies par la Commission** ; il est amené à évoluer très prochainement, la publication d'un paquet de mesures **omnibus sur le numérique** étant imminente. A l'heure où nous écrivons ces lignes, nous ne savons pas ce que contiendra cette proposition, qui sera soumise à l'adoption de la Commission à la fin de l'année. Elle devrait prévoir quelques ajustements ciblés et peut-être le report de certaines dates d'entrée en application, sans toutefois remettre en cause les notions fondamentales qui seront abordées ici.

La majorité des entreprises étant des « **déployeurs** » de SIA plutôt que des « fournisseurs », nous avons choisi de revenir sur quelques **notions clés** les concernant et sur leurs **obligations**. Nous proposerons pour finir un **plan d'attaque** pour aider les entreprises à se mettre en conformité avec ce texte exigeant.

Quand est-on un déployeur ?

Rappelons d'abord que les utilisateurs finaux ne sont pas des déployeurs.

[1] Règlement (UE) 2024/1689.

Un déployeur est « une personne physique ou morale, une autorité publique, une agence ou un autre organisme **utilisant un système d'IA sous son autorité**, sauf si le système d'IA est utilisé dans le cadre d'une activité personnelle non professionnelle » (article 3 al. 4 du RIA).
L'indication « sous sa propre autorité » est utile pour écarter du périmètre les simples utilisateurs (employés, clients qu'ils soient professionnels ou particuliers) qui n'ont aucun contrôle sur le SIA.

Exemple
Un client B2B qui utilise le chatbot déployé par un acteur de la distribution ne détient pas ce contrôle : il peut poser des questions, mais c'est le distributeur qui paramètre l'assistant virtuel et fait évoluer son fonctionnement. C'est bien le distributeur qui sera reconnu comme déployeur, et non le client.

Il convient également de distinguer le statut de déployeur de celui de fournisseur car les obligations diffèrent sensiblement.

Le fournisseur est celui qui conçoit ou développe un SIA et le met sur le marché. Le déployeur (l'organisation utilisatrice) acquiert le système d'IA pour l'utiliser, le mettre à disposition de ses employés ou de ses clients, dans le cadre de ses usages.

***Remarque** : le statut de déployeur n'est pas immuable. Si l'entreprise apporte une « modification substantielle » ou appose son nom ou sa marque à un SIA à haut risque existant, l'entreprise devient fournisseur de ce SIA.*

Le fournisseur est le principal responsable du SIA mais le déployeur n'est pas exempt d'obligations, bien au contraire. Ses obligations varient en fonction du niveau de risque du ou des SIA déployés.

Classification des systèmes IA par niveaux de risque

Le règlement répartit les systèmes d'IA en quatre niveaux de risque afin d'orienter les obligations.

1. **Systèmes d'IA à risque inacceptable** : tout SIA qui porte atteinte aux droits fondamentaux, comme les systèmes de notation sociale ou ceux recourant à des techniques subliminales. Le développement de tels SIA est purement et simplement interdit.

2. **Systèmes d'IA à haut risque** : tout SIA qui peut avoir une incidence négative sur la sécurité des personnes ou sur leurs droits fondamentaux. Cette catégorie inclut par

exemple les logiciels médicaux fondés sur l'IA, les SIA utilisés pour le recrutement et les systèmes d'identification biométrique à distance.

3. **Systèmes à risque limité** : tout SIA qui interagit directement avec des personnes physiques. Ces SIA sont soumis à des obligations de transparence vis-à-vis des utilisateurs qui doivent être informés lorsqu'ils interagissent avec un chatbot ou un système génératif.

4. **Systèmes à risque minimal** : **pour tous les autres systèmes d'IA, le RIA ne prévoit pas d'obligations spécifiques.** Il s'agit de la très grande majorité des systèmes d'IA actuellement utilisés dans l'UE ou susceptibles de l'être selon la Commission européenne.

Des obligations étendues pour les déployeurs de SIA à haut risque

La majorité des obligations définies par l'AI Act concernent essentiellement les SIA à haut risque. Un déployeur de SIA à haut risque doit pouvoir garantir une utilisation sûre et conforme de ces technologies. Il doit pour cela :

- Déployer un **système de gestion des risques** (définition d'une méthodologie d'évaluation des risques et de suivi de leur remédiation),

- Déployer un système de gestion de la qualité en structurant **des mesures techniques et organisationnelles** appropriées tout au long du cycle de vie du SIA – en tant que déployeur, il conviendra notamment de demander aux fournisseurs une documentation technique claire sur le fonctionnement des SIA, ses limites et ses performances,

- Mettre en place des **mesures de surveillance humaine** de façon à détecter et traiter les dysfonctionnements inattendus et conserver une certaine vigilance quant aux biais d'automatisation,

- Veiller à ce que les **données d'entrée** dont se nourrissent les systèmes soient pertinentes pour limiter les risques et éviter les résultats discriminatoires,

- Produire et maintenir à jour une **documentation** détaillée pouvant être remise aux autorités, et fournir des informations claires aux utilisateurs.

- Informer les fournisseurs, les importateurs ou distributeurs, ainsi que les autorités de surveillance compétentes **en cas de risque ou d'incident grave**.

S'agissant des autres SIA (les SIA « à risque limité »), les principales obligations des déployeurs ont trait à la **transparence**. Il s'agit d'informer de manière claire les personnes concernées lorsqu'elles interagissent avec un SIA ou lorsqu'un contenu généré par une IA leur est présenté. Ainsi, sans être exhaustif :

- Les déployeurs doivent informer les personnes exposées aux SIA qui utilisent leurs données personnelles pour détecter des émotions ou qui comportent un système de catégorisation biométrique ;

- Lorsqu'un texte concernant un sujet d'intérêt public a été généré par une IA, le déployeur doit l'indiquer, à moins que le texte ait fait l'objet d'un processus d'examen humain ou d'un contrôle éditorial.

Une proposition de trajectoire en 10 étapes

Nous venons de le voir, les obligations pour les déployeurs de SIA à haut risque et il n'est pas évident de savoir par où commencer pour répondre aux attentes du régulateur. Nous proposons donc ici une trajectoire de mise en conformité en 10 étapes pour les entreprises qui ne se seraient pas encore emparées du sujet.

1. Nommer un **pilote**. Celui-ci doit avoir une solide compréhension de l'AI Act et des règlementations associées (RGPD en tête), ainsi qu'un réel intérêt pour les enjeux technologiques liés à l'intelligence artificielle.

2. Mettre en place une **comitologie** : former un comité de gouvernance de l'IA en incluant des représentants des départements concernés (par exemple, juridique et conformité, cybersécurité et IT, risques et contrôle interne, opérations).

3. Elaborer une **politique** facilement consultable et pragmatique énumérant les principes et les règles d'or en la matière.

4. **Cartographier** les SIA utilisés et analyser leur niveau de risques, en évaluant pour chaque système sa finalité, son secteur d'application et son impact potentiel sur les droits des individus. Déterminer pour chaque SIA le rôle de l'organisation (fournisseur, déployeur ou autre) et en déduire les obligations à respecter.

5. Construire un **RACI** afin de garantir une gestion des SIA conforme à la politique élaborée.

6. Sensibiliser les équipes au travers de **sessions de formation** rappelant les obligations de l'AI Act mais aussi les enjeux éthiques.

7. Déployer les **mesures organisationnelles et techniques** permettant de se conformer à la réglementation (voir plus haut dans l'article).

8. S'assurer du respect de la règlementation par les fournisseurs de SIA à haut risque.

9. Elaborer et diffuser une **procédure de gestion des contestations** à destination des utilisateurs.

10. S'assurer de la mise œuvre des règles prévues dans la politique au travers de **missions d'audit interne.**

Pour conclure

L'AI Act nous impose une vigilance accrue, aussi bien sur le plan technique qu'organisationnel, afin de garantir la sécurité, la transparence et le respect des droits fondamentaux des utilisateurs.

C'est seulement au travers d'une approche collaborative, que les acteurs économiques pourront non seulement répondre aux obligations légales, mais aussi instaurer une culture de confiance autour de l'IA. L'anticipation, la pédagogie et la documentation seront les clés pour transformer cette contrainte réglementaire en une opportunité d'innovation responsable et durable.