AI ACT

GUIDE À L'USAGE DES PROFESSIONNELS DE L'INTELLIGENCE ARTIFICIELLE

IMPALAVOCATS
AVOCATS À LA COUR

AVANT-PROPOS

Ce guide pratique a pour ambition de répondre à deux questions que tous les acteurs de l'IA se posent en 2024 :

- Dans quelle mesure suis-je concerné par le Règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (« AI Act » ou « Règlement ») ?
- Comment m'y préparer ?

L'Intelligence Artificielle (IA), générative en particulier, est considérée comme une révolution technologique incontournable par la commission dédiée à l'IA en France. Malgré cette reconnaissance, les petites et moyennes entreprises (TPE/PME) semblent avoir du mal à adopter cette technologie. Selon une étude de BPI France, réalisée à la fin de l'année dernière et portant sur plus de 3000 dirigeants de ces entreprises, seuls 15% utilisent l'IA générative, dont seulement 3% de manière régulière[1].

Les raisons de cette réticence sont diverses. Premièrement, la plupart des petits patrons ne comprennent pas comment l'IA générative pourrait bénéficier à leur entreprise ou à leur activité. Deuxièmement, ils manquent d'expertise dans ce domaine, ce qui les empêche de saisir les opportunités offertes par cette technologie. En outre, il existe des craintes concernant le mauvais usage des outils d'IA, notamment en ce qui concerne la sécurité des données et la diminution de la capacité des salariés à raisonner.

Pourtant, pour les quelques TPE/PME qui ont franchi le pas, les bénéfices sont tangibles (économies sur les services d'une agence de communication, de traduction etc.).

Par le cadre qu'il impose, l'AI Act vise à encourager le recours à l'IA pour tous les opérateurs économiques en instaurant plus de transparence et plus de garanties.

Initialement axé sur la sécurité des produits, l'AI Act a évolué pour prendre en compte les défis posés par les systèmes d'IA générative comme ChatGPT. Cette évolution a conduit à un texte complexe[2], divisé en trois volets, abordant la protection des droits fondamentaux, la sécurité des produits et la régulation des modèles d'IA à risque.

Le premier volet se concentre sur la définition des systèmes d'IA et la protection des droits fondamentaux, avec des obligations de transparence et de limitation d'impact

[1] https://www.francetvinfo.fr/replay-radio/c-est-mon-boulot/les-tpe-et-pme-reticentes-face-aux-intelligences-artificielles-generatives_6412462.html

[2] L'IA Act déjà obsolète face aux IA de nouvelle génération ? L'exemple de ChatGPT, Juliette Sénéchal, Professeur à l'Université de Lille, Dalloz février 2023

sur lesdits droits fondamentaux. Ainsi, les pratique d'IA manipulatrices et les risques pour les individus sont interdits, des mesures de transparence sont imposées pour les interactions entre humains et IA.

Le deuxième volet définit les systèmes d'IA à haut risque et établit des obligations pour les opérateurs économiques impliqués dans leur mise sur le marché. Des critères spécifiques déterminent quels sont ces systèmes à haut risque, déclenchant des obligations de conformité et de certification.

Le troisième volet aborde les modèles d'IA à risque systémique, comme ChatGPT, et s'inspire du Digital Services Act[3] pour imposer des obligations de diligence aux fournisseurs de modèles d'IA, y compris la transparence et l'évaluation des risques systémiques.

QUELS SONT LES OBJECTIFS DE L'AI ACT ?

L'AI Act est une législation européenne visant à établir un cadre pour la responsabilité des acteurs et utilisateurs de l'intelligence artificielle.

La loi sur l'intelligence artificielle vise à instaurer un cadre de confiance. Même si la plupart des systèmes d'IA ne présentent aucun risque et peuvent contribuer à résoudre divers problèmes sociaux, certains systèmes engendrent des risques nécessitant une intervention pour éviter des conséquences indésirables.

Par exemple, il est souvent difficile de comprendre les raisons sous-jacentes à une décision ou une prédiction spécifique prise par un système d'IA, rendant complexe l'évaluation d'une éventuelle injustice, comme dans le cas d'une décision d'embauche ou d'une demande de régime d'utilité publique.

Bien que la législation en place offre une certaine protection, elle se révèle insuffisante pour relever les défis particuliers présentés par les systèmes d'IA.

L'AI Act vise à garantir que les systèmes et modèles d'intelligence artificielle commercialisés au sein de l'Union européenne soient utilisés de manière éthique, sûre et respectueuse des droits fondamentaux de l'UE.

Ce premier objectif doit se concilier avec un second objectif a priori antagoniste : encourager l'expérimentation continue et permettre le développement de l'innovation pour que l'UE reste compétitive sur la scène internationale. La Vice-Présidente de l'UE, Margrethe Vestager, déclarait lors de la présentation du projet qu' « avec ces règles qui feront date, l'UE prend l'initiative d'élaborer de nouvelles normes mondiales qui garantiront que l'IA soit digne de confiance. En matière d'intelligence artificielle,

[3] Voir DSA – Guide pratique à l'usage des professionnels du numérique, Impala Avocats, février 2023

la confiance n'est pas un luxe, mais une nécessité absolue » (https://ec.europa.eu/commission/presscorner/detail/fr/ip_21_1682).

L'AI Act s'inscrit dans une logique prospective, ce qui la distingue des réglementations habituelles qui établissent des règles pour des situations déjà connues. Elle anticipe ainsi les différents cas d'usage que l'IA pourrait faire éclore et instaure des règles à la croisée du droit et de l'éthique en fondant son approche sur les risques.

CONCRÈTEMENT, QU'EST-CE QUE LE RÈGLEMENT VA CHANGER ?

L'AI Act crée une réglementation à laquelle les professionnels du secteur vont devoir se conformer pour pouvoir développer et commercialiser leurs systèmes d'IA.

Dans les grandes lignes, les règles instaurées par l'AI Act visent à :

1. Aborder de manière ciblée les risques engendrés par les applications d'intelligence artificielle.
2. Établir une liste d'applications considérées à haut risque.
3. Définir des exigences claires pour les systèmes d'IA utilisés dans les applications à haut risque.
4. Énoncer des obligations spécifiques à l'égard des utilisateurs d'IA et des fournisseurs d'applications à haut risque.
5. Proposer une évaluation de la conformité préalable à la mise en service ou à la mise sur le marché d'un système d'IA.
6. Proposer des directives pour l'application après la mise sur le marché d'un tel système d'IA.
7. Présenter une structure de gouvernance tant au niveau européen que national.

Pour se conformer au cadre réglementaire, les professionnels de l'IA vont devoir définir une stratégie propre ainsi qu'une feuille de route des actions à mener.

QUI DOIT SE CONFORMER ?

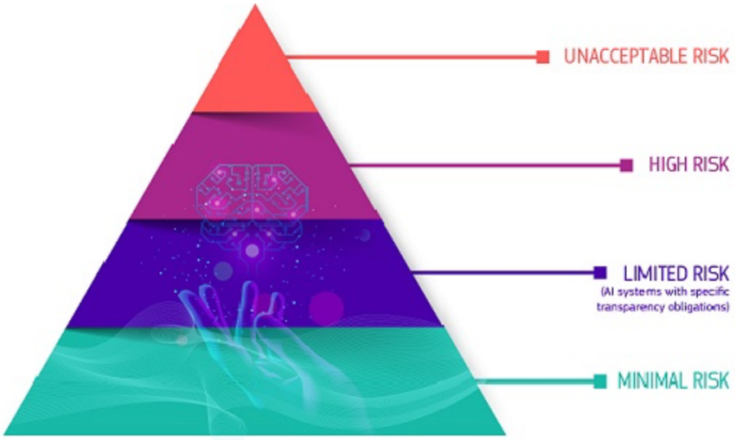
Tous les opérateurs économiques dont le siège social se situe dans l'Union européenne, ou lorsque le siège social est situé en dehors de l'Union européenne, s'ils commercialisent leur système ou modèle d'IA dans l'Union européenne.

Les activités de recherche, sans objectif commercial, ne sont pas concernées.

TOUS LES SYSTEMES D'IA SONT-ILS CONCERNÉS ?

Le niveau d'exigence réglementaire dépend du risque que présente le système ou le modèle d'IA.

Il existe 4 niveaux de risques[4] :



SOUS QUEL DELAI FAUT-IL SE METTRE EN CONFORMITE ?

L'AI Act étant un règlement, il sera d'application directe dans tous les États membres de l'Union européenne, sans qu'il soit besoin de le transposer. Des délais entre 6 et 36 mois s'appliqueront selon le niveau de risque des systèmes et modèles d'IA pour se mettre en conformité à compter de l'entrée en vigueur du Règlement prévue en 2025.

En 2022 déjà nous alertions les acteurs de l'industrie sur la nécessité d'initier une réflexion stratégique en vue du développement d'une IA éthique et légale[5].

Quel que soit le délai, il est essentiel d'être préparé et d'anticiper la mise en conformité qui va venir perturber les roadmaps tech, produit et légales des entreprises.

Attention : *Une mise en conformité pertinente suppose une approche sur mesure en fonction des spécificités de votre organisation et de vos services. Un accompagnement par un professionnel du droit est fortement conseillé tout au long de votre démarche de mise en conformité pour tenir compte de vos caractéristiques propres. Les références numéraires aux articles de l'AI Act dans ce guide sont susceptibles d'évoluer en fonction du texte définitif.*

IMPALA AVOCATS, Avril 2024

[4] https://digital-strategy.ec.europa.eu/fr/policies/regulatory-framework-ai

[5] https://www.efl.fr/actualite/projet-reglement-ue-matiere-intelligence-artificielle-guide-usage-operateurs_f3bfc59ba-3685-433b-9ab5-f34997327b3d

SE METTRE EN CONFORMITÉ EN 6 ÉTAPES

L'anticipation est au cœur d'une stratégie réussie pour vous permettre d'adapter votre projet dès son stade de développement et jusqu'à sa mise sur le marché.

La méthodologie proposée pourra être sujette à des adaptations en fonction des bonnes pratiques qui se développeront sur le marché après l'entrée en vigueur du règlement.

De manière très pragmatique, la mise en conformité à l'AI Act peut s'établir en suivant six étapes résumées ci-après :

	**ÉTAPE 1** : DESSINER LA CARTOGRAPHIE DE VOS SOLUTIONS D'IA
	**ÉTAPE 2** : DÉTERMINER QUEL EST VOTRE RÔLE
	**ÉTAPE 3** : CLASSIFIER VOS SOLUTIONS SELON LES RISQUES
	**ÉTAPE 4** : ORGANISER LA MISE EN CONFORMITÉ
	**ÉTAPE 5** :DÉFINIR LES OBLIGATIONS DES UTILISATEURS
	**ÉTAPE 6** : ENCADRER LES RELATIONS AVEC CHAQUE MAILLON DE LA CHAÎNE

ÉTAPE 1 : ÉTABLIR LA CARTOGRAPHIE DE VOS SOLUTIONS D'IA

Un « système d'intelligence artificielle » est défini comme un logiciel développé à partir d'une ou de plusieurs techniques listées en annexe du Règlement et pouvant « pour un ensemble donné d'objectifs définis par un être humain, générer des résultats de sortie tels que du contenu, des prédictions, des recommandations ou des décisions influençant les environnements avec lesquels il interagit » (art. 3 (1)).

Les techniques concernées visent les systèmes auto-apprenants ou « *machine learning* », basés sur de l'apprentissage supervisé, profond et/ou par renforcement. Sont également pris en compte les systèmes suivant une trame logique prédéterminée pour parvenir à un résultat, ainsi que les systèmes statistiques, incluant les estimations bayésiennes, les méthodes de recherche et d'optimisation.

▶ En pratique :

Établir une cartographie de mes solutions d'IA : il s'agit ici d'identifier au sein de votre organisation, toutes les solutions d'intelligence artificielle que vous utilisez, que ce soit en interne ou en externe.

▶ **Exemple** : une société de logistique de colis appelée LogiFast a réalisé la cartographie suivante basée sur les solutions d'IA qu'elle utilise dans son quotidien :

ÉTAPE 2 : DETERMINER QUEL EST VOTRE RÔLE

Les acteurs visés par le texte, également désignés par le terme « opérateurs », sont le fournisseur, l'utilisateur, le mandataire, l'importateur et le distributeur (art. 3 (8)) :

a) Le fournisseur d'intelligence artificielle

Le fournisseur devient le pivot de la règlementation, il est celui qui développe ou possède un système d'IA en vue de sa mise sur le marché ou de sa mise en service, sous son propre nom ou sa propre marque, à titre onéreux ou gratuit (art. 3 (2)).

⚠ La qualité de fournisseur s'applique également à l'entité qui en modifie la destination ou qui en apporte une modification substantielle. Dans ce cas, la qualité de fournisseur du premier opérateur (qui aurait par exemple mis sur le marché le système d'IA) disparaît (mais pas ses responsabilités, voir étape 6 ci-dessous).

Le fournisseur d'IA va devoir se conformer à un certain nombre d'obligations en fonction de la catégorie de risques à laquelle appartient son système d'IA.

b) L'importateur

L'importateur est défini comme la personne établie dans l'UE qui met sur le marché un système d'intelligence artificielle pour lequel est apposé le nom ou la marque d'une personne établie hors UE (art. 3 (6)). L'AI Act fait peser sur l'importateur une obligation de vérification et de vigilance quant aux démarches effectuées par le fournisseur (art.26).

c) Le distributeur

Le distributeur est une personne physique ou morale (autre que le fournisseur ou l'importateur), qui dans la chaîne d'approvisionnement rend disponible un système d'intelligence artificielle sans en affecter ses propriétés (art. 3 (7)).

Avant de mettre un système d'IA à haut risque à disposition sur le marché, les distributeurs devront vérifier que le système d'IA à haut risque porte le marquage de conformité CE requis.

d) L'utilisateur

L'utilisateur est la personne physique ou morale, l'autorité publique, l'agence ou un autre organisme, qui utilise un système d'IA. La notion d'utilisateur est directement

liée à l'usage professionnel d'un système d'IA et exclut expressément l'utilisation à des fins personnelles (art. 3 (4)).

▶ En pratique :

Déterminer pour chaque système d'IA identifié lors de l'étape 1, quel est votre rôle. Cette analyse vous permettra également d'initier une réflexion sur les mécanismes de responsabilité dans la chaîne contractuelle entre les différents protagonistes de l'IA (étape 6). Ainsi, le fournisseur d'IA ayant apposé sa marque sur des systèmes d'IA importés pourra négocier avec les fabricants des mécanismes de recours et de garantie pour le cas où, par exemple, les systèmes seraient défaillants ou causeraient des préjudices à leurs utilisateurs.

ÉTAPE 3 : CLASSIFIER VOS SOLUTIONS D'IA SELON LES RISQUES ASSOCIES

Concrètement, l'AI Act distingue quatre catégories d'intelligence artificielle selon que les risques liés à leur usage sont inacceptables, élevés (médecine, justice, recrutement, crédit etc.), faibles ou minimes.

La première catégorie sera tout simplement interdite tandis que la quatrième ne sera que très peu concernée par la réglementation.

Les catégories d'IA à risques élevés devront quant à elles, se conformer à des règles contraignantes destinées à assurer un développement éthique et respectueux des droits fondamentaux.

	⛔ **Risque inacceptable**	⚠️ **Haut risque**	🚦 **Risque modéré**	✅ **Risque faible**
Responsabilités	Commercialisation interdite	Déclaration de conformité Enregistrement dans la base de données de l'UE Marquage CE	Transparence	Respect volontaire de code de conduite
Sanctions	35 millions € ou 15% CA annuel mondial	15 millions € ou 3% CA annuel mondial	7,5 millions € ou 1% CA annuel mondial	N/A

Enfin, le Règlement prévoit un régime spécifique pour certains autres systèmes d'IA qu'ils soient à hauts risques ou non. Sont ainsi pris en compte les risques systémiques qui pourraient découler des modèles d'IA à usage général, y compris les grands modèles d'IA générative. Ceux-ci peuvent être utilisés pour une variété de tâches et deviennent la base de nombreux systèmes d'IA dans l'Union européenne. Certains de ces modèles pourraient comporter des risques systémiques s'ils sont très performants ou largement utilisés. Par exemple, des modèles puissants pourraient provoquer des accidents graves ou être utilisés à mauvais escient pour des cyberattaques de grande envergure. De nombreuses personnes pourraient être

affectées si un modèle propage des biais nuisibles dans de nombreuses applications.

a) Les IA à risque inacceptable

La liste des pratiques interdites englobe tous les systèmes d'IA dont l'usage est jugé inacceptable en raison de leur antagonisme avec les valeurs de l'Union européenne.

Ainsi, sont interdits les systèmes d'intelligence artificielle :

- Lorsqu'ils recourent à des techniques subliminales au-dessous du seuil de conscience d'une personne, pour altérer substantiellement son comportement, pouvant causer un préjudice physique ou psychologique à cette personne ou à un tiers.
- Lorsqu'ils exploitent la vulnérabilité due à l'âge ou au handicap physique ou mental d'un groupe de personnes donné pour altérer substantiellement le comportement d'un membre de ce groupe, pouvant causer un préjudice physique ou psychologique à cette personne ou à un tiers.
- Lorsqu'ils reposent sur une logique de notation sociale.
- Lorsqu'ils permettent une identification biométrique à distance en temps réel dans des espaces accessibles au public à des fins répressives, sauf exception (et sous conditions) telle que la recherche ciblée de victimes d'actes criminels ou la prévention d'une menace spécifique, substantielle et imminente pour la vie ou la sécurité physique des personnes physiques. L'identification biométrique à distance n'est ainsi pas visée par l'interdiction lorsqu'elle est réalisée en temps différé alors même que cette pratique peut induire des risques élevés pour les personnes.

▶ En pratique :

Réaliser une analyse d'impact le plus tôt possible avant d'engager des ressources sur un projet d'IA à risques inacceptables pour limiter les risques d'une interdiction. Les entreprises pourront à ce stade envisager des solutions alternatives pour rendre leurs projets plus éthiques et leur permettre d'être classifiés comme des IA à haut risque ou risque acceptable.

b) Les IA à haut risque

Les systèmes d'IA à haut risque peuvent être autorisés sur le marché européen, à condition qu'ils respectent certaines règles et qu'une évaluation préalable de la conformité soit effectuée.

La classification des risques est basée sur l'utilisation prévue du système d'IA, c'est-à-dire qu'elle dépend de la fonction remplie par le système d'IA et de l'objectif et des modalités spécifiques pour lesquels le système est utilisé.

Les systèmes d'intelligence artificielle identifiés comme étant à haut risque couvrent l'IA utilisée dans :

1) **Les composants de sécurité des produits**, par exemple, l'application d'IA dans la chirurgie assistée par robot.
2) **L'identification biométrique et catégorisation des personnes physiques :** Le traitement de données biométriques soulève des inquiétudes quant à la vie privée et à la protection des données personnelles.
3) **La gestion et l'exploitation des infrastructures critiques :** Les défaillances dans la gestion de ces systèmes pourraient avoir des conséquences graves sur la sécurité et le fonctionnement des infrastructures essentielles.
4) **L'éducation et la formation professionnelle :** L'utilisation de l'IA dans ces domaines peut influencer de manière significative les opportunités d'apprentissage et les parcours professionnels, impactant ainsi les droits des individus.
5) **L'emploi, la gestion de la main-d'œuvre et l'accès à l'emploi indépendant :** L'IA peut jouer un rôle majeur dans les décisions liées à l'emploi, ce qui soulève des questions de transparence, d'équité et de discrimination.
6) **L'accès et le droit aux services privés essentiels, aux services publics et aux prestations sociales :** Les décisions automatisées dans ces domaines peuvent influencer l'accès aux services et aux avantages sociaux, nécessitant une vigilance particulière.
7) **Les autorités répressives :** L'utilisation de l'IA dans les activités répressives soulève des inquiétudes quant aux droits civils et individuels, nécessitant une supervision appropriée.
8) **La gestion de la migration, de l'asile et des contrôles aux frontières :** L'IA dans ces contextes peut avoir des répercussions sur les droits des migrants et des demandeurs d'asile, impliquant des considérations éthiques et humanitaires.
9) **L'administration de la justice et processus démocratiques :** L'IA peut influencer les décisions judiciaires et les processus démocratiques, nécessitant une surveillance étroite pour garantir l'équité et la justice.

La Commission pourra étendre la liste des systèmes d'IA à haut risque utilisés dans certains domaines prédéfinis, en appliquant un ensemble de critères et une méthode d'évaluation des risques.

En l'état, nous avons tendance à considérer que la catégorie des systèmes d'IA est si vaste que la grande majorité des solutions d'IA devraient entrer dans cette catégorie et donc faire l'objet d'une vigilance accrue.

▶ En pratique :

Mener une analyse pratique et minutieuse, au cas par cas, de chaque système d'IA identifié au point 1, afin de déterminer s'il appartient à l'une de ces nombreuses catégories. Cette classification permettra d'anticiper la mise en conformité du système d'IA telle que définie ci-après.

Focus sur les IA Génératives :

Dans la version adoptée par le Parlement européen de l'AI Act, les systèmes d'Intelligence Artificielle Génératives (« IAG ») entreraient dans la catégorie des « IA à haut risques » soumises à des règles spécifiques en raison des dangers particuliers de manipulation qu'ils présentent. Ces règles incluraient des obligations telles que le marquage des contenus générés, la mise en place de mesures pour empêcher la création de contenus illégaux, et la fourniture de rapports détaillant les types de données utilisées pour former le système, y compris les données protégées par le droit d'auteur[6].

Le règlement prévoit que la transparence doit être appliquée aux systèmes d'IAG qui interagissent avec les humains, détectent des émotions ou déterminent des associations basées sur des données biométriques, ou génèrent/manipulent des contenus, tels que des trucages vidéo ultraréalistes. Les utilisateurs doivent être informés lorsqu'ils interagissent avec de tels systèmes, et il est obligatoire de déclarer lorsque des contenus sont générés de manière automatisée.

Bien que le Parlement européen considère que toutes les IAG sont à risque en raison de leur nature technologique, tous les auteurs ne partagent pas cet avis. Certains estiment que la classification des IAG en tant qu'IA à risque devrait dépendre de l'usage spécifique de l'IAG, comme dans le domaine de la santé, plutôt que de la technologie utilisée.

[6] Rapport d'information déposé en application de l'article 145 du règlement par la commission des lois constitutionnelles, de la législation et de l'administration générale de la République, en conclusion des travaux d'une mission d'information sur les défis de l'intelligence artificielle générative en matière de protection des données personnelles et d'utilisation du contenu généré et présenté par MM. Philippe Pradal et Stéphane Rambaud, députés

Suite à des négociations entre le Parlement européen et le Conseil, un compromis a été trouvé en décembre 2023. Ce compromis prévoit une régulation plus stricte pour les modèles d'IAG à "fort impact", ceux qui pourraient présenter un risque systémique en raison de la quantité de données utilisées pour leur entraînement et de leurs performances de calcul. Cette approche permet de réguler les acteurs majeurs du marché sans pénaliser les nouveaux arrivants, bien qu'il soit nécessaire de s'assurer que cette norme puisse évoluer avec les avancées technologiques du secteur.

c) Les IA à risques acceptables

Les risques acceptables ne sont pas définis dans le Règlement. Selon notre lecture de l'AI Act, la catégorie des systèmes d'IA à haut risque est si large qu'il est difficile à ce stade de prédire quels systèmes d'IA pourraient être qualifiés d'IA à risques acceptables.

▶ En pratique :

Pour anticiper l'évolution d'un système d'intelligence artificielle et de ses fonctionnalités, nous recommandons par défaut de considérer tout système d'IA comme étant à risque élevé. Bien que la mise en conformité à la réglementation implique de mettre en œuvre des démarches plus ou moins lourdes d'un point de vue organisationnel, elle a le mérite d'assurer le respect de bonnes pratiques par les équipes et de réduire le risque d'impact sur les droits fondamentaux des utilisateurs d'IA. D'ailleurs, le titre IX du Règlement établit un cadre pour la création de codes de conduite visant à encourager les fournisseurs de systèmes d'IA ne présentant pas de risque élevé à appliquer volontairement les exigences obligatoires pour les systèmes d'IA à haut risque.

d) Les autres systèmes d'IA réglementés

Selon le Règlement, lorsque des personnes interagissent avec un système d'IA ou que leurs émotions ou caractéristiques sont reconnues par des moyens automatisés, elles doivent en être informées. Cette catégorie vise plusieurs systèmes d'IA, qu'ils soient :

- **Destinés à interagir** avec des personnes physiques : les fournisseurs de ce type de système doivent s'assurer qu'ils sont conçus de manière à ce que les utilisateurs aient conscience qu'ils communiquent avec une entité artificielle ;
- **De reconnaissance des émotions** et de **catégorisation biométrique** : le Règlement impose le recueil du consentement pour le recours à ce type d'instrument ;

- De « *deep fake* » c'est-à-dire manipulant une image, un son ou une vidéo qui ressemblent à des personnes, choses ou autres entités ou évènements existants afin d'en générer un contenu apparaissant à tort comme étant la réalité : les personnes devront être informées que le contenu consulté a été généré artificiellement, sauf si les systèmes ont été autorisés par la loi et sont destinés à détecter, prévenir, enquêter et poursuivre des infractions pénales.

ÉTAPE 4 : ORGANISER LA MISE EN CONFORMITÉ

a) La mise en conformité des systèmes d'IA à haut risque

Le Règlement impose une mise en conformité avant la mise sur le marché d'un système d'IA à haut risque. Les systèmes en question devront satisfaire à un ensemble d'obligations garantissant une IA digne de confiance et faire l'objet de procédures d'évaluation de la conformité avant de pouvoir être mis sur le marché.

Ainsi, pour les systèmes d'IA à risques élevés, le fournisseur devra effectuer les opérations suivantes :

1) Évaluer la conformité : le fournisseur devra pouvoir démontrer qu'il a bien appliqué des normes harmonisées visées à l'article 40 ou, le cas échéant, les spécifications communes visées à l'article 41. Pour ce faire, il devra suivre l'une des **procédures** suivantes : une procédure d'évaluation de la conformité fondée sur le contrôle interne (visée à l'annexe VI de l'AI Act) ; **ou** une procédure d'évaluation de la conformité fondée sur l'évaluation du système de gestion de la qualité et l'évaluation de la documentation technique, avec l'intervention d'un organisme notifié (visée à l'annexe VII).
2) Gérer les risques : en mettant en place des mesures de gestion des risques (art. 9) grâce à un système de **surveillance post-commercialisation** documenté, destiné à évaluer la performance du système d'IA tout au long de sa vie (art. 61). La politique de gestion des risques doit permettre d'assurer un niveau de risque acceptable lorsque le système d'IA à haut risque est utilisé conformément à sa destination ou dans des « conditions de mauvaise utilisation raisonnablement prévisible ». Elle nécessite d'identifier et analyser les risques connus et prévisibles, d'estimer et évaluer les risques susceptibles d'apparaître, d'évaluer d'autres risques susceptibles d'apparaître grâce à l'analyse des données post-commercialisation et d' adopter des mesures appropriées de gestion des risques.
3) Données et gouvernance des données : les systèmes d'IA à haut risque développés sur la base de jeux de données d'entraînement, de validation et de test devront satisfaire des critères de qualité pour garantir la fiabilité du système et minimiser le risque d'erreur.
4) Lutter contre les biais : en instaurant une surveillance, détection et correction des biais grâce à une politique contraignante de **gouvernance des données**

d'entraînement, de validation et de test (art. 10). Les jeux de données d'entraînement, de validation et de test devront être sélectionnés selon de bonnes pratiques définies dans le Règlement, permettant de s'assurer qu'ils sont pertinents, représentatifs, exempts d'erreurs, complets et tiennent comptent des caractéristiques ou éléments propres au contexte géographique, comportemental ou fonctionnel spécifique dans lequel le système d'IA à haut risque est destiné à être utilisé.

5) Rédiger une documentation technique : celle-ci doit être conforme aux exigences de la réglementation (art. 11). A ce titre, un certain nombre de documents doivent être conservés et mis à la disposition des autorités nationales durant dix ans après la mise sur le marché ou la mise en service du système d'IA (art. 50).

6) Assurer une journalisation des événements (art. 12) pendant le fonctionnement du système.
   Cette journalisation est cruciale pour tracer les actions du système et permettre une analyse rétrospective des performances, des erreurs éventuelles, et une compréhension approfondie de son comportement.

   Le fournisseur doit mettre en place des mécanismes de journalisation robustes, enregistrant les activités du système, les décisions prises et les résultats obtenus. Cela contribue à la transparence et facilite les enquêtes en cas d'incident.

7) Informer les utilisateurs (art. 13) : Informer les utilisateurs sur le fonctionnement du système est une démarche essentielle pour promouvoir la compréhension et la confiance dans l'utilisation de l'IA.

   Le fournisseur devra élaborer des moyens clairs et accessibles pour informer les utilisateurs sur les fonctionnalités, les limitations et les risques associés au système d'IA. Cela pourrait prendre la forme de notices explicatives, de guides d'utilisation ou d'autres supports adaptés.

8) Assurer une surveillance humaine (art. 14) : La surveillance humaine, réalisée via des interfaces homme-machine appropriées, vise à maintenir le contrôle et à atténuer les risques pour la santé, la sécurité et les droits fondamentaux.

   Le fournisseur devra intégrer des interfaces permettant une surveillance active et une intervention humaine lorsque cela est nécessaire, renforçant ainsi la capacité à anticiper et à remédier aux situations critiques.

9) Assurer la robustesse, la sécurité et l'exactitude des données : Garantir la robustesse, la sécurité et l'exactitude des données est essentiel pour prévenir

les erreurs, les biais et les défaillances qui pourraient compromettre l'intégrité du système.

Le fournisseur devra mettre en œuvre des pratiques solides en matière de sécurité des données, de validation des modèles d'IA et de gestion des erreurs pour assurer la fiabilité et la qualité du système.

10) Apposer le marquage CE : Apposer le marquage CE est une déclaration du fournisseur attestant que le système est conforme aux exigences réglementaires.

    Le fournisseur devra démontrer la conformité en réalisant les évaluations et les tests nécessaires, puis apposer le marquage CE de manière visible sur le produit ou la documentation associée.

11) Informer les autorités compétentes en cas d'incident grave ou de dysfonctionnement (art. 22 et 62) et coopérer avec elles : Le fournisseur devra établir des protocoles clairs pour la notification des incidents, coopérer activement avec les autorités compétentes et participer à des enquêtes post-incident pour comprendre les causes profondes.

Si le fournisseur n'est pas établi sur le territoire de l'UE et qu'un importateur ou un distributeur est identifiable, celui-ci devra s'empêcher d'importer un système d'IA non conforme et s'assurer de la bonne exécution de la procédure de mise en conformité et son marquage correct, l'établissement de la documentation technique, l'apposition de ses coordonnées sur l'emballage ou la documentation technique, des bonnes conditions de stockage ou de transport pour éviter de compromettre la conformité du système et de la fourniture aux autorités de tout document nécessaire à prouver la conformité.

Pour le cas où aucun importateur ne serait identifiable, un mandataire désigné devra justifier de la conformité aux exigences précitées.

▶ En pratique :

La mise en conformité d'un système d'IA implique une réflexion stratégique en amont pour pouvoir en aval, définir des procédures adaptées à l'organisation de l'entreprise et conformes à la réglementation. Tous les maillons de la chaîne devront pouvoir être sensibilisés aux bonnes pratiques et à l'éthique en matière d'IA afin de limiter les risques liés à une utilisation qui ne serait pas totalement maîtrisée. En outre, des systèmes d'audit réguliers, la mise en place de règles de sécurité conformes aux standards de l'ANSSI et une vigilance permanente doivent permettre de gagner en sérénité dans le déploiement d'une IA digne de confiance.

Nous recommandons d'entamer dès à présent la rédaction d'une **documentation** fournie sur le fonctionnement du système d'IA ainsi que la rédaction d'un guide d'utilisation, de tracer et qualifier les données d'entraînement, de décrire comment les éventuels biais seront suivis et corrigés ainsi que les règles de sécurité mises en place, de prévoir une procédure de rappel des produits d'IA non conformes.

Focus sur la politique *corporate* de l'usage de l'IA :

La charte informatique est à la fois une garantie essentielle et un outil de gestion efficace des ressources technologiques au sein d'une entreprise.

Destinée à être intégrée au règlement intérieur de l'entreprise, la Charte informatique complète ce dernier. Elle peut être régulièrement mise à jour pour s'adapter aux nouvelles pratiques émergeantes impactant les usages et notamment pour sensibiliser le personnel de votre entreprise aux bonnes pratiques en matière d'IA.

IMPALA AVOCATS a élaboré un modèle en Annexe 1.

ÉTAPE 5 : DÉFINIR LES OBLIGATIONS DES UTILISATEURS

L'AI Act prévoit une véritable responsabilisation des utilisateurs de systèmes d'IA. En raison de la nature des systèmes d'intelligence artificielle et des risques potentiels pour la sécurité et les droits fondamentaux liés à leur utilisation, l'utilisateur joue un rôle déterminant.

Le Règlement indique quelles informations doivent être communiquées aux utilisateurs, et la nécessité de s'y conformer ou de suspendre l'utilisation du système en cas de doute sur sa conformité. L'utilisateur devra également conserver les journaux générés automatiquement et lorsqu'il exerce un contrôle sur les données d'entrée du système, veiller à la pertinence de ces données (art. 29).

▶ En pratique :

Les fournisseurs ou distributeurs de systèmes d'IA ont tout intérêt à rédiger une documentation détaillée et des guides d'utilisation pédagogiques à destination des utilisateurs afin de faciliter l'usage de leurs systèmes mais aussi de limiter leurs risques en responsabilisant les utilisateurs desdits systèmes, tant en ce qui concerne l'utilisation de la (i) solution que de son (ii) résultat.

Par exemple, s'agissant d'un modèle LLMs, sur le premier point (i), les utilisateurs devront être sensibilisés aux risques les plus fréquents et s'engager à ne pas réaliser certaines actions telles que l'injection de prompts par le biais d'extensions ou *chatbots*, la technique du « bourrage de crâne » consistant à répéter plusieurs le même mot pour faire dérailler un système d'IA, ou bien la technique dite de la « grand-mère ». Aussi loufoque que cela puisse paraître, cette technique consiste à demander à une IA générative un contenu interdit sous prétexte d'une histoire mêlant une grand-mère[7].

Sur le second point (ii), le fournisseur d'IA aura tout intérêt de prévoir dans ses conditions d'utilisation, une clause spécifique visant à responsabiliser l'utilisateur sur son usage du résultat obtenu grâce à la solution. La qualité du résultat dépend de la qualité des données alimentant le système d'IA, en ce compris les requêtes et interactions de l'utilisateur.

[7] https://www.lemonde.fr/economie/article/2023/02/12/cybersecurite-quand-les-ordinateurs-s-attaquent-entre-eux_6161556_3234.html

ÉTAPE 6 : ENCADRER LES RELATIONS AVEC CHAQUE MAILLON DE LA CHAÎNE

Lorsqu'il s'agit de collaborer dans le développement, la gestion ou l'utilisation d'un système d'IA, la répartition des rôles, des responsabilités et des risques entre les différents opérateurs est cruciale. Pour formaliser cette répartition de manière effective, les opérateurs devront encadrer contractuellement leurs obligations tout au long du cycle de vie du système d'IA.

Chaque opérateur doit clairement définir ses rôles et responsabilités spécifiques tout au long du cycle de vie du système d'IA. Cela pourrait inclure des étapes telles que la conception, le développement, le déploiement, la maintenance et la surveillance.

Les opérateurs doivent procéder à une évaluation minutieuse des risques associés à leurs différentes responsabilités. Cela pourrait inclure des risques liés à la qualité des données, à la sécurité, à la conformité réglementaire, etc.

▶ En pratique :

Les contrats entre les opérateurs doivent inclure des clauses précises détaillant les responsabilités de chacun. Par exemple, un opérateur responsable de la collecte des données pourrait avoir une clause spécifique concernant la qualité et l'origine des données.

Les clauses de recours en garantie devront être rédigées de manière à refléter équitablement le niveau d'implication de chaque opérateur. Si un opérateur est plus directement impliqué dans une étape particulière, sa responsabilité et son recours en garantie correspondant devraient être proportionnels.

Les contrats devront être révisés périodiquement pour tenir compte des évolutions technologiques, des changements réglementaires et des nouveaux risques identifiés.

Il est recommandé d'impliquer des experts juridiques spécialisés dans les questions liées à l'IA pour garantir que les contrats sont conformes aux normes légales et éthiques en constante évolution.

QUELLES SONT LES SANCTIONS EN CAS D'INFRACTION ?

En cas de mise sur le marché ou d'utilisation de systèmes d'IA ne respectant pas les exigences du Règlement, les États membres devront prévoir des sanctions effectives, proportionnées et dissuasives, y compris des amendes administratives dont le seuil est fixé par l'AI Act :

- Jusqu'à 35 millions d'euros ou 7 % du chiffre d'affaires annuel mondial total de l'exercice précédent (le montant le plus élevé étant retenu) pour les infractions relatives aux pratiques interdites ou au non-respect des exigences en matière de données ;
- Jusqu'à 15 millions d'euros ou 3 % du chiffre d'affaires annuel mondial total de l'exercice précédent pour non-respect de l'une des autres exigences ou obligations du règlement, y compris la violation des règles relatives aux modèles d'IA à usage général ;
- Jusqu'à 7,5 millions d'euros ou 1,5 % du chiffre d'affaires annuel mondial total de l'exercice précédent pour la fourniture d'informations incorrectes, incomplètes ou trompeuses aux organismes notifiés et aux autorités nationales compétentes en réponse à une demande ;

Pour chaque catégorie d'infraction, le seuil serait le moins élevé des deux montants pour les PME et le plus élevé pour les autres entreprises.

Afin d'harmoniser les règles et pratiques nationales en matière de fixation des amendes administratives, la Commission élaborera des lignes directrices en s'appuyant sur l'avis du conseil d'administration.

Les institutions, agences ou organes de l'UE devant donner l'exemple, ils seront également soumis aux règles et à d'éventuelles amendes administratives.

LES AUTORITÉS COMPÉTENTES

En France, deux autorités qui ne sont pas encore désignées seront responsables de veiller à ce que l'AI Act soit correctement appliqué et harmonisé avec d'autres autorités nationales et européennes.

L'AI Office, intégré à la Commission européenne et composé d'experts indépendants, sera créé prochainement. L'AI Office aura pour mission de développer des méthodes pour évaluer les modèles d'IA et de surveiller les risques de sécurité associés aux modèles d'IA à usage général, en collaboration avec les autorités nationales. Si vous

avez un système ou modèle d'IA à haut risque, l'AI Office sera votre principal interlocuteur pour soumettre une déclaration de conformité.

L'AI Pact encouragera et soutiendra les entreprises dans la planification des mesures prévues par l'AI Act.

La Commission a lancé l'AI Pact afin d'encourager les initiatives de l'industrie pour anticiper la mise en œuvre de l'AI Act. Les entreprises sont incitées à communiquer volontairement les processus et les pratiques qu'elles mettent en place pour se préparer à la mise en conformité et garantir que la conception, le développement et l'utilisation de l'IA soient dignes de confiance.

Les engagements seront rassemblés et publiés par la Commission, afin d'assurer la visibilité, d'accroître la crédibilité et de renforcer la confiance dans les technologies développées par les entreprises participant à ce pacte.

Le pacte sur l'IA réunira, sur une base volontaire, les principaux acteurs industriels de l'UE et des pays tiers pour qu'ils participent à une communauté d'échange de bonnes pratiques visant à mieux faire connaître les principes qui sous-tendent la future loi sur l'IA et (après l'adoption de la loi) à garantir l'engagement d'anticiper et de combler le fossé avant l'applicabilité de la réglementation sur l'IA.

Pour en savoir plus : https://digital-strategy.ec.europa.eu/en/policies/ai-pact

- En conclusion :

Les obligations et les responsabilités de l'AI Act nécessitent que l'ensemble des opérateurs des systèmes d'IA entament dès aujourd'hui une réflexion sur leur mise en conformité à venir et commencent à imaginer des procédures internes visant à garantir des systèmes d'IA dignes de confiance.

ANNEXE – MODÈLE DE CHARTE INFORMATIQUE

RELATIVE AUX USAGES DE L'IA

***Attention** : Ce modèle a été élaboré sur la base des dispositions du Règlement IA dans sa version adoptée au 17 février 2024. La Commission est susceptible d'élaborer des modèles à l'avenir auxquels il conviendra de se référer en priorité. Ce modèle de politique est destiné à fournir des lignes directrices générales et doit être utilisé comme référence. Il peut ne pas prendre en compte toutes les lois locales ou nationales et ne constitue pas un document juridique. Son application à chaque salarié doit faire l'objet d'une analyse préalable afin de déterminer l'instrument juridique approprié pour le faire appliquer. Ni l'auteur ni IMPALA AVOCATS n'assument de responsabilité juridique pouvant découler de l'utilisation de cette charte.*

I. SYNTHESE ET OBJECTIF DE LA POLITIQUE

La présente politique d'utilisation des outils d'intelligence artificielle décrit les meilleures pratiques pour l'utilisation des outils d'intelligence artificielle sur le lieu de travail, en particulier en ce qui concerne l'utilisation de données sensibles et d'informations exclusives sur l'entreprise et ses clients.

II. CHAMP D'APPLICATION

Les outils d'intelligence artificielle (IA) transforment notre façon de travailler. Ils ont le potentiel d'automatiser les tâches, d'améliorer la prise de décision et de fournir des informations précieuses sur nos opérations.

Cependant, l'utilisation d'outils d'IA présente également de nouveaux défis en termes de sécurité de l'information et de protection des données.

La présente politique est un guide pour les employés sur la façon d'utiliser les outils d'IA de manière sécurisée, en particulier lorsqu'elle implique le partage d'informations potentiellement sensibles sur l'entreprise et ses clients.

III. OBJECTIF

L'objectif de cette politique est de veiller à ce que tous les employés utilisent les outils d'IA de manière sûre, responsable et confidentielle. La politique décrit les exigences que les employés doivent respecter lorsqu'ils utilisent des outils d'IA, y compris l'évaluation des risques de sécurité et la protection des données confidentielles.

IV. DECLARATION DE POLITIQUE GENERALE

Notre organisation reconnaît que l'utilisation d'outils d'IA peut présenter des risques pour nos opérations et nos clients. Par conséquent, nous nous engageons à protéger la confidentialité, l'intégrité et la disponibilité de toutes les données de l'entreprise et de ses clients. Cette politique exige que tous les employés utilisent les outils d'IA d'une manière conforme à nos meilleures pratiques en matière de sécurité.

V. MEILLEURES PRATIQUES EN MATIERE DE SECURITE

Tous les employés sont tenus de respecter les bonnes pratiques de sécurité suivantes lorsqu'ils utilisent des outils d'intelligence artificielle :

a. Évaluation des outils d'IA : Les employés doivent évaluer la sécurité de tout outil d'IA avant de l'utiliser. Ils doivent notamment examiner les fonctions de sécurité de l'outil, ses conditions d'utilisation et sa politique en matière de protection de la vie privée. Les employés doivent également vérifier la réputation du développeur de l'outil et de tout service tiers utilisé par l'outil.

b. Protection des données confidentielles : Les employés ne doivent pas télécharger ou partager des données confidentielles, exclusives ou protégées par la réglementation sans l'autorisation préalable du service compétent. Il s'agit notamment des données relatives aux clients, aux employés ou aux partenaires.

c. Contrôle d'accès : Les employés ne doivent pas donner accès aux outils d'IA à l'extérieur de l'entreprise sans l'approbation préalable du service ou du responsable concerné et sans les processus ultérieurs nécessaires pour répondre aux exigences de conformité en matière de sécurité. Cela inclut le partage des identifiants de connexion ou d'autres informations sensibles avec des tiers.

d. Utilisation d'outils d'IA réputés : Les employés ne doivent utiliser que des outils d'IA réputés et faire preuve de prudence lorsqu'ils utilisent des outils développés par des personnes ou des entreprises dont la réputation n'est pas établie. Tout outil d'IA utilisé par les employés doit répondre à nos normes de sécurité et de protection des données.

e. Respect des politiques de sécurité : Les employés doivent appliquer les mêmes bonnes pratiques de sécurité que celles que nous utilisons pour toutes les données de l'entreprise et des clients. Cela inclut l'utilisation de mots de passe forts, la mise à jour des logiciels et le respect de nos politiques de conservation et d'élimination des données.

f. Confidentialité des données : Les employés doivent faire preuve de discernement lorsqu'ils partagent des informations avec le public. Dans un premier temps, ils doivent se poser la question suivante : "Serais-je à l'aise pour partager ces informations en dehors de l'entreprise ? Serions-nous d'accord pour que ces informations soient divulguées publiquement ?" avant de télécharger ou de partager des données dans des outils d'IA. La deuxième étape consiste à suivre le point b) ci-dessus.

VI. EXAMEN ET REVISION

Cette politique sera revue et mise à jour régulièrement afin de garantir son actualité et son efficacité. Toute révision de la politique sera communiquée à tous les employés.

VII. CONCLUSION

Notre organisation s'engage à veiller à ce que l'utilisation des outils d'IA soit sûre et sécurisée pour tous les employés et clients, ainsi que pour l'organisation elle-même. Nous pensons qu'en suivant les lignes directrices décrites dans cette politique, nous pouvons maximiser les avantages des outils d'IA tout en minimisant les risques potentiels associés à leur utilisation.

VIII. RECONNAISSANCE ET CONFORMITE

Tous les employés doivent lire et signer cette politique avant d'utiliser des outils d'IA au sein de l'organisation. Le non-respect de cette politique peut entraîner des mesures disciplinaires pouvant aller jusqu'au licenciement.

En signant la présente politique, je reconnais avoir lu et compris les exigences qui y sont énoncées. J'accepte d'utiliser les outils d'IA d'une manière conforme aux meilleures pratiques en matière de sécurité décrites ci-dessus et de signaler tout incident ou problème de sécurité au service ou au responsable compétent.

Signature de l'employé : _____

Date : _____